

# TRUSTIE

## 国家软件资源共享与协同生产环境 软件资源可信分级规范介绍

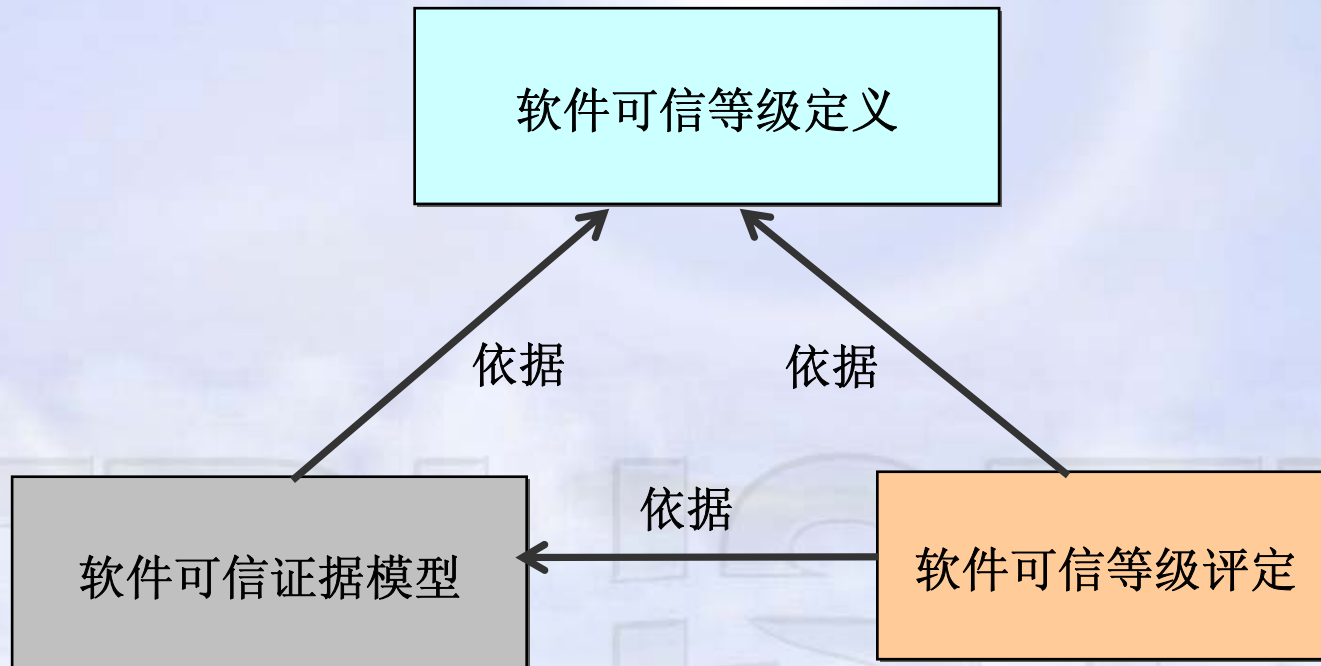
北京航空航天大学

2009年1月16日

- 软件可信分级规范目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

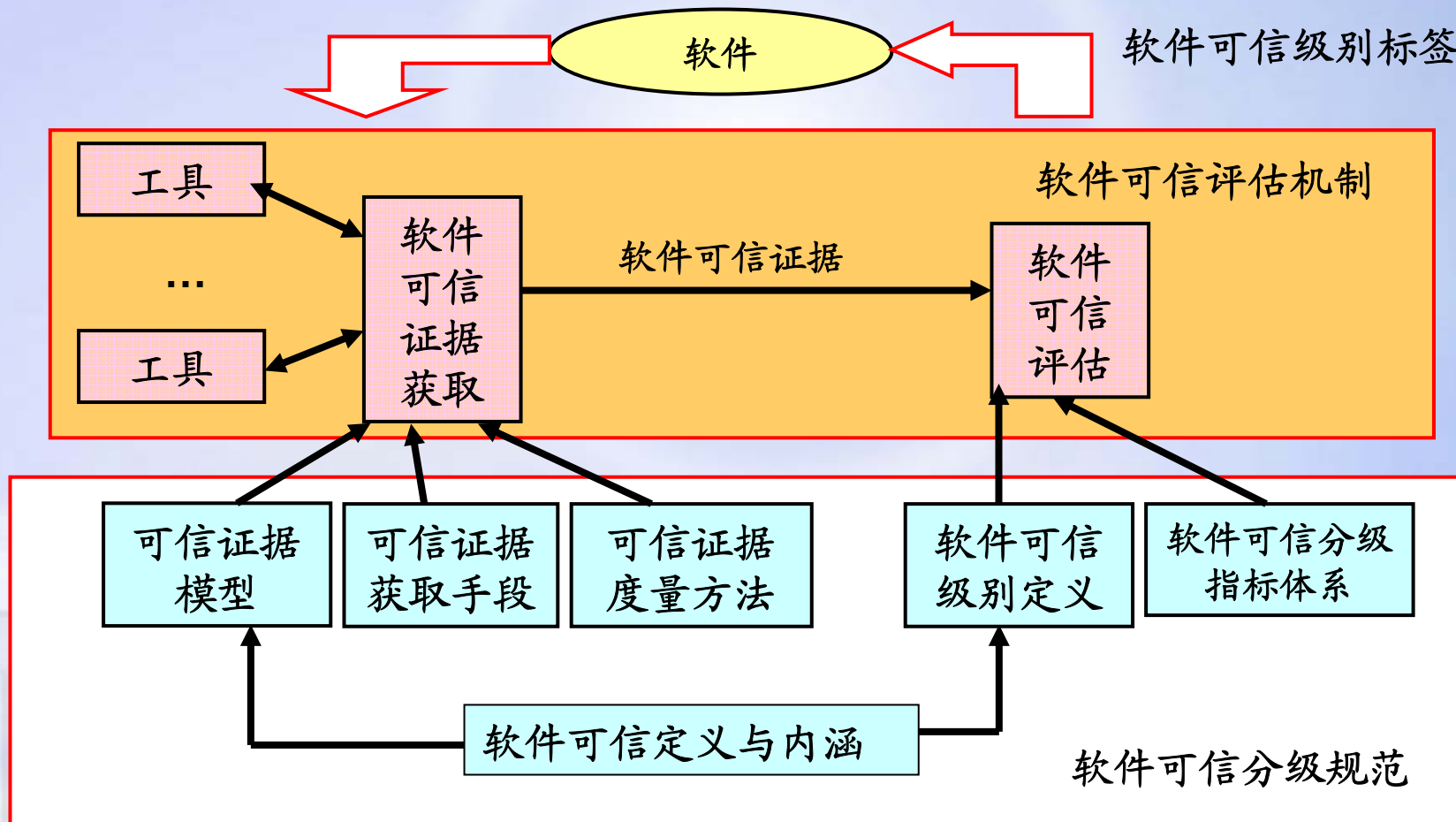
# 软件可信分级规范的目标

- 可信规范目标：对软件可信评估中的基本概念、模型、机制进行明确规定，为软件可信评估机制的建立提供依据和指导。



软件可信评估证据模型（王怀民教授提出）

# 软件可信评估中的基本概念、模型、机制



- 本规范规定了用于评估软件可信性的软件可信属性模型、软件的可信等级定义、软件可信分级方法、软件可信属性的度量方法，以及软件可信分级评估的基本方法。
- 本规范适用于软件制品的可信分级，也适用于有需要的组织和个体对目标软件进行可信评估和改进。

- 广泛调研（2008.1-2008.3）
- 确定软件可信概念与内涵，初步确定软件可信分级定义（2008.3）
- 确定软件可信证据参考模型（2008.6）
- 确定层次化的可信规范框架，基本确定可信分级规范由可信分级总论、可信证据模型以及可信评估等三部分组成（2008.10）
- 基本确定软件可信证据框架规范草案（2008.12）
- 提出软件可信分级参考规范V1.0及软件可信证据框架规范草案（2009.1）

## 软件可信分级规范的内容摘要

- 本规范围绕软件资源可信评估问题，从软件可信等级定义、软件可信证据框架以及软件可信分级评估三个方面，描述了软件可信的内涵（定义）、可信属性模型、可信证据模型、软件可信等级定义和软件可信分级评估机制等，为软件可信评估奠定了基础，为软件可信评估机制的建立提供了指导。



## 软件可信分级规范引用和参考

- ISO/IEC 9126 Software engineering – Product quality
- ISO/IEC 14598-1:1999 Information technology—  
Software product evaluation-Part 1: Grneral overview
- 美国国防部，《可信计算机系统评估准则》，TCSEC
- GB17859 计算机信息系统安全保护等级划分准则
- ISO/IEC15408，《信息技术安全评估通用准则》

TRUSTIE

- 软件可信分级规范的目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

## 软件可信分级相关概念——软件可信与软件可信性

- **软件可信**：如果一个软件系统的**行为总是与预期相一致**，则可称之为可信。
- **软件可信性**：软件**按用户期望**提供安全可靠服务的**能力**。
- **软件可信属性**：描述和刻画软件可信性的若干**软件关键性质**。

TRUSTIE

## 软件可信分级相关概念——软件可信等级与证据

- **软件可信等级（软件可信级别）**：以0-n个若干连续等级的形式对软件可信性进行的标度。等级越高，表明软件可信性越高。
- **软件可信证据**：软件所具有的能够反映软件某种可信属性的数据。

TRUSTIE

## 软件可信分级相关概念——软件可信评估

- **软件可信分级指标体系**：定义了每个可信等级应该具有的软件可信证据和可信证据的度量值。
- **软件可信分级评估**：依据特定的已成文的软件可信评估准则，确定特定的软件模块、软件包或软件产品是否达到某一特定可信等级的活动，称为软件可信分级评估，简称为软件可信评估。

## 软件可信分级相关概念定义参考

- **Trusted**（可信计算组织TCG提出）
- **Trustworthy Computing**（微软提出）
- **High Confidence**（美国信息与通信委员会CIC提出）
- **Dependability**（A.Avizienis 教授等人）
- **高可信**（High Confidence，陈火旺）
- 闵应骅，梅宏，王怀民，吕建

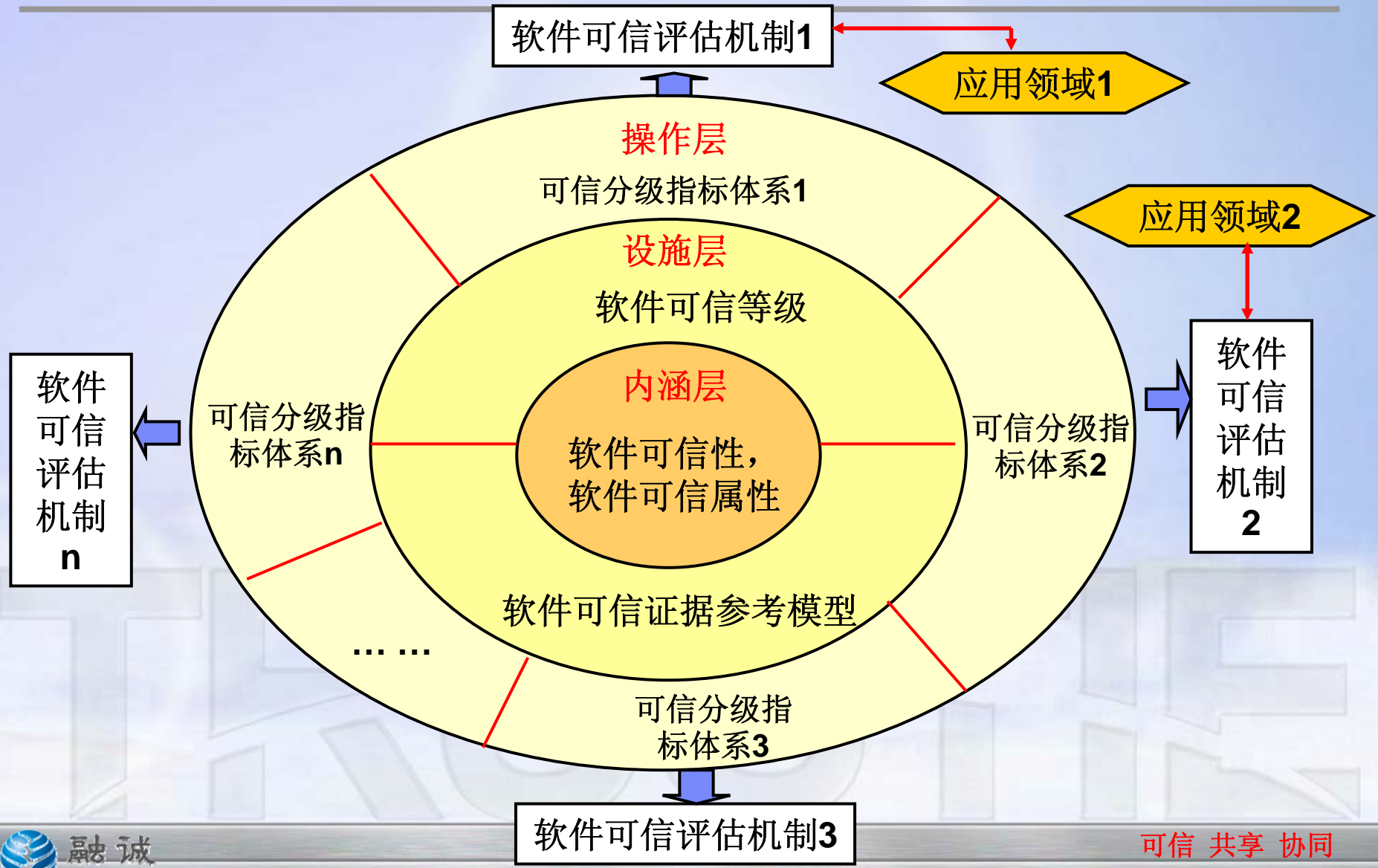
TRUSTIE

- 软件可信分级规范的目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

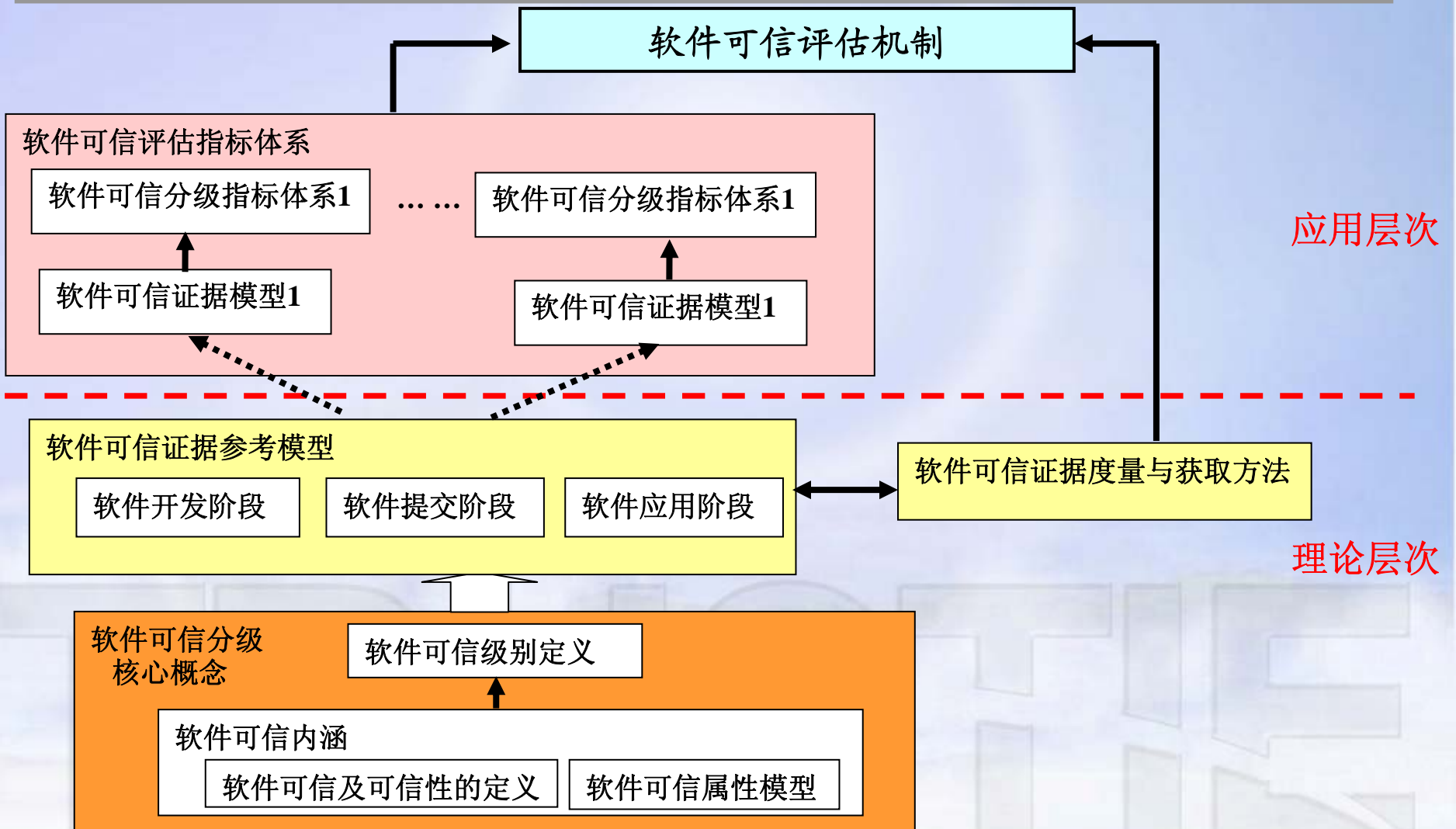
## 软件可信规范框架建设思想

- 不同应用领域的软件，用户所关注的可信属性以及关注的程度都存在很大差异，很难给出一种适用于所有软件的统一的可信分级指标体系
- 用户对可信内涵的理解是基本一致的
- 将与软件类型无关的可信概念与模型抽象为规范的理论基础，在此基础上建立多种面向不同类型软件的可信分级指标体系，建立层次化的可信规范框架

# 软件可信规范框架层次结构



# 软件可信规范体系结构

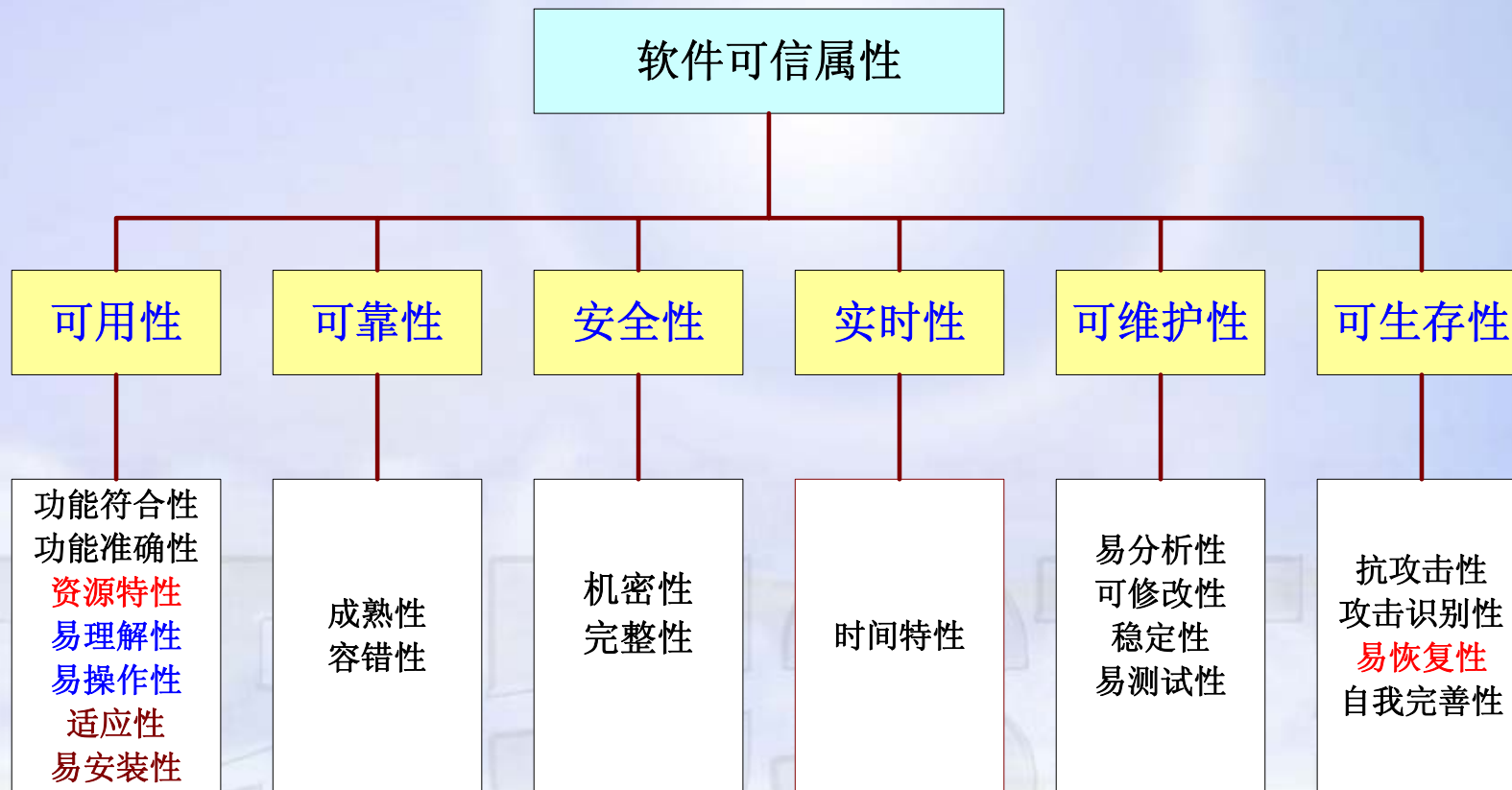


应用层次

理论层次

- 软件可信分级规范的目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

■ 软件可信属性模型是描述软件可信性的关键软件性质的集合



- **可用性（Availability）**：软件产品持续提供满足明确和隐含需求的功能的能力，以及软件产品被理解、学习、使用和移植的能力。
  - ◆ **功能符合性**：软件产品为指定的任务和用户目标提供一组合适的功能的能力。
  - ◆ **功能准确性**：软件产品提供具有所需精确度的正确或相符的结果及效果的能力。
  - ◆ **易理解性**：软件产品能够使用户理解软件是否满足要求，使用户知道在特定背景下如何使用软件，以及使用的条件。
  - ◆ **易操作性**：软件产品使用户能操作和控制它的能力。
  - ◆ **适应性**：软件产品无需采用特殊手段就可能适应不同的指定环境的能力。
  - ◆ **易安装性**：软件产品在指定环境中被安装的容易程度。

- **可靠性（Reliability）**：在规定的环境下、规定的时间内软件无失效运行的能力。
  - ◆ **成熟性**：软件本身存在的故障而导致的软件失效的可能程度。
  - ◆ **容错性**：在软件出现故障或者违反指定接口的情况下，软件产品维持规定的性能级别的能力。

TRUSTIE

## 软件可信属性模型——安全性与实时性

- **安全性（Security）**：软件系统对数据和信息提供保密性、完整性、可用性、真实性保障的能力
  - ◆ 机密性：软件系统中的信息不被非法用户所获取
  - ◆ 完整性：软件系统中的信息不被非法篡改
- **实时性（Real time）**：软件在指定的时间内完成反应或提交输出的能力

- **可维护性（ Maintainability ）**：软件产品可被修改的能力。修改可能包括修正、改进或软件适应环境、需求和功能规格说明所做的变化。
  - ◆ **易诊断性**：软件产品诊断软件中的缺陷或失效原因以及标识待修改部分的能力。
  - ◆ **可修改性**：软件产品使指定的修改可以被实现的能力。
  - ◆ **稳定性**：软件产品避免由于软件修改而造成意外结果的能力。
  - ◆ **易测试性**：软件产品使已修改部分能被确认的能力。

- **可生存性（Survivability）**：软件在受到攻击或失效出现时连续提供服务并在规定时间内恢复所有服务的能力。
  - ◆ **抗攻击性**：软件抵抗攻击的能力。
  - ◆ **攻击识别能力**：软件探测已经发生的入侵并评估其危害程度的能力。
  - ◆ **恢复性**：软件在被攻击后，恢复服务的能力。
  - ◆ **自我完善性**：针对从干扰及攻击中获得的信息来改进系统生存性的策略，从整体上增强系统的可生存性的能力。

- Avizienis 2000年提出的可信性（dependability）的概念框架
- 陈火旺院士提出的高可信性质概念与内涵
- 国标《软件工程 产品质量 第1部分：质量模型》（GB/T 16260-2006）提出的软件质量模型

- 软件可信分级规范的目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

- 软件可信等级是对软件可信性的标度。
- 软件可信等级划分的重要依据是软件对用户所期望的可信属性的满足程度。
- 软件可信等级：0级，1级，2级，3级，4级，5级
- 软件可信等级之间的关系：
  - ◆ 等级越高，表明软件可信性越高
  - ◆ 可信等级为*i*的软件满足0~*i-1*各可信等级的定义，即  
0级可信软件  $\supset$  1级可信软件  $\supset$  ...  $\supset$  5级可信软件

# 软件可信等级定义

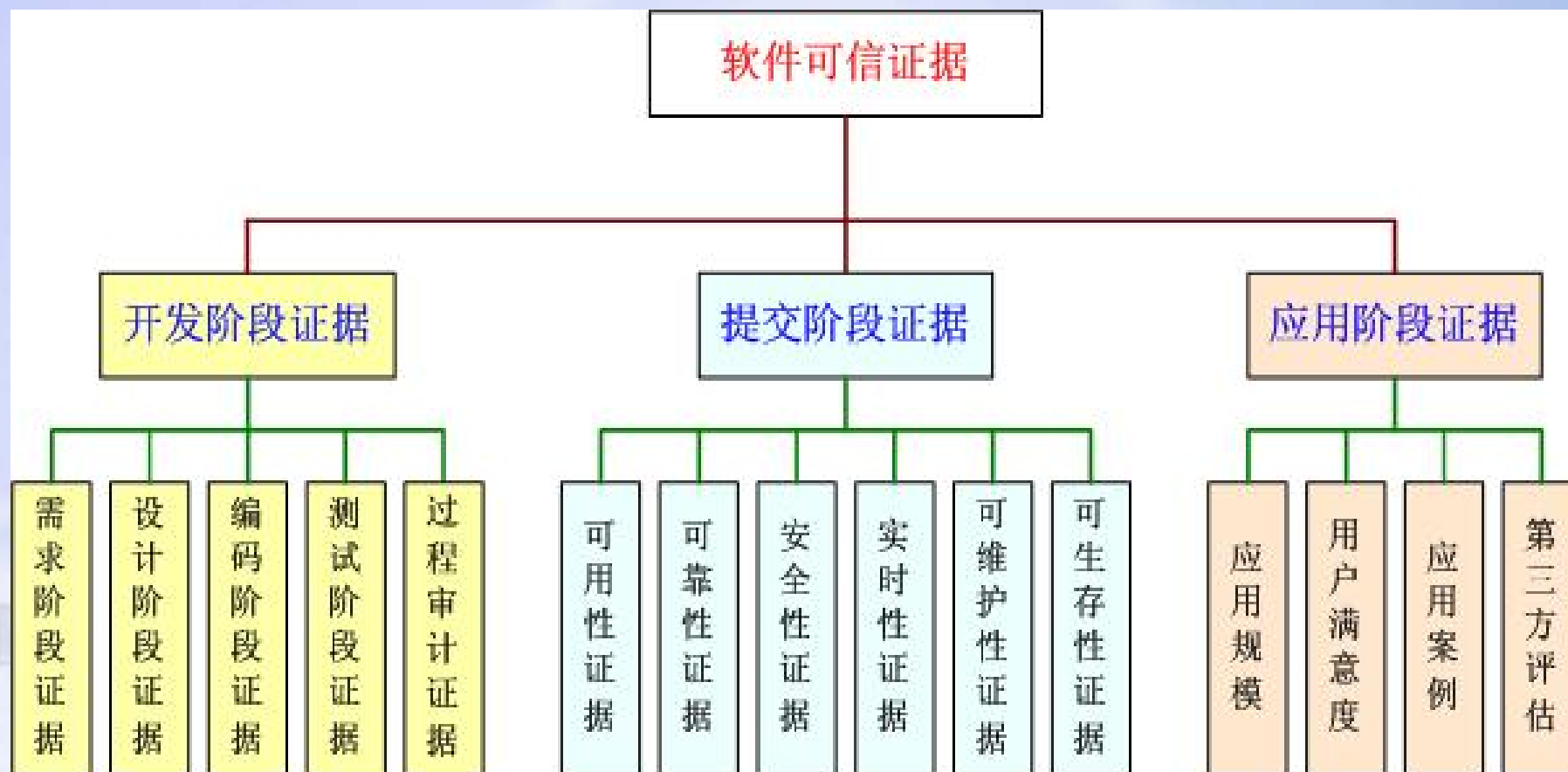
可信级别	定义
软件制品 <b>0级 未知级</b>	未获得关于软件可信性的任何证据，不能判定软件是否能满足用户对该类别软件可信属性的期望。
软件制品 <b>1级 可用级</b>	软件实体可访问，并且能按照软件提供者指定的模式正常运行，隐含表明该软件能满足用户对该类别软件可信属性的 <b>基本期望</b> 。
软件制品 <b>2级 验证级</b>	在可用级的基础上，软件提供者依据特定的已成文的软件可信属性发布规范 <b>发布软件可信属性可确认的声明</b> ，表明该软件能满足用户对该类别软件可信属性的 <b>普遍期望</b> ，且用户期望的可信属性均得到了确认。
软件制品 <b>3级 实用级</b>	在验证级的基础上，软件已在相关应用领域得到应用，并且有 <b>可证实的成功应用案例</b> ，隐含表明该软件能满足用户对该类别软件可信属性的 <b>普遍期望</b> ，且得到 <b>实际应用的证实</b> 。
软件制品 <b>4级 评估级</b>	在实用级的基础上，软件的可信性 <b>通过了权威软件可信分级评估机构依据特定的已成文的可信分级评估规范进行的评估</b> ，表明该软件能满足用户对给类别软件可信属性的 <b>较高期望</b> ，且用户期望的可信属性均得到了权威机构的评估保证。
软件制品 <b>5级 证明级</b>	在评估级的基础上，所提交的 <b>软件可信性属性都是可被严格证明的</b> ，软件的可信等级定义为证明级。

- 软件可信分级规范的目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

## 软件可信证据参考模型构造方法

- 由软件所有可信证据的集合构成，是一种不特定于任何类型软件、通用的可信证据参考模型，对于建立特定的可信证据模型具有指导作用
- 从软件生命周期的三个阶段出发，定义软件可信评估的证据模型
  - ◆ 软件开发阶段 ---- 软件过程保障
  - ◆ 软件提交阶段 ---- 软件实体
  - ◆ 软件应用阶段 ---- 软件应用信誉

## 软件可信证据参考模型



## 软件可信证据参考模型——软件开发阶段证据

### ■ 关注如何通过规范化软件生产过程得到符合设定目标的软件实体，增强用户对实体符合期望的信心

- ◆ 需求阶段证据：需求规范描述方法；需求变更比率；需求评审结论等
- ◆ 设计阶段证据：设计阶段的需求变更数，设计评审结论，设计阶段的评审缺陷密度和缺陷清除率等
- ◆ 编码阶段证据：编码阶段的需求变更数，单元测试强度、代码规模、代码可维护性等
- ◆ 测试阶段证据：测试人员的能力等级、测试工具支持的有效性以及测试缺陷趋势等
- ◆ 过程审计证据：过程不合格项趋势等

## 软件可信证据参考模型——软件提交阶段证据

- 关注软件可信属性模型中的各个可信特性证据，是用户判断“实体是否符合期望”的主要依据
  - ◆ 软件可用性证据
  - ◆ 软件安全性证据
  - ◆ 软件可靠性证据
  - ◆ 软件可生存性证据
  - ◆ 软件实时性证据
  - ◆ 软件可维护性证据

## 软件可信证据参考模型——软件应用阶段的证据

- 关注软件应用广泛程度、用户的满意程度和第三方的评价等，是建立用户对软件实体信心的重要依据
  - ◆ 应用方面证据：主要指软件的应用范围是否广阔以及用户对软件的满意程度等。
  - ◆ 第三方评价：独立第三方对该软件的综合评价也将作为评估该软件可信性的重要证据。

TRUSTIE

## ■ 度量方法

- ◆ **原始度量**：基于软件系统测试或人工的数值结果；
- ◆ **分级度量**：采用相对模糊的描述（如有很多问题，有较多问题，有问题，略有问题，完全正确等），对被度量的属性值域进行分割，一个分割为一个等级，便于对原始度量数值进行分级。
- ◆ **证据影响因子**：如果证据的原始度量值的受到提供者信任度的影响，可将证据提供者的信任度作为**证据影响因子**。
- ◆ **度量方法**：参考ISO/IEC 14598-1:1999

## 可信证据度量示例

可信证据名称	值域	原始度量定义	分级度量定义
可用性	$0 \leq X \leq 1$	$X = cf * (1 - A/B)$ ( $0 \leq X \leq 1$ ) A=在评价中检测有问题的功能数 B=被评价的功能数 cf = 评测机构的影响因子(信任度)	5级: 功能完全正确 ( $X=1$ ) 4级: 功能略有问题 ( $0.85 \leq X < 1$ ) 3级: 功能有问题 ( $0.7 \leq X < 0.85$ ) 2级: 功能有较多问题 ( $0.5 \leq X < 0.7$ ) 1级: 功能有很多问题 ( $0 \leq X < 0.5$ )
准确性	$0 \leq X \leq 1$	$X = 1 - A$ ( $0 \leq X \leq 1$ ) A=软件产品没有提供所需精确度的功能数的比例	5级: 准确 ( $X=1$ ) 4级: 比较准确 ( $0.85 \leq X < 1$ ) 3级: 基本准确 ( $0.7 \leq X < 0.85$ ) 2级: 部分准确 ( $0.5 \leq X < 0.7$ ) 1级: 不准确 ( $0 \leq X < 0.5$ )
资源利用率	$0 \leq X \leq 1$ , 单位:	内存使用大小, CPU 使用率等	5级: 好 4级: 较好 3级: 中 2级: 较差 1级: 差
易理解性	$0 \leq X \leq 1$	$X = cf * (1 - A/B)$ ( $0 \leq X \leq 1$ ) A=不能被理解的功能(或功能的类型)数 B=功能(或功能的类型)总数 cf= 用户的影响因子(信	5级: 好 ( $X=1$ ) 4级: 较好 ( $0.85 \leq X < 1$ ) 3级: 中 ( $0.7 \leq X < 0.85$ ) 2级: 较差 ( $0.5 \leq X < 0.7$ ) 1级: 差 ( $0 \leq X < 0.5$ )

### ■ 证据获取手段

- ◆ 软件提供者提供
- ◆ 第三方或权威机构（分析、测试、评估）
- ◆ 用户反馈
- ◆ **QoS** 监控

TRUSTIE

## 可信证据获取方式示例

可信证据名称		可信证据获取阶段与手段		
		软件提交阶段		软件应用阶段
		软件测试与分析	QoS 监测	用户反馈
可用性	功能适合性	√		
	准确性	√		
	资源利用率	√		
	易理解性			√
	易操作性			√
	适应性			√
	易安装性			√
可靠性	成熟性	√		
	容错性	√		
安全性	机密性	√		
	完整性	√		
可生存性	抗攻击性	√		
	攻击识别能力	√		
	恢复性	√		
	自我完善能力	√		
	实时性	√	√	
可维护性	易诊断性	√		
	可改变性	√		
	稳定性	√		
	易测试性	√		

- 软件可信分级规范的目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

## 建立软件可信评估机制的基本方法

分析特定软件用户的期望



确定用户关注的可信属性



建立软件可信证据模型



建立软件可信分级指标体系



构造软件可信评估机制

- 评估者能够获取的证据类型与准确程度受限于环境因素和技术上的可操作性，因此评估机制中可信证据可能有多种形态。
  - ◆ 特定的可信证据模型可能是可信证据参考模型的字集
  - ◆ 一些实际可获取的证据数据与可信证据参考模型是间接对应关系

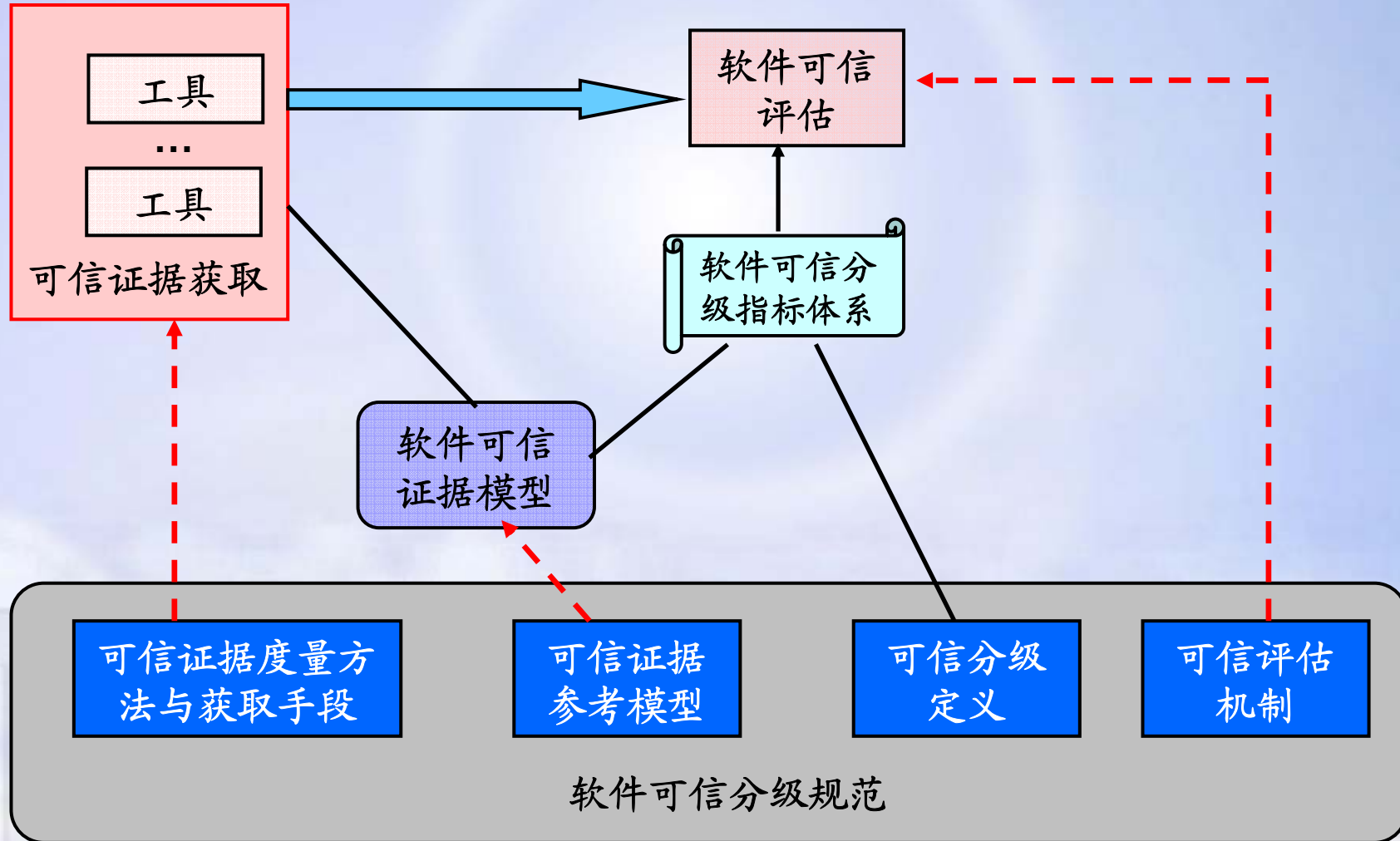
TRUSTIE

- 软件可信分级应该是具有动态性，即随着软件自身可信特性的提高/降低、软件可信证据的增加/减少或增强/减弱，软件的可信级别也随着动态变化

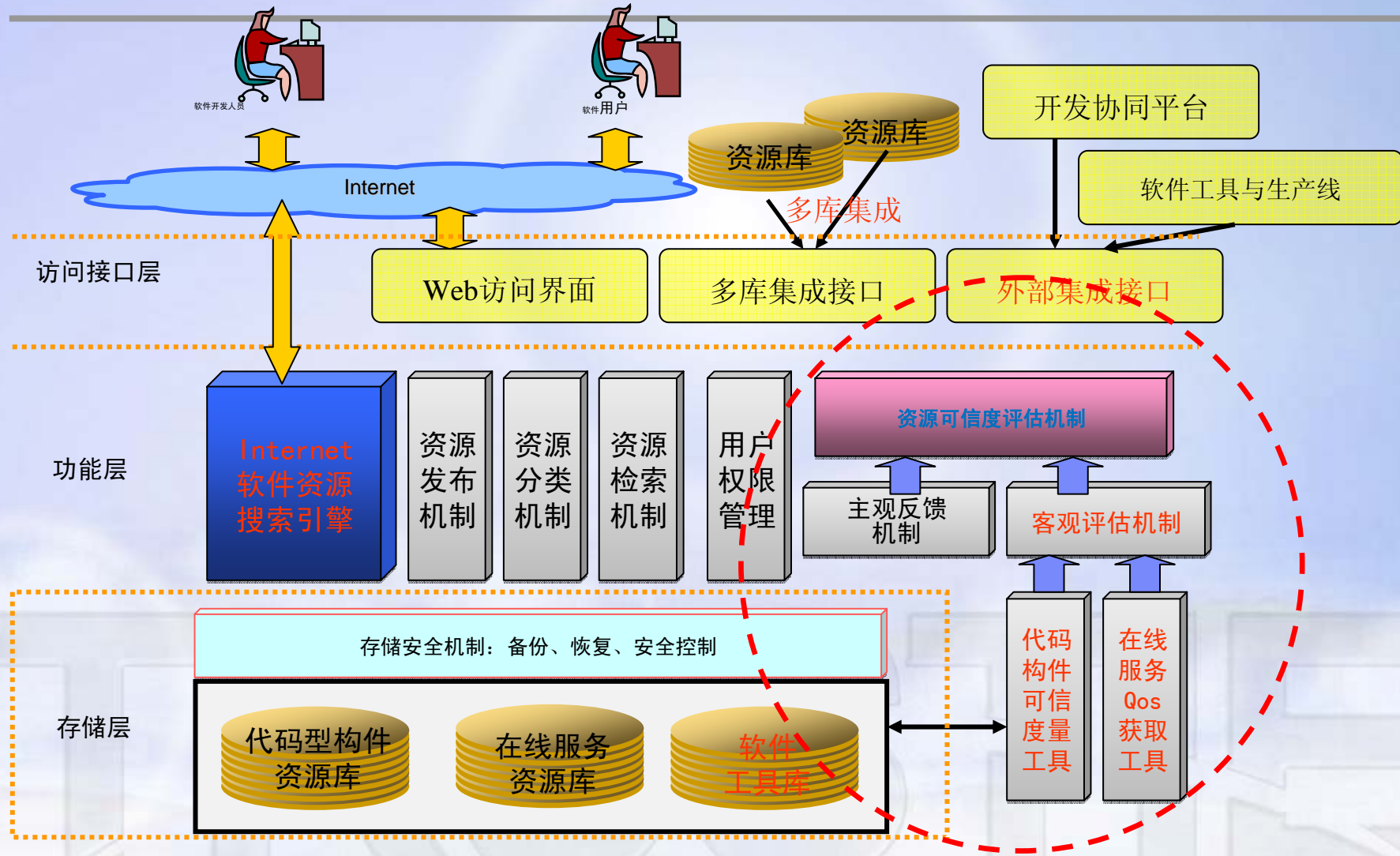
TRUSTIE

- 软件可信分级规范的目标与范围
- 软件可信分级规范的主要内容
  - ◆ 软件可信分级相关概念
  - ◆ 软件可信规范基本框架
  - ◆ 软件可信属性模型
  - ◆ 软件可信分级定义
  - ◆ 可信证据参考模型
  - ◆ 软件可信评估机制
- 软件可信分级规范的执行方式

# 软件可信分级规范的作用



# 北大资源库软件可信分级机制



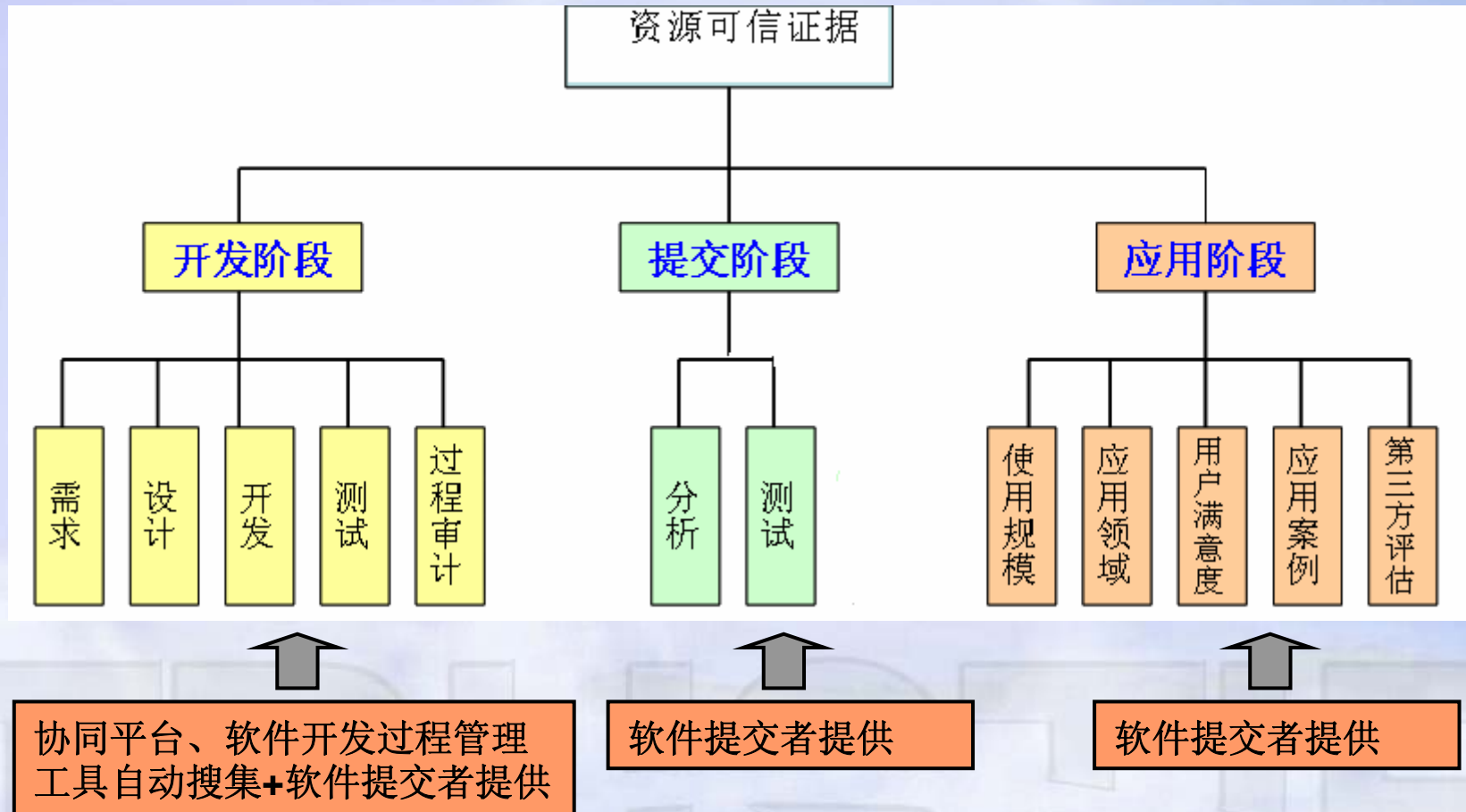
### ■ 资源可信证据特征

- ◆ 客观性：即证据是不以人们的意志为转移的客观存在的事实。这是证据的本质特征
- ◆ 关联性：或称相关性，是指证据和需要证明的质量软件可信性间有一定的关系或联系
- ◆ 可获得性：是指证据是可以依照确定的程序收集、审查、判断、获得和检验的

TRUSTIE



# 资源库中软件可信分级的证据框架及证据获取方式



满足用户期望可信属性集中最基本可信属性的指标要求。

	未知级	可用级	验证级	实用级	评估级	证明级
相关领域已使用		√	√	√	√	√
可信属性可验证			√	√	√	√
成功应用案例				√	√	√
通过权威机构可信评估					√	√
可信属性可证明						√

## 软件可信分级指标体系

基本满足用户期望可信属性集的要求。

	未知级	可用级	验证级	实用级	评估级	证明级
相关领域已使用		√	√	√	√	√
可信属性可验证			√	√	√	√
成功应用案例				√	√	√
通过权威机构可信评估					√	√
可信属性可证明						√

## 软件可信分级指标体系

对于用户期望可信属性集经过自主验证和分析。比较好地满足用户期望。

	未知级	可用级	验证级	实用级	评估级	证明级
相关领域已使用		√	√	√	√	√
可信属性可验证			√	√	√	√
成功应用案例				√	√	√
通过权威机构可信评估					√	√
可信属性可证明						√

# 软件可信分级指标体系

	未知级	可用级	验证级	实用级	评估级	证明级
相关领域已使用		√	√		√	√
可信属性可验证			√		√	√
成功应用案例					√	√
通过权威机构可信评估					√	√
可信属性可证明						√

用户期望可信属性集经过自主验证分析，并经过独立权威验证分析机构的验证与分析。很好地满足用户期望。

# 软件可信分级指标体系

	未知级	可用级	验证级	实用级	评估级	证明级
相关领域已使用		√	√	√	√	√
可信属性可验证			√	√	√	√
成功应用案例				√	√	√
通过权威机构可信评估					√	√
可信属性可证明						√

对于用户期望可信属性集经过自主验证分析，经过独立权威验证分析机构的验证与分析，并且经过证明与验证。完全满足用户期望。



融诚  
Trustie

谢谢!

TRUSTIE



融诚  
Trustie

可信 共享 协同