第四讲.可信软件体系与评价

高可信软件工程

授课安排

- 可信软件评价指标体系建立
- 可信软件过程和可信软件产品相关性研究
- 软件过程可信评价模型研究
- 软件可信度评价模型研究

可信软件评价指标体系建立

可信软件评价指标体系建立

- 问题描述
- 软件过程的可信属性及评价指标体系
- 软件产品的可信属性及评价指标体系

可信软件评价指标体系建立

问题描述

软件产品可信依赖于软件过程的可信，软件过程管理的不完善、不可信，使得软件产品在推出时就含有许多未知的缺陷。研究软件过程可信目的在于保证正确的开发过程输入可以产生正确的过程输出，即可信的软件产品。

软件评价指标体系建立原则

- 覆盖软件项目开发和应用的全过程
- 评价指标体系的完整性
- 易于收集和估算指标数据
- 注重可信过程和可信产品的有机结合

软件过程的可信属性及评价指标体系

- 三个视角研究可信属性
  - 从影响软件过程可信的内因与外因
  - 从过程的构成
  - 从过程的效果

- 两个方面研究可信属性
  - 从通用软件过程的可信性属性
  - 从特殊软件过程的可信性属性

软件过程的可信属性及评价指标体系

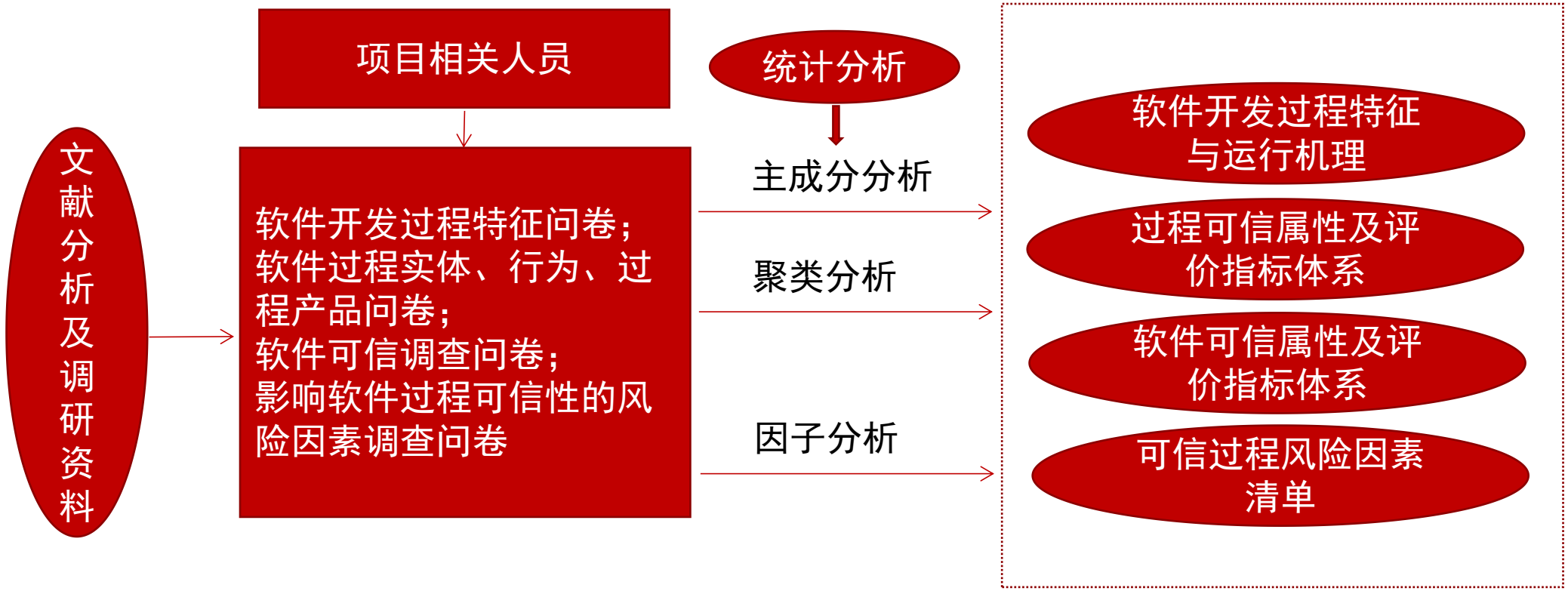
可信属性

子特性

指标体系映射关系

通过加强过程的方式来保障可信过程的开发

软件过程可信属性及评价指标体系建立



过程实体可信评价指标体系

- 过程实体
  - 负责执行的过程人员
  - 执行该软件过程的组织资产、过程管理方法、标准以及各类指南
  - 开发过程中所遵循的一系列规约
- 过程实体可信评价指标体系
  - 工具的集成化程度
  - 应用程序语言经验和工具经验
  - 组织资产可信度
  - 开发工具复杂度
  - 开发人员能力水平
  - 开发系统复杂度

过程行为可信评价指标体系

- 过程行为

过程实体在项目计划、监控、度量、审计、评估以及执行这个过程的行为方式

- 具体表现

项目开发各项任务执行过程（系统规划、需求分析、软件设计、编码、测试、验收与运行、维护与升级等）

过程行为可信评价指标体系

行为可信评价指标体系

- 各阶段缺陷密度
- 各阶段评审缺陷分类比率
- 缺陷注入率
- 各阶段评审缺陷平均关闭天数
- 各阶段遗留BUG密度
- 需求变更比率
- 各阶段工作产品规模偏差
- 各阶段BUG平均修改效率
- 任务报告遗漏率
- 个人报告遗漏率
- 阶段各类产品的生产率
- 过程成熟度水平

需求变更的频繁程度

- 需求变更比率=变更的需求数/需求总数×100%

缺陷注入率

- 缺陷注入率=总缺陷数/软件功能点数×100%

行为可信评价指标体系

□过程成熟度水平

CMMI将过程成熟度水平分为5个级别，共计22个过程域，对于每个过程域进行成熟度评分，即各个过程域的成熟度水平为

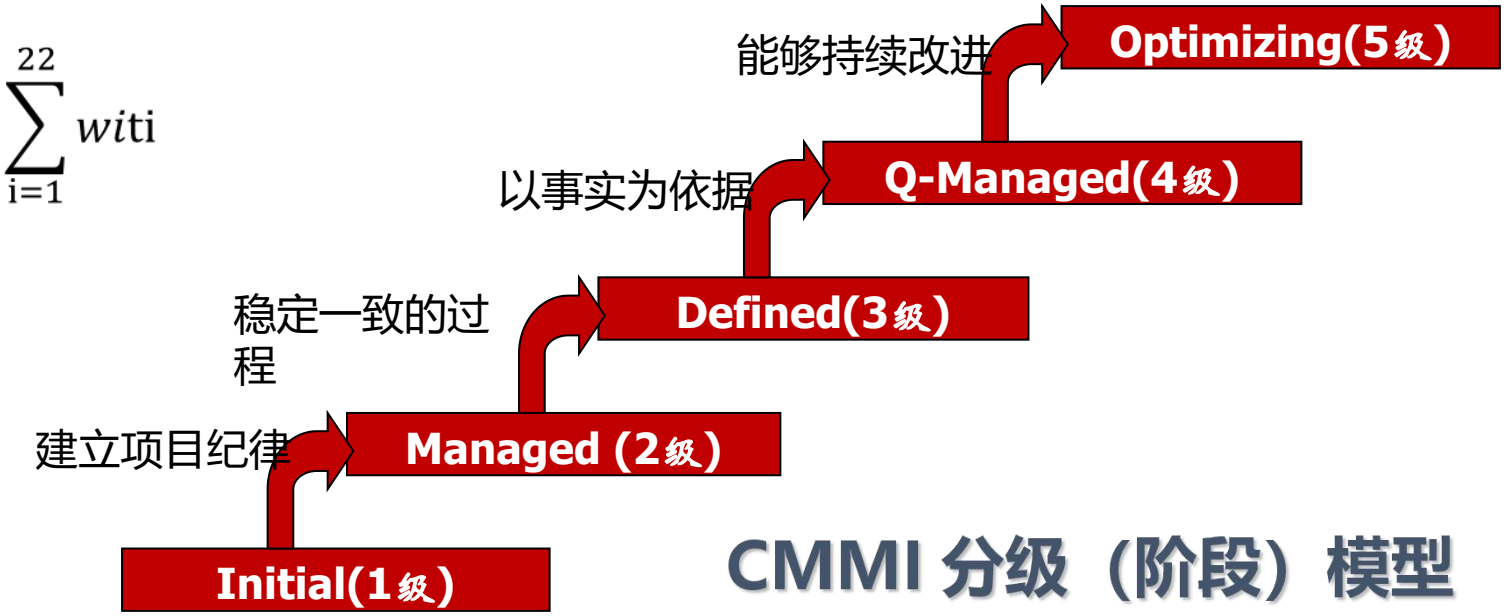
$ti \subseteq [0,1]$,i=1,2…,22

根据软件项目的特征以及有关要求，给出各个过程域相对于开发项目的权重（0~1）

$$\sum_{i=1}^{22} wi = 1, \qquad i = 1,2,\dots 22, \qquad wi \subseteq [0,1]$$

结合计算软件过程的成熟度水平为

$$T = \sum_{i=1}^{22} witi$$



CMMI 分级（阶段）模型

行为可信评价指标体系表示

时间有效率

$$Mp = \frac{\sum_{j=1}^{m} T_{Wj}}{\sum_{j=1}^{m} T_{Wj} + \sum_{j=1}^{m} T_{Bj}}$$

- T_{wj}为第j个软件开发人员在整个项目开发期间有效的工作时间
- T_{Bj}为第j个软件开发人员在整个项目开发期间的阻塞等待时间
- m为开发人员数量

进度偏差率

$$s = \left| \frac{S_s - S_j}{S_j} \right|$$

- S_s为项目的实际进度
- S_j为项目的计划进度

过程产品可信评价指标体系

- 过程产品

开发过程的阶段性产品，如软件需求说明书、软件设计报告、软件测试报告等

- 过程产品可信评价指标体系

各测试报告遗留BUG密度、过程遗留缺陷的比率、各测试报告BUG发现趋势、软件过程产品复杂度、各测试报告BUG分类比率、各测试报告BUG发现效率和产品规模偏差

过程产品可信评价指标体系的定义

产品规模偏差

过程产品规模偏差=（过程产品实际总规模-过程产品估计总规模）/过程产品规模总数×100%

软件过程产品复杂度

- 产品的文档页数
- 项目规模
- 功能或模块间耦合和内聚程度

过程遗留缺陷的比率

过程遗留缺陷的比率=遗留BUG总数/过程产品规模

成本有效率

$$M''_P = \frac{\sum_{j=1}^{n}(C_{wj} + \sum_{i=1}^{m} T_{wij} C_i)}{\sum_{j=1}^{n}(C_{wj} + \sum_{i=1}^{m} T_{wij} C_i) + \sum_{j=1}^{n}(C_{bj} + \sum_{i=1}^{m} T_{bij} C_i)}$$

- T_{wij}为第i个软件开发人员在第j个过程片段的有效工作时间
- T_{bij}为第i个软件开发人员在第j个过程步的阻塞等待时间
- n为过程片段数目
- m为开发人员数量
- C_i是第i个开发人员的单位时间成本
- C_{wj}在第j个过程片段的除人员费用外发生的其他一切有效费用
- C_{bj}在第j个过程片段的除人员无效费用外发生的其他一切无效费用

成本偏差率

$$c = \left| \frac{C_s - C_j}{C_j} \right|$$

- C_s为项目的实际成本
- C_j为项目的计划成本

软件过程可信性属性及评价指标体系

序号	属性分类	过程可信属性	评价指标体系	指标类型
1	客观属性	行为可信ξ_1	需求变更的频繁程度 x_{11}	成本型指标
			缺陷注入率 x_{12}	成本型指标
			过程成熟度水平 x_{13}	效益型指标
		产品可信ξ_2	产品规模偏差 x_{21}	成本型指标
			软件过程产品复杂度 x_{22}	成本型指标
			过程遗留缺陷的比率 x_{23}	成本型指标
		实体可信ξ_3	工具的集成化程度 x_{31}	效益型指标
			组织资产可信度 x_{32}	效益型指标
			开发人员能力水平 x_{33}	效益型指标
2	主观属性	进度可信$\xi4$	进度偏差率 x_{41}	成本型指标
			时间有效率 x_{42}	效益型指标
		成本可信ξ_5	成本偏差率 x_{51}	成本型指标
			成本有效率 x_{52}	效益型指标

软件产品可信性属性及评价指标体系

软件产品可信性属性

正确性、可靠性、安全性、完整性、可用性

软件质量（ISO/IEC 9126）

- 6个质量特性

功能性、可靠性、易使用性、效率、可维护性、可移植性

- 21个质量子特性

功能性:适合性、准确性、互操作性、依从性、安全性;
可靠性:成熟性、容错性、易恢复性;
易使用性:易理解性、易学性、易操作性;
效率:时间特性、资源特性;
可维护性:易分析性、易更改性、稳定性、易测试性;
可移植性:适应性、易安装性、一致性、易替换性。

软件产品可信性属性及评价指标体系

综合软件功能性和非功能性，定义可信属性为：保密安全性、生存性、容错性、可靠性和防危性

- 保密安全性

软件对于产生信息不会泄露的属性

- 生存性

软件受到攻击时连续提供服务并在规定时间恢复所有服务的能力

- 容错性

软件在故障出现时保障提供服务的能力

- 可靠性

从一个系统能够正常工作时间长短来描述系统的可靠性

- 防危性

软件系统能否防止关键系统发生重大灾难性事故能力

软件产品可信性评价指标体系

序号	软件产品可信属性	软件产品可信评价指标	指标类型
1	保密安全性 η_1	信息保密性 y_{11}	效益型指标
		信息完整性 y_{12}	效益型指标
2	生存性 η_2	软件防止危害漏洞能力 y_{21}	成本型指标
		软件抗攻击能力 y_{22}	效益型指标
3	容错性 η_3	并发处理控制能力 y_{31}	效益型指标
		程序错误可修正性 y_{32}	效益型指标
		非法输入数据的容错能力 y_{33}	效益型指标
		非法组合的容错能力 y_{34}	效益型指标
		输出数据合理的容错能力 y_{35}	效益型指标
4	可靠性 η_4	平均失效时间比率 y_{41}	成本型指标
		平均修复时间比率 y_{42}	效益型指标
		平均故障间隔时间比率 y_{43}	效益型指标
5	防危性 η_5	非安全失效的平均时间比率 y_{51}	成本型指标
		非安全失效的平均间隔时间比率 y_{52}	效益型指标

可信软件过程与产品相关性研究

可信软件过程和可信软件产品相关性研究

根据软件可信属性和评价指标体系，建立软件过程可信和软件产品可信映射关系模型。详细分析软件可信影响因素，对于软件过程管理提供定量化的参考依据。

- 问题分析

过程可信与产品可信关系评价是多目标多因素的系统评价问题。

- 指标多
- 各因素间关系复杂

为建立过程可信与产品可信映射关系，需要处理多原因多结果之间的复杂因果关系，结构方程模型适合解决此类问题。

结构方程模型

结构方程模型简介

- 什么是结构方程模型
- 结构方程模型的优点
- 结构方程模型常用图标
- 结构方程模型中的变量
- 结构方程模型的结构
- 结构方程模型实例

结构方程模型

□结构方程模型

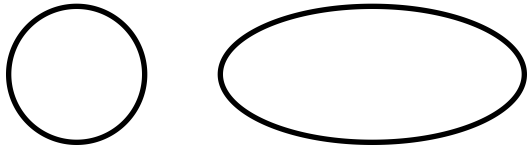
结构方程模型（ Structural Equation Model）是基于变量的协方差矩阵来分析变量之间关系的一种统计方法。所以，有时候也叫协方差结构分析。

该方法在20世纪80年代就已经成熟，可惜国内了解的人并不多。“在社会科学以及经济、市场、管理等研究领域，有时需处理多个原因、多个结果的关系，或者会碰到不可直接观测的变量（即潜变量），这些都是传统的统计方法不能很好解决的问题。**20世纪80年代以来，结构方程模型迅速发展，弥补了传统统计方法的不足，成为多元数据分析的重要工具。**

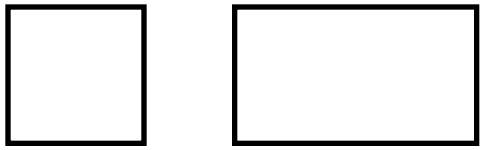
结构方程模型是**基于因子分析和线性回归分析方法，检验因果关系的多元统计分析模型**。分为结构模型和测量模型两种。结构模型反应潜变量之间的结构关系，也称潜变量模型或因果模型，测量模型描述潜变量、显变量和观测变量之间的关系。

结构方程模型常用于：**验证性因子分析、高阶因子分析、路径及因果分析**、多时段(multiwave)设计、单形模型(Simple Model)、及多组比较等 。

结构方程模型图标及含义



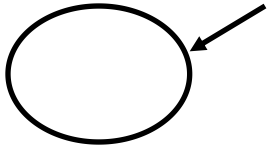
潜变量因子



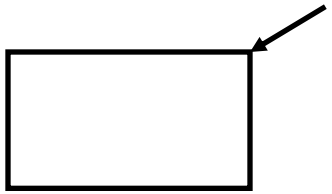
观测变量或指标

单向影响或效应

相关



内生潜变量未被解释的部分



测量误差

结构方程模型变量

潜变量 显变量	变量 指标
内生变量 外生变量	自变量 因变量

结构方程模型变量

根据变量能否被直接测量而将其分为潜变量和显变量：

- 变量：具有多个值的概念。
- 指标：测量某个变量的项目（item）,或者叫条目。

- 潜变量：不可以直接观察的变量，或叫因子。
  - 潜在变量是用理论或假设来建立的、无法直接测量的变量，如智力、性格等，不过它也可以用观测变量来构建。
- 显变量：也称为“观测变量”和“指标变量”，指可以直接观察的变量。
  - 显变量是可以直接被测量的变量，如年龄、文化程度、身高、体重等。

结构方程模型变量

从相互关系上分为**外生变量（自变量）和内生变量（因变量）**

- 自变量：仅有单向箭头指出的变量
- 因变量：只要有单向箭头指入的变量

- 内生变量：被影响的变量
  - 内生变量则是受其他变量影响而变化的变量。四种变量结合起来形成四类变量，即**内生观测变量**和**外生观测变量，内生潜变量**和**外生潜变量**
- 外生变量：作用于其它变量的变量
  - 外生变量是引起其他变量变化和自身变化，且假设有系统外其他因素所决定的变量

结构方程模型的结构

结构方程模型可分为：测量模型和结构模型

- 测量模型：描述观测变量和潜变量的函数关系

$$x = \Lambda_x \xi + \delta$$

$$y = \Lambda_y \eta + \varepsilon$$

说明：

- x,y是外生及内生指标；
- δ,ε是X，Y测量上的误差；
- Λx是x指标在ξ上的因子载荷；
- Λy是y指标在η上的因子载荷。

结构方程模型的结构

- 结构模型：描述潜变量之间的关系

$$\eta = \mathrm{B}\eta + \Gamma\xi + \zeta$$

- η是内生潜变量；
- ξ是外生潜变量；
- ζ是随机干扰项；
- B是内生潜变量系数阵，描述内生潜变量η之间彼此的影响；
- Γ是外生潜变量系数阵，描述外生潜变量ξ之间彼此的影响

软件过程可信与软件产品可信结构方程模型

- 软件可信属性相互影响分析
- 反应性指标与形成性指标
- 模型设定

软件可信属性相互影响分析

软件过程可信属性相互影响分析

- 过程可信属性ξ_1~ξ_5

行为可信ξ_1 影响过程产品可信ξ_2

实体可信ξ_3 影响过程产品可信ξ_2 、行为可信ξ_1 和进度可信ξ_4

进度可信ξ_4 影响成本可信ξ_5 和行为可信ξ_1

软件产品可信属性相互影响分析

- 产品可信属性η_1~η_5

生存性η_2 影响容错性η_3 和可靠性η_4

容错性η_3 影响可靠性

防危性η_5 影响可靠性

软件可信属性相互影响分析

- 软件过程可信属性对软件产品可信属性影响分析
  - 直接影响因素

过程产品可信ξ_2 、实体可信ξ_3

  - 间接影响因素

行为可信ξ_1 、进度可信ξ_4 、成本可信ξ_5对于软件产品可信只是通过产品可信和实体可信间接影响产品可信

  - 过程产品可信ξ_2 和实体可信ξ_3 影响软件产品可信属性

反映性指标与形成性指标

- 结构变量和观测变量

结构变量和观测变量之间有不同的因果关系

结构变量是被观测变量所影响，是效果

观测变量是因子，两者之间是线性关系

- 形成性指标

观测变量的集合

- 反映性指标

结构变量产生某些被观测到的指标项，反映这种结构变量的指标，被称为反映性指标

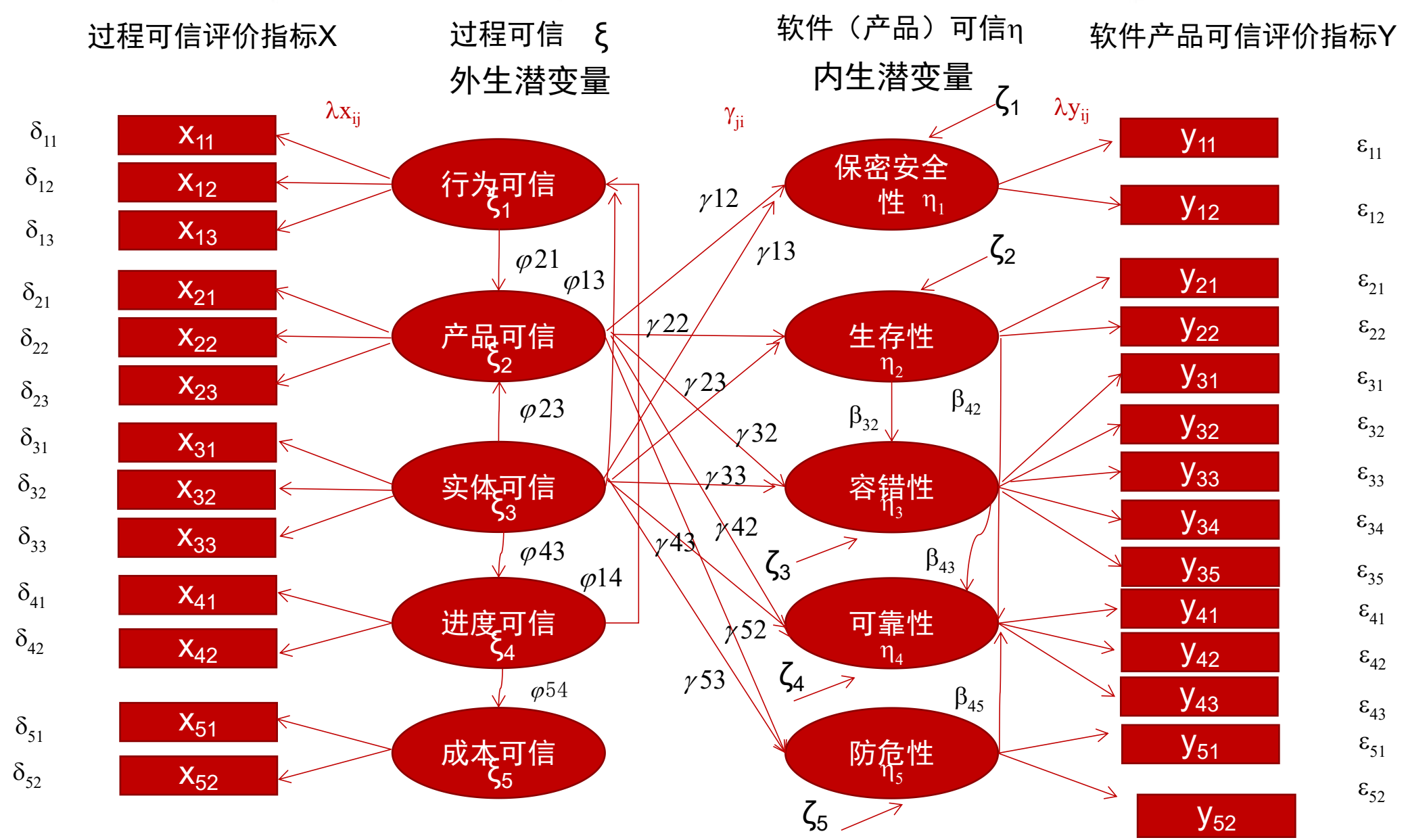
模型设定

- 确定可信软件测度模型的外生潜变量为：
  - 行为可信
  - 过程产品可信
  - 实体可信
  - 进度可信
  - 成本可信
- 确定可信软件测度模型的内生潜变量为：
  - 生存性
  - 保密安全性
  - 容错性
  - 可靠性
  - 防危性

模型设定

- 对于软件可信结构模型，做出如下定义：
  - x_{11}~x_{52}为外生潜变量的可测变量
  - y_{11}~y_{52}为内生潜变量的可测变量
  - δ_{11}~δ_{52}为软件过程可信指标的测量误差
  - ε_{11}~ε_{52}为软件产品可信指标的测量误差
  - λx_{11}~λx_{52}为外生潜变量的因子载荷
  - λy_{11}~λy_{52}为内生潜变量的因子载荷
  - ψ_{14}~ψ_{54}为外生潜变量属性之间的相关系数
  - β_{32}~β_{45}为内生潜变量属性之间的相关系数
  - γ_{12}~γ_{53}为外生潜变量过程可信因素对内生潜变量软件产品可信影响的相关系数

软件可信结构模型路径图



- x_{11}~x_{52}为外生潜变量的可测变量
- y_{11}~y_{52}为内生潜变量的可测变量
- δ_{11}~δ_{52}为软件过程可信指标的测量误差
- ε_{11}~ε_{52}为软件产品可信指标的测量误差
- λx_{11}~λx_{52}为外生潜变量的因子载荷
- λy_{11}~λy_{52}为内生潜变量的因子载荷
- $\varphi 14$ ~$\varphi 54$为外生潜变量属性之间的相关系数
- β_{32}~β_{45}为内生潜变量属性之间的相关系数
- γ_{12}~γ_{53}为外生潜变量过程可信因素对内生潜变量软件产品可信影响的相关系数

测量模型（描述观测变量和潜变量的函数关系）

- 外生潜变量的测量模型，公式为：

$$x_{11}=\lambda_{x_{11}}\xi_1+\delta_{11},\quad x_{12}=\lambda_{x12}\xi_1+\delta_{12},\quad x_{13}=\lambda_{x3}\xi_1+\delta_{13}$$

$$x_{21}=\lambda_{x_{21}}\xi_2+\delta_{21},\quad x_{22}=\lambda_{x22}\xi_2+\delta_{22},\quad x_{23}=\lambda_{x23}\xi_2+\delta_{23}$$

$$x_{31}=\lambda_{x_{31}}\xi_3+\delta_{31},\quad x_{32}=\lambda_{x32}\xi_3+\delta_{32},\quad x_{33}=\lambda_{x33}\xi_3+\delta_{33}$$

$$x_{41}=\lambda_{x_{41}}\xi_4+\delta_{41},\quad x_{42}=\lambda_{x42}\xi_4+\delta_{42}$$

$$x_{51}=\lambda_{x_{51}}\xi_5+\delta_{51},\quad x_{52}=\lambda_{x52}\xi_5+\delta_{52}$$

测量模型（描述观测变量和潜变量的函数关系）

- 内生潜变量的测量模型，公式为：

$$y_{11} = \lambda_{y_{11}}\eta_1 + \varepsilon_{11},\quad y_{12} = \lambda_{y12}\eta_1 + \varepsilon_{12}$$

$$y_{21} = \lambda_{y_{21}}\eta_2 + \varepsilon_{21},\quad y_{22} = \lambda_{y22}\eta_2 + \varepsilon_{22}$$

$$y_{31} = \lambda_{y_{31}}\eta_3 + \varepsilon_{31},\quad y_{32} = \lambda_{y32}\eta_3 + \varepsilon_{32}$$

$$y_{33} = \lambda_{y_{33}}\eta_3 + \varepsilon_{33},\quad y_{34} = \lambda_{y34}\eta_3 + \varepsilon_{34},\quad y_{35} = \lambda_{y35}\eta_3 + \varepsilon_{35}$$

$$y_{41} = \lambda_{y_{41}}\eta_4 + \varepsilon_{41},\quad y_{42} = \lambda_{y42}\eta_4 + \varepsilon_{42},\quad y_{43} = \lambda_{y43}\eta_4 + \varepsilon_{43}$$

$$y_{51} = \lambda_{y_{51}}\eta_5 + \varepsilon_{51},\quad y_{52} = \lambda_{y52}\eta_5 + \varepsilon_{52}$$

结构模型（描述潜变量之间的关系）

$$\xi_1 = \varphi_{13}\xi_3 + \varphi_{14}\xi_4, \quad \xi_2 = \varphi_{21}\xi_1 + \varphi_{23}\xi_3, \quad \xi_5 = \varphi_{54}\xi_4$$

$$\eta_1 = \gamma_{12}\xi_2 + \gamma_{13}\xi_3 + \zeta_1, \quad \eta_2 = \gamma_{22}\xi_2 + \gamma_{23}\xi_3 + \zeta_2,$$

$$\eta_3 = \gamma_{32}\xi_2 + \gamma_{33}\xi_3 + \beta_{32}\eta_2 + \zeta_3$$

$$\eta_4 = \gamma_{42}\xi_2 + \gamma_{43}\xi_3 + \beta_{42}\eta_2 + \beta_{43}\eta_3 + \beta_{45}\eta_5 + \zeta_4$$

$$\eta_5 = \gamma_{52}\xi_2 + \gamma_{53}\xi_3 + \zeta_5$$

潜变量间的路径关系

潜变量	行为可信	产品可信	实体可信	进度可信	成本可信	保密安全性	生存性	容错性	可靠性	防危性
行为可信	0	0	1	1	0	0	0	0	0	0
产品可信	1	0	1	0	0	0	0	0	0	0
实体可信	0	0	1	0	0	0	0	0	0	0
进度可信	0	0	0	1	0	0	0	0	0	0
成本可信	0	1	1	0	0	0	0	0	0	0
保密安全性	0	1	1	0	0	0	0	0	0	0
生存性	0	1	1	0	0	0	0	0	0	0
容错性	0	1	1	0	0	0	1	0	0	0
可靠性	0	1	1	0	0	0	1	1	0	1
防危性	0	1	1	0	0	0	0	0	0	0

案例研究

- 调查问卷
- 模型识别
- 结论分析
  - 调查问卷的内部一致性信度分析
  - 主成分特征分析
  - 潜变量相关性分析
  - 外生潜变量和指标变量关系模型
  - 内生潜变量和指标变量关系模型
  - 指标变量和外生潜变量关系模型
  - 指标变量和内生潜变量关系模型
  - 标准化结构模型系数

调查问卷

- 调查问卷

过程可信的13个评价指标+软件产品可信的14个评价指标

- 量表编制

不可信		低可信		基本可信		可信		高可信	
极低	低	较低	偏低	中等	偏高	较高	高	很高	极高
1分	2分	3分	4分	5分	6分	7分	8分	9分	10分

- 调查范围

某项目开发小组成员+该软件项目的用户

- 数据统计

共发放问卷79份，回收75份，其中有效问卷59份

模型识别

结构方程模型识别主要是判定模型中的待估计参数能否由观测数据求出估计值，模型参数估计采用偏最小二乘法（PLS）。

➢PLS分析

一种新型的多元统计数据分析方法，在一个算法下，可以同时实现回归建模(多元线性回归)、数据结构简化(主成分分析)以及两组变量之间的相关性分析(典型相关分析)

结论分析

- 调查问卷的内部一致性信度分析
- 主成分特征分析
- 潜变量相关性分析
- 外生潜变量和指标变量关系模型
- 内生潜变量和指标变量关系模型
- 指标变量和外生潜变量关系模型
- 指标变量和内生潜变量关系模型
- 标准化结构模型系数

调查问卷的内部一致性信度分析

- 调查问卷的内部一致性信度分析结果

潜变量	行为可信	产品可信	实体可信	进度可信	成本可信	保密安全性	生存性	容错性	可靠性	防危性
信度	0.603	0.47	0.338	0.653	0.532	0.712	0.754	0.414	0.768	0.71

PLS算法要求信度大于0.6就可以接受；
大于0.7表明问卷具有较好的信度

主成分特征分析

潜变量	行为可信	产品可信	实体可信	进度可信	成本可信	保密安全性	生存性	容错性	可靠性	防危性
第一主成分特征值	1.707	1.536	1.342	1.484	1.362	1.552	1.605	1.819	2.057	1.54
第一主成分方差贡献率	0.569	0.512	0.447	0.742	0.681	0.776	0.802	0.364	0.686	0.775

第一主成分特征值均大于1，表明潜变量选择的指标比较合适；
第一主成分方差贡献率在36.4%~80.2%，说明构建的结构方程模型能够很好地的解释样本数据。

潜变量相关性分析

潜变量	行为可信	产品可信	实体可信	进度可信	成本可信	保密安全性	生存性	容错性	可靠性	防危性
行为可信	1	0	0	0	0	0	0	0	0	0
产品可信	0.235	1	0	0	0	0	0	0	0	0
实体可信	0.865	0.207	1	0	0	0	0	0	0	0
进度可信	0.134	-0.224	0.129	1	0	0	0	0	0	0
成本可信	0.051	-0.282	0.029	0.639	1	0	0	0	0	0
保密安全性	0.569	0.203	0.627	0.334	0.061	1	0	0	0	0
生存性	0.442	0.575	0.472	-0.004	-0.156	0.068	1	0	0	0
容错性	0.296	0.737	0.338	-0.383	-0.194	0.189	0.504	1	0	0
可靠性	0.254	0.732	0.201	-0.163	-0.214	0.134	0.536	0.633	1	0
防危性	0.486	0.359	0.532	0.104	0.108	0.301	0.471	0.391	0.391	1

外生潜变量和指标变量关系模型

外生潜变量和指标变量关系模型，公式为：

$$\xi_1 = 0.463x_{11} + 0.639x_{12} + 0.134x_{13}$$

$$\xi_2 = 0.127x_{12} + 0.763x_{22} + 0.362x_{23}$$

$$\xi_3 = 0.39x_{31} + 0.818x_{32} + 0.043x_{33}$$

$$\xi_4 = 0.526x_{41} + 0.652x_{42}$$

$$\xi_5 = 0.234x_{51} + 0.908x_{52}$$

过程可信属性	评价指标体系
行为可信ξ_1	需求变更的频繁程度x_{11}
	缺陷注入率x_{12}
	过程成熟度水平x_{13}
产品可信ξ_2	产品规模偏差x_{21}
	软件过程产品复杂度x_{22}
	过程遗留缺陷的比率x_{23}
实体可信ξ_3	工具的集成化程度x_{31}
	组织资产可信度x_{32}
	开发人员能力水平x_{33}
进度可信ξ4	进度偏差率x_{41}
	时间有效率x_{42}
成本可信ξ_5	成本偏差率x_{51}
	成本有效率x_{52}

内生潜变量和指标变量关系模型

- 内生潜变量和指标变量关系模型，公式为：

$$\eta_1 = 0.532\mathrm{y}_{11} + 0.621 y_{12} + \zeta_1$$

$$\eta_2 = 0.698\mathrm{y}_{21} + 0.428 y_{22} + \zeta_2$$

$$\eta_3 = 0.436\mathrm{y}_{31} + 0.582 y_{32} + 0.191\mathrm{y}_{33} + 0.204 y_{34} - 0.03$$

$$\eta_4 = 0.442\mathrm{y}_{41} + 0.423 y_{42} + 0.364 y_{43} + \zeta_4$$

$$\eta_5 = 0.665\mathrm{y}_{51} + 0.485 y_{52} + \zeta_5$$

软件产品可信属性	软件产品可信评价指标
保密安全性 η_1	信息保密性 y_{11}
	信息完整性 y_{12}
生存性 η_2	软件防止危害漏洞能力 y_{21}
	软件抗攻击能力 y_{22}
容错性 η_3	并发处理控制能力 y_{31}
	程序错误可修正性 y_{32}
	非法输入数据的容错能力 y_{33}
	非法组合的容错能力 y_{34}
	输出数据合理的容错能力 y_{35}
可靠性 η_4	平均失效时间比率 y_{41}
	平均修复时间比率 y_{42}
	平均故障间隔时间比率 y_{43}
防危性 η_5	非安全失效的平均时间比率 y_{51}
	非安全失效的平均间隔时间比率 y_{52}

指标变量和外生潜变量关系模型

- 指标变量和外生潜变量关系模型，公式为：

$$x_{11}=0.463\xi_1+\delta_{11},\quad x_{12}=0.639\xi_1+\delta_{12},\quad x_{13}=0.134\xi_1+\delta_{13}$$

$$x_{21}=0.127\xi_2+\delta_{21},\quad x_{22}=0.763\xi_2+\delta_{22},$$

$$x_{23}=0.362\xi_2+\delta_{23}$$

$$x_{31}=0.390\xi_3+\delta_{31},\quad x_{32}=0.818\xi_3+\delta_{32},$$

$$x_{33}=0.043\xi_3+\delta_{33}$$

$$x_{41}=0.526\xi_4+\delta_{41},\quad x_{42}=0.652\xi_4+\delta_{42}$$

$$x_{51}=0.234\xi_5+\delta_{51},\quad x_{52}=0.908\xi_5+\delta_{52}$$

指标变量和内生潜变量关系模型

- 指标变量和内生潜变量关系模型，公式为：

$$y_{11}=0.532\eta_1+\varepsilon_{11},\quad y_{12}=0.621\eta_1+\varepsilon_{12}$$

$$y_{21}=0.698\eta_2+\varepsilon_{21},\quad y_{22}=0.428\eta_2+\varepsilon_{22}$$

$$y_{31}=0.436\eta_3+\varepsilon_{31},\quad y_{32}=0.582\eta_3+\varepsilon_{32}$$

$$y_{33}=0.191\eta_3+\varepsilon_{33},\quad y_{34}=0.204\eta_3+\varepsilon_{34},\quad y_{35}=-0.034\eta_3+\varepsilon_{35}$$

$$y_{41}=0.442\eta_4+\varepsilon_{41},\quad y_{42}=0.423\eta_4+\varepsilon_{42},\quad y_{43}=0.364\eta_4+\varepsilon_{43}$$

$$y_{51}=0.665\eta_5+\varepsilon_{51},\quad y_{52}=0.485\eta_5+\varepsilon_{52}$$

标准化结构模型系数

潜变量	行为可信	产品可信	实体可信	进度可信	成本可信	保密安全性	生存性	容错性	可靠性	防危性
行为可信	0	0	0.862	0.023	0	0	0	0	0	0
产品可信	0.221	0	0.017	0	0	0	0	0	0	0
实体可信	0	0	0	0	0	0	0	0	0	0
进度可信	0	0	0.129	0	0	0	0	0	0	0
成本可信	0	0	0	0.639	0	0	0	0	0	0
保密安全性	0	0.076	0.661	0	0	0	0	0	0	0
生存性	0	0.499	0.368	0	0	0	0	0	0	0
容错性	0	0.686	0.186	0	0	0	0.021	0	0	0
可靠性	0	0.481	-0.106	0	0	0	0.152	0.184	0	0.138
防危性	0	0.26	0.478	0	0	0	0	0	0	0

内生潜变量间的影响关系

- 行为可信

  实体可信对行为可信影响较大，进度可信对行为可信影响较小

- 产品可信

  行为可信对产品可信影响较大，实体可信对产品可信影响较小

- 进度可信

  实体可信对进度可信影响较小

- 成本可信

  进度可信对成本可信影响较大

外生可测变量间的影响关系

- 容错性

  生存性对容错性影响较小

- 可靠性

  生成性和容错性对可靠性影响较大，防危性对可靠性影响较小

外生潜变量对内生潜变量的影响关系

- 保密安全性

实体可信对保密安全性影响较大，产品可信对保密安全性影响较小

- 生存性

产品可信对生存性影响较大，实体可信对生存性影响较小

- 容错性

产品可信对容错性影响较大，实体可信对容错性影响较小

- 可靠性

产品可信对可靠性影响较大，实体可信对可靠性影响较小

- 防危性

实体可信对防危性影响较大，产品可信对防危性影响较小

案例总结

- 案例结果表明可信软件评价指标体系能够很好地反映可信软件属性之间的定量关系，软件过程的可信对于软件产品可信具有较大的影响。
- 因此，加强软件过程管理，提高软件过程的可信水平，对于确保软件产品可信具有重要作用。

软件过程可信评价模型研究

软件过程可信评价模型研究

- 问题描述
- 软件过程可信评价模型建立主要过程
- 软件过程可信评价模型算法的选择
- 模糊层次分析模型基本原理
- 案例分析

软件过程可信评价模型研究

问题描述

我们知道软件过程可信对软件产品可信的影响，所以只有在保证软件过程可信性的前提下，才能保证最终软件产品的可信性。

软件过程可信评价主要研究：

- 软件开发过程是否符合项目开发的要求
- 过程质量是否满足项目开发的需要
- 对开发过程的各个角色能力和过程中产品可信程度的综合评价

本节研究内容

根据软件过程可信属性和评价指标项，构建能够量化的软件过程可信度评价模型。

软件过程可信评价模型研究

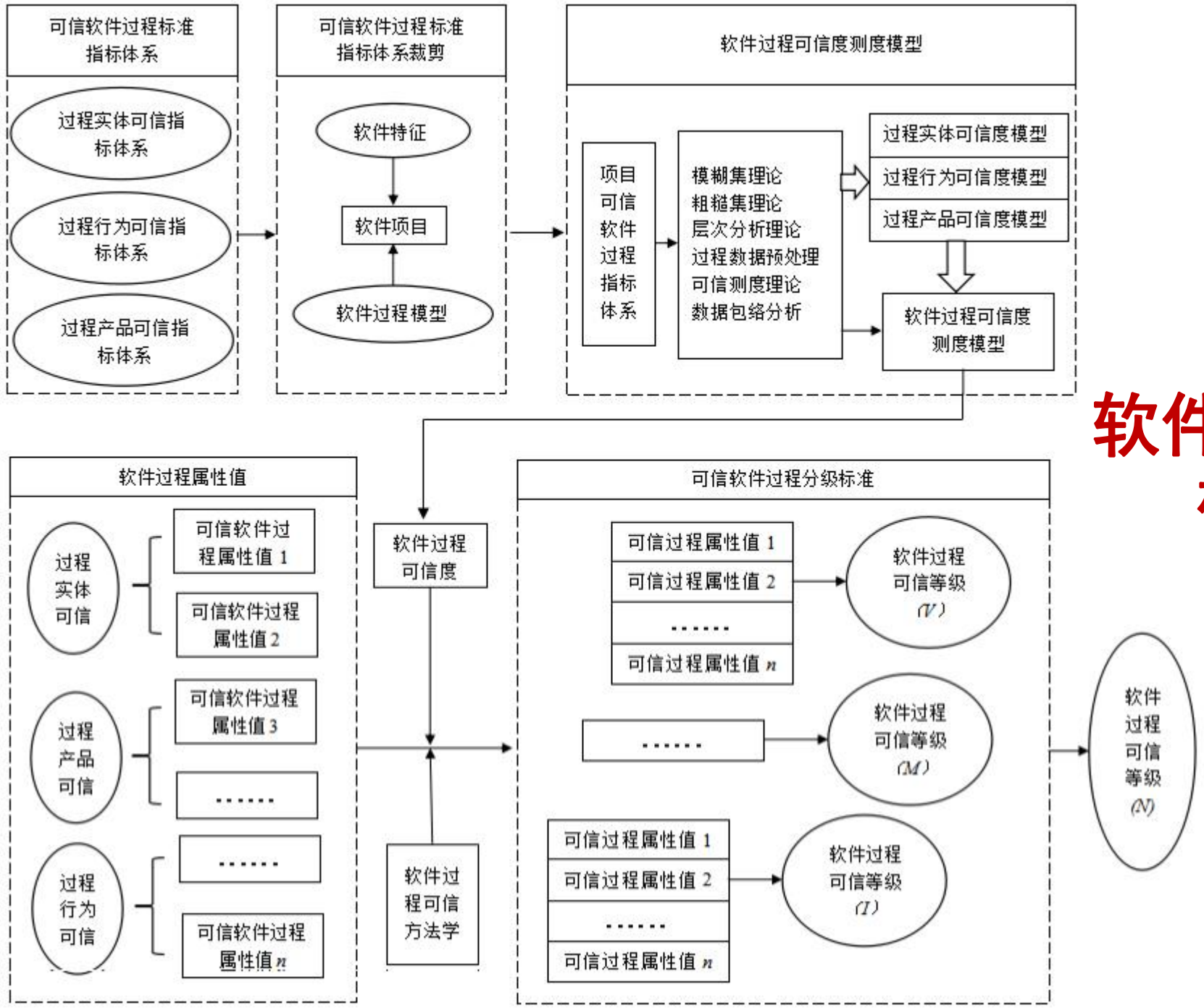
软件过程可信评价模型建立主要过程

根据可信软件标准测度指标体系，对测量属性即指标体系，进行有效裁剪，构建符合特定具体项目的可信过程评价指标体系；

应用模糊层次分析等理论，确定各个指标的权重，数据预处理根据具体的数据特征采取不同的办法进行数据预处理，如数据变换、归一化等，把数据转换成满足软件过程可信度测度模型需要的数据；

应用软件测度理论和改进数学模型方法，建立软件过程实体可信度(trustworthy process entity, TPE)测度模型，过程行为可信度(trustworthy process behavior, TPB)评价模型和过程产品可信度(trustworthy process products, TPP)测度模型以及软件过程可信综合测度模型。

软件过程可信度评价模型建立过程



软件过程可信评价模型研究

软件过程可信评价模型算法的选择

软件过程可信属性

- 行为可信
- 产品可信
- 实体可信
- 进度可信
- 成本可信

这些定性属性或指标属于某一等级的判断往往很难用数值表示，只能用**“不可信”“低可信”“基本可信”“可信”和“高可信”**等模糊概念来描述，同时软件工程从“不可信”到“可信”是一个渐变过程，各个可信状态间没有明显的转换标志，因此，确定软件过程可信程度是个十分困难的问题。

软件过程可信评价模型研究

□软件过程可信评价模型算法的选择

模糊数学理论能够定量地分析复杂系统中的各种模糊因素，既可用于主观定性指标的综合评价，又可用于客观定量指标的综合分析，通过评价软件过程各因素对过程可信隶属程度情况来综合评价软件过程可信程度，可以准确地刻画软件过程的模糊状况，因此，运用**模糊数学**评价软件过程可信更符合软件过程实际。

考虑不同软件过程影响因素对于工程可信影响程度的不同，下面介绍一种**支持模糊数据的软件过程可信度评价方法**，采用**层次分析法确定软件过程可信属性度量指标项的权重，从而使主观评价客观化**；同时对传统的**模糊综合评价方法**加以改进，以适应多种数据输入形式，支持定性与定量的度量数据及相应的量化评价，最终给出**软件过程在“不可信”“低可信”“基本可信”“可信”和“高可信”上的隶属度。**

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 层次分析模型

层次分析法(AHP)是系统工程中对非定量事件做定量分析的一种简单有效的方法，它把复杂的问题分解成各个组成因素，并按其支配关系分组形成有层次的结构，通过指标两两比较的方式确定层次中诸因素的相对重要性，然后，综合人的判断以决定诸因素的相对重要性的总排序。

软件过程可信评价属于半结构化决策问题，其中既有定量计算的内容，同时也包括定性分析的内容，各属性和评价指标项影响过程可信重要程度不同，应用AHP确定软件过程可信属性和评价指标项的权重。

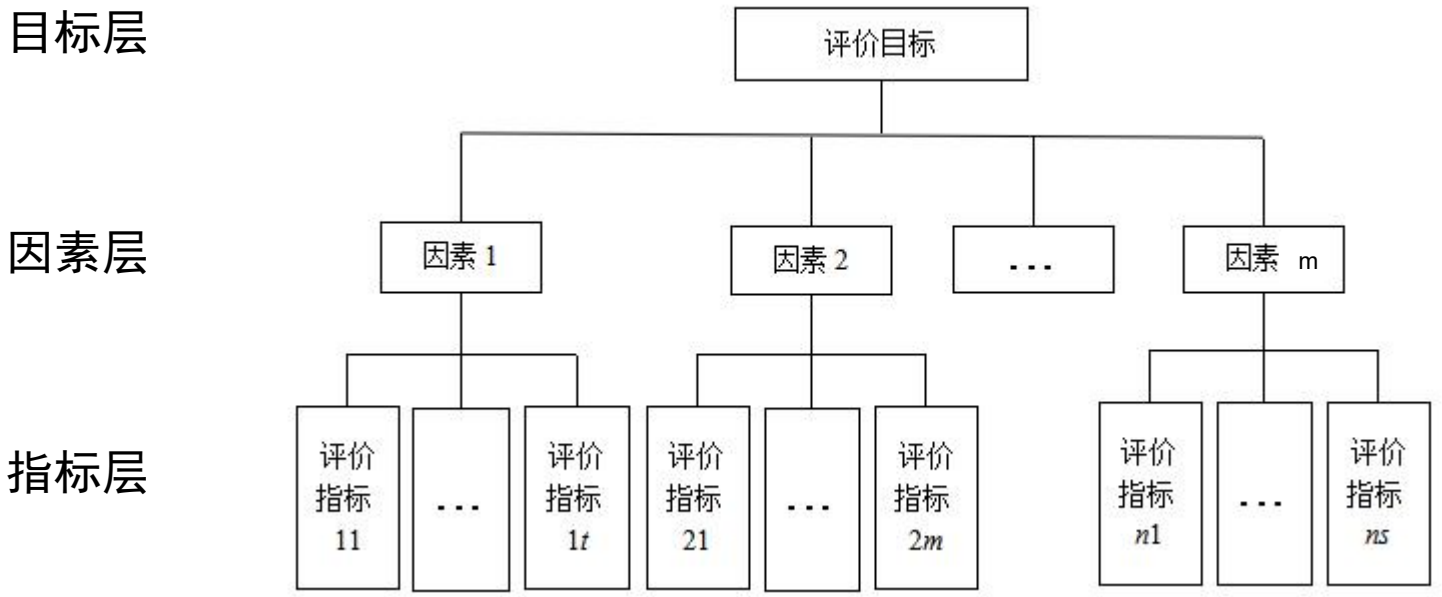
软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 层次分析模型

◆ 建立层次结构模型

对于复杂的决策问题，首先将决策问题层次化分解，复杂问题被分解为因素的组成部分，**构造出一个包括目标层、因素层和指标层的层次结构模型**，其中目标层为分析问题的预定目标，因素层为评价目标的属性或者目标的影响因素，指标层包括所需考虑的评价指标项，为因素的具体表现。层次模型关系由若干层次构成，上一层次元素对下一层次有关元素起支配作用，下一层元素影响上一层次的重要程度。



层次结构模型图

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 层次分析模型

◆ 构造判断矩阵

设软件过程可信评价有m个影响因素$G_1,G_2,\ldots,G_m$，指标向量为$A_1,A_2,\ldots,A_n$，指标$A_i(i=1,2,...,n)$在因素$G_j(j=1,2,...,m)$下的取值为a_{ij}，由矩阵表示为

$$A=\begin{array}{c} \begin{matrix} G_1, & G_2, & \ldots, & G_m \end{matrix} \\ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix} \end{array}=(a_{ij})_{n\times m}$$

上式为指标A1,A2,... ,An关于G1,G2,... ,Gm的指标矩阵，采用AHP法对n个指标进行排序，求出指标层的指标项相对于因素层的因素和因素层相对于目标的权重。

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 层次分析模型

◆ 构造判断矩阵

从层次结构模型图中可以看出，这类多目标决策问题有三个层次：目标层、因素层、指标层，设指标层n个指标，相对于因素层中某一影响因素G_j，**通过两两比较指标的重要性**，一般按照1~9判断矩阵标准度(如下表)得到比较矩阵C_j。

重要性标度	含义
1	两个元素相比，具有同等的重要性
3	两个元素相比，前者比后者相对重要
5	两个元素相比，前者比后者明显重要
7	两个元素相比，前者比后者强烈重要
9	两个元素相比，前者比后者绝对重要
2,4,6,8	表示上述判断的中间值
1,1/2,.....1/9	若元素i与元素j的重要性之比为c_{ij}，则元素j与元素i的重要性之比为$c_{ji}=1/c_{ij}$

$$C_j=\begin{pmatrix} c_{11}^j & c_{12}^j & \cdots & c_{1n}^j \\ c_{21}^j & c_{22}^j & \cdots & c_{2n}^j \\ \vdots & \vdots & & \vdots \\ c_{n1}^j & c_{n2}^j & \cdots & c_{nn}^j \end{pmatrix}$$

$$c_{ik}^j=\begin{cases} 3\sim 9 \\ 1 \\ 1/9\sim 1/3 \end{cases}$$

构造判断矩阵(书上表述有错误)

$$r_i^j = \sum_{k=1}^{n} c_{ik}^j$$

$$b_{ik}^j = \begin{cases} r_i^j - r_k^j & \text{当 } r_i^j > r_k^j \text{ 时} \\ 1 & \text{当 } r_i^j = r_k^j \text{ 时} \\ r_k^j - r_i^j - 1 & \text{当 } r_i^j < r_k^j \text{ 时} \end{cases}$$

写成矩阵形式

$$B^j = \begin{bmatrix} b_{11}^j & b_{12}^j & \cdots & b_{1n}^j \\ b_{21}^j & b_{11}^j & \cdots & b_{1n}^j \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1}^j & b_{n2}^j & \cdots & b_{nn}^j \end{bmatrix}$$

计算上述B^j矩阵的最大特征值，可计算一致性判断系数如下：

$$C \bullet R = \frac{\lambda_{max} - n}{(n-1) \bullet (R \bullet I)}$$

其中： $R \bullet I$ 查下表：

矩阵的阶	3	4	5	6	7	8	9	10	11	12	.....	.....
R . I	0.58	0.9	1.12	1.24	1.32	1.41	1.46	1.49	1.52	1.54	.....	.....

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 层次分析模型

◆ 层次单排序

判断矩阵除了表示各个指标之间的重要程度外，还可以利用**特征向量法**计算同层指标相对上层因素的相对权重。

之后要进行一致性检验，**求因素$G_j(j=1,2,...,m)$的判断矩阵C_j的特征根λ_{max}，特征向量**$X_j=\left[X_{1j},X_{2j},...,X_{nj}\right]^T$。检验每个矩阵的一致性，若不满足一致性条件，则要修改判断矩阵，直至满足为止。经归一化后，即为下一层次相应因素或指标对于上一层次某因素相对重要性的排序权重，成为层次单排序。

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 层次分析模型

◆ 层次总排序

上面得到的是指标层对于因素层的权重向量，总排序权重要自上而下地将单准则下的权重进行合成，得到最低层中各指标对于目标的排序权重。

尽管各层次已经过层次单排序的一致性检验，各成对比较判断矩阵都已满足一致性，但层次总排序后，各层次的非一致性仍有可能积累起来，引起最终分析结果较严重的不一致性，因此，还需要从目标层向因素层、因素层向指标层逐层进行一致性检验。

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 模糊评价模型

模糊综合评价应用模糊关系合成的原理，将一些边界不清晰、定性因素或指标项定量化，进行综合评价的一种方法。

具体步骤如下：

◆ 确定因素集U

根据评价指标体系，建立影响软件过程可信的因素集，记为:

$$U=\{u_1,u_2,...,u_n\}$$

◆ 评语集V

针对可信软件过程评价因素和指标体系的要求，便于评价结果的量化，确定表明可信程度等级的评语，记为:

$$V=\{v_1,v_2,...,v_m\}$$

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 模糊评价模型

◆ 隶属度R

首先进行指标层的单指标评价，即对指标项的评定，建立一种模糊映射，即 $f:u\to v$ 。其次对因素集U中的指标集 $u_i(i=1,2,...,n)$ 作单因素评判，再次对评价指标分别给出评价方案 $v_j(j=1,2,...,m)$ 的隶属度，确定该因素对选择等级V的隶属度r_{ij}，即得出单因素u_i的隶属度向量为 $R_i=(r_{i1},r_{i1},...,r_{in})$, R_i是评语集V上的模糊子集，从而构造模糊评价矩阵。

可以采用调查问卷的方式确定模糊隶属度，将$V=\{v_1,v_2,...,v_m\}$的每个选项在问卷出现的频率作为某个指标项的隶属度，并由指标项隶属度构建可信软件过程模糊关系矩阵。

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 模糊评价模型

◆ 单因素评价

单因素评价即通过主要因素的模糊评价矩阵右乘指标相对于该因素的权重求得。公式为$B_{ij} = W_{ij} \bullet R_{ij}$，进行模糊矩阵复合运算得到对主要因素的单因素模糊评价。

◆ 模糊综合评价

单因素模糊评价仅反映了一个因素对评价对象的影响，综合考虑所有因素的影响，采用模糊评价得出正确的评价结果。

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 模糊评价模型

◆ 模糊综合评价

➢ 指标层各指标项评价

根据上一步的单因素评价方法，可以得到指标层u_{ij}上各指标的评价结果，建立评价矩阵。公式为

$$R_i = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{pmatrix}$$

➢ 可信因素层的权重分配

对应因子$v_1, v_2, \ldots, v_n$权重 $w = \{\omega_1, \omega_2, \ldots, \omega_n\}$，其中$\sum_{i=1}^{n} \omega_i = 1, 0 \le \omega_i \le 1$。

软件过程可信评价模型研究

模糊层次分析模型基本原理

✓ 模糊评价模型

◆ 模糊综合评价

➢ 可信指标的权重分配

对应因子$v_{i1},v_{i2},...,v_{in}$权重 $w_{ij}=\{\omega_{i1},\omega_{i2},...,\omega_{in}\}$，其中$\sum_{i=1}^{n}\omega_{ij}=1,0\le\omega_{ij}\le1$，指标权重集 $\omega_i=\{\omega_{i1},\omega_{i2},...,\omega_{in}\}$。

➢ 准则层各因素评价

由指标层上各指标的评价结果构成的模糊评价矩阵右乘指标层各指标的权重向量，可得到准则层上个因素的评价结果，即 $\mathrm{B_i}=W_i\bullet R_i$

$$\{b_1,b_2,...,b_m\}=\{\omega_1,\omega_2,...,\omega_m\}\begin{bmatrix}r_{11}&r_{12}&\cdots&r_{1m}\\r_{21}&r_{22}&\cdots&r_{2m}\\\vdots&\vdots&&\vdots\\r_{n1}&r_{n2}&\cdots&r_{nm}\end{bmatrix}$$

模糊层次分析模型基本原理

✓ 模糊评价模型

◆ 模糊综合评价

➢ 目标层综合评价结果

用准则层上各因素的评价结果构成的模糊评价矩阵右乘准则层各因素的权重得到目标层综合评价结果，即

$$A = W_A \cdot R_A = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{bmatrix}$$

➢ 确定评价等级，并对结果进行分析

软件过程可信评价模型研究

案例分析

- ✓ 评价数据的获取
- ✓ 软件过程可信评价模型建立
- ✓ 软件过程可信评价模型的验证

软件过程可信评价模型研究

案例分析

✓ 评价数据的获取

由于软件过程可信度测度模型验证，需要软件组织长期积累反映项目开发状态的历史数据，短时间内很难获得这些数据，采用调查问卷的方式，由软件项目开发人员、软件测试人员，对软件过程可信的评价指标项进行相对重要程度的评价，然后对每个指标进行相对等级评判，经统计分析获取软件过程测度模型的有关数据。

根据软件过程可信评价指标体系，设计调查问卷，问卷包含过程可信的5个影响因素和13个评价指标，表的编制采用“不可信”“低可信”“基本可信”“可信”“高可信”。

软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型建立

◆ 确定指标层和因素层权重

结合专家对于过程可信指标项的重要程度排序，应用层次分析法确定指标层和因素层的权重。

◆ 确定因素集U

根据评价指标体系，建立影响软件可信的因素集 $U=\{B_1,B_2,...,B_5\}$

$\{B_1,B_2,...,B_5\}\rightarrow\{$行为可信，产品可信，实体可信，进度可信，成本可信$\}$

软件过程可信的指标体系为$(x_{11},x_{12},...,x_{52})$，建立软件过程可信评价层次结构，如图所示。

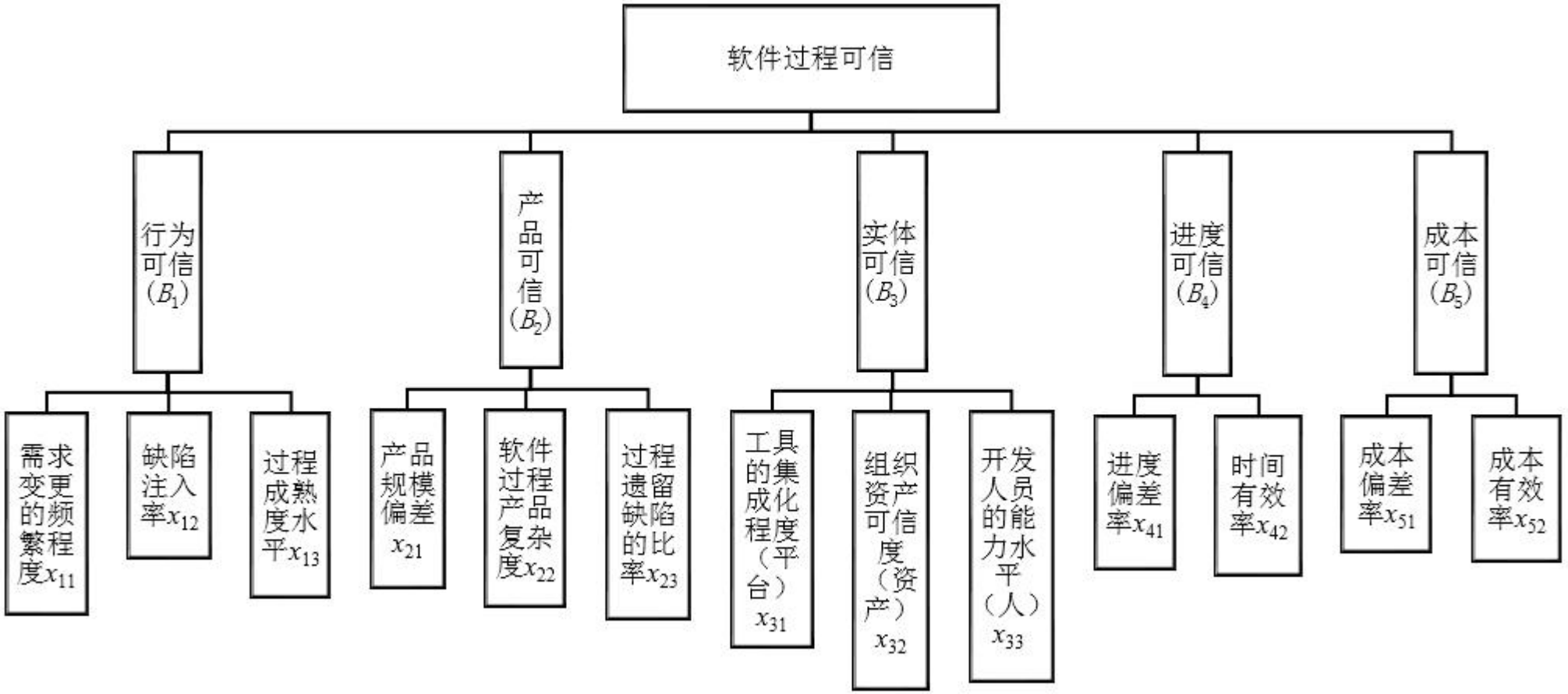
软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型建立

◆ 确定因素集U

软件过程可信测度层次模型结构图



软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型建立

◆ 软件过程可信评语集V

根据软件过程可信属性及评价指标体系编制调查问卷，结合模糊层次分析原理，对于指标层的每个评价指标项，按照“不可信”“低可信”“基本可信”“可信”“高可信”设计选项。公式为

$$V = \{v_1, v_2, v_3, v_4, v_5\}$$

其中v_1表示不可信，v_2表示低可信，v_3表示基本可信，v_4表示可信，v_5表示高可信。

软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型建立

◆ 软件过程可信隶属度R

根据调查问卷，统计各个指标对评语集评价的数据，计算指标层隶属度r'_{2ij}，公式为$r'_{2ij}=T_{vl}/T$

其中，T_{vl}表示某指标隶属于v_l的总数，T表示合格调查问卷总数。通过统计得到过程可信指标层隶属度，下面列出的是行为可信指标层隶属度的表格，相应的还有产品可信指标层隶属度表等共5个表，如下所示

行为可信指标层隶属度

指标项	不可信	低可信	基本可信	可信	高可信
x_{11}	0.1538	0.2115	0.25	0.1730	0.2115
x_{12}	0.0961	0.1923	0.4038	0.1730	0.1346
x_{13}	0.1346	0.1153	0.2884	0.25	0.2115

软件过程可信评价模型研究

产品可信指标层隶属度

指标项	不可信	低可信	基本可信	可信	高可信
x_{21}	0.0961	0.1346	0.3067	0.3076	0.1538
x_{22}	0.0961	0.1730	0.3461	0.2307	0.1538
x_{23}	0.0961	0.2307	0.2692	0.25	0.1538

实体可信指标层隶属度

指标项	不可信	低可信	基本可信	可信	高可信
x_{31}	0.1153	0.1730	0.2115	0.2884	0.2115
x_{32}	0.0961	0.1730	0.3076	0.2692	0.1538
x_{33}	0.0961	0.1538	0.2884	0.2307	0.2307

软件过程可信评价模型研究

进度可信指标层隶属度

指标项	不可信	低可信	基本可信	可信	高可信
x_{41}	0.0961	0.1538	0.3067	0.2307	0.2115
x_{42}	0.0576	0.1346	0.3269	0.25	0.2307

成本可信指标层隶属度

指标项	不可信	低可信	基本可信	可信	高可信
x_{51}	0.1153	0.1346	0.3269	0.25	0.1730
x_{52}	0.0961	0.1346	0.2307	0.3269	0.2115

软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型的验证

◆ 应用层次分析法确定软件过程可信评价指标权重

通过专家对过程可信各个指标项相对重要程度进行分析评判，构建如下成对比较矩阵。

行为可信比较矩阵

B_1	x_{11}	x_{12}	x_{13}
x_{11}	1	1/3	1/5
x_{12}	3	1	1/7
x_{13}	5	7	1

产品可信比较矩阵

B_2	x_{21}	x_{22}	x_{23}
x_{21}	1	1/3	1/9
x_{22}	3	1	1/7
x_{23}	9	7	1

软件过程可信评价模型研究

实体可信比较矩阵

B_3	x_{31}	x_{32}	x_{33}
x_{31}	1	1/3	1/5
x_{32}	3	1	1/7
x_{33}	5	7	1

进度可信比较矩阵

B_4	x_{41}	x_{42}
x_{41}	1	1/7
x_{42}	7	1

成本可信比较矩阵

B_5	x_{51}	x_{52}
x_{51}	1	1/5
x_{52}	5	1

过程可信比较矩阵

B	B_1	B_2	B_3	B_4	B_5
B_1	1	1/9	1/5	7	5
B_2	9	1	7	3	5
B_3	5	1/7	1	5	7
B_4	1/5	1/5	1/7	1	1/5
B_5	1/7	1/3	1/5	5	1

软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型的验证

◆ 应用层次分析法确定软件过程可信评价指标权重

根据层次分析法的原理，得到判定矩阵，各指标和各个过程可信影响因素的权重。

行为可信判断矩阵

B_1	x_{11}	x_{12}	x_{13}	w_i
x_{11}	1.0000	0.6703	0.4493	0.1981
x_{12}	1.4918	1.0000	0.3012	0.2263
x_{13}	2.2255	3.3201	1.0000	0.5756

产品可信判断矩阵

B_2	x_{22}	x_{23}	x_{21}	w_i
x_{22}	1.0000	0.6703	02019	0.1343
x_{23}	1.4918	1.0000	0.3012	0.2004
x_{21}	4.9530	0.3012	1.0000	0.6653

实体可信判断矩阵

B_3	x_{31}	x_{32}	x_{33}	w_i
x_{31}	1.0000	0.6703	0.4493	0.1981
x_{32}	1.4918	1.0000	0.3012	0.2263
x_{33}	2.2255	3.3201	1.0000	0.5756

进度可信判断矩阵

B_4	x_{41}	x_{42}	w_i
x_{41}	1.0000	0.6703	0.1343
x_{42}	1.4918	1.0000	0.2004

软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型的验证

◆ 应用层次分析法确定软件过程可信评价指标权重

成本可信判断矩阵

B_5	x_{51}	x_{52}	w_i
x_{51}	1.0000	0.3012	0.2315
x_{52}	3.3201	1.0000	0.7685

软件过程可信判断矩阵

A	B_1	B_2	B_3	B_4	B_5	w_i
B_1	1.0000	1.0000	1.4918	3.3201	4.9530	0.3271
B_2	1.0000	1.0000	3.3201	1.4918	3.3201	0.3019
B_3	0.6703	0.3012	1.0000	3.3201	2.2255	0.1868
B_4	0.3012	0.6703	0.3012	1.0000	1.4918	0.1067
B_5	0.2019	0.3012	0.4493	0.6703	1.0000	0.0775

以上所有的可信判定矩阵一致性比例均为<0.1，一致性检验通过。

软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型的验证

◆ 可信指标层评价

过程可信指标项通过主要因素的模糊评价矩阵，右乘主要指标项相对于该因素的权重。软件过程可信因素层评价结果如下表：

软件过程可信因素层评价结果

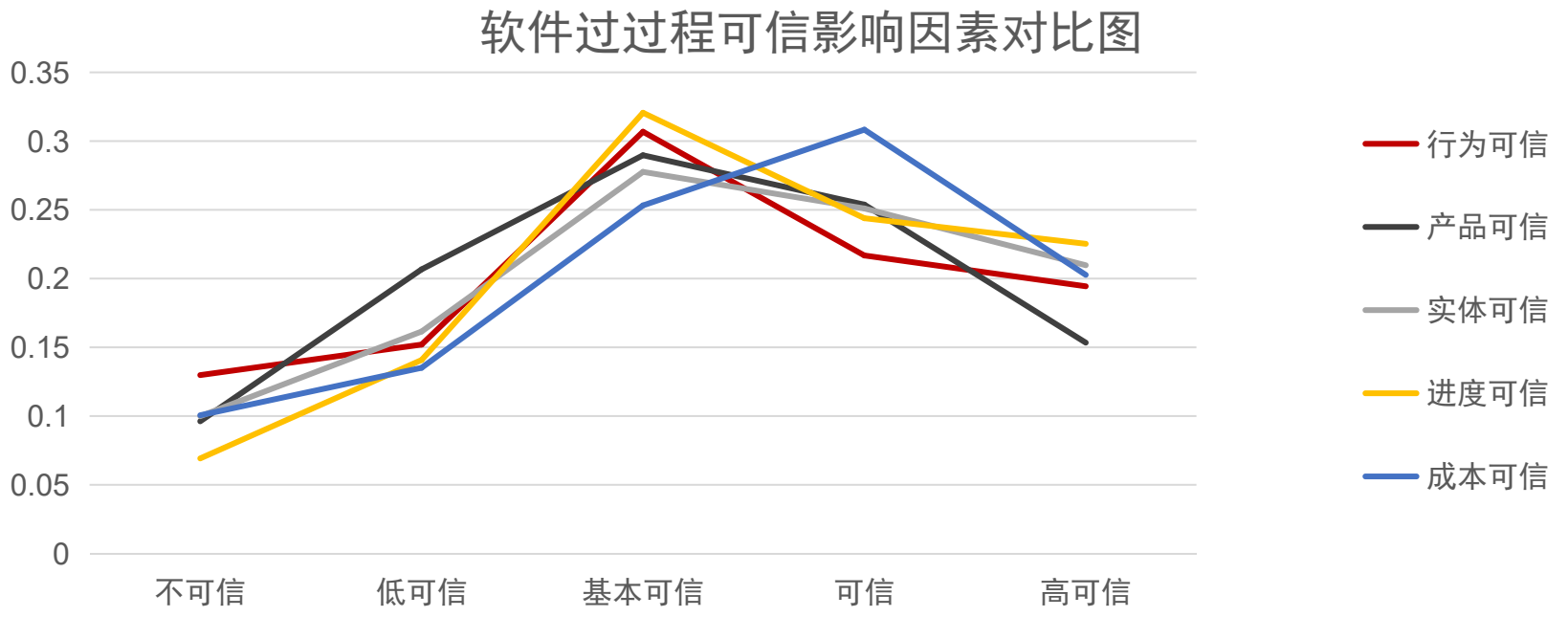
指标项	不可信	低可信	基本可信	可信	高可信
B_1	0.1298	0.1520	**0.3068**	0.2168	0.1944
B_2	0.0962	0.2067	**0.2897**	0.2538	0.1534
B_3	0.0999	0.1615	**0.2776**	0.2510	0.2097
B_4	0.0692	0.1408	**0.3206**	0.2439	0.2253
B_5	0.1006	0.1351	**0.2532**	0.3083	0.2027

软件过程可信评价模型研究

案例分析

◆ 可信指标层评价

从表中可以看出，针对该软件过程行为可信“基本可信达到30.68%”，产品可信“基本可信达到28.97%”，实体可信“基本可信达到27.76%”，进度可信“基本可信达到32.06%”，成本可信“基本可信达到30.38%”，表明各个影响因素基本可信。从下图中也可以看出来，该软件过程的进度可信和产品可信的“基本可信”隶属度相对于实体可信和产品可信水平较高。



软件过程可信评价模型研究

案例分析

✓ 软件过程可信评价模型的验证

◆ 软件过程总体可信水平评价

根据软件过程可信因素层评价结果和软件过程可信判断矩阵确定的因素权重，对软件过程整体可惜水平进行评价，评价结果如下表：

软件过程总体可信水平评价

指标项	不可信	低可信	基本可信	可信	高可信
总结果	0.1045	0.1678	0.2935	0.2443	0.1888

从表中可以看出该软件过程相对于各指标项的隶属度，进一步可以计算出软件总体可信隶属度为72.66%，不可信隶属度为27.23%。表明该项目的软件过程整体管理水平较高、项目开发人员满足项目的需要，所选用的开发工具、平台等符合项目要求。

软件可信度评价模型研究

软件可信度评价模型研究

- 问题描述
- 软件可信度评价模型建立主要过程
- 证据理论原理
- 基于证据理论的软件可信评价层次模型
- 软件可信评价模型案例分析

软件可信度评价模型研究

问题描述

软件可信评价是通过分级的方式对用户的主观感受进行评价，用户根据证据描述软件对某种可信属性的满足程度。

软件可信评价主要考虑的问题包括以下内容：

- 可信软件产品属性和评价指标既包含定量指标，也有定性指标，评价模型首先要解决两类指标在模型中的融合计算问题。
- 软件可信指标的类型有成本型，也有效益型，在融合计算过程中要解决如何处理两类指标的类型差异。
- 对于软件运行环境的不确定性问题，以及根据项目的具体情况软件可信评价指标如何取舍。
- 由于有些缺陷需要软件较长时间的运行才能反映出来，甚至只有在特定条件下激活某些缺陷，所以，软件可信评价要考虑如何获取数据问题。

软件可信度评价模型研究

软件可信度评价模型建立主要过程

根据可信软件属性和评价指标体系，首先分析现有的软件，如可靠性模型、保密安全性模型、生存性模型、容错性模型、可靠安全性和实时性等模型，充分考虑软件运行环境的不确定性和软件特征，构建适合测度软件可靠性测度模型、保密安全性测度模型、生存性测度模型、容错性测度模型、可靠安全性测度模型和实时性测度模型；应用相关的数学算法模型，结合软件可信基本属性模型，建立软件能力可信测度模型、软件行为可信测度模型、用户行为可信测度模型和软件可信度测度综合模型。

为了验证可信软件评价模型，首先建立软件可信测度的影响因素和评价指标体系，采用问卷的方式收集有关数据，应用证据理论信息处理技术，建立基于Dempster合成规则的软件可信测度模型。

软件可信度评价模型研究

- 证据理论原理

可信软件评价需要一种能够处理不确定、不准确、不完整、模糊信息的分析评价模型。证据理论(the D-S theory of evidence)是Glenn Shafer在1976年撰写专注《证据的数学理论》中提出的一种针对不确定性的推理方法。

证据理论由取值在单位区间(0,1)中的信度函数(belief functions)与似然函数(plausibility functions)两个数值组成的区间表示在给定的证据下对假设和命题的信度，并用Dempster规则对不同来源的证据产生信度进行综合处理，对不确定信息做出不确定性度量，使不确定性度量更贴近软件可信水平，指导软件过程改进和软件运行维护。

软件可信度评价模型研究

证据理论原理

证据

证据是知识和经验的一部分，是对评价目标对象有关问题进行观察和研究的结果，是支持某事件成立的信息，是一个抽象概念。证据分为客观信息和主观信息，即客观证据和主观证据。客观证据是客观事物存在和发生所表现出的信息，主观证据是由人的经验、知识和推理判断提供的信息。

识别框架

针对一个具体评价问题，评价主体认为评价客体所有可能结果构成的集合，即该评价客体的识别框架(frame of discernment)，用Θ表示。公式为：

$$\Theta=\{\theta_1,\theta_2,...,\theta_n\}$$

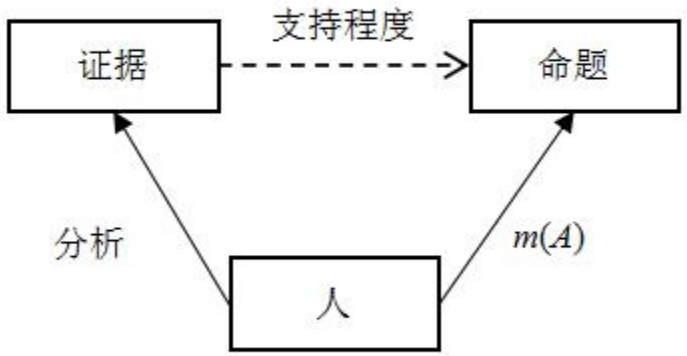
其中，θ_i是评价问题的可能结果之一。

软件可信度评价模型研究

证据理论原理

信度函数

在一批给定的证据与一批给定的命题之间不存在一种客观必然的联系能够确定一个精确的支持程度，需要人们通过对证据的分析得出对命题的信任程度的判定。通过对证据的分析得出问题的基本可信度分配函数(*mass*)，用$m(A)$表示。在证据理论中，人、证据和命题关系，如下图所示：



软件可信度评价模型研究

证据理论原理

信度函数

定义1 基本概率赋值

在识别框架 Θ下，如果集函数m: $2^{\Theta} \to [0,1]$ 满足：

$$m(\phi)=0$$

$$\sum_{A\subset\Theta} m(A)=1$$

则称m为框架 Θ上的基本可信度分配； $m(A)$反映了证据支持命题A的程度。2^{Θ}表示 Θ的所有子集的集合，即 Θ的幂集。

如果 $A\subset\Theta$， $m(A)$称为A的基本可信数。基本可信数反映了证据对A本身的支持度，即信度大小。

证据理论原理

信度函数

定义2 信度函数

Θ为识别框架，如果$A \subset \Theta$， $m: 2^{\Theta} \to [0,1]$为框架Θ上的基本可信度分配，则信度函数Bel：$2^{\Theta} \to [0,1]$ 为

$$\text{Bel(A)}=\sum_{B \subset A} m(B)$$

Bel(A)表示命题A中所有子集B的基本概率分配函数之和，即对A的总信任程度。如果$m(A)>0$，则A为信度函数Bel的焦元，由于证据是个抽象的概念，只能借助于它对状态空间的作用来表示，$m(A)$可视为证据的强度。

软件可信度评价模型研究

证据理论原理

Dempser合成法则

两个证据的合成法则

（参见课本126页）

多个证据的合成法则
（参见课本126页）

软件可信度评价模型研究

证据理论原理

◆ 证据冲突及其处理方法

证据冲突是指证据之间所支持命题的不一致性。Dempster合成法则是反应证据融合作用的规则，解决了专家评价合成问题，但是该法则并没有明确指明其实际应用范围。

证据冲突是由Dempster合成法则中的K值归一化算法设计不符合当前评价的问题所造成的，目前有许多解决证据冲突的算法，但不同的算法适合不同的证据冲突问题。

$$k = \sum_{A_i \cap B_j = \phi} m_1(A_i) m_2(B_j)$$

k表示证据间的冲突程度，K值越大，说明冲突越大

软件可信度评价模型研究

证据理论原理

证据冲突及其处理方法

首先，需要加强来自不同来源的证据数据进行预处理，对识别框架中的元素进行基本可信度分配时，在证据构建和证据融合时充分地考虑冲突上的产生问题，能够将评判人员给出的mass函数进行调整使评价人员的焦元尽量趋于一致，那么证据冲突就会很好地解决，最终达到消除悖论的目的。其次，采用基于专家权威的证据冲突处理方法，改进证据融合算法，根据专家的评价，对不同来源的证据赋予相应的权重，降低证据间的冲突。

软件可信度评价模型研究

证据理论原理

证据融合算法的改进

了降低证据冲突，需对证据进行预处理。首先审核调查问卷的基础数据，对于明显冲突的或者悖论的数据进行删除；其次，根据软件可信影响因素和指标项权重，增强权重较大的因素或指标项的可信性，使证据聚焦。

改进后的可信度分配函数为：$m'(Ai)=（w_i/w_{max}）m(Ai)$

可信度分配值：$m'(A)=\sum_{A_1,\ldots,A_n\subset\Theta} m_1'(A_1)\ldots m_n'(A_n) <1$

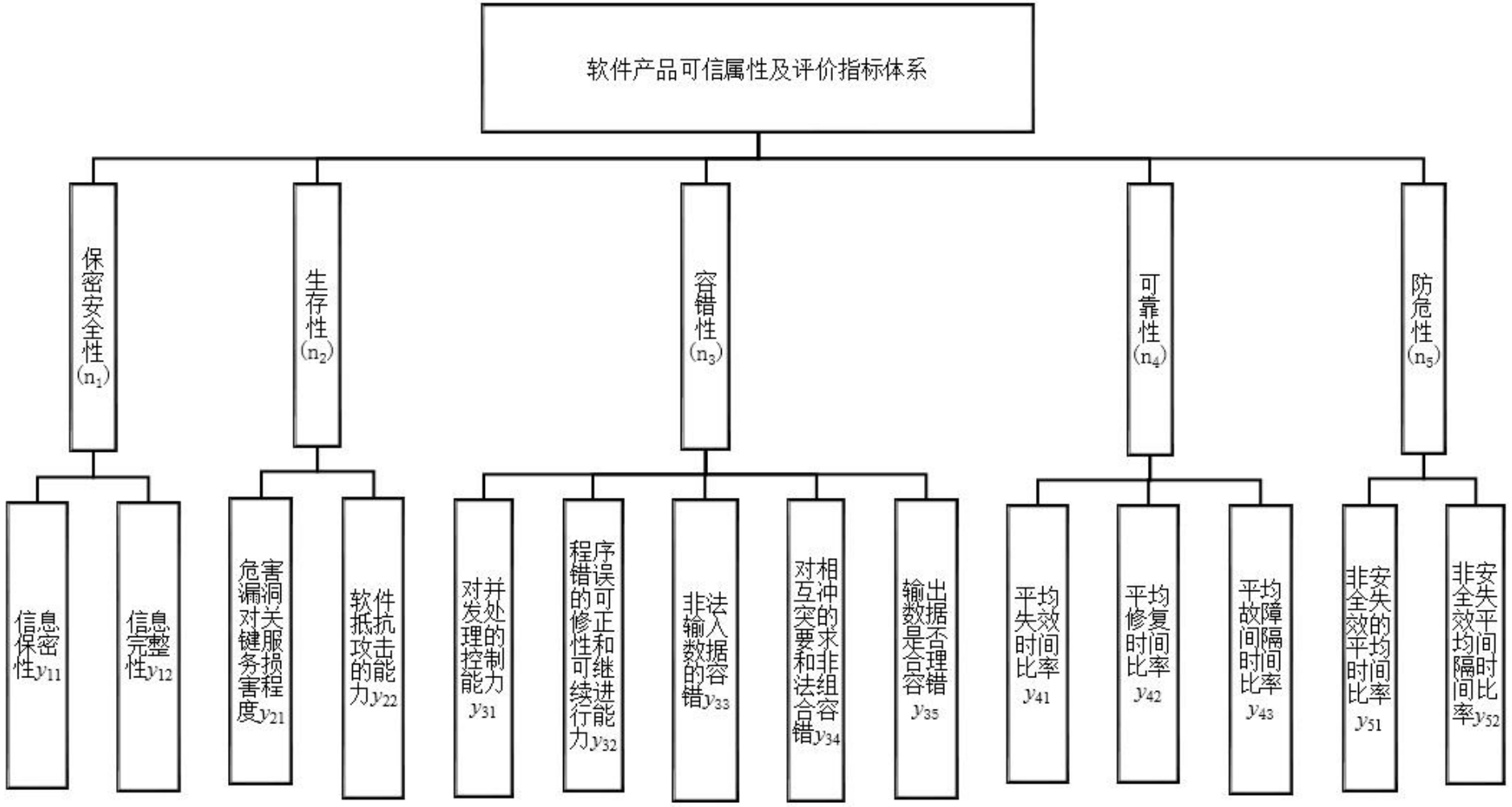
补充定义：$m'(\Theta)=1-\sum_{A_1,\ldots,A_n\subset\Theta} m_1'(A_1)\ldots m_n'(A_n)$

$m'(\Theta)$表示证据支持命题的不确定程度。

软件可信度评价模型研究

基于证据理论的软件可信评价层次模型

根据之前建立的可信软件评价指标体系，结合软件可信测度的特点，构造如图所示的软件可信评价结构模型。



软件可信度评价模型研究

软件可信评价模型案例分析

- ✓ 测度数据的获取
- ✓ mass函数的建立
- ✓ 软件可信因素和评价指标权重确定
- ✓ 软件可信证据合成

软件过程可信评价模型研究

软件可信评价模型案例分析

✓ 测度数据的获取

由于软件可信度测度模型验证，需要开发同一软件项目的开发人员、测试人员和该软件用户共同积累项目的开发书籍和反映软件运行维护的历史书籍，这些数据短时间内很难获取，采用调查问卷的方式，由软件项目开发人员、软件测试人员和软件用户，对同一软件可信评价指标进行相对可信等级(不可信、低可信、基本可信、可信、高可信)评判，收集软件可信评价的有关数据。

项目的开发人员、测试人员可以从项目开发视角评价软件的可信性，软件用户往往是软件可信的直接体验者，因此，以这三类人员作为软件可信评价模型验证数据调查对象，并要求问卷的填写者针对一个项目从开发过程到软件交付使用综合考虑软件产品的可信性。

软件过程可信评价模型研究

软件可信评价模型案例分析

✓ mass函数的建立

证据理论只是给出判别命题可信程度的推理模式，但没有给出基本可信度分配函数的一般形式。

确定可信度分配函数为命题识别框架选项出现的频率作为mass函数的形式：

$$m_i(x)=\frac{p_{i(x)}}{p},i=1,2,...,5$$

其中$p_{i(x)}$为各个可信属性和指标项在识别框架下第i个识别项出现的频率，p为可信问卷的份数。通过对调查问卷的整理分析，得到可信软件测度的基本可信度数据。

软件过程可信评价模型研究

软件可信评价模型案例分析

✓ mass函数的建立

软件测度的基本可信度数据（部分）

软件产品可信属性	软件产品可信评价指标	可信水平	不可信	低可信	基本可信	可信	高可信
保密安全性(n_1)	信息保密性 y_{11}	软件开发人员	0.0667	0.1333	0.2	0.3333	0.2667
		测试人员	0.0588	0.0588	0.1765	0.353	0.3529
		软件用户	0.0323	0.0645	0.2258	0.3226	0.3548
	信息完整性 y_{12}	软件开发人员	0	0.1333	0.2	0.3334	0.3333
		测试人员	0.0588	0	0.1765	0.4118	0.3529
		软件用户	0.0323	0.0645	0.0968	0.3871	0.4193

软件过程可信评价模型研究

软件可信评价模型案例分析

✓ 软件可信因素和评价指标权重确定

专家对软件可信影响因素和指标项的重要程度进行排序打分，应用前面章节给出的层次分析理论，计算软件产品可信因素和指标项权重，软件产品可信指标项相对于因素层和因素层相对于目标层的权重。

软件过程可信评价模型研究

✓ 软件可信因素和评价指标权重确定

软件可信属性	权重W_i	软件产品可信评价指标	权重w_{ij}
保密安全性	0.1005	信息保密性	0.2315
		信息完整性	0.7685
生存性	0.1984	危害漏洞对关键服务损害程度	0.31
		软件抵抗攻击的能力	0.69
容错性	0.2523	对并发处理的控制能力	0.1586
		程序错误可修正性和可继续执行能力	0.2184
		非法输入数据的容错能力	0.1351
		对相互冲突的要求和非法组合容错能力	0.3528
		输出数据合理的容错能力	0.1351
可靠性	0.2523	平均失效时间比率	0.3057
		平均修复时间比率	0.557
		平均故障间隔时间比率	0.1373
防危性	0.2065	非安全失效的平均时间比率	0.2315
		非安全失效平均间隔时间比率	0.7685

软件过程可信评价模型研究

软件可信评价模型案例分析

✓ 软件可信证据合成

根据D-S的基本原理和Dempster-Shafer合成法则，针对可信软件基本可信度数据中的每个指标中的3个证据，将指标可信证据融合，得到指标层的可信度数据，即指标层基本可信度分配表(下表显示部分数据)。

指标	不可信	低可信	基本可信	可信	高可信	k	W
y_{11}	0.0016	0.0063	0.0997	0.4747	0.4177	0.920048	0.2315
y_{12}	0	0	0.0323	0.5019	0.4658	0.894117	0.7685
y_{21}	0	0.0092	0.1469	0.3854	0.4585	0.917276	0.31
y_{22}	0	0.0201	0.2408	0.4181	0.321	0.924349	0.69

由于基本可信度的k值较大，说明证据存在着较大的冲突，所以，应用基于软件可信评价指标权重的冲突解决方法，根据指标项权重数据，对于软件可信指标层基本可信度分配数据进行处理，改进后的可信度分配情况如下表(部分数据)。

软件过程可信评价模型研究

软件可信评价模型案例分析

✓ 软件可信证据合成

指标层改进后的可信度分配表(部分)

指标	不可信	低可信	基本可信	可信	高可信	w_i/w_{max}	Θ
y_{11}	0.0005	0.0019	0.03	0.143	0.1258	0.301236	0.6988
y_{12}	0	0	0.0323	0.5019	0.4658	1	0
y_{21}	0	0.0041	0.066	0.1732	0.206	0.449275	0.5507
y_{22}	0	0.0201	0.2408	0.4181	0.321	1	0

改进后的可信度分配函数为：$m'(Ai)=（w_i/w_{max}）m(Ai)$

可信度分配值：$m'(A)=\sum_{A_1,\ldots,A_n\subset\Theta} m_1'(A_1)\ldots m_n'(A_n) \quad <1$

$$m'(\Theta)=1-\sum_{A_1,\ldots,A_n\subset\Theta} m_1'(A_1)\ldots m_n'(A_n)$$

Θ 表示证据支持命题的不确定程度。

软件过程可信评价模型研究

软件可信评价模型案例分析

✓ 软件可信证据合成

应用证据理论模型和基于权重的可信证据合成算法，剔除指标项的不确定性后，计算得到软件可信因素层的可信度分配情况，最后将软件可信因素的可信度分配数据，应用证据理论模型，进行合成运算，得到软件可信测度的最终结果。

指标	不可信	低可信	基本可信	可信	高可信	k
Y	0	0	0	0.4257	0.5743	0.216293

从表中看出该软件“可信”水平为42.57%，“高可信”水平为57.43%，“不可信”水平为0，表明该软件从开发过程、测试、应用维护都满足基本要求，软件可信整体水平较高。证据的冲突程度k=0.216293，表明问卷的一致性较好。

谢谢大家！