第三部分　SSE-CMM

第三部分　SSE-CMM

- SSE-CMM综述
- SSE-CMM过程域
- SSE-CMM能力级别

SSE-CMM综述

主要内容

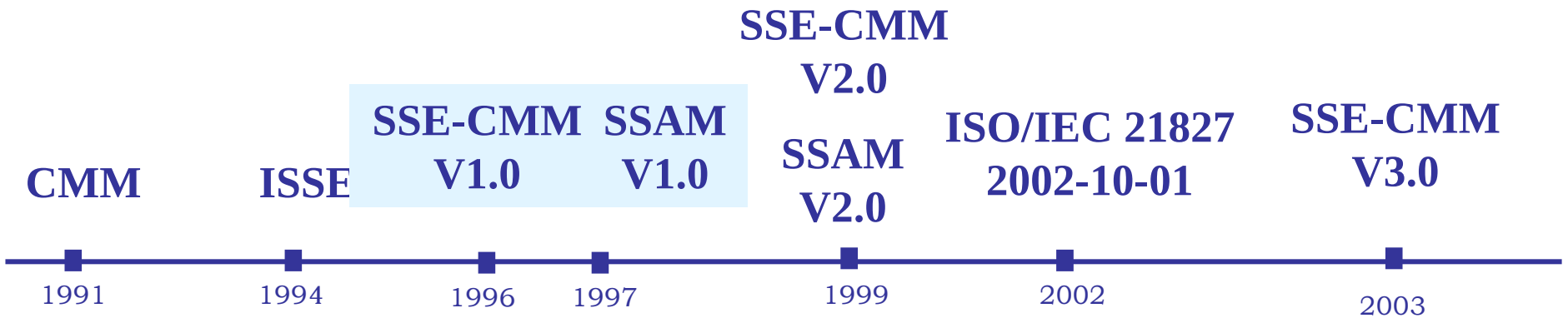
- SSE-CMM简介
- SSE-CMM方法学
- SSE-CMM的应用

SSE-CMM简介主要内容

■ SSE-CMM简介

- 什么是SSE-CMM
- 开发SSE-CMM的动因
- SSE-CMM的适用范围
- SSE-CMM的用户
- 如何使用SSE-CMM
- SSE-CMM的益处

信息安全工程的发展



■ SSE-CMM

- 由能力成熟度模型（CMM）发展而来
- 以工程域维和能力维来诠释信息安全工程过程的方法学
- 重要用途：对信息安全工程能力进行评估

什么是SSE-CMM

- SSE-CMM是系统安全工程能力成熟模型（Systems Security Engineering Capability Maturity Model）的缩写，它描述了一个组织的安全工程过程必须包含的本质特征，这些特征是完善的安全工程保证。尽管SSE-CMM没有规定一个特定的过程和步骤，但是它汇集了工业界常见的实施方法。

什么是SSE-CMM（续）

本模型是安全工程实施的标准化评估准则，它覆盖了：

- 整个生命期，包括开发、运行、维护和终止；
- 整个组织，包括其中的管理活动、组织活动和工程活动；
- 与其它学科和领域相并行的相互作用，如系统、软件、硬件、人的因素、测试工程、系统管理、运行和维护等；
- 与其它机构的相互作用，包括采办、系统管理、认证、认可和评估机构。

什么是SSE-CMM（续）

在SSE-CMM模型描述中，提供了

- 基本原理（方法学）
- 模型的高层综述
- 对SSE-CMM实施的建议
- 对模型的属性描述
- 开发该模型的需求
- 体系结构的全面描述
- 适当运用此模型的建议

SSE-CMM评定方法部分描述了针对SSE-CMM来评价一个组织的安全工程能力的过程和工具。

SSE-CMM简介主要内容

■ SSE-CMM简介

- 什么是SSE-CMM
- 开发SSE-CMM的动因
- SSE-CMM的适用范围
- SSE-CMM的用户
- 如何使用SSE-CMM
- SSE-CMM的益处

信息安全工程学的必要性

信息安全的特性决定了

- 信息保障是对信息和信息系统的安全属性及功能、效率进行保障的动态行为过程。
- 复杂的系统工程——信息安全工程
- 信息安全工程是采用工程的概念、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

能力成熟度模型的发展现状

– 质量保证概念在全世界兴起

– 以软件工程CMM为代表的CMM思想占据主流地位

- SSE-CMM（系统安全工程-能力成熟度模型）
- SE-CMM（系统工程-能力成熟度模型）
- P-CMM（人员能力成熟度模型）
- TCMM（可信能力成熟度模型）
- CMMI（CMM集成）
- IA-CMM（INFOSEC评估-能力成熟度模型）

SSE-CMM的意义

- 各方对信息安全工程过程能力的改进与评估的需要
  - 对安全工程质量不断提高的需求
  - 对安全工程评估的需求
- **为信息安全工程方法的应用提供了一个衡量和不断改进的途径**

SSE-CMM的意义（续）

- SSE-CMM项目的目标是发展一个得到良好定义的、成熟的且可度量的信息系统安全工程方法，从而使得
  - 通过区分投标者的能力级别和相关的项目风险来选择合格的安全工程提供商；
  - 使安全工程机构把安全投资集中在安全工程工具、培训、过程定义、管理实施和改进上；
  - 提供基于能力的保证，也就是说，信赖是基于对工程机构安全措施和过程成熟性的信心

SSE-CMM简介主要内容

■ SSE-CMM简介

- 什么是SSE-CMM
- 开发SSE-CMM的动因
- SSE-CMM的适用范围
- SSE-CMM的用户
- 如何使用SSE-CMM
- SSE-CMM的益处

SSE-CMM的适用范围

- 涉及可信产品或可信系统的整个生命周期的安全工程活动，包括概念定义、需求分析、设计、开发、集成、安装、运行、维护和终止。
- 可用于安全产品开发商、安全系统开发商及集成商、提供安全服务和安全工程的组织机构。
- 可应用于所有类型和大小的安全工程机构，如商务机构、政府机构和学术机构

SSE-CMM的适用范围（续）

- SSE-CMM是开放性的
- SSE-CMM是面向工程的

SSE-CMM简介主要内容

■ SSE-CMM简介

- 什么是SSE-CMM
- 开发SSE-CMM的动因
- SSE-CMM的适用范围
- SSE-CMM的用户
- 如何使用SSE-CMM
- SSE-CMM的益处

SSE-CMM的用户

– 包括涉及安全工程的各类机构，其中包括产品开发者，服务提供者，系统集成者，系统管理者，直至安全专家。其中部分组织处理高层问题（如运行使用或系统体系结构有关的问题），部分组织处理底层问题（如机制选择和设计），还有一部分组织涉及到这两个层面。

安全服务提供者（例）

- 为测量一个组织的从事风险评估的过程能力，会涉及到多个实施组共同参与。在系统开发或集成期间，需要评估该组织决定与分析安全脆弱性的能力，并且评估运行的影响。在这种运行情况下，评估组织对系统安全态势监控的能力，识别并分析安全脆弱性，以及评估运行的影响。

安全对策开发者（例）

- 在一个机构致力于开发安全对策为主的情况下，组织的过程能力使用SSE-CMM的实施组合来特征化。该模型包含的实施提供了决定和分析安全脆弱性、评估运行影响和为其它组织（如软件组织）提供指南和提供输入。提供安全对策的开发机构或有关人员需要理解上述实施间的关系。

产品开发者 （例）

- SSE-CMM包括致力于获得顾客安全需求的了解的实施。这些安全要求需通过与用户的交互来确定。
- 安全工程的实施者认识到产品开发的环境和方法如同产品本身一样是可变化的。然而，已知一些关于产品和项目环境的问题会影响到产品的构想、生产、交付和维护。以下问题特别对SSE-CMM具有重要影响:
  - 顾客群类型（产品，系统或服务）
  - 保证要求 (高或低)
  - 开发或运行机构的支持

特殊的行业或部门（例）

- 每个工业都自身有特殊的文化、术语和交流模式。为减少角色相关性和组织结构的影响，SSE-CMM期望能容易地将其概念转化为所有工业部门自身的语言和文化，从而在最大程度上减小业内各行业和部门的独特性对信息安全工程过程的影响

SSE-CMM简介主要内容

■ SSE-CMM简介

- 什么是SSE-CMM
- 开发SSE-CMM的动因
- SSE-CMM的适用范围
- SSE-CMM的用户
- 如何使用SSE-CMM
- SSE-CMM的益处

SSE-CMM与SSAM的应用方式

- 作为工程机构的工具来评估其安全工程实施活动，并实现对这些工程实施的改进
- 作为安全工程评估机构（如系统认证机构、产品评估机构）的工作基础，基于机构的能力为被评估机构建立起信任度（作为系统或产品安全保证的要素）
- 为客户建立起用以评估提供商的安全工程能力的标准机制

SSE-CMM简介主要内容

■ SSE-CMM简介

- 什么是SSE-CMM
- 开发SSE-CMM的动因
- SSE-CMM的适用范围
- SSE-CMM的用户
- 如何使用SSE-CMM
- SSE-CMM的益处

以更成熟的方式实施安全工程

- 现实要求机构以一个更成熟的方式来实施安全工程。特别地，在安全系统和安全产品生产和操作过程中要求以下特性：
  - 连续性 - 以前获得的知识将用于将来的工作
  - 重复性 - 保证项目可成功重复实施的方法
  - 有效性 - 可帮助开发者和评价者都更有效工作的方法
  - 保证 - 落实安全需求的信心
- 为了达到这些要求，需要有一个机制来指导组织机构去理解和改进其安全工程实施。SSE-CMM正是出于这个目的，用于改进安全工程实施的现状，以利用它达到提高安全系统、安全产品和安全工程服务的质量和可用性并降低成本的目的

工程机构

- 工程机构包括系统集成商，应用开发者，产品厂商和服务供应商。这些机构使用SSE-CMM的益处包括：
  - 通过可重复和可预测的过程和实施来减少返工
  - 获得真正工程执行能力的认可，特别在资源选择方面
  - 侧重于可度量组织的资格（成熟度）和改进

采办机构

- 采办机构包括从内部/外部得到系统、产品和服务的机构以及最终用户。这些机构使用SSE-CMM的益处包括：
  - 可重用的标准化提议请求语言和评定方法
  - 减少选择不合格投标者的风险（性能，成本，工期风险）
  - 基于工业标准的统一评估以减少争议
  - 在产品生产或提供服务过程中建立可预测和可重复级的可信度

评价机构

- 评价机构包括系统认证机构、系统认可机构、产品评价机构和产品评估机构。这些机构使用SSE-CMM的益处包括：
  - 与系统或产品变化无关的可重用的过程评定结果
  - 在安全工程中和安全工程与其它工程集成中的信任度
  - 基于能力的显见可信度，减少安全评估工作量

SSE-CMM方法学主要内容

SSE-CMM方法学

- 对安全工程的理解
- 安全工程过程的分类
- SSE-CMM的体系结构

安全工程的现状与意义（SSE-CMM）

- 安全工程正成为日益紧迫的领域，并将成为跨越多领域、协同工作的工程组中一个关键的部分
- 安全工程将应用到系统和应用的开发、集成、操作、管理、维护和进化以及产品的开发、交付和进化中。在企业和业务过程中的定义、管理和重建中必须强调安全的考虑。这样安全工程就能够在一个系统、一个产品或一个服务中得到体现。

安全工程的一些目标

- 获取对企业的安全风险的理解。
- 根据已识别的安全风险建立一组平衡的安全需求。
- 将安全需求转换成安全指南，使其集成到一个项目实施的其它领域活动中和系统配置中或运行的定义中。
- 在正确有效的安全机制下建立信心和保证。
- 判断系统中和系统运行时残留的安全脆弱性对运行的影响是否可容忍（即可接受的风险）。
- 将所有科目和专业活动集成为一个系统安全可信性的综合理解。

安全工程机构

- 安全工程机构是一个笼统的概念，泛指实施安全工程活动的各类机构
  - 开发者
  - 产品销售者
  - 集成商
  - 购买者（获取组织或最终用户）
  - 安全评估机构（系统认证者、产品评价者、运行许可批准者）
  - 系统管理机构
  - 可信第三方（认证授权）
  - 咨询/服务组织

安全工程与其它领域

– 因为残留的运行安全影响的保证和可接受性是在开发者、集成商、买主、用户、独立评价者和其它组织中建立的，因此安全工程活动必须要与其它外部实体进行协调。也正是因为存在这些与其它部分的接口并交互贯穿于组织的方方面面，所以使安全工程与其它工程相比更加复杂和不同。

- 企业工程
- 系统工程
- 软件工程
- 人力因素工程
- 通信工程
- 硬件工程
- 测试工程
- 系统管理

安全工程特点

- 安全工程与传统安全领域及新兴的安全领域必须“结合”
- 信息安全问题的整体性

相关领域

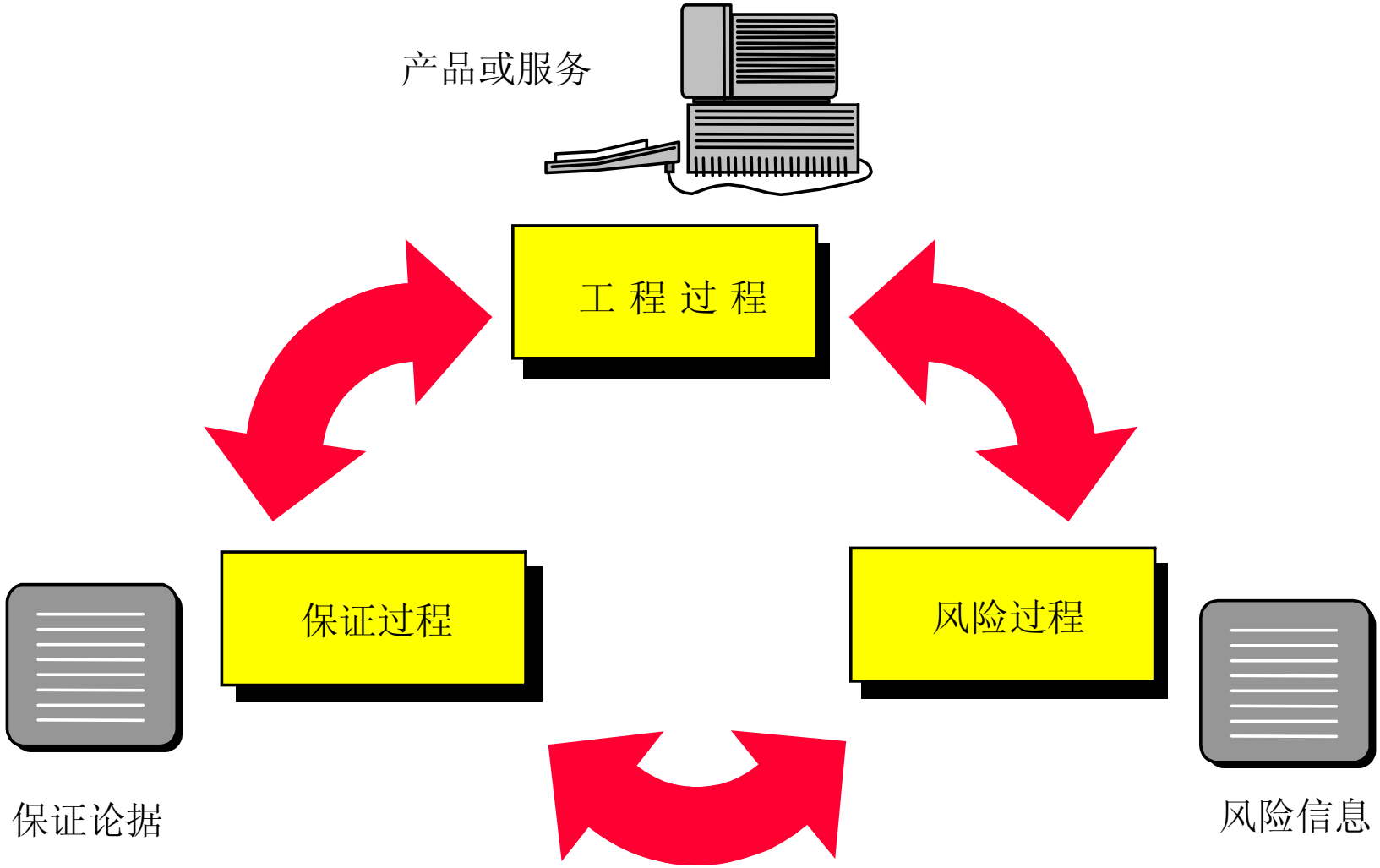
- 运行安全——运行环境安全和安全运行态势维护。
- 信息安全——在操作和处理中的信息和信息安全维护。
- 网络安全——包括网络硬件、软件和协议的保护，也包括在网络上通信的信息。
- 物理安全——注重于建筑和物理场所的保护。
- 人员安全——有关人员、他们的可信度和他们的安全意识。
- 管理安全——有关安全管理方面和管理系统的安全。
- 通信安全——有关安全域之间的通信保护，特别是信息在传输介质上传输时的保护。
- 辐射安全——涉及到所有机器设备将未期望产生的信号发射到安全域外部。
- 计算机安全——专门处理所有类型的安全计算设备

SSE-CMM方法学主要内容

■ SSE-CMM方法学

- 对安全工程的理解
- 安全工程过程的分类
- SSE-CMM的体系结构

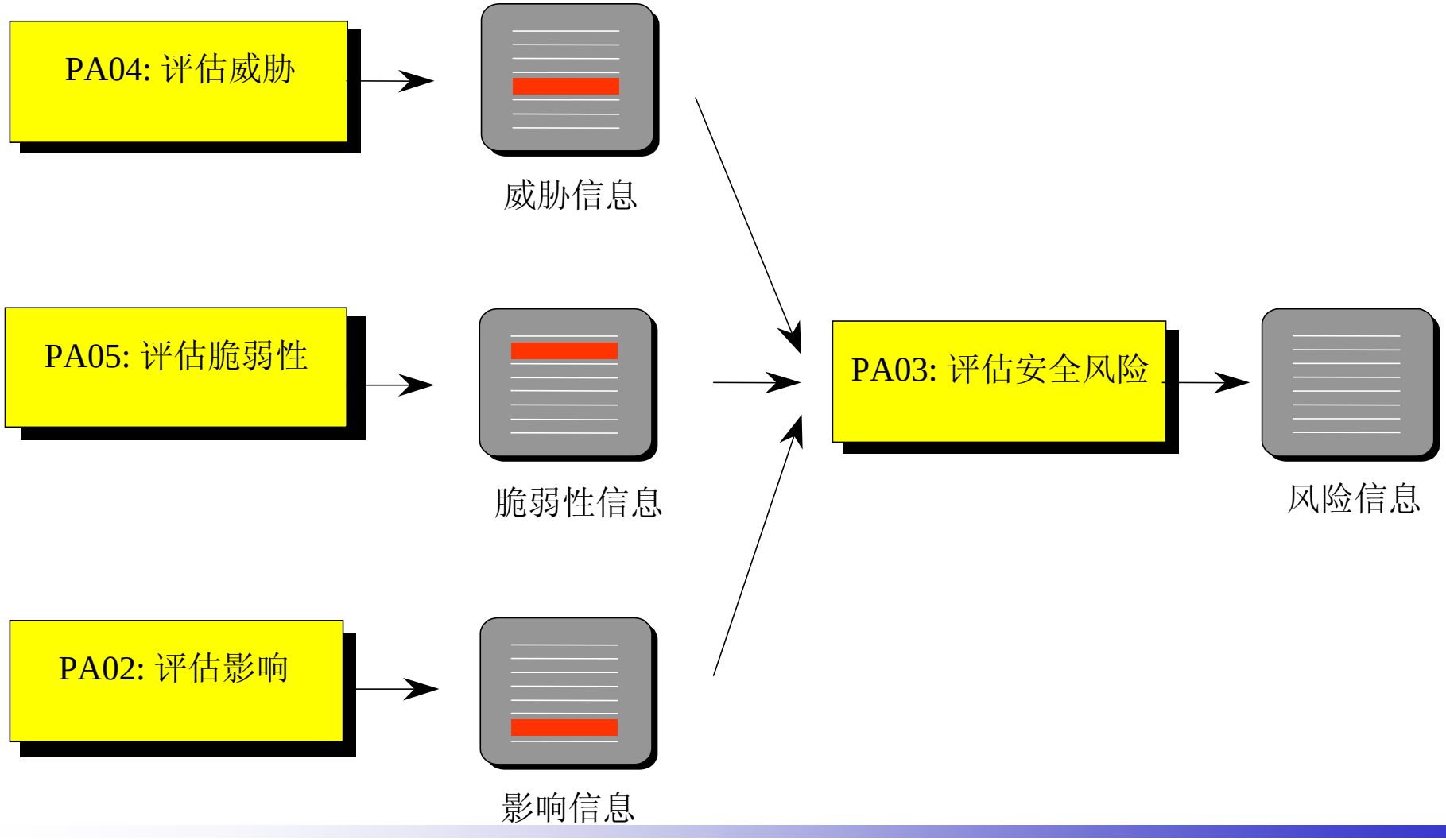
安全工程过程的分类



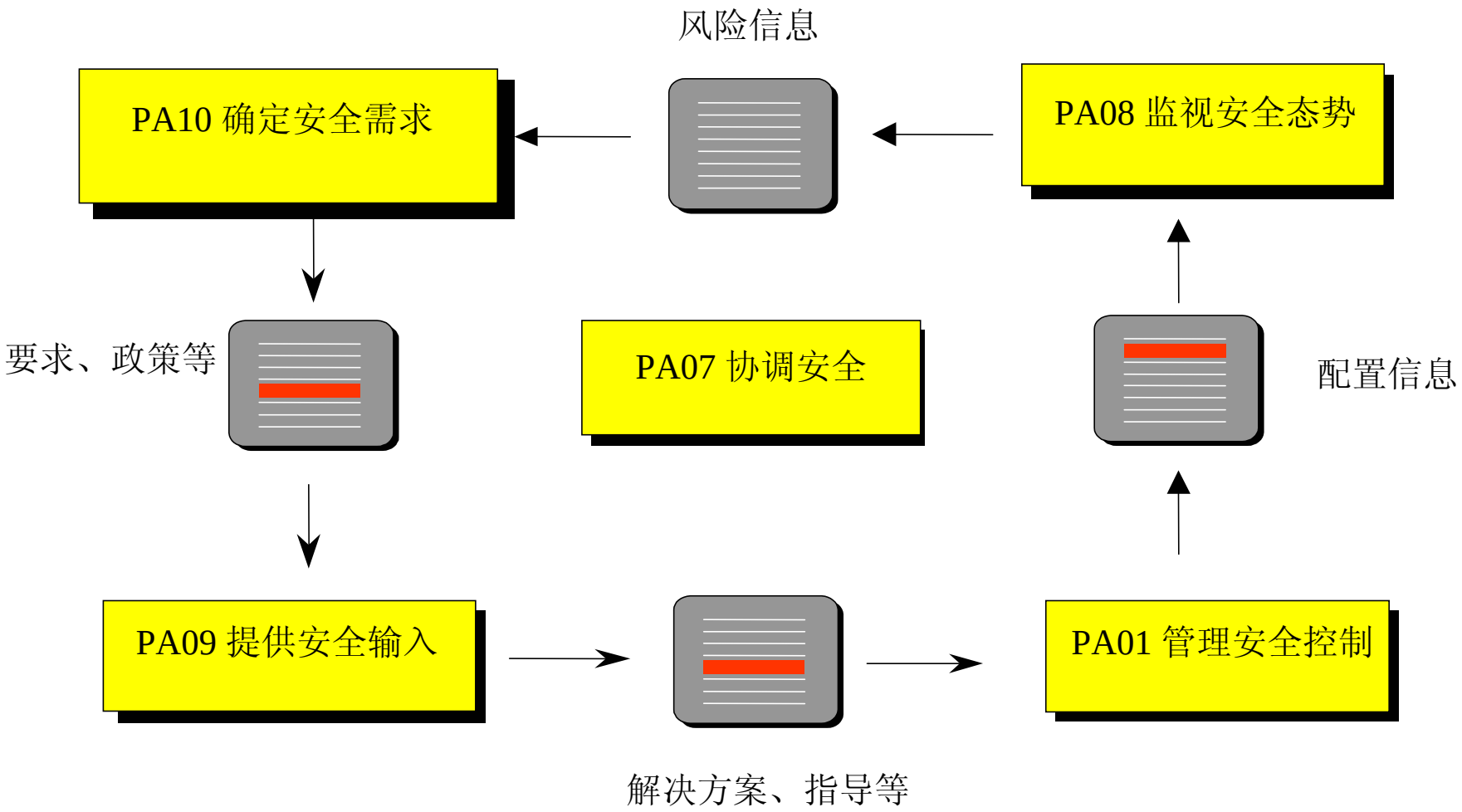
三个基本过程域组的关系

- 风险过程将标识出所开发产品或系统中存在的危险（风险）并对这些危险进行优先级排序；
- 针对危险所可能导致的问题（后果），安全工程过程要与其它工程方法一起合作，确定并实施解决方案；
- 最后，安全保证过程将为解决方案建立起信任度，并将这种信任度传达给客户
- 三者相互联系，又自成焦点

与风险过程相关的过程域



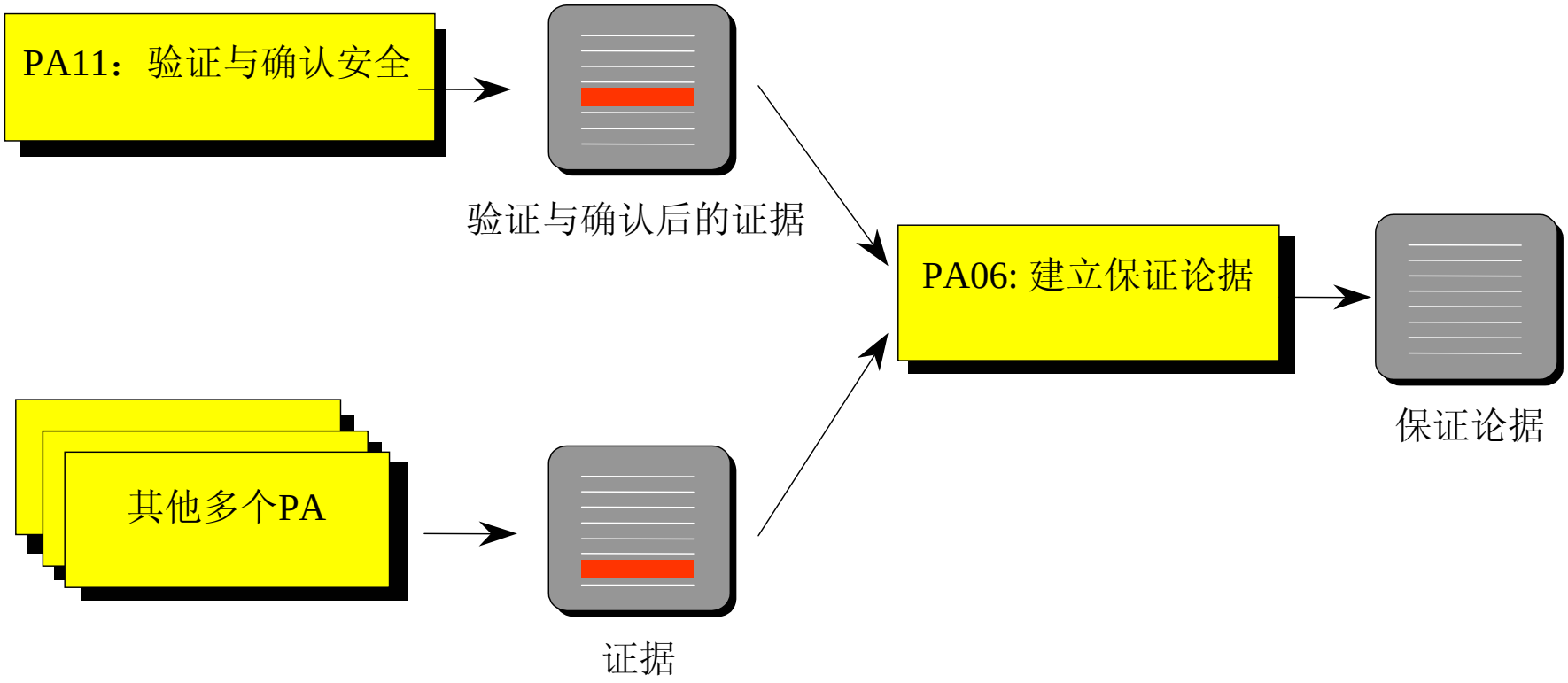
与工程过程相关的过程域



安全工程

- 安全工程是一个包括概念、设计、实现、测试、部署、运行、维护、终止的完整过程，具有周期性。在这个过程中，安全工程的实施必须紧密地与其它部分的系统工程组相合作。SSE-CMM强调安全工程师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。这会有助于保证安全成为一个大的项目过程中一个整体部分，而不是一个分开的独立活动。

与保证过程相关的过程域



安全保证

- 保证是指安全需要得到满足的信任程度
- 是安全工程非常重要的产品。存在着有许多的保证形式。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。这种信任的基础是成熟机构比不成熟机构更可能产生出重复的结果。
- 安全保证并不能添加任何额外的对安全相关风险的抗拒能力，但它能为减少预期安全风险控制提供信心。

安全保证（续)

- 安全保证也可看作是安全措施按照要求运行的信心。这种信心来自于正确性和有效性。正确性保证了安全措施按设计实现了需求。有效性则保证了提供的安全措施可充分地满足顾客的安全需要。安全机制的强度也会起作用，但会受到保护级别和安全保证程度的制约。

安全保证（续)

- 安全保证通常以安全论据的形式出现。安全论据包括一组对系统属性的声明集。这些声明集都要有证据来支持。证据在安全工程活动的正常过程期间获得并常常记录在文档中。
- SSE-CMM活动本身涉及到与安全相关证据的产生。例如，过程文件能够表示开发是遵循一个充分定义的、成熟工程过程，这个过程需加以连续改进。安全验证和证实在建立一个可信产品或系统中起到主要作用。
- 过程区中包括的许多典型工作产品可作为证据或证据的一部分。

安全保证的理论基础

- 现代统计过程控制表明如果注重产品生产过程，则可以较低的成本重复地生产出较高质量和安全保证的产品。组织措施的成熟能力将会对这个过程有影响和帮助。

SSE-CMM方法学主要内容

SSE-CMM方法学

- 对安全工程的理解
- 安全工程过程的分类
- SSE-CMM的体系结构

体系结构是方法学的核心

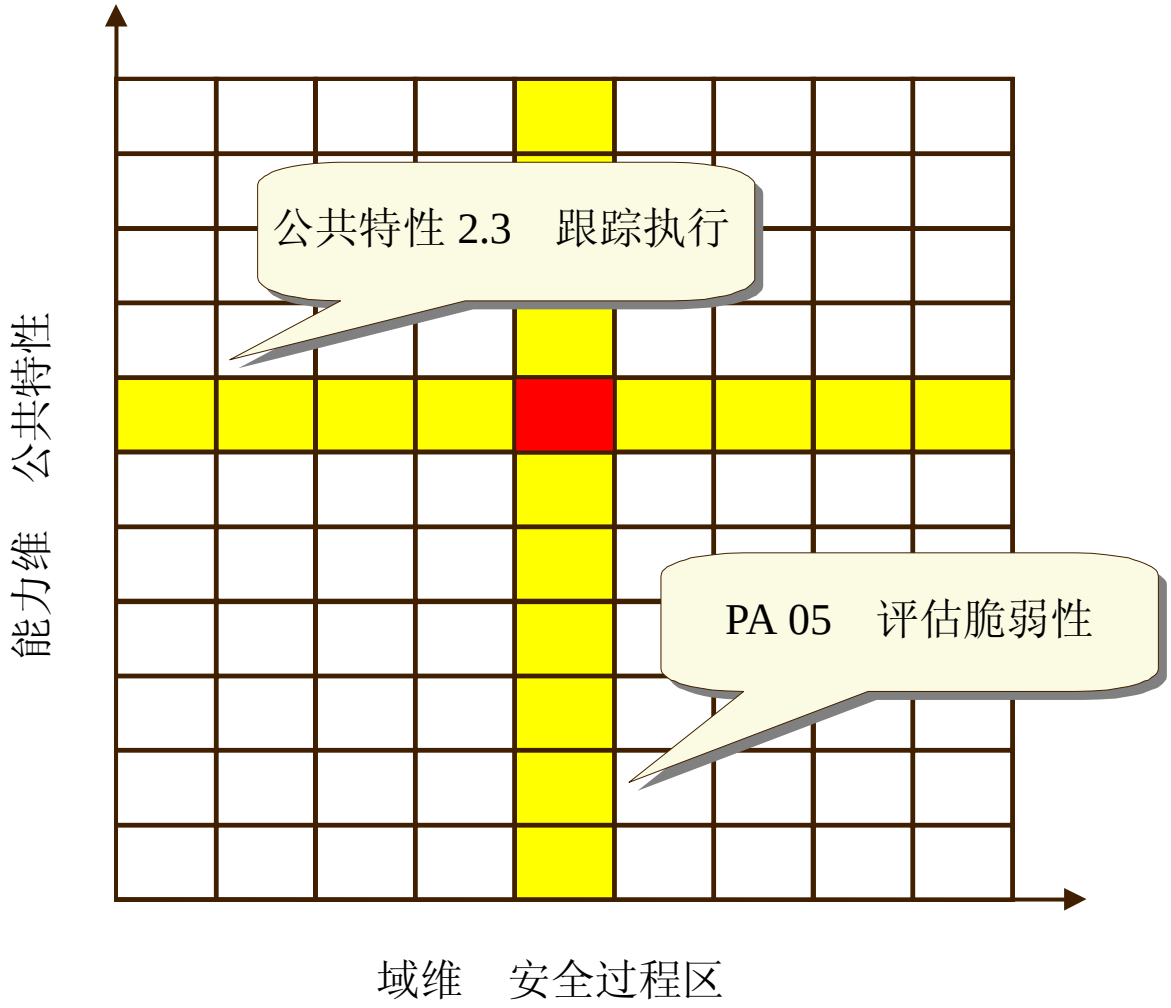
– 这个体系结构的目标是清晰地从管理和制度化特征中分离出安全工程的基本特征。为了保证这种分离，这个模型是两维的，分别称为“域”和“能力”

- SSE-CMM并不意味着在一个组织中任何项目组或角色必须执行这个模型中所描述的任何过程，也不要求使用最新的和最好的安全工程技术和方法论。然而，这个模型要求是一个组织机构要有一个适当过程，这个过程应包括这个模型中所描述的基本安全实施。组织机构以任何方式随意创建符合他们业务目标的过程以及组织结构。
- SSE-CMM也并不意味着执行通用实施的专门要求，一个组织机构一般可随意以他们所选择的方式和次序来计划、跟踪、定义、控制和改进他们的过程。然而，由于一些较高级别的通用实施依赖于较低级别的通用实施，因此组织机构应在试图达到较高级别之前，应首先实现较低级别通用实施。

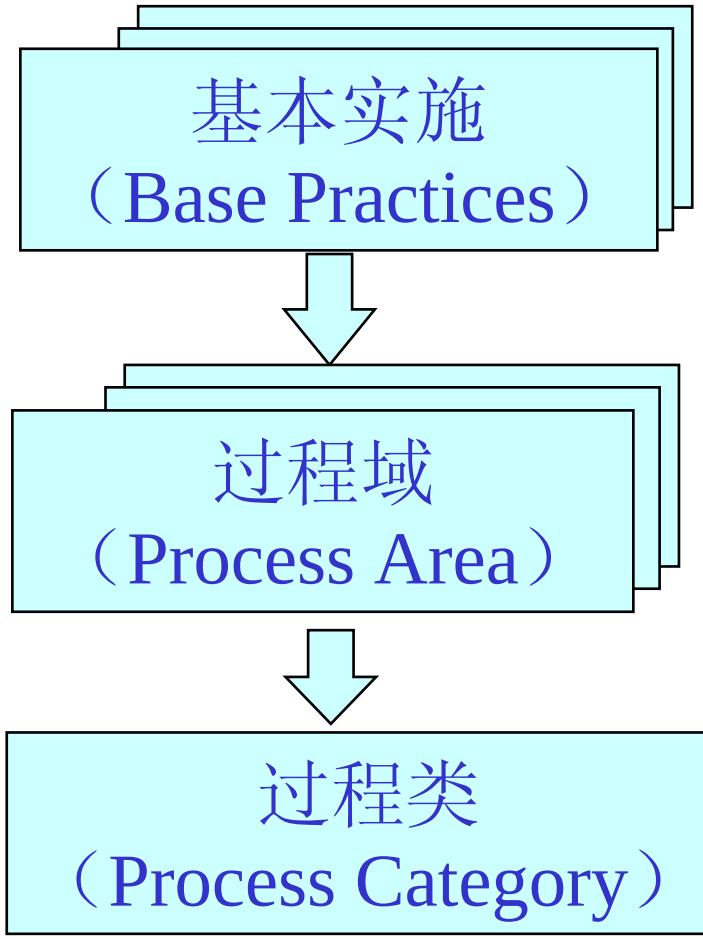
基本定义

- “域”维：仅仅由所有定义安全工程的工程实施活动构成，这些实施活动称为“基本实施”（Base Practice BP）。
- “能力”维：由一系列的工程实施活动组成，但这些工程实施活动代表的是机构对过程的管理和制度化能力。被称为“通用实施”（Generic Practice,GP），通用实施是基本实施过程中必须完成的活动

通用实施与基本实施之间的关系



基本实施与过程域



构成过程域，当全部实现后可满足过程域的要求

一组相关的基本实施，完成后可达到过程域的目的

一组过程域的集合，属于同一领域的活动

基本实施与过程域（续）

- SSE-CMM包含了61个基本实施过程，并被归入了11个安全工程过程域（Process Area ,PA），他们覆盖了安全工程的主要领域。
- 一个基本实施：
  - 应用于整个生命周期
  - 和其它BP互相不覆盖
  - 代表安全业界“最好的实施”
  - 不是简单地反映最新技术
  - 可在多种业务环境下以多种方法使用
  - 不指定具体的方法或工具

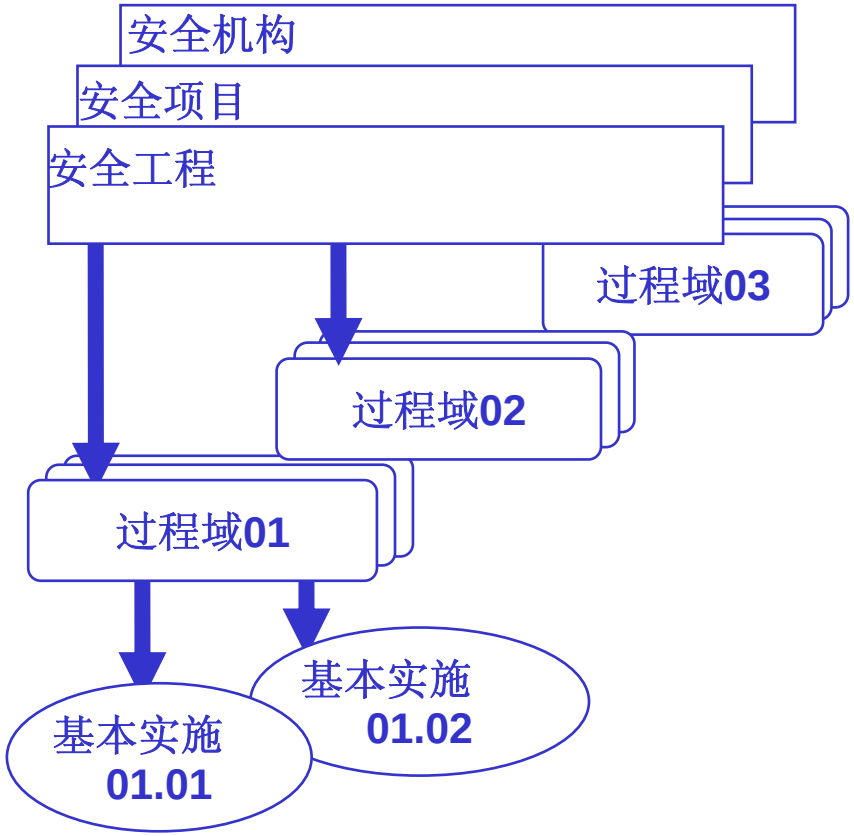
过程域

- 每一个过程域包括一组表示机构成功执行过程域的目标。每一个过程域也包括一组集成的“基本实施”或简称为“BP”。基本实施定义了取得过程域目标的必要步骤。

- 一个过程域：
  - 汇集一个域中的相关活动，以便于使用
  - 与有价值的安全工程服务相联系
  - 可在整个机构生命周期中应用
  - 能在多机构和多种产品背景下实现
  - 能作为一个独立的过程加以改进
  - 能够由类似兴趣的工程组进行改进
  - 包括能满足该过程域目标的所有BP

基本实施与过程域的关系

域维



11个过程域

- 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 建立安全论据
- PA07 协调安全性
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

其它过程域

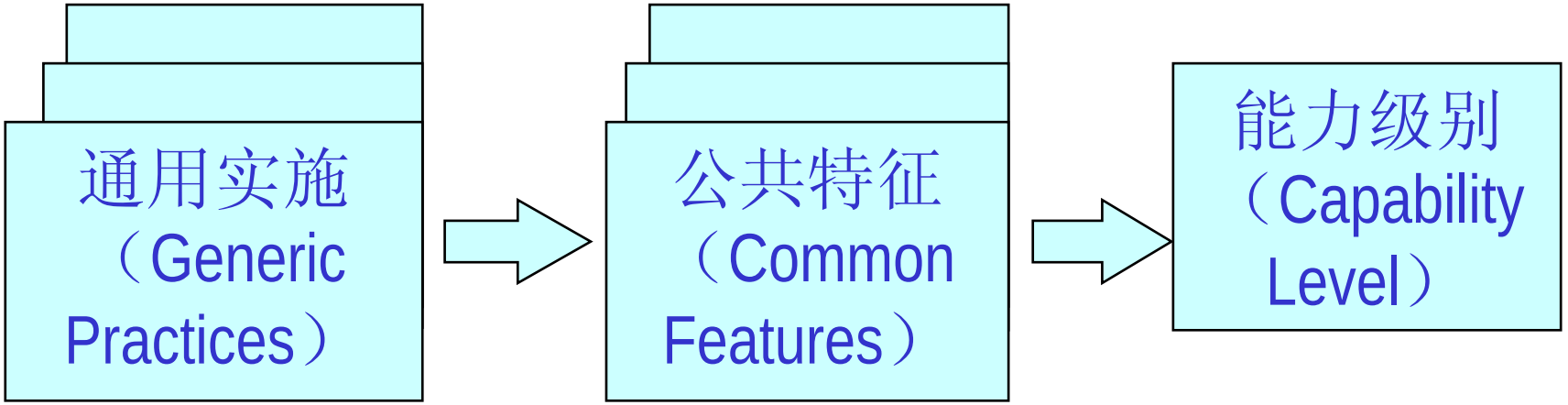
- PA12 确保质量
- PA13 管理配置
- PA14 管理项目风险
- PA15 监视和控制技术工作
- PA16 规划技术工作
- PA17 定义机构的系统工程过程
- PA18 改善机构的系统工程过程
- PA19 管理产品线发展
- PA20 管理系统工程支持环境
- PA21 提供不断发展的技能和知识
- PA22 与提供商相协调

- SSE-CMM还包括其余11个与项目和机构活动相关的过程域。它们来自于SE-CMM（系统工程——能力成熟模型）。
- 这些过程域不是与安全直接相关的，但是它们也会对安全造成影响。

通用实施与公共特征

- 通用实施是应用于所有过程域中的活动。针对的是过程的管理、测量和制度化。
- 通用实施被归入了12个不同逻辑域，称之为“公共特征” （Common Features）
- 12个公共特征被分为五个级别，依次表示增加的安全工程能力。
- 与域维基本实施不同的是，能力维的通用实施按成熟性排序，因此表示高级别通用实施位于能力维的高端。

通用实施、公共特征、能力级别



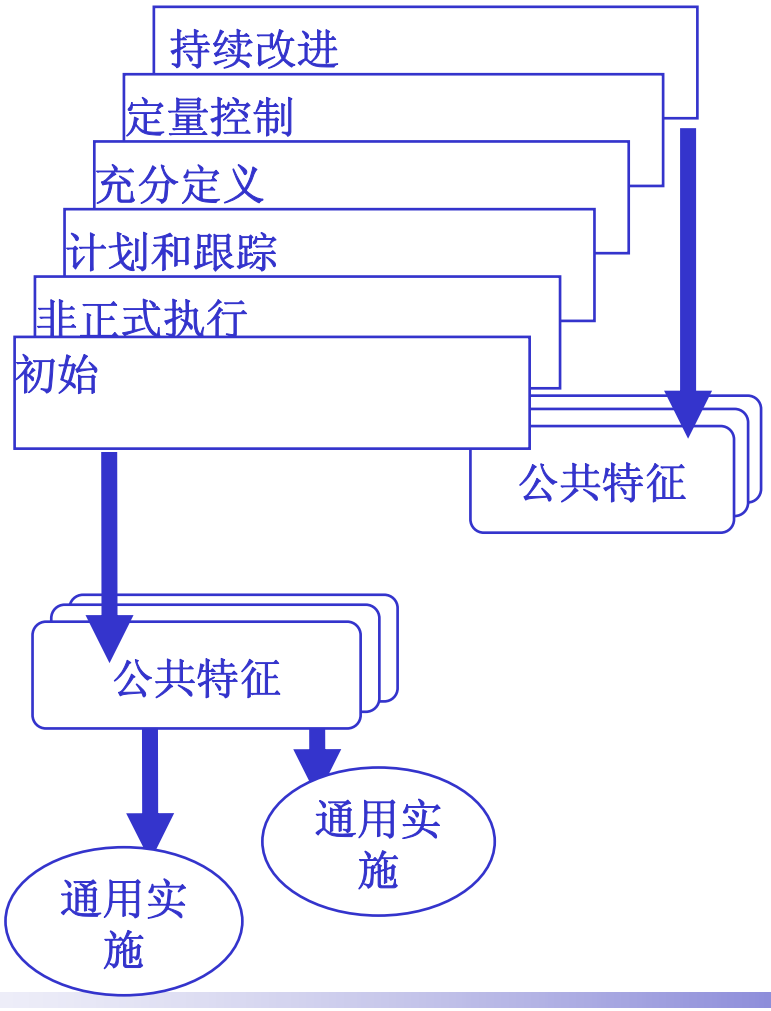
以实施或制度化为手段来提高工程过程的实施能力

通用实施的集合，每一集合中的公共特征面向的是同一类过程的管理和制度化问题

若干个（第一级是一个）公共特征的组合，显示了安全工程过程的实施能力级别

能力维中通用实施与公共特征的关系

能力维



能力维的原则

原则	如何在 SSE-CMM 中表述
在管理一个对象之前，必须首先实现该对象	非正式实施级将关注一个机构是否实现了基本实施中的工程过程
在定义机构层面的过程之前要理解项目的全部信息（例如该项目的产物是什么）	计划和跟踪级将关注项目层面的定义、规划和实施事项
使用从项目中学到的最佳知识来创建机构层面的过程	充分定义级将关注对在机构层面上定义的过程进行（融合了多个专业领域知识的）裁剪
只有清晰了解了一个对象，才能测量该对象	在计划和跟踪级，对安全工程项目进行基本的测量是很重要的，但直到充分定义级，SSE-CMM 才开始注意在机构层面上搜集测量数据，直到量化控制级，全面的项目测量成为可能
只有测量了正确的对象，基于测量的管理才有意义	量化控制级将关注对机构业务目标的测量
一个持续改进的文化必须以良好的管理措施、既定过程、可测量的目标为基础	持续改进级将通过以前的能力级获得最大可能的收益，强调文化的形成，以保持这种收益

SSE-CMM的5个能力级别

持续发展要求健全的管理实施，已定义的过程、可测量的目标作为基础

知道是什么后才能测量，测量对象正确时测量才由意义

持续改进级：从各级中获得并保持平衡

以项目中所学习的最好的东西定义机构层面的过程

量化控制级：与组织的商务目标联系的量化和测量

定义机构层面过程前先理解项目过程

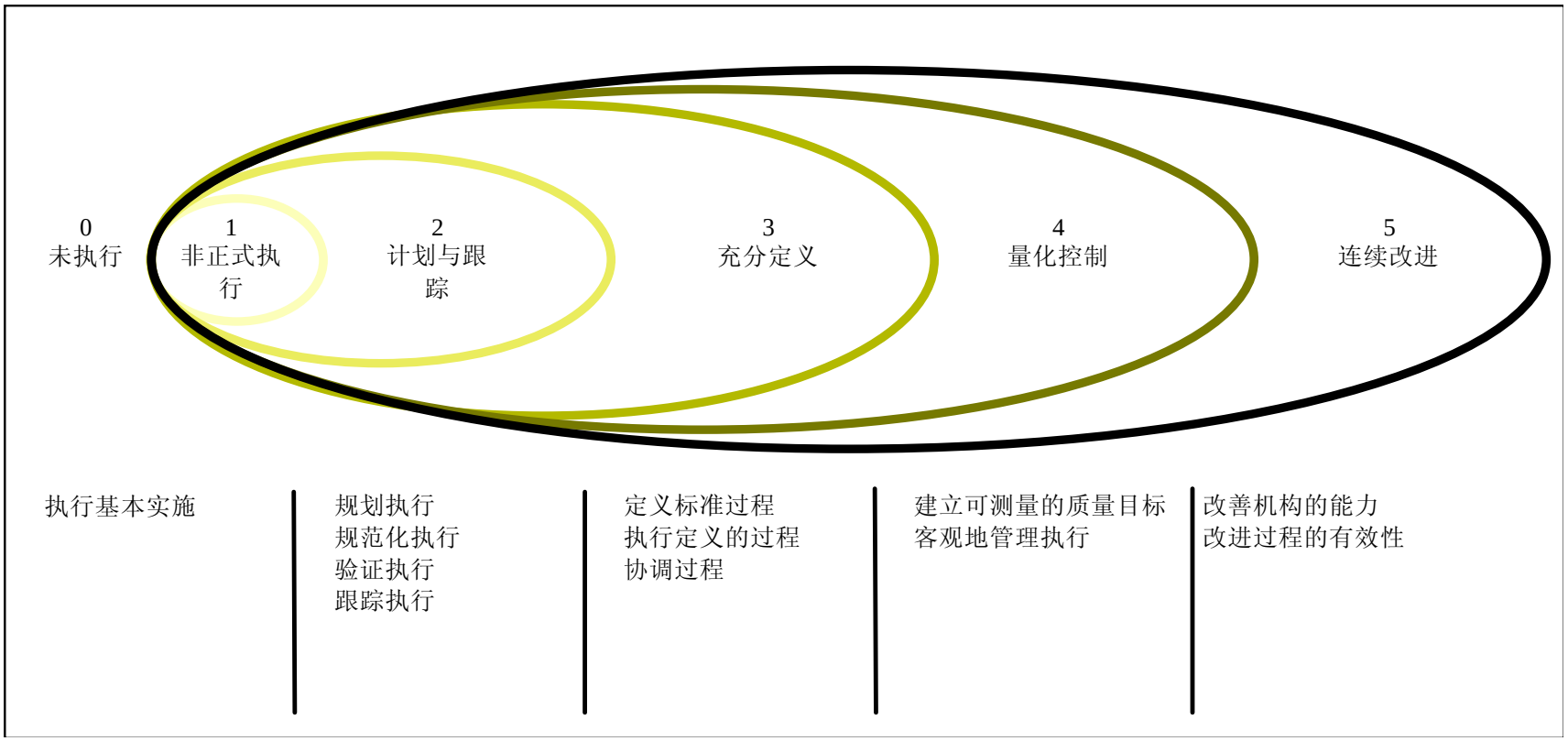
充分定义级：在组织级别上规范化的剪裁过程

先实施才能管理

计划跟踪级：在项目级别上定义、计划、执行过程

非正式执行级：执行包含基本实施的过程

5个能力级别与包含的公共特征



主要内容

- **SSE-CMM的应用**
  - 理解SSE-CMM的应用
  - 应用于过程改进
  - 应用于能力评定
  - 应用于获得保证

SSE-CMM的用户

- 安全产品开发商
- 安全系统开发商及集成商
- 安全服务提供商
- 安全工程机构
- 安全对策开发人员
- 评估机构

SSE-CMM的应用目的

- 过程改进
- 能力评定
- 获得保证

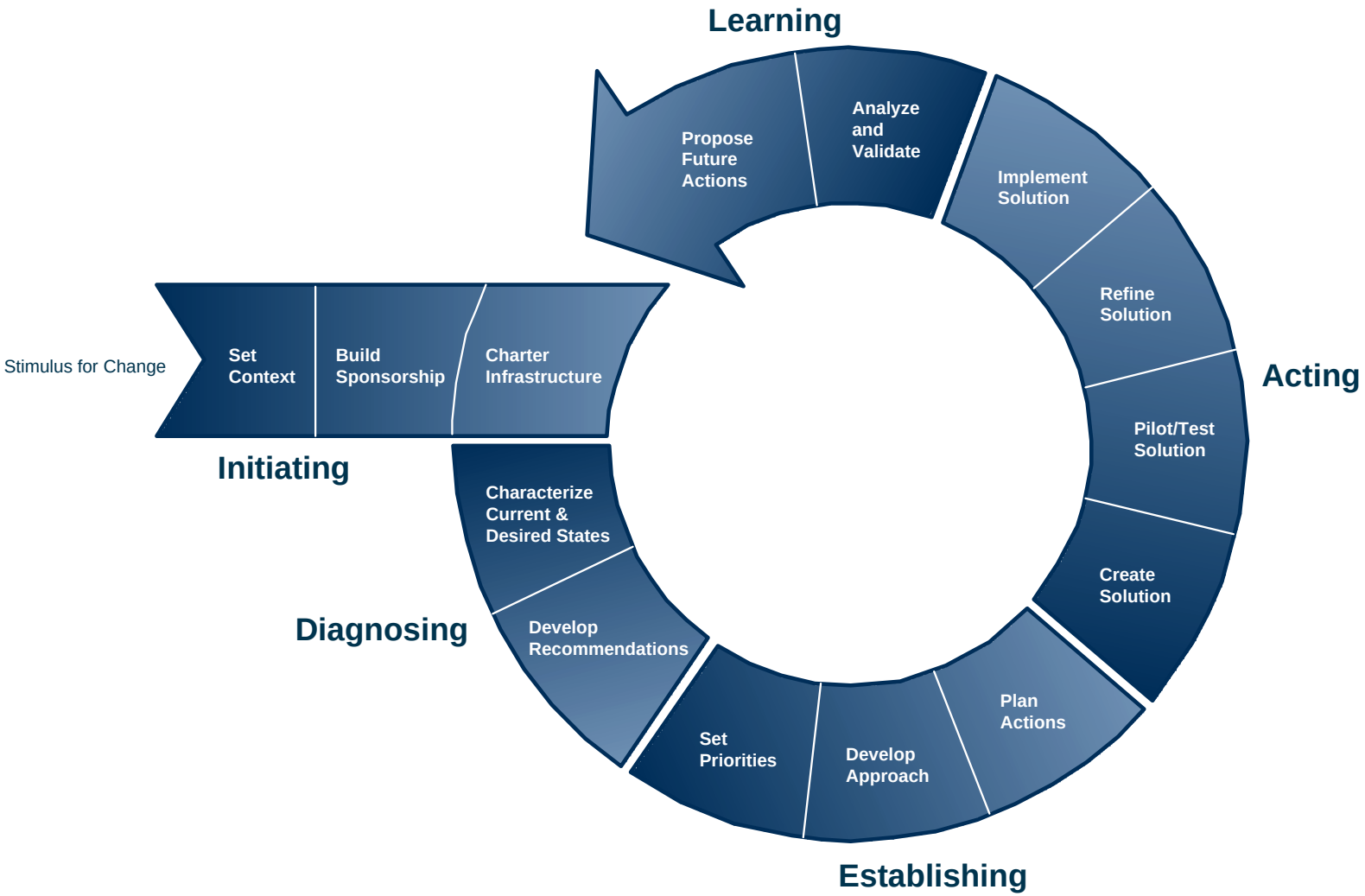
主要内容

- **SSE-CMM的应用**
  - 理解SSE-CMM的应用
  - 应用于过程改进
  - 应用于能力评定
  - 应用于获得保证

SSE-CMM应用于过程改进

- 过程是产品成本、进度和质量的决定性因素之一(其它决定因素为人员和技术)

过程改进的IDEAL方法

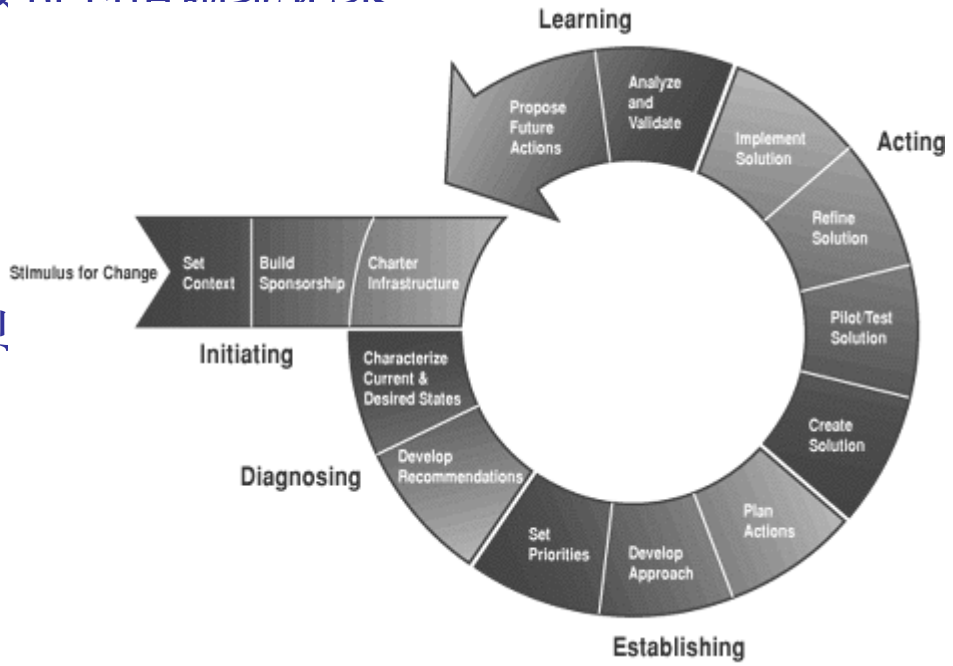


过程改进的IDEAL方法（续）

- 启动 Initiating：为安全工程过程的成功改进奠定基础
- 诊断 Diagnosing：判断当前的工程过程能力现状
- 建立 Establishing：建立详细的行动计划，为实现目标做出规划
- 行动 Acting：根据计划展开行动
- 学习 Learning：吸取经验，改进过程能力

启动阶段

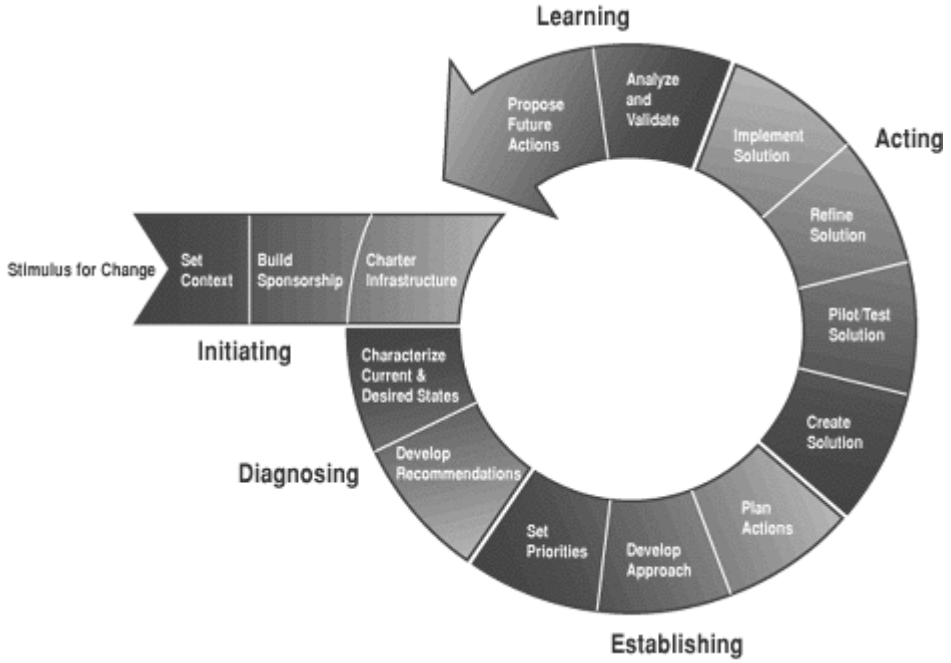
- 确定改进的动因
- 设置上下文
  - 目的是标识出改进工作对机构当前的业务战略和目标的支持关系。预期的改进效果应该得到清晰地记录
- 建立支持
- 获得基础设施
  - 建立改进工作的实现机制



诊断阶段

目的是了解机构当前以及未来期望的工程过程成熟度

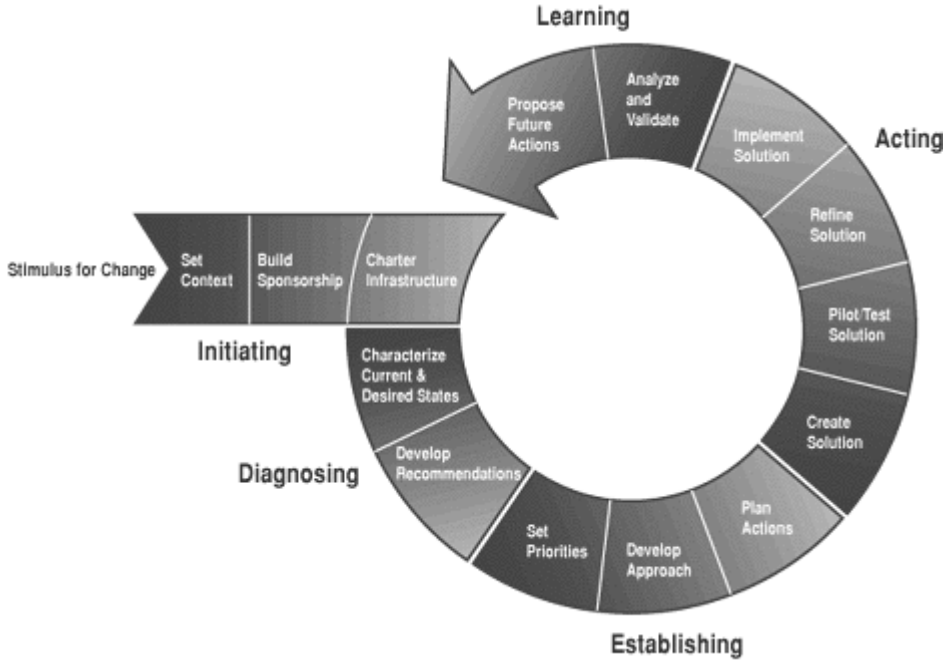
- 描述当前及未来期望的工程过程成熟度
- 制定建议
  - 对机构本身的深入认识
  - 对过程改进方法的理解



建立阶段

基于工作目标和前一阶段形成的建议而开发详细的计划

- 设定优先级
- 制定方法
- 对行动作计划
  - 责任分配
  - 可用资源
  - 具体任务
  - 追踪工具
  - 工期进度和时间
  - 应急计划

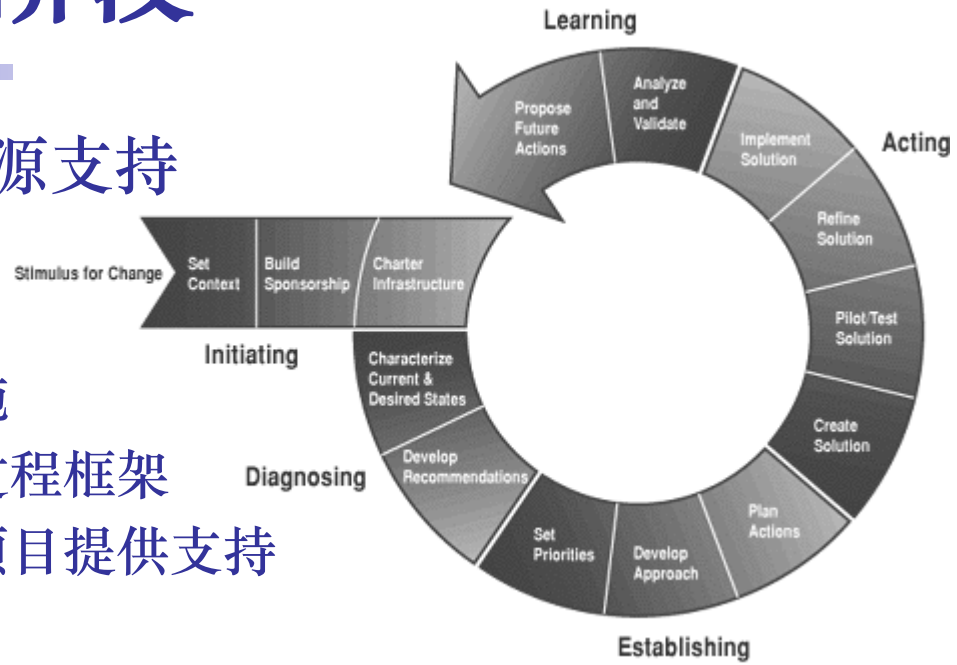


行动阶段

该阶段需要充分的时间和资源支持

– 创建解决方案

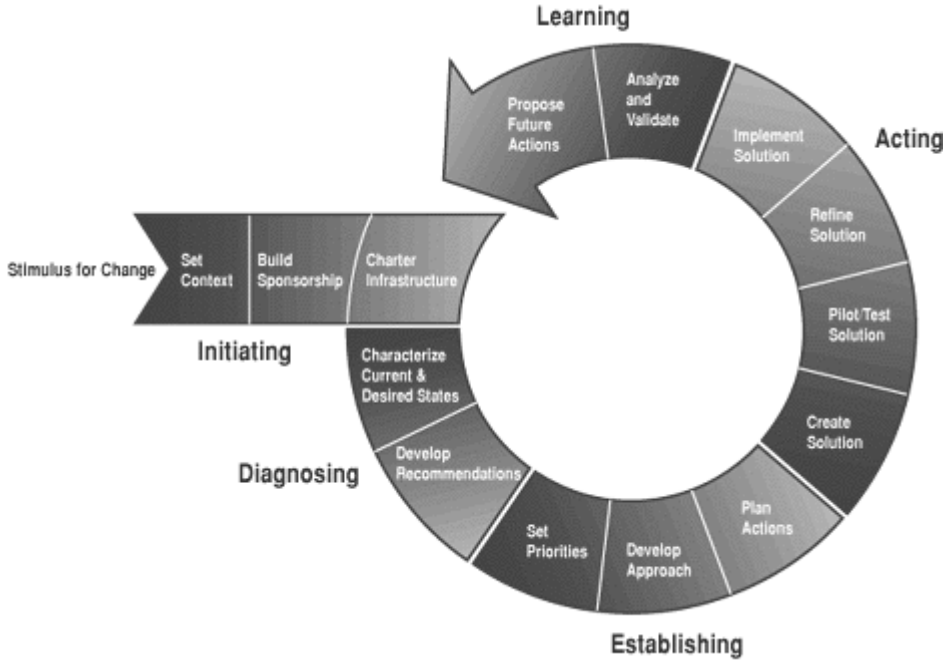
- 安全工程如何在机构中实施
- 用何种生命周期模型作为过程框架
- 机构中的组织结构如何对项目提供支持
- 如何处理支撑功能
- 机构中管理者、实施者的角色如何发挥作用
- 待改进的过程对于机构的成功起着怎样关键作用



行动阶段（续）

该阶段需要充分的时间和资源支持

- 创建解决方案
- 试验/测试解决方案
- 优化解决方案
- 实施解决方案

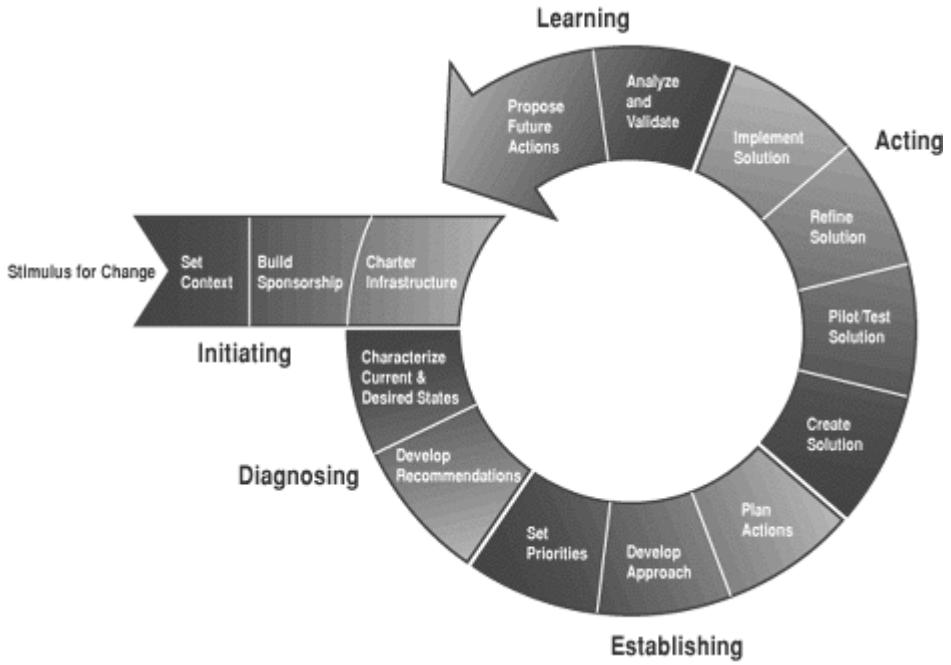


学习阶段

该阶段既是一次过程改进工作的终结

也为下一次的过程改进提供了出发点

- 分析与验证
- 提出未来行动



主要内容

- **SSE-CMM的应用**
  - 理解SSE-CMM的应用
  - 应用于过程改进
  - 应用于能力评定
  - 应用于获得保证

SSE-CMM评定与SE-CMM评定

- SSE-CMM的开发是基于如下考虑的，即安全性通常在系统工程相关环境（如大的系统集成者）中实施。它也认识到安全工程服务提供者可以将安全工程作为独立的活动来实施，该活动与一个独立的系统或软件（或其它）工程活动协调。得出下述评定大纲：
  - 系统工程能力评定后，SSE-CMM评定可集中于组织的安全工程过程。
  - 通过与系统工程能力评定的结合，SSE-CMM评定可裁剪以适合于与SE-CMM的集成。
  - 当执行独立的系统工程能力评定时，SSE-CMM的评定应从高于安全性的角度，考虑是否存在支持安全工程过程的项目和组织基础。

SSE-CMM的评定方法SSAM

- 开发SSAM旨在为系统安全工程界提供一种公开可理解的办法，供准备实施和正在实施SSE-CMM评定之用
- SSAM可用于评价产品开发者、服务提供者、系统集成者、系统管理者和安全专家，根据在SSE-CMM中详述的标准获得实际实施的基线或基准的过程
- 尽管SSAM的基本概念适用于其它评定，但它是专为支持SSE-CMM而设计的
- SSAM包含了为实现对组织机构的系统安全工程过程能力和成熟度的评定所需的信息和方向

SSAM的目的

SSAM是组织层面或项目层面的评定方法。该方法从待评机构或项目中，获取过程实施方面的信息，目的为：

- 收集组织或项目内与安全工程相关现行实施的基线或基准。
- 创建或支持组织结构的多层次改进动力

SSAM的特点

- SSAM写成了方便由第三方实施的评定，但也包含对自评文档解释的指南
- SSAM可被剪裁以适用于组织或项目需要。SSAM描述文档中提供了一些剪裁方面的指南
- SSAM采用多重数据收集方法
  - 直接反映模型的内容问卷。
  - 一系列有组织或随机的与涉及过程实施的关键人员(具有安全工程活动执行责任的人员)的会谈。
  - 审阅生成的安全工程的证据。

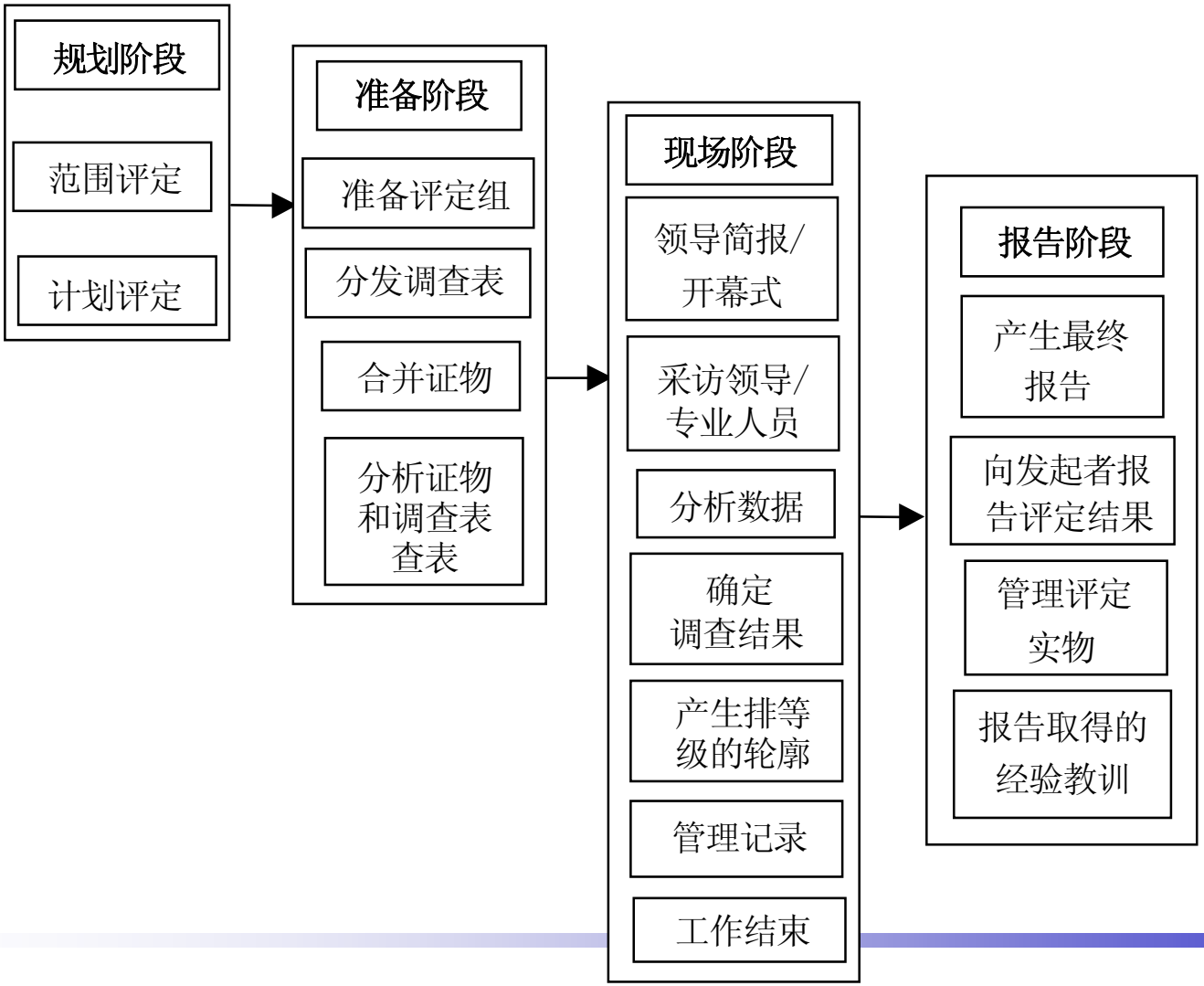
SSAM的适用范围

- 安全工程可在任何工程环境下实施，尤其是系统，软件，和通信工程等环境。SSAM也适用于所有环境
- 确定机构安全工程实施环境是评估一个机构安全工程能力的第一步
  - 哪个过程区适用于这个机构?
  - 怎样解释过程域（如开发相对于运行环境）
  - 哪个人员需要参与评定

SSAM评定方法的四个阶段

- 规划：为评定实施建立框架及为现场阶段做后勤准备。
- 准备：为现场活动准备评定小组及通过调查表实施数据的初步采集和分析。
- 现场：探索初步数据分析结果，进一步收集评定数据，以及为被评实体的专业人员提供参与数据采集和证实的过程的机会，最后完成划级工作并形成初步评定结果。
- 后期评定：小组实施对在此前三个阶段中采集到的所有数据的最终分析，形成最终的评定报告，并将调查结果呈送发起者。

SSAM评定方法的四个阶段



SSAM评定的二个方面

- 基本实施
- 通用实施

SSAM评定中过程域的序列

- 在整个项目生命周期中，许多过程域将多次被使用。当需要把一个过程域的目标结合到项目或机构的过程中时，就实施而言过程域应视为一个源。在评定中，SSE-CMM不是一个过程序列。真正的序列应根据机构或项目所选择的生命周期和其它业务参数决定。

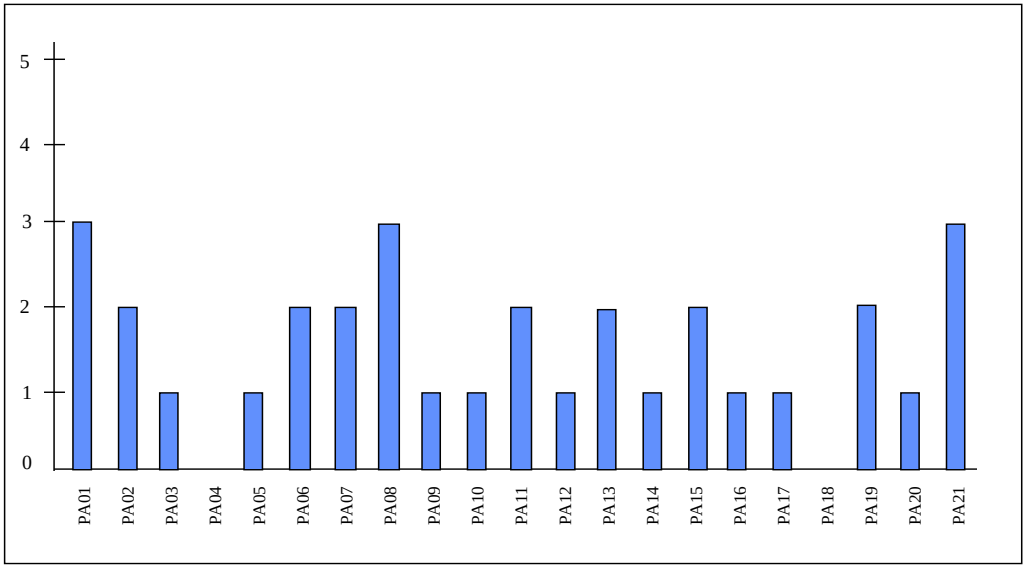
SSAM的主要工作成果

- SSAM的主要工作成果是调查结果简报和评定报告。
- 调查结果简报包括**评分轮廓**和**调查结果**表，评分轮廓表明机构每一个PA的能力等级，调查结果说明被评机构的强项和弱项。通常它是为发起者而开发的，但是在发起者的要求下也可交给被评定的组织机构。
- 评定报告只写给发起者，其中包括有关每个调查结果的附加细节以及发起者所需的调查结果暗示的问题。此外，应按照发起者的要求分发最终报告。

评分轮廓和调查结果

– 评分轮廓的形式

- 饼图
- 柱形图
- 表格



– 调查结果是评定的关键成果，它们是综合在整个现场阶段所收集的所有数据和对调查表的回答的结果。调查结果通常限于大约七个，以突出最重要的评定调查结果。

主要内容

■ SSE-CMM的应用

- 理解SSE-CMM的应用
- 应用于过程改进
- 应用于能力评定
- 应用于获得保证

SE-CMM项目的保证目标

- 对于将顾客安全需求转化为安全工程过程的途经来说，提供一个测量和改进的方法，以有效的生产出满足顾客要求的产品。
- 为不需要正式安全保证的顾客提供了一个可变化的保证，正式安全保证一般通过全面的评价、认证和认可活动来实现。
- 为使顾客获得其安全要求已被充分满足的信心提供一个参考标准。

过程证据的角色

- 机构的SSE-CMM表示产品或系统的生命周期遵循特定的过程。这种“过程证据”可被用于证明产品的可信度
- 但这种过程证据只能作为支持性的和间接的角色
- 但是，过程证据可用作为广泛和多样论据，因而其重要性不可低估。
- 进一步，一些传统形式的证据和这些证据支持的声明之间的关系也并非如其所说的那样有力。关键在于为产品和系统建立一个综合的证据集，以确信为什么这些产品和系统是充分可信的。