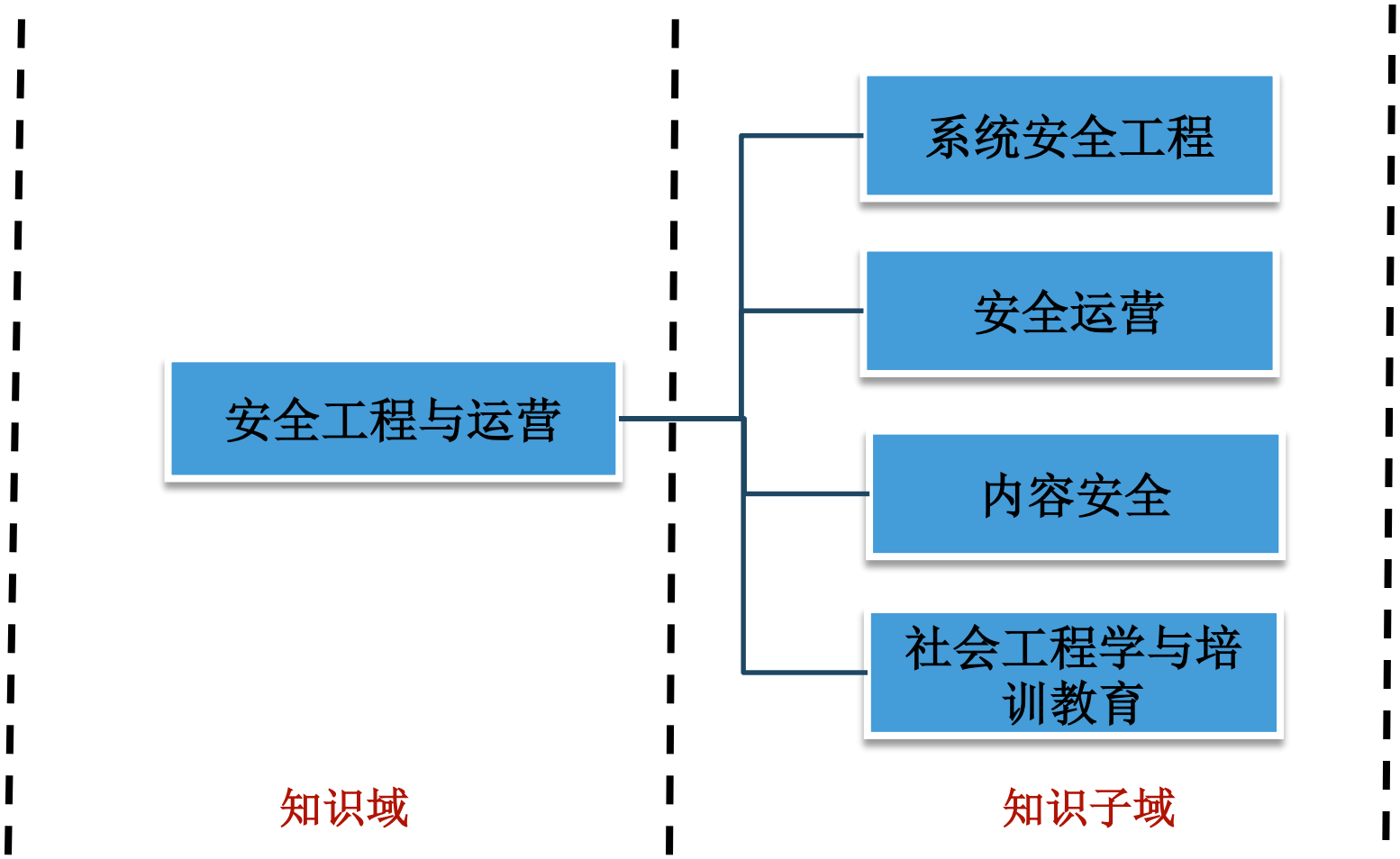
安全工程与运营

版本：4.2

东方瑞通

课程内容

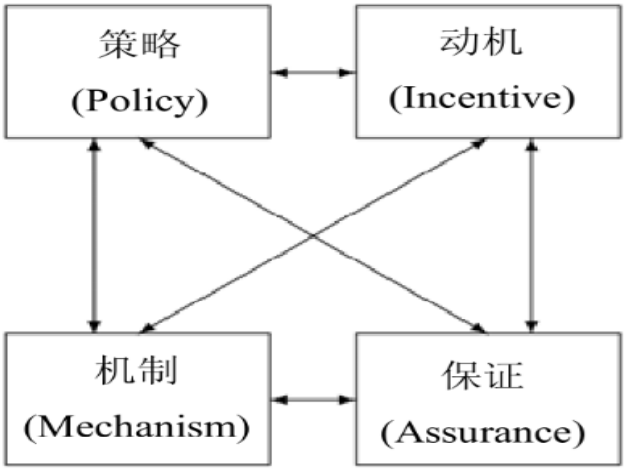


知识子域：系统安全工程

- 系统安全工程基础
  - 理解系统安全工程的概念及系统安全工程的必要性。
- 系统安全工程理论基础
  - 了解系统工程思想、项目管理方法、质量管理体系、能力成熟度模型等基础理论；
  - 理解能力成熟度模型的基本思想及相关概念；

什么是安全工程

- 采用工程的概念、原理、技术和方法，来研究、开发、实施与维护信息系统安全的过程
- 信息化建设活动中有关加强系统安全性活动的集合
- 良好安全工程的四个方面
  - 策略
  - 机制
  - 保证
  - 动机



为什么需要系统安全工程

- 信息系统安全保障要素之一
- 解决信息系统生命周期的“过程安全”问题
  - 信息安全是信息化的有机组成部分，必须与信息化同步规划、同步建设
  - 信息系统的建设是一项系统工程，具有复杂性，安全工程是以最优费效比提供并满足安全需求

“建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。”
--《中华人民共和国网络安全法》

系统安全工程理论基础

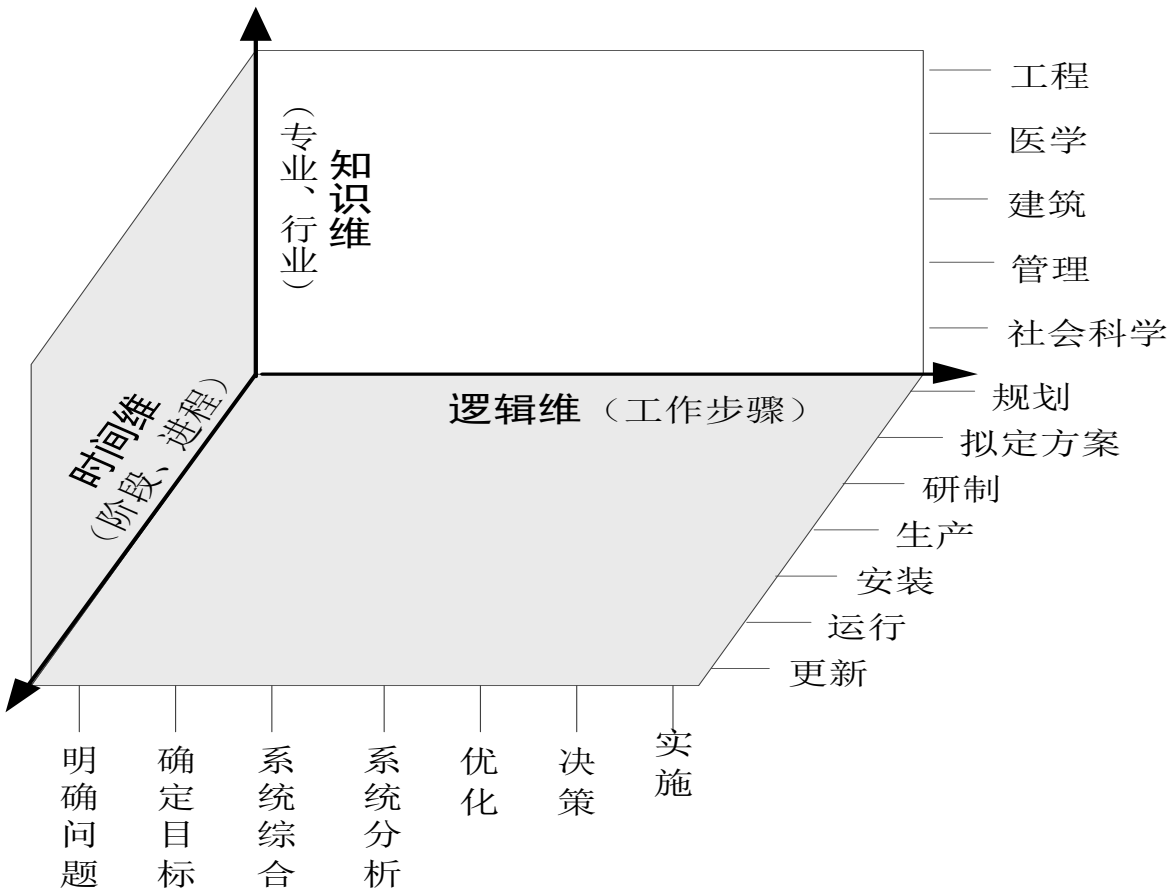
- 系统工程
- 项目管理
- 质量管理
- 能力成熟度模型

系统安全工程理论基础-系统工程

- 什么是系统工程
  - 以大型复杂系统为研究对象，按一定目的进行设计、开发、管理与控制，以期达到总体效果最优的理论与方法
- 系统工程的概念
  - 系统工程不是基本理论，也不属于技术实现，而是一种方法论
  - 系统工程是一门高度综合性的管理工程技术，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

系统安全工程理论基础-系统工程

- 霍尔三维结构图
  - 时间维
  - 逻辑维
  - 知识维



系统安全工程理论基础-项目管理

- 什么是项目管理
  - 项目管理者在有限的资源约束下，运用系统的观点、方法和理论，对项目涉及的全部工作进行有效管理
  - 项目管理是系统工程思想针对具体项目的实践应用
- 项目管理的知识领域
  - 范围、时间、成本、质量、人力资源、沟通、风险、采购和集成
- 项目的过程控制
  - 启动、计划、执行、控制和收尾

系统安全工程理论基础-质量管理

- 质量管理基本概念
  - 质量：是一组固有特性满足要求的程度
  - 质量管理：为了实现质量目标，而进行的所有管理性质的活动
- 质量管理体系
  - 指挥和控制一个组织质量相关的管理体系
  - 国际标准ISO9000系列

ISO9000规范质量管理的四个方面

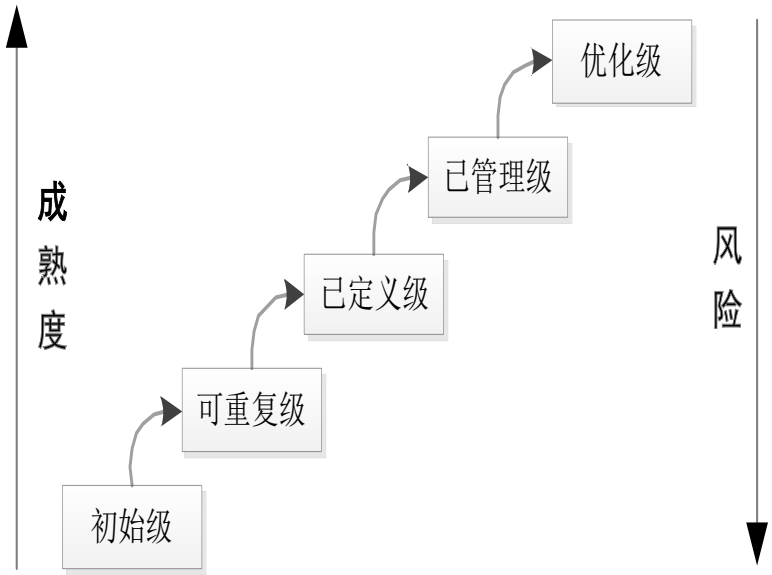
- 机构
  - 标准明确规定了为保证产品质量而必须建立的管理机构及职责权限
- 程序
  - 对组织的产品生产必须制定规章制度、技术标准、质量手册、质量体系和操作检查程序，并使之文件化
- 过程
  - 质量控制是对生产的全部过程加以控制，是面的控制，不是点的控制
- 总结
  - 不断地总结、评价质量管理体系，不断地改进质量管理体系，使质量管理呈螺旋式升

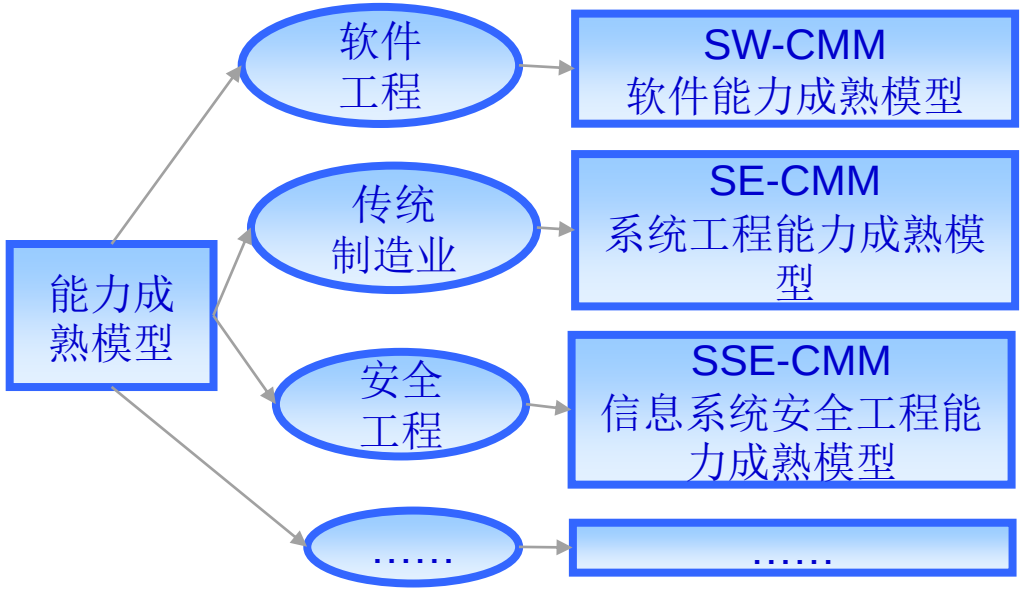
系统安全工程理论基础-能力成熟度模型

- 能力成熟度模型（Capability Maturity Model）
  - 一种衡量工程实施能力的方法
  - 建立在统计过程控制理论基础上的
- 能力成熟度模型基础
  - 现代统计过程控制理论表明通过强调生产过程的高质量和在过程中组织实施的成熟性可以低成本地生产出高质量产品；
  - 所有成功企业的共同特点是都具有一组严格定义、管理完善、可测可控从而高度有效的业务过程；
  - CMM模型抽取了这样一组好的工程实践并定义了过程的“能力”；

能力成熟度模型基本思想

- 工程实施组织的能力成熟度等级越高，系统的风险越低
- CMM为工程的过程能力提供了一个阶梯式的改进框架





知识子域：系统安全工程

- 系统安全工程能力成熟度模型
  - 了解系统安全工程能力成熟度模型基本概念；
  - 了解系统安全工程能力成熟度模型的体系结构及域维、能力维相关概念；

系统安全工程能力成熟度模型

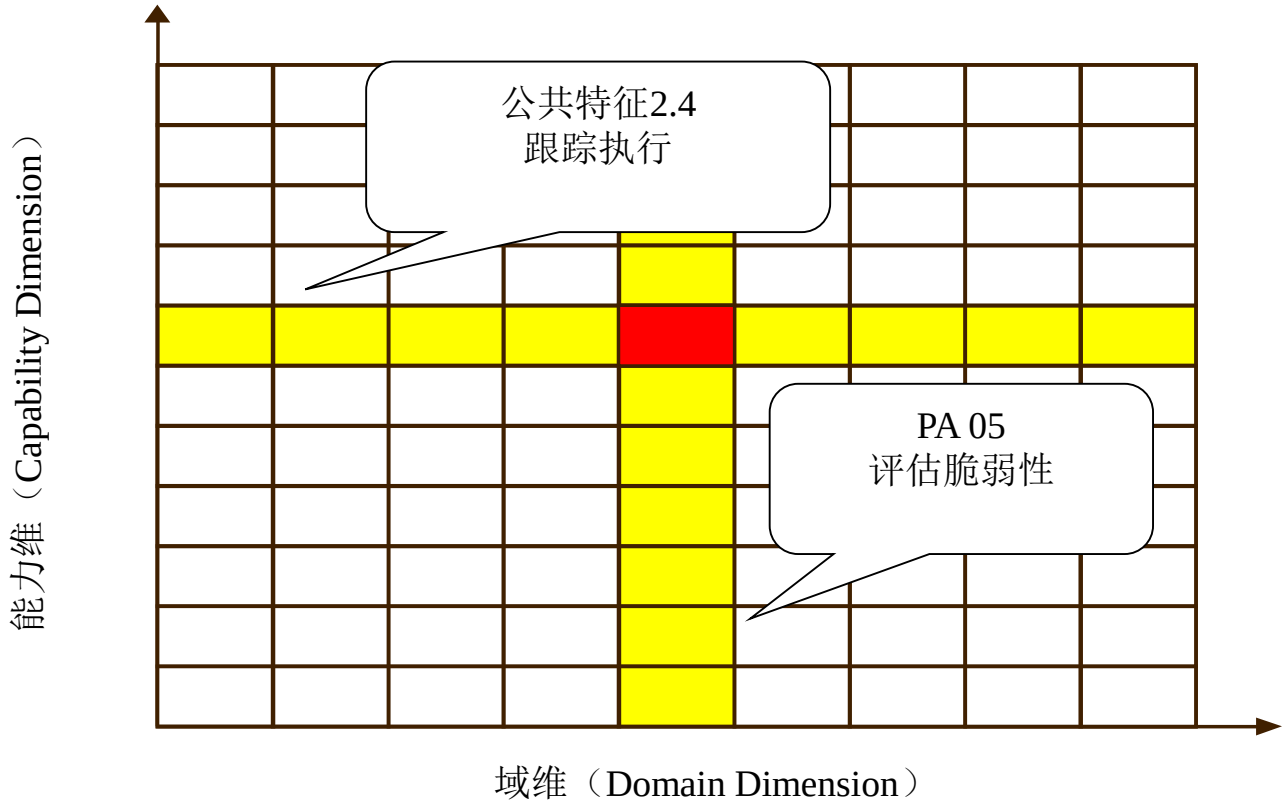
- 什么是系统安全工程能力成熟模型（SSE-CMM）
  - 一种衡量SSE实施能力的方法
  - 为信息安全工程过程改进建立一个框架模型
- SSE-CM描述了一个组织的**系统安全工程过程**必须包含的**基本特征**
  - 这些特征是完善的安全工程**保证**
  - 也是系统安全工程实施的度量标准
  - 还是一个易于理解的评估系统安全工程实施的框架

SSE-CMM的作用

- 获取组织（系统、产品的采购方）
  - 帮助选择合格的投标者，以统一的标准对安全工程过程进行监管提高工程实施质量，减少争议
- 工程组织（系统开发和集成商）
  - 通过可重复、可预测的过程减少返工、提高质量、降低成本；改进安全工程实施能力；获得证明安全工程实施能力的资质
- 认证评估组织
  - 获得独立于系统和产品的可重用的过程评估标准，用来确定被评估者将安全工程集成在系统工程之中，并且其系统安全工程是可信的

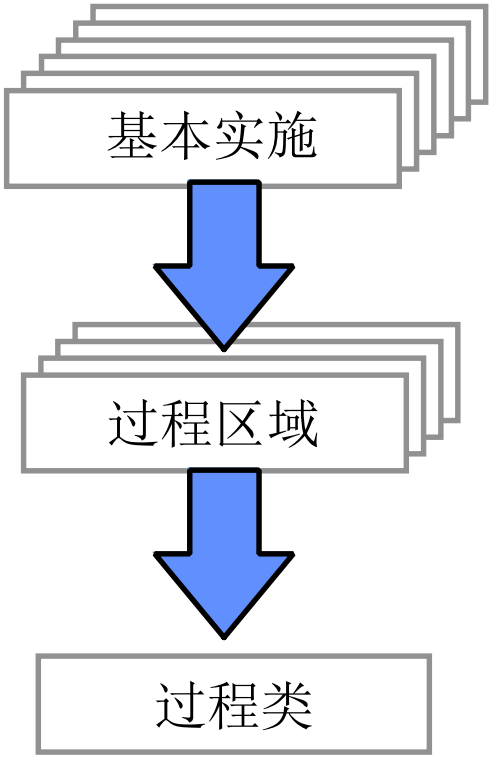
SSE-CMM体系结构

- “域维” 由所有定义的安全工程过程区构成
- “能力维”代表组织实施这一过程的能力



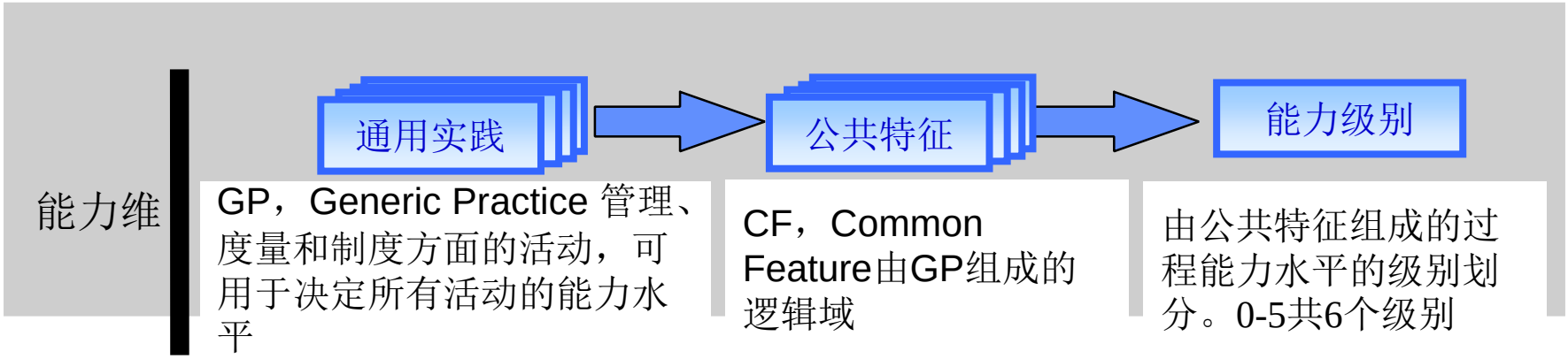
域维-过程区域

- 过程区域（PA，Process Area）
  - 过程区域是过程的一种**单位**
- 基本实施（BP，Base Practice）
  - 过程区域由BP组成
  - BP是强制实施
- 过程类
  - SSE-CMM包含22个PA，分为工程、项目、组织三类



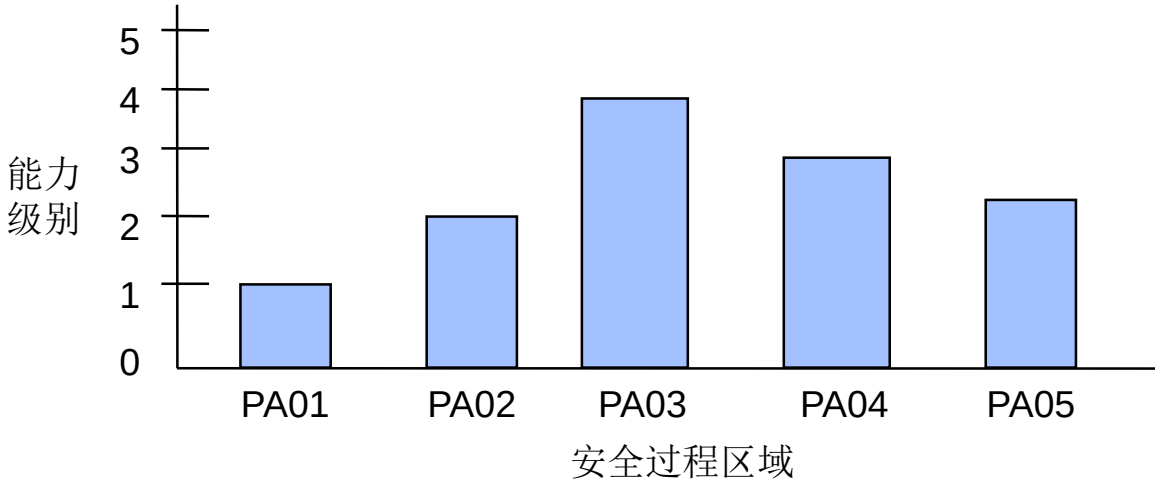
能力维-过程能力

- 过程能力（Process Capability）
  - 对过程控制程度的衡量方法，采用成熟度级别划分
- 过程能力的作用
  - 衡量组织达到过程目标的能力
  - 成熟度低，成本、进度、功能和质量都不稳定
  - 成熟度高，达到预定的成本、进度、功能和质量目标的就越有把握



SSE-CMM能力成熟度评价体系

- 通过设置这两个相互依赖的维，SSE-CMM在各个能力级别上覆盖了整个安全活动范围。
- 给每个PA赋予一个能力级别评分，所得到的两维图形便形象地反映一个工程组织整体上的系统安全工程能力成熟度，也间接的反映其工作结果的质量及其安全上的可信度。



知识子域：系统安全工程

- SSE-CMM安全工程过程
  - 掌握风险过程包括的评估威胁、评估脆弱性、评估影响及评估安全风险这四个过程区域及其基本实施；
  - 掌握工程过程包括的确定安全需求、提供安全输入、管理安全控制、监控安全态势及协调安全五个过程区域及其基本实施；
  - 掌握保证过程中验证和证实安全及建立保证论据两个过程区域及其基本实施。

域维-SSE-CMM的过程控制

- 工程类
  - 11个PA，描述了系统安全工程中实施的与安全直接相关的活动
- 组织和项目过程类
  - 11个PA，并不直接同系统安全相关，但常与11个工程过程区域一起用来度量系统安全队伍的过程能力成熟度

PA01	管理安全控制
PA02	评估影响
PA03	评估安全风险
PA04	评估威胁
PA05	评估脆弱性
PA06	建立保证论据
PA07	协调安全
PA08	监视安全态势
PA09	提供安全输入
PA10	明确安全需求
PA11	核实和确认安全

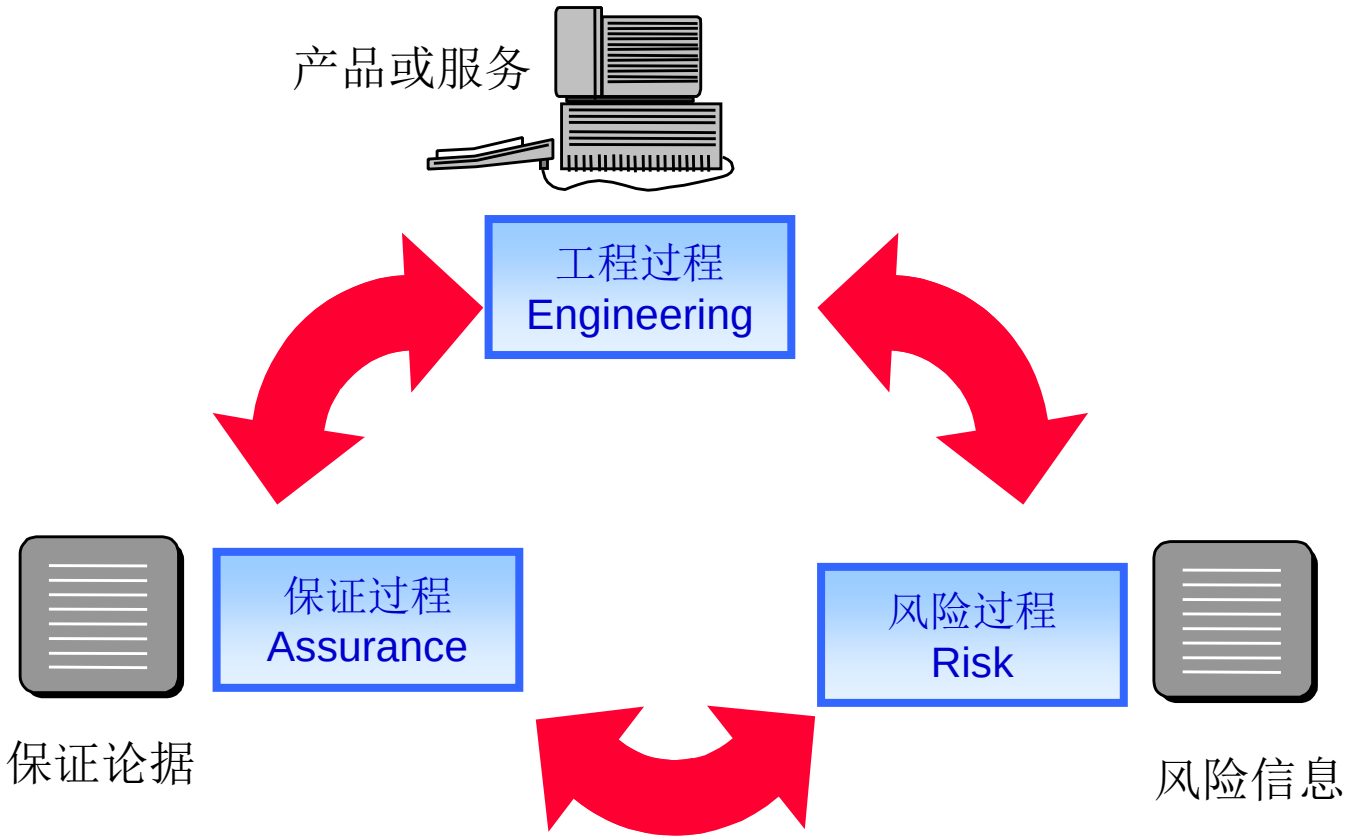
风险过程

工程过程

保证过程

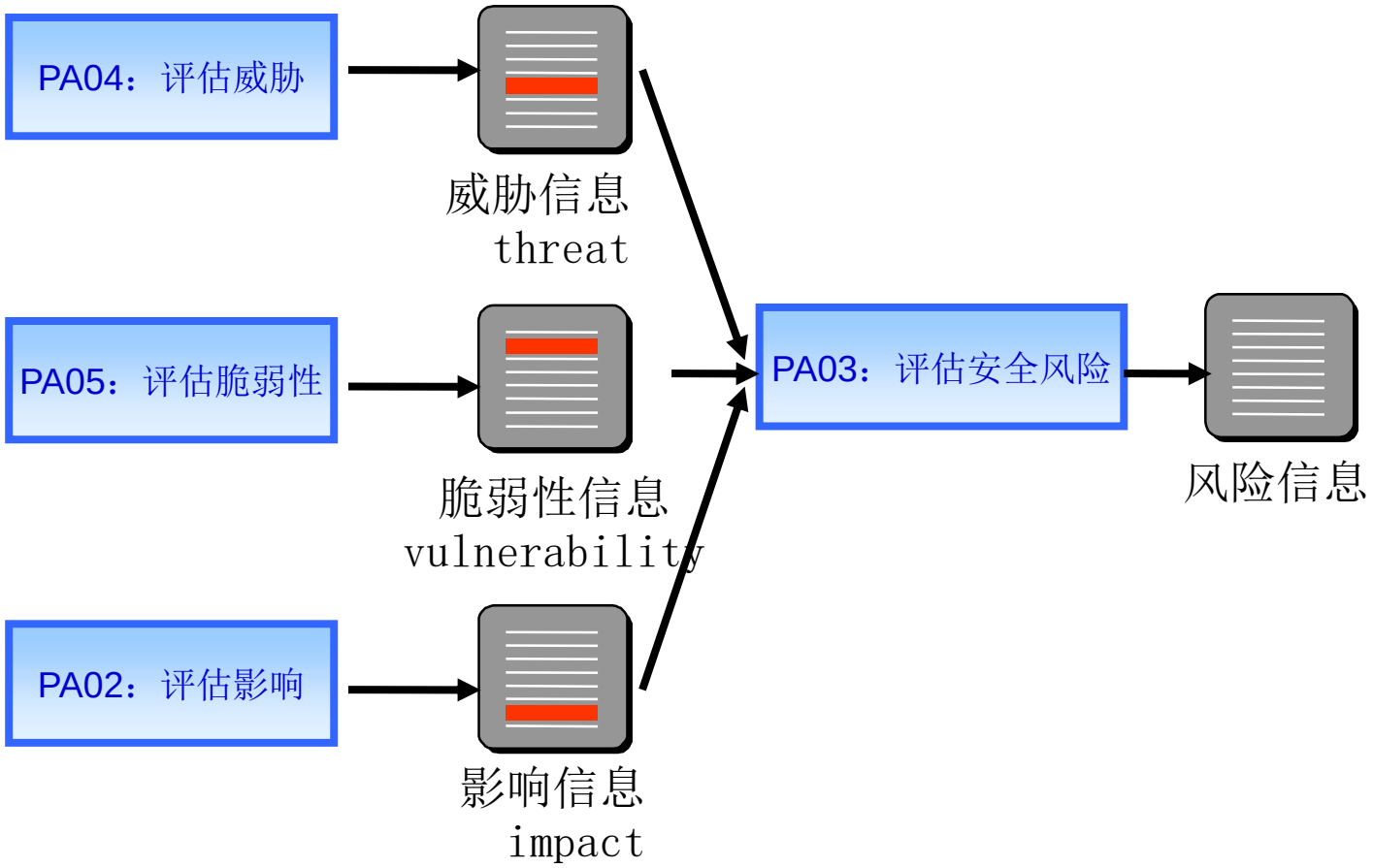
工程类过程之间关系

- 11个PA分为风险过程、工程过程、保证过程



风险过程

- 调查和量化风险的过程



PA04：评估威胁

- 识别和描述系统面临的安全威胁及其特征
  - BP. 04. 01识别由自然因素所引起的有关威胁
  - BP. 04. 02识别由人为因素所引起的有关威胁
  - BP. 04. 03制定评判威胁的测度单位
  - BP. 04. 04评估威胁源的动机和能力
  - BP. 04. 05评估威胁事件出现的可能性
  - BP. 04. 06 监控威胁的变化

PA05：评估脆弱性

- 识别和描述系统存在的脆弱性及其特征
  - BP. 05. 01选择识别和描述系统脆弱性的方法、技术和标准
  - BP. 05. 02识别系统存在的脆弱性
  - BP. 05. 03 收集与脆弱性特征有关的数据
  - BP. 05. 04 对脆弱性进行综合分析，评判脆弱性或脆弱性组合可能带来的危害
  - BP. 05. 05 监控脆弱性的变化

PA02：评估影响

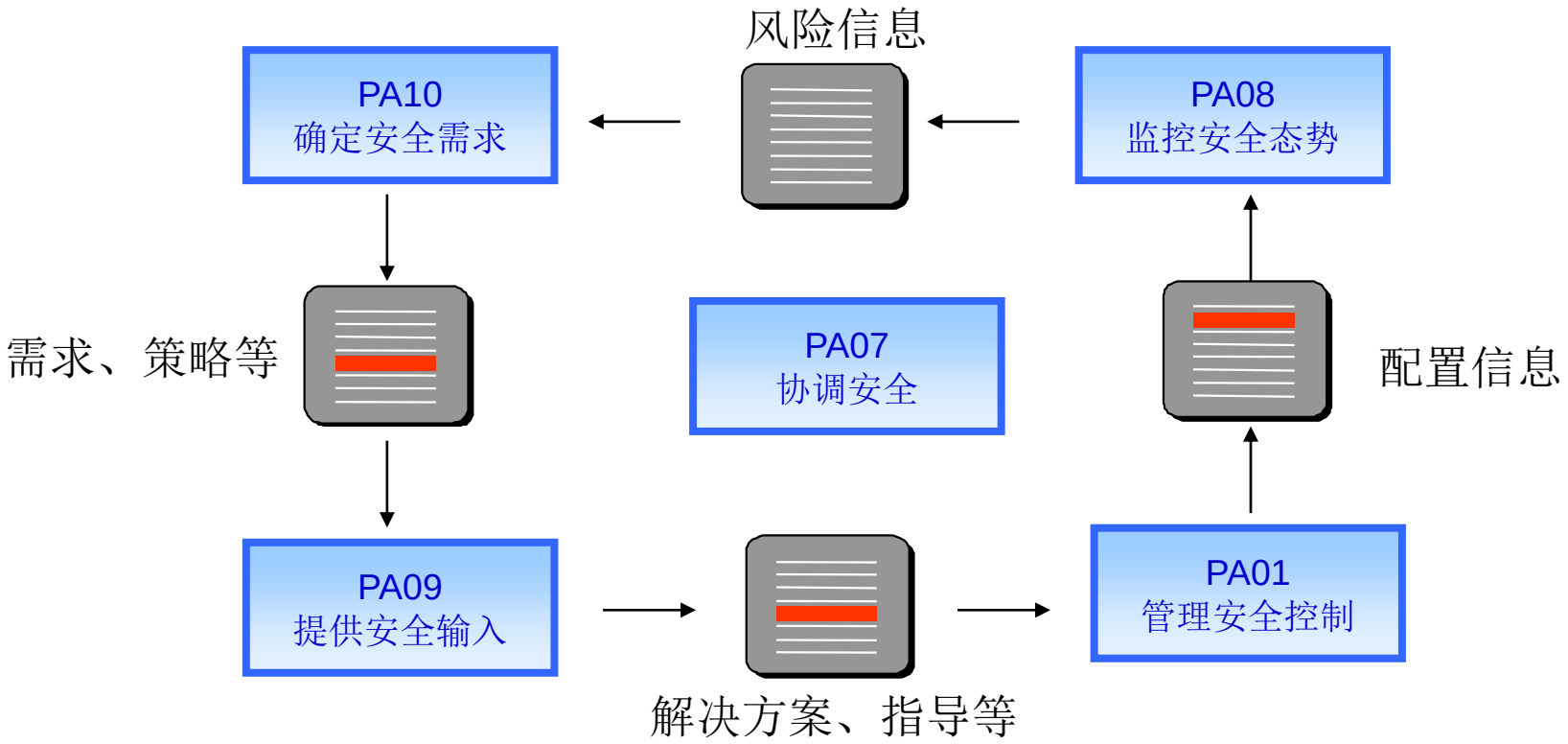
- 识别和描述安全事件造成的影响
  - BP.02.01　对运行、业务或任务指令进行识别、分析和优先级排列
  - BP.02.02　识别系统资产
  - BP.02.03　选择用于评估影响的度量标准
  - BP.02.04　标识度量标准以及（若需要）度量标准转换因子之间的关系
  - BP.02.05　识别影响
  - BP02.06　监控影响中发生的变化

PA03：评估安全风险

- 识别和描述系统面临的安全风险
  - BP. 03. 01　选择风险所依据的方法、技术和准则
  - BP. 03. 02　识别威胁/脆弱性/影响三组合（暴露）
  - BP. 03. 03　评估与每个暴露有关的风险
  - BP. 03. 04　评估总体不确定性
  - BP. 03. 05　风险优先级排列
  - BP. 03. 06　监控风险的变化

工程过程

- 安全工程是一个包括概念、设计、实现、测试、部署、运行、维护、退出的完整过程。
- SSE-CMM强调安全工程是一个大的项目队伍中的一部分，需要与其它科目工程师的活动相互协调。



PA10：确定安全需求

- 本过程区域实现依赖的7项基本实施
  - BP.10.01　获得对顾客安全需求的理解
  - BP.10.02　识别可用的法律、策略、标准、外部影响和约束
  - BP.10.03　识别系统用途，以确定其安全关联性
  - BP.10.04　捕捉系统运行的安全视图
  - BP.10.05　捕捉高层的安全目标
  - BP.10.06　定义安全相关需求
  - BP.10.07　达成安全协议

PA09：提供安全输入

- 此过程区域包括以下6项基本实施
  - BP. 09. 01　理解安全输入需求
  - BP. 09. 02　确定安全约束和需要考虑的问题
  - BP. 09. 03　识别安全解决方案
  - BP. 09. 04　分析工程可选方案的安全性
  - BP. 09. 05　提供安全工程指南
  - BP. 09. 06　提供运行安全指南

PA01：管理安全控制

- 此过程区域包括以下4项基本实施
  - BP.01.01　建立安全职责
  - BP.01.02　管理安全配置
  - BP.01.03　管理安全意识、培训和教育大纲
  - BP.01.04　安全服务及控制机制的管理

PA08：监控安全态势

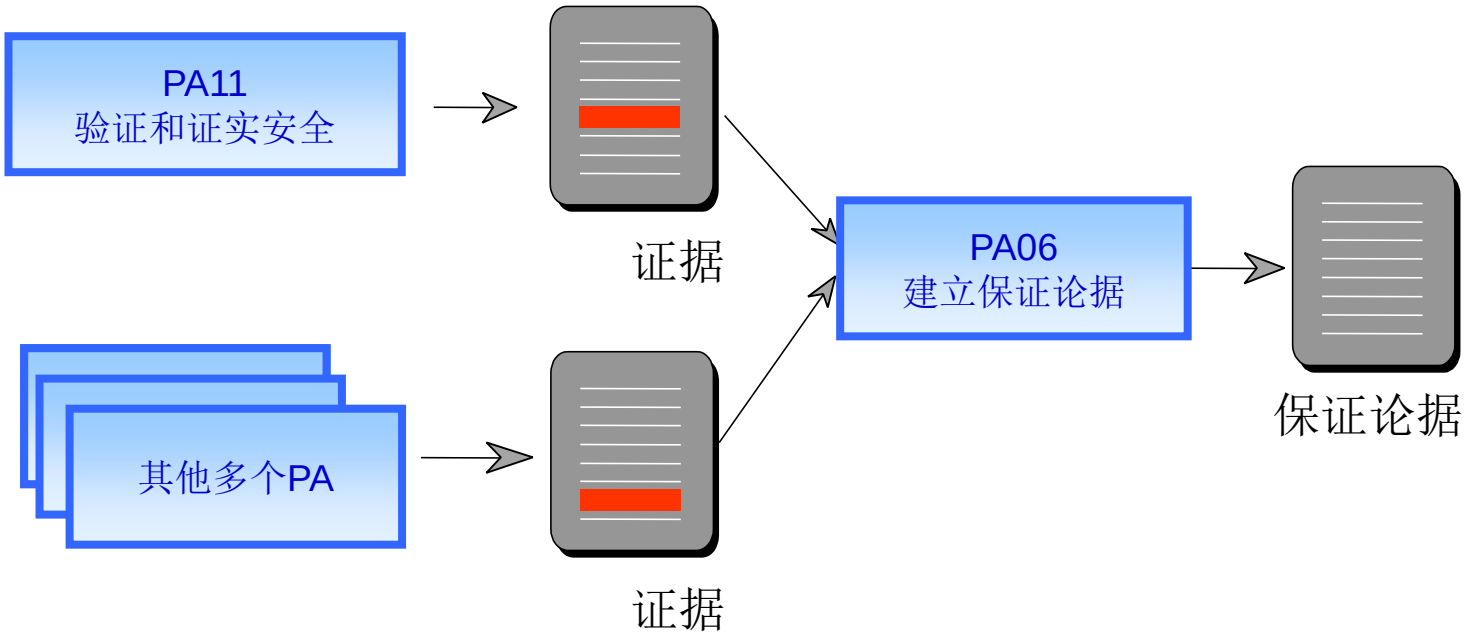
- 此过程区域包括以下7项基本实施
  - BP. 08. 01　分析事件记录
  - BP. 08. 02　监视变化
  - BP. 08. 03　识别安全突发事件
  - BP. 08. 04　监控安全防护措施的有效性
  - BP. 08. 05　审核安全态势
  - BP. 08. 06　管理对安全突发事件的响应
  - BP. 08. 07　保护安全监视的记录数据

PA07：协调安全

- 此过程区域包括以下4项基本实施
  - BP.07.01　定义协调目标
  - BP.07.02　识别协调机制
  - BP.07.03　促进协调
  - BP.07.04　协调安全决定和建议

保证过程

- 保证是指安全需要得到满足的信任程度
- SSE-CMM的信任程度来自于安全工程过程可重复性的结果质量



PA11：验证和证实安全

- 此过程区域包括以下5项BP
  - BP.11.01　识别验证和证实的目标
  - BP.11.02　定义验证和证实方法
  - BP.11.03　执行验证
  - BP.11.04　执行证实
  - BP.11.05　提供验证和证实的结果

PA06：建立保证论据

- 本过程区域包括以下5项基本实施
  - BP.06.01　识别保证目标
  - BP.06.02　定义保证策略
  - BP.06.03　控制保证证据
  - BP.06.04　分析证据
  - BP.06.05　提供保证论据

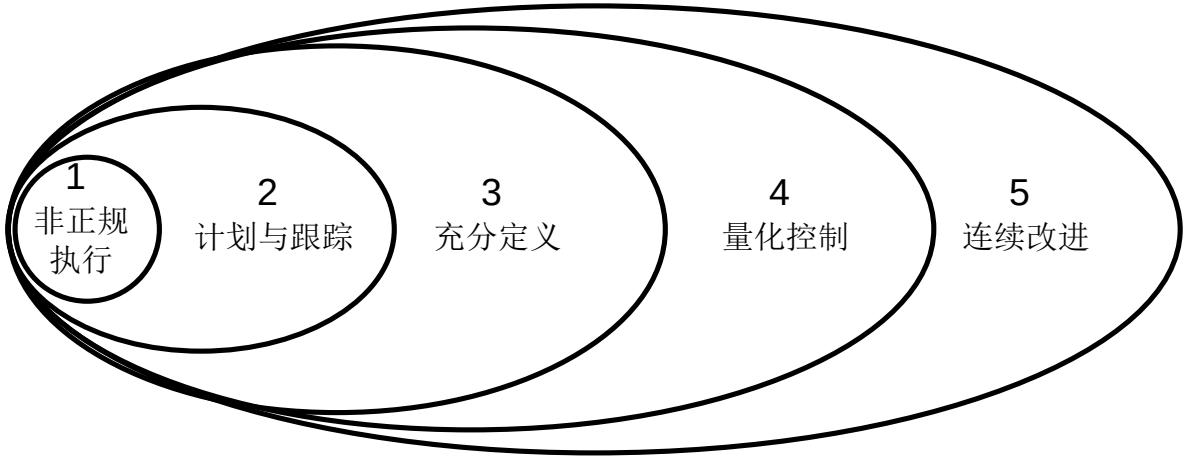
知识子域：系统安全工程

- SSE-CMM安全工程能力
  - 理解能力成熟度级别的概念；
  - 掌握1~5级不同成熟度级别应具有的公共特征。

能力级别：表示了过程的成熟性

- 组织的过程管理和制度化能力的强弱

能力级别



公共特征

•执行基本实施	•计划执行 •规范化执行 •跟踪执行 •验证执行	•定义标准过程 •协调安全实施 •执行已定义的过程	•建立可测量的质量目标 •客观地管理过程的执行	•改进组织能力 •改进过程的有效性

能力级别-1级

- 非正规执行级
  - 该级别过程区域的基本实施均被执行，但未经过严格的计划和跟踪，而是基于个人的知识和努力
  - 该级别包括一个公共特征——执行基本实施
    - 所有BP以某种方式执行
    - 工作产品的一致性、性能和质量会因为缺乏适当控制而存在极大的差异

能力级别-2级

- 规划和跟踪级
  - 该级别包括四个公共特征：
    - 规划执行：分配资源、指定责任、提供工具、将规划形成文档
    - 规范化执行：使用标准和规程、进行配置管理
    - 跟踪执行：跟踪过程实施、采取修正措施
    - 验证执行：验证工作过程、验证工作产品

能力级别-3级

- 充分定义级
  - 该级别包括三个公共特征：
    - 定义标准化过程：制定标准化过程，从组织标准化过程中裁剪出针对特定需求的过程
    - 执行已定义过程：PA的实施使用充分定义的过程，对执行结果进行缺陷评审，使用充分定义的数据
    - 协调安全实施：执行组内协调、执行组间协调、执行外部协调

能力级别-4级

- 量化控制级
  - 该级别包括两个公共特征：
    - 建立可测量的质量目标：为工作产品建立可测度的目标
    - 对执行情况实施客观管理：为工作过程能力建立量化测量和改进的标准

能力级别-5级

- 持续改进级
  - 该级别包括两个特征
    - 改进组织能力：建立过程有效性目标，持续改进标准过程
    - 改进过程有效性：进行因果分析，消除缺陷根源，持续改进已定义过程

知识子域：安全运营

- 安全运营概念
  - 了解安全运营的概念；
- 安全运营管理
  - 了解漏洞的概念及漏洞检测、漏洞评估等漏洞管理工作；
  - 了解补丁管理的重要性及补丁管理工作步骤；
  - 了解变更管理的作用及工作步骤；
  - 了解配置管理的基本概念；
  - 了解事件管理的基本概念。

安全运营概念

- 安全运营的概念
  - 建立机制对信息系统运行状况进行监控，对运行中的问题进行分析，发现问题的根源并协调资源进行解决以实现安全目标
  - 安全运营面向组织机构业务，与IT运营相辅相成；
- 安全运营参考标准
  - COBIT:IT控制和IT度量评价
  - ITIL: IT过程管理、强调IT支持和IT交付
  - ISO27000:IT安全控制

安全漏洞的概念

- 什么是安全漏洞（Vulnerability）
  - 也被称为脆弱性，计算机系统天生的类似基因的缺陷，在使用和发展过程中产生意想不到的问题（冯•诺依曼）
  - 漏洞是存在于评估对象（TOE）中的，在一定的环境条件下可能违反安全功能要求的弱点（ISO/IEC15408）
- 安全漏洞的范畴
  - 漏洞本身随着信息技术的发展而具有不同的含义与范畴
  - 基于访问控制的定义逐步发展到涉及系统安全流程、设计、实施、内部控制等全过程的定义

漏洞管理的重要性

- 为什么需要漏洞管理
  - 漏洞是信息系统中必然存在的安全问题，对漏洞进行管理是保障信息系统安全的重要工作
- 漏洞管理工作
  - 漏洞检测
  - 漏洞评估

补丁管理

- 基本意义
  - 有效的补丁管理程序能够确保系统安装当前最新的补丁。
- 主要步骤
  - 评估补丁（较为重要）
  - 测试补丁（较为关键）
  - 批准补丁（常与变更管理联动）
  - 部署补丁（人工、自动）
  - 验证补丁（伴随跟进的过程）

变更管理与配置管理

- 保证项目在变化过程中始终处于可控状态，并随时可跟踪回溯到某个历史状态
- 变更管理的过程
  - 提交变更申请
  - 变更审核
  - 变更批准
  - 变更实施
  - 变更记录
- 配置管理
  - 定义和控制服务与基础设施的部件，并保持准确的配置信息

事件管理

- 减少或消除事件（包括IT事件和安全事件）对信息系统运行带来的干扰
- 检测事件然后准确确定正确的支持资源以便尽快解决事件的能力
- 为管理层提供关于影响组织的事件的准确信息，以便他们能够确定必需的支持资源，并为支持资源的供给做好计划。
- 事件管理流程涉及运营的整个生命周期

知识子域：内容安全

- 内容安全基础
  - 了解内容安全的概念、重要性及内容安全管理的需求。
- 数字版权
  - 了解著作权、版权的概念；
  - 了解数字版权管理相关概念及技术；
  - 了解使用数据版权保护信息的措施。

内容安全基础

- 数字资源基本概念
  - 将计算机技术、通信技术及多媒体技术相互融合而形成的以数字形式发布、存取、利用的信息资源总和
- 国家制定多条法律法规来保障数字资源的安全性
  - 《中华人民共和国网络安全法》第十二条
  - 《中华人民共和国网络安全法》第四章第四十条与第四十二条
  - 《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》

内容安全需求

- 内容来源可靠
  - 数字资源来源可靠，借助数字版权管理技术，对其加以控制。
- 信息泄露
  - 敏感信息泄露控制
- 非法信息
  - 不良信息传播控制

版权与数字版权

- 版权
  - 我国现行著作权法第五条规定：“著作权与版权系同义语”。
  - 天赋人权：凡是中国公民，法人或者非法人单位的作品，不论是否发表都享有著作权
- 数字版权
  - 指各类出版物、信息资料的网络出版权，可以通过新兴的数字媒体传播内容的权利。

数字版权管理相关技术

- 数字版权管理(Digital Rights Management,DRM)
  - 用于保护数字作品的版权的一种方式，从技术上防止数字媒体的非法复制和非法使用，确保最终用户在得到授权后才能使用的数字媒体。
- 主要采用的技术
  - 数字水印、版权保护、数字签名、数据加密
- DRM六大功能：
  - 数字媒体加密、阻止非法内容注册、用户环境检测、用户行为监控、认证机制、付费机制和存储管理

数字版权保护措施

- 数字对象标识符（Digital Object Identifier，DOI）系统，即在数字环境下标识知识产权对象的一种开放性系统。
- 数字版权唯一标识符DCI（Digital Copyright Identifier）体系，它是数字作品权属的唯一标识，以有效应对互联网版权保护面临的挑战。
  - 数字作品版权登记平台
  - 数字版权费用结算平台
  - 数字版权检测取证平台

知识子域：内容安全

- 信息保护
  - 理解信息的价值；
  - 了解信息泄露的途径；
  - 了解隐私保护的概念和隐私保护措施。
- 网络舆情
  - 了解网络舆情的概念；
  - 了解网络舆情管理措施及网络舆情监控技术。

信息保护

- 信息
  - 泛指人类社会传播的一切内容。
  - 任何的信息都是有价值的
- 信息泄露途径
  - 个人隐私信息泄漏
    - 社交网络、各类单据等
  - 组织机构的敏感信息泄漏
    - 信息公示过于细致
    - 缺乏敏感信息标记

信息保护

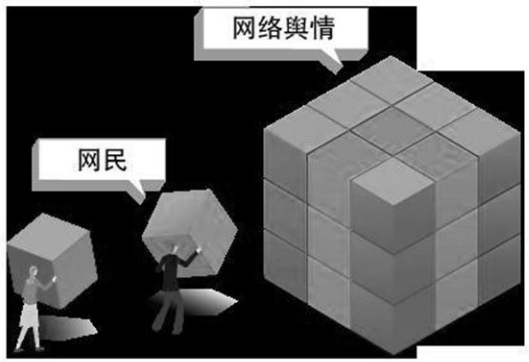
- 个人隐私信息保护
  - 如重要证件（身份证、军官证）等不随身携带，银行卡、U盾等应及时升级等
- 组织信息保护
  - 技术措施
    - 敏感信息泄露防护措施包括数据加密、信息拦截、访问控制等具体实现。
  - 管理措施
    - 结合各类管理措施并落实相关安全工程

网络舆情

- 基本概念
  - 在一定的社会空间内，通过网络围绕中介性社会事件的发生、发展和变化，民众对公共问题和社会管理者产生和持有的社会政治态度、信念和价值观。
  - 以网络为载体，以事件为核心，广大网民情感、态度、意见、观点的表达、传播与互动，以及后续影响力的集合。
- 表现方式
  - 新闻评论、BBS论坛、博客、播客、微博、聚合新闻(RSS)、新闻跟帖及转帖等等

网络舆情管理措施

- 及时且有效控制并降低舆情事态的扩大，是网络舆情管理的首要前提，其主要措施包含如下：
  - 确立政府主导地位，发挥媒体监督功能
  - 夯实网络舆情理论研究，积极开发网络舆情监测软件
  - 把握网络舆情管理的原则，建立和完善网络舆情管理机制



网络舆情系统监控技术

- 采集：搜索引擎、爬虫等、数据格式的转换、元数据的标引等
- 分析：分类、聚类、摘要等
- 呈现：信息再组织及结果推送

知识子域：社会工程学与培训教育

- 社会工程学
  - 理解社会工程学攻击的概念及在信息安全中的重要性；
  - 了解社会工程学利用的6种“人类天性基本倾向”；
  - 理解社会工程学攻击方式及防御措施。
- 培训教育
  - 了解“人”在信息安全体系中的作用；
  - 理解以建立持续化体系的方式实施信息安全培训的必要性；

利用人性弱点-社会工程学攻击

- 什么是社会工程学攻击
  - 利用人性弱点（本能反应、贪婪、易于信任等）进行欺骗获取利益的攻击方法
- 社会工程学的危险
  - 永远有效的攻击方法
  - 人是最不可控的因素

社会工程学利用的漏洞

- 人性的弱点（Robert B Cialdini）
  - 信任权威
  - 信任共同爱好
  - 获得好处后报答
  - 期望守信
  - 期望社会认可
  - 短缺资源的渴望
  - ……

传统社会中的社会工程学

- 中奖通知
- 欠费电话
- 退税短信
- 催交房租
- ……

网络社会的社会工程学

- 直接用于攻击
  - 正面攻击（直接索取）
  - 建立信任
  - 利用同情、内疚和胁迫
  - ……
- 间接用于攻击
  - 口令破解中的社会工程学利用
  - 网络攻击中的社会工程学利用

社会工程学防御

- 安全意识培训
  - 知道什么是社会工程学攻击
  - 社会工程学攻击利用什么
- 建立相应的安全响应应对措施
  - 构建完善的技术防御体系
  - 有效的安全管理体系和操作流程
- 注意保护个人隐私
  - 保护生日、年龄、email邮件地址、手机号码、家庭电话号码等信息

培训教育

- 人员培训的重要性
- 培训应持续性
- 建立培训计划
- 培训与发展挂钩

总结

- 系统安全工程
  - 系统安全工程重要性
  - 成立成熟度模型、系统安全工程能力成熟度模型
  - 过程区域与过程能力
- 安全运营
- 内容安全
- 社会工程学与培训教育

谢谢观看