

# Process Trustworthiness as a Capability Indicator for Measuring and Improving Software Trustworthiness

Ye Yang, Qing Wang, Mingshu Li

Lab for Internet Software Technology  
Institute of Software Chinese Academy of Sciences

2009-5-16

# Outline

- Background and Motivations
- Collaborative Research Project
- Process Trustworthiness
- Towards the Trustworthy Process Management Framework

# Background

- New characteristics of software production
  - Globally distributed development
  - Largely reusing commercial or open-source third-party products/assets
  - Increasing needs for software criticality and dependability
- Sources of software failures
  - Wrong/incomplete/volatile requirements
  - Inexperienced developers introducing errors
  - Low confidence in V&V activities
  - ...
- As software size and complexity increase dramatically, assessing and improving software trustworthiness become more and more challenging.
- It is always too late till the software is produced.
  - Needing a process-oriented approach to guide trusted software development

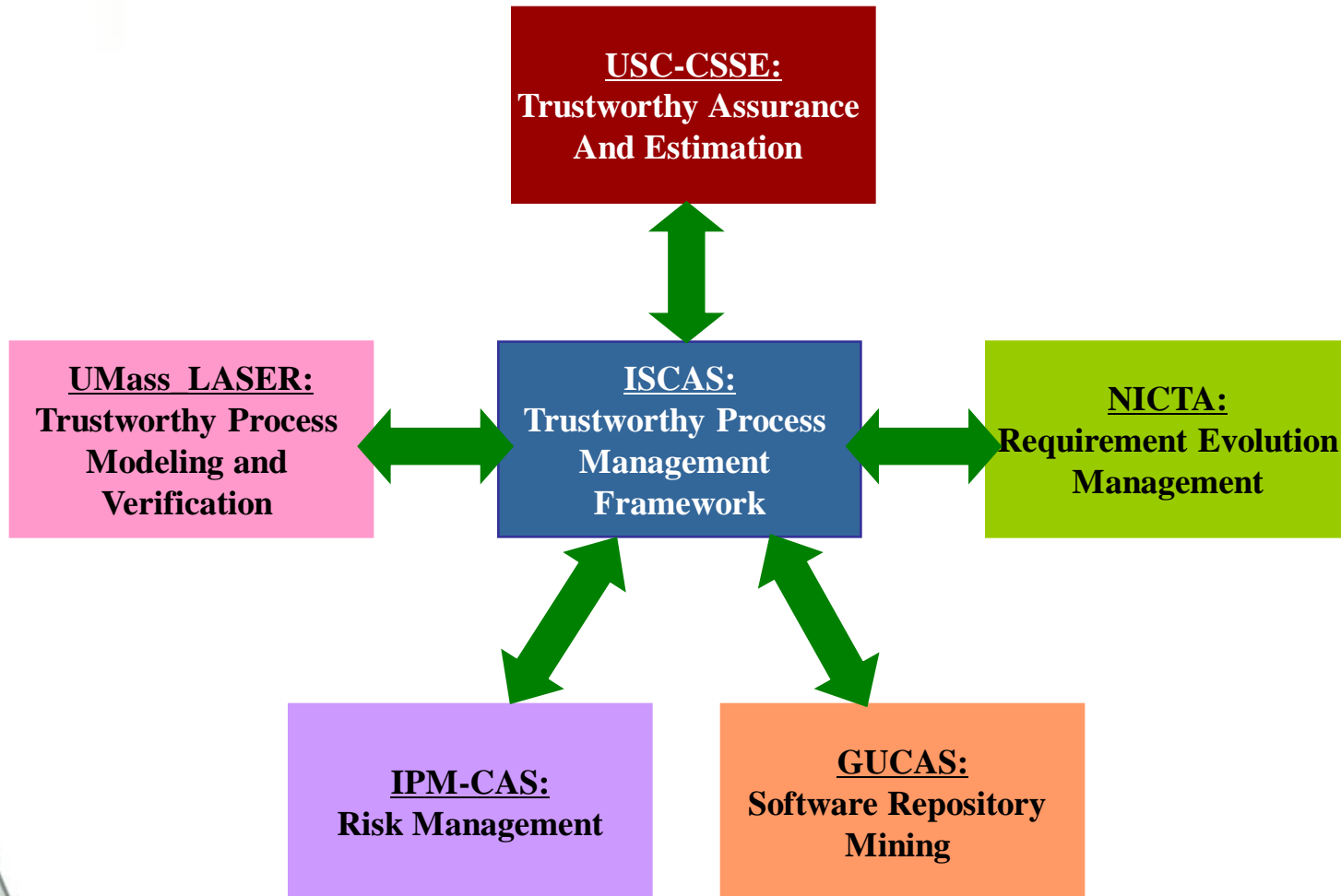
# Motivations

- Currently lack of common understanding on trusted software development
  - Properties are scattered and studied individually
    - Security, Reliability, Safety, Quality, etc.
- No definitive scope of software trustworthiness
  - Lack of evidence for evaluation and comparison
- Lack of systematic approaches in measuring and improving process capability in producing trusted software.

# A Collaborative Research Project

- Research on Trustworthy Software Process Management and Risk Control Models and Methods (2008-2010)
  - Funded by NSF of China,
- Collaborated by 6 univ./institutes
  - Institute of Software Chinese Academy of Sciences (ISCAS)
  - Center for Systems and Software Engineering at the University of Southern California (USC-CSSE)
  - Laboratory for Advanced Software Engineering Research at the University of Massachusetts (UMass-Laser)
  - Empirical Software Engineering Group at the Australia's Information and Communications Technology Centre of Excellence (NICTA)
  - Institute of Policy and Management Chinese Academy of Sciences
  - Graduate University Chinese Academy of Sciences

# Collaboration Structure



# Research Progress

- Trustworthiness-related literature review
- Proposal of Process Trustworthiness
  - as a capability indicator to measure the relative degree of confidence for certain software process to deliver a trustworthy product
- Proposal of a Trustworthy Process Management Framework
  - to demonstrate the conceptual structure in establishing and managing the process trustworthiness for assessing and

# Literature Review on Major Trustworthiness Influencing Factors

- Goal
  - Compare the difference of understanding about trustworthiness in different research communities and application fields.
  - Establish a unified understanding and concept in our research project
- Eight in-depth analyzed international standards and models
  - Trusted Software Methodology (TSM)
  - Common Criteria (CC)
  - System Security Engineering- CMM (SSE-CMM)
  - Software Assurance for Project Management (SA-PM)
  - Software Security Assurance (SSA)
  - Safety and Security Extension for Integrated CMM (iCMM)
  - ISO 27000
  - ISO 9126

# Summary of Results from Literature Review

Standards/Models	Trustworthiness Attributes	Related process work products	Measure/Appraisal guideline
TSM	all quality attributes	44 Trust Principles	6 Trust Classes
CC	security	appraisal objects, security requirements, EAL	7 EAL level
Software Assurance	Functionality, reliability, safety, security	Apply mature methods and processes such as Microsoft Trusted Computing, SDL	Apply different measure and assess methods, e.g. COSECMO and PSM
iCMM	Safety, security	Extension of Application Area on Security and Safety: 4 Application Practice Goals	CMMI Appraisal Method
SSE-CMM	security	22 security related practices	6 security capability levels
ISO 9126	all quality attributes	6 Major Characteristics	internal quality, external quality, usage quality and relevant metrics
ISO 27000 2009-6-1	security	Information security management model and practice guideline	-

# TSM

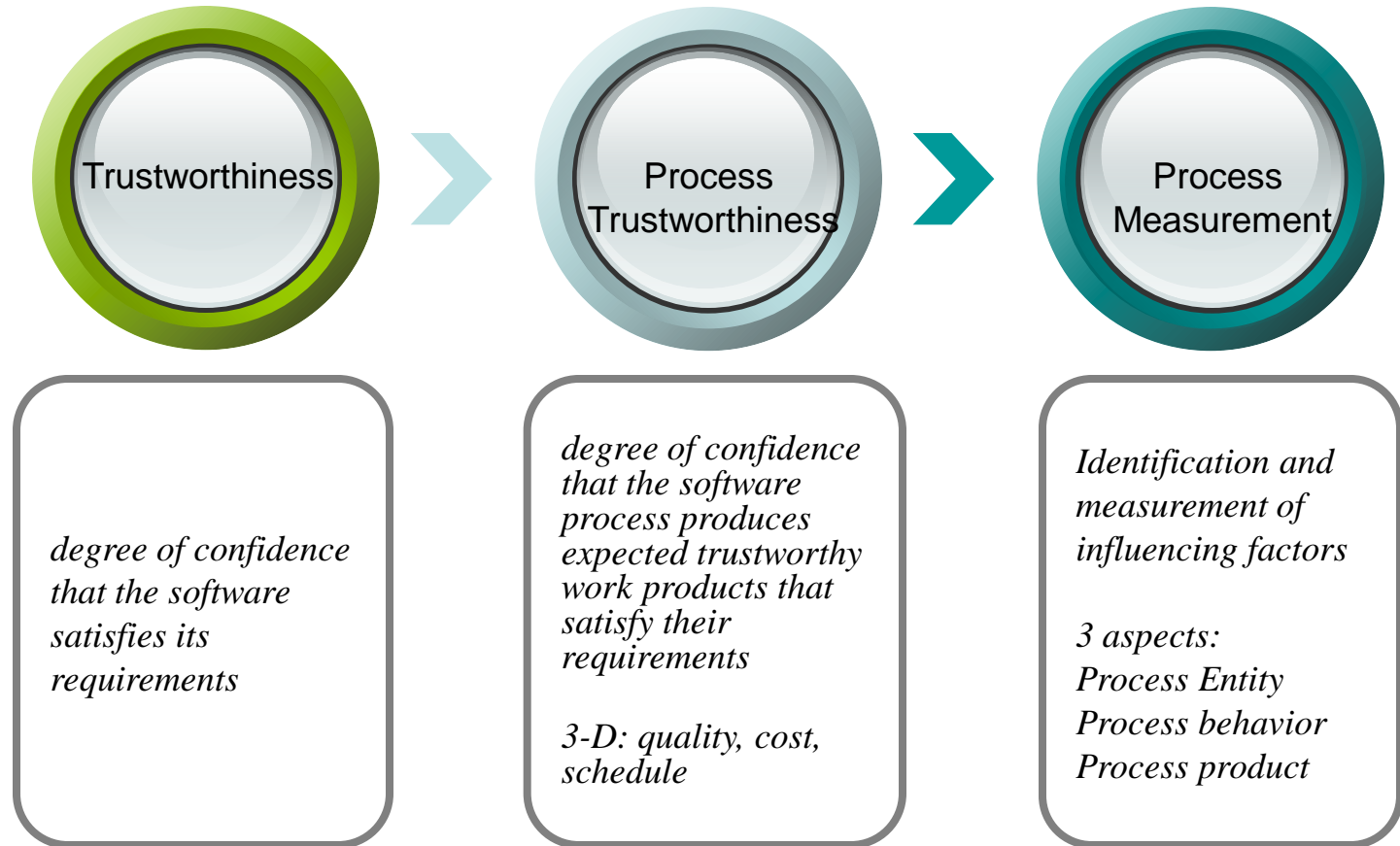
- Trustworthy Software Methodology
  - Software trustworthiness highly depends on
    - Management decisions
    - Technical decisions
    - Specified set of requirements
  - First introduced the process-oriented approach

Source: E. Amoroso, C. Taylor, J. Watson, J. Weiss: A process-oriented methodology for assessing and improving software trustworthiness. Proceedings of the 2nd ACM Conference on Computer and communications security. Virginia, USA, 1994, pp.39 – 50.

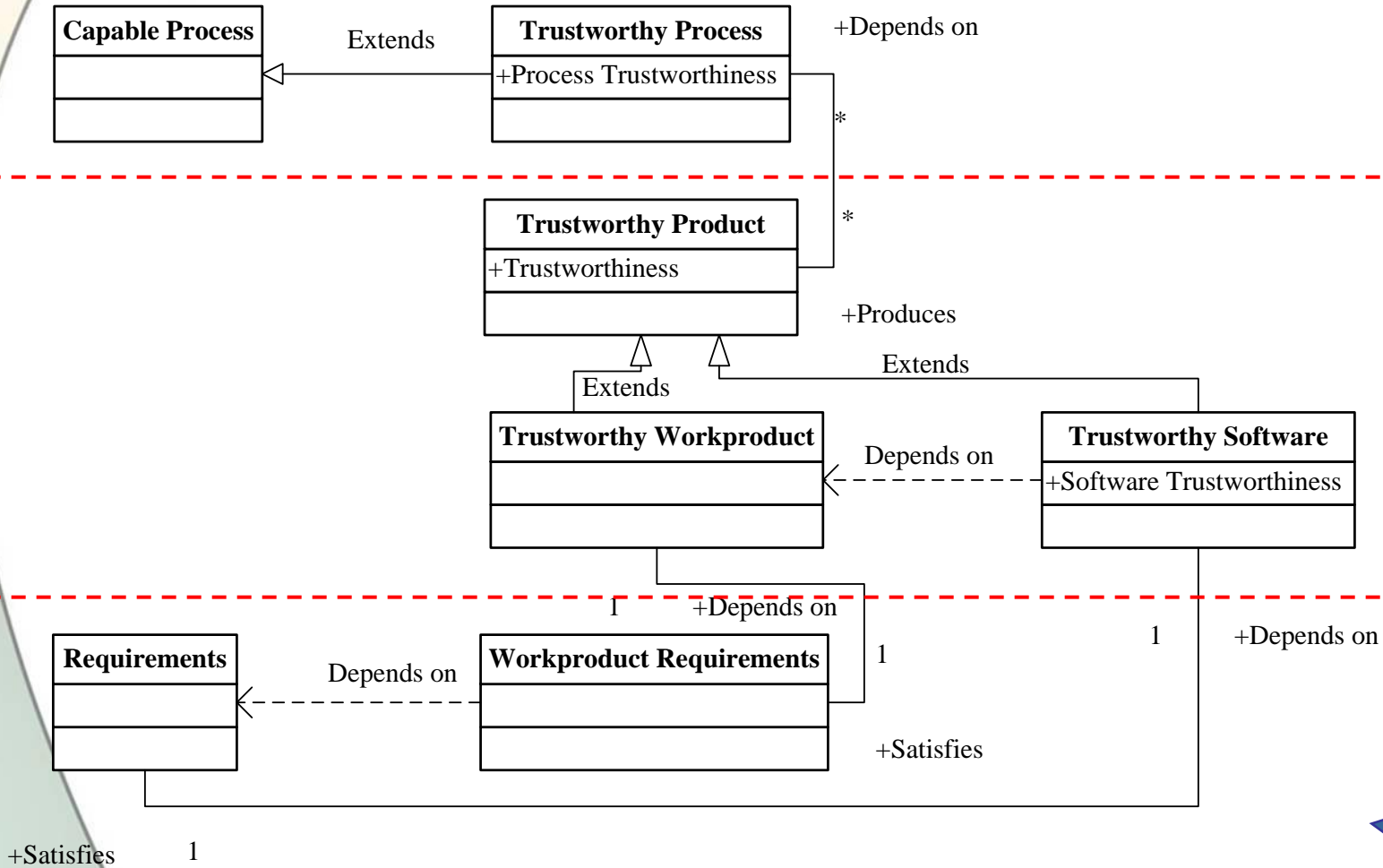
# Basic Definitions

- Trustworthiness as “*level of confidence or degree of confidence*”
- **Software Trustworthiness** as “*degree of confidence that the software satisfies its requirements*”
  - **Trustworthy Product (i.e. work product, software)** as a product (*i.e. work product, software*) that satisfies a range of its *trustworthiness objectives established based on its requirements.*
- **Process Trustworthiness** is the *degree of confidence that the software process produces expected trustworthy work products that satisfy their requirements.*
  - **Trustworthy Process** is a *capable process that produces a range of trustworthy products.*

# Modeling the Measurement of Trustworthiness



# Meta-Model of a Trustworthy Process



**Conclusion:  
Assessment  
results**



**Confidence:  
Evidence  
Expertise**



**Context:  
Explicit**

+Satisfies 1

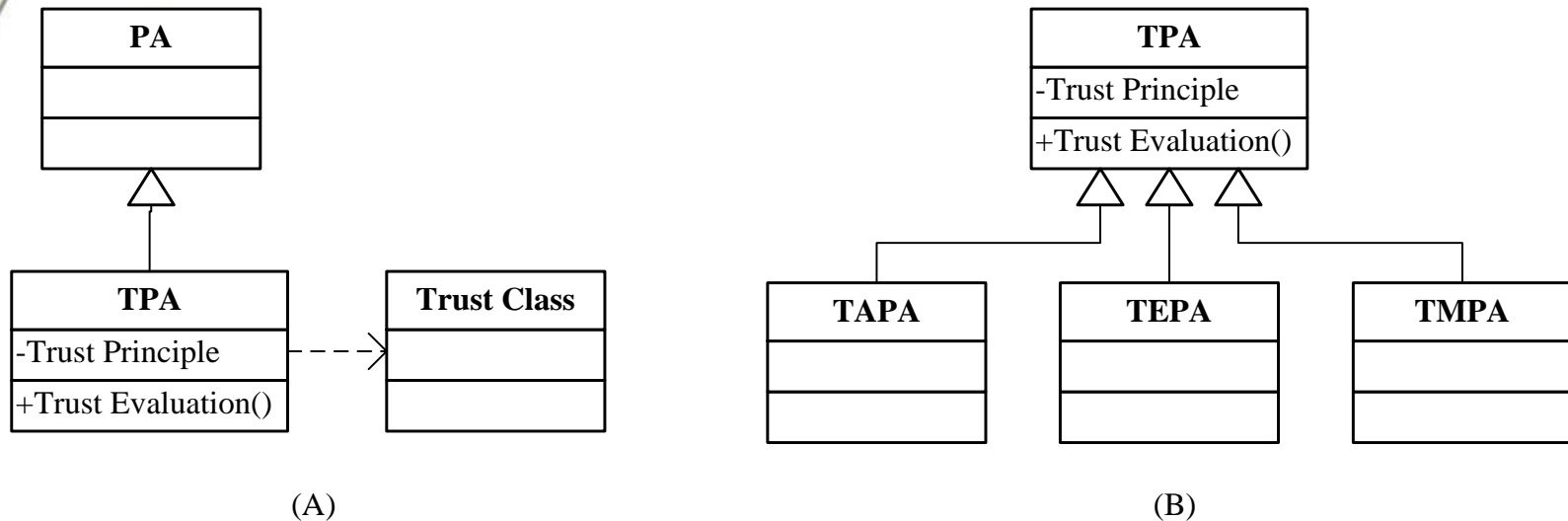
# Modeling Software Trustworthiness

- Software trustworthiness = ( $\{\text{Attribute}\}$ ,  $\{\text{Traceability}\}$ ,  $\{\text{Objective}\}$ ,  $\{\text{Priority}\}$ ), where
  - Attribute set is a subset of critical quality attributes extracted from software requirements, e.g. a subset tailored from the list of characteristics or sub-characteristics defined in ISO 9126;
  - Traceability set reflects the mapping between an attribute and the original requirements;
  - Objective set is a target profile of trustworthiness level (either qualitative or quantitative) for each attribute defined in  $\{\text{Attribute}\}$ ;
  - Priority set captures the relative degree of importance for each attribute of the end product meeting its trustworthiness objective.

# Modeling Processes Trustworthiness

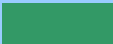

- Process Area (PA) concept from CMMI:
  - a cluster of related practices that, when implemented collectively, satisfy a set of goals considered important for making improvement in that area
- Trustworthy Process Areas (TPAs):
  - integrate trust principles, trust levels, and evaluation methods from TSM with PAs from CMMI
- Benefits:
  - to include provision for a specific development process to deal with untrustworthy process factors, e.g. less capable or malicious developers;
  - to provide an organizational improvement infrastructure for process trustworthiness.

# Trustworthy Process Areas



- TAPA: Trustworthy Assurance Process Area
- TEPA: Trustworthy Engineering Process Area
- TMPA: Trustworthy Monitoring Process Area

# Assessment Framework - Matching Trust Principles with Process Areas

		T0	T1	T2	T3	T4	T5
Trustworthiness Assurance Process Areas	Auditing	Green	Green	Green	Green	Orange	Orange
	Identification & Authentication	Green	Green	Orange	Orange	Orange	Orange
	Authorization	Green	Green	Green	Orange	Blue	Blue
	Multi-person Control	Green	Green	Green	Green	Orange	Blue
	Trust Path	Green	Green	Green	Green	Orange	Blue
	...	Green	Blue	Blue	Blue	Blue	Blue
Trustworthiness Engineering Process Areas	Trustworthy Requirement	Green	Orange	Orange	Orange	Orange	Blue
	Trustworthy Design	Green	Orange	Orange	Orange	Orange	Orange
	Trustworthy Implementation	Green	Orange	Orange	Orange	Orange	Orange
	Trustworthy Test	Green	Orange	Orange	Orange	Orange	Orange
	Formal Methods	Green	Green	Green	Green	Orange	Orange
	...	Green	Blue	Blue	Blue	Blue	Blue
Trustworthiness Monitoring Process Areas	Project Management	Green	Orange	Orange	Orange	Blue	Blue
	Risk Management	Green	Orange	Orange	Orange	Blue	Blue
	Configuration Management	Green	Green	Orange	Blue	Blue	Blue
	Review	Green	Orange	Orange	Orange	Blue	Blue
	V&V	Green	Green	Orange	Blue	Blue	Blue
	...	Green	Blue	Blue	Blue	Blue	Blue
Legend		 No Requirement		 Additional Requirement			

# Trustworthy Process Model Structure

## Trustworthy Framework

### Trust Assurance

Trustworthy Goal

Goal Description

Human Dependability  
Characteristics

Behavioral Assurance  
Process/Tasks

Artifacts Guarantee  
Products/Documents

### Trust Enhancement

Trustworthy Goal

Goal Description

Human Dependability  
Characteristics

Behavioral Assurance  
Process/Tasks

Artifacts Guarantee  
Products/Documents

### Trust Support

Trustworthy Goal

Goal Description

Human Dependability  
Characteristics

Behavioral Assurance  
Process/Tasks

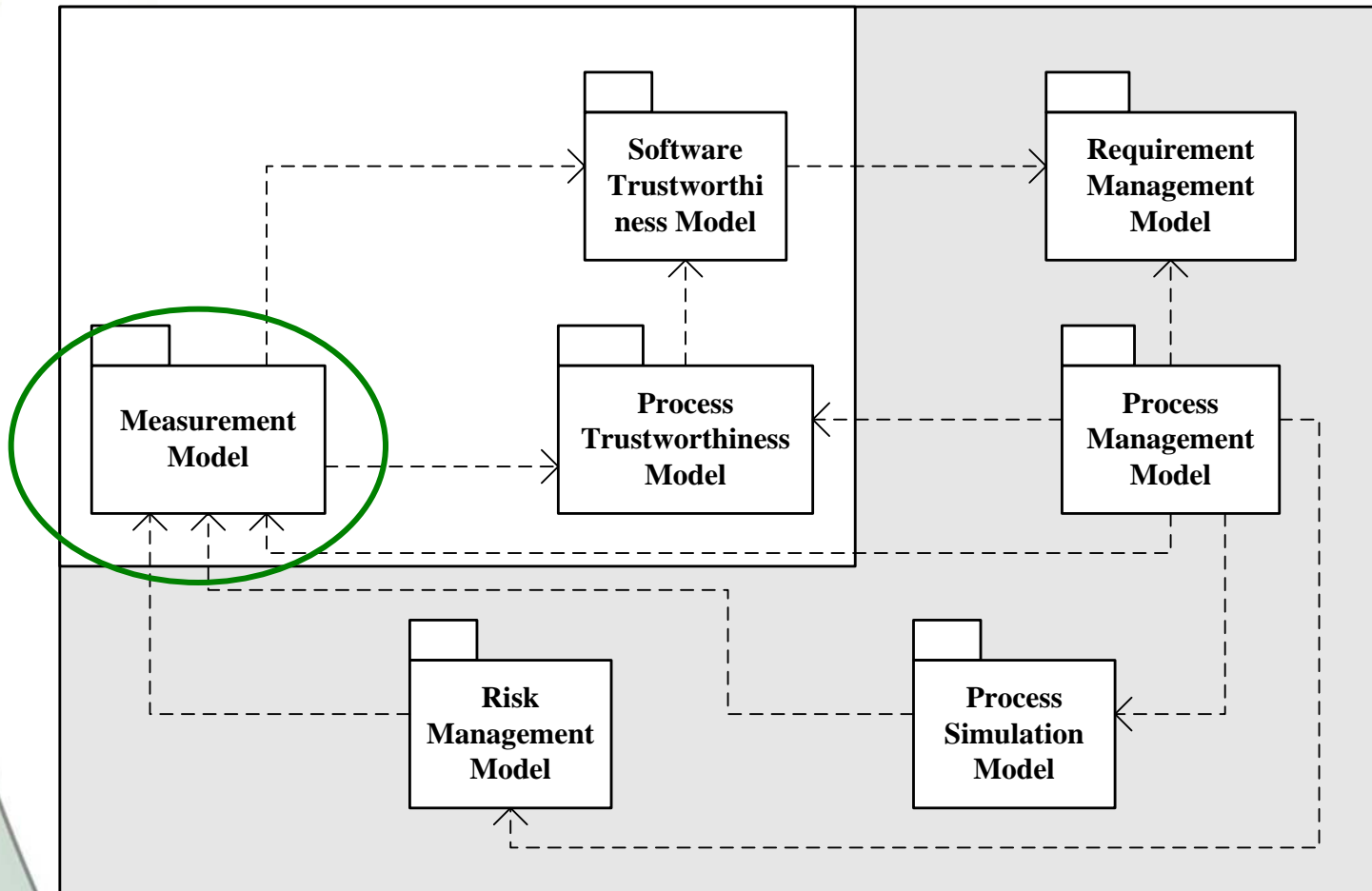
Artifacts Guarantee  
Products/Documents

# Software Process Trustworthiness Attribute and Measurement Model

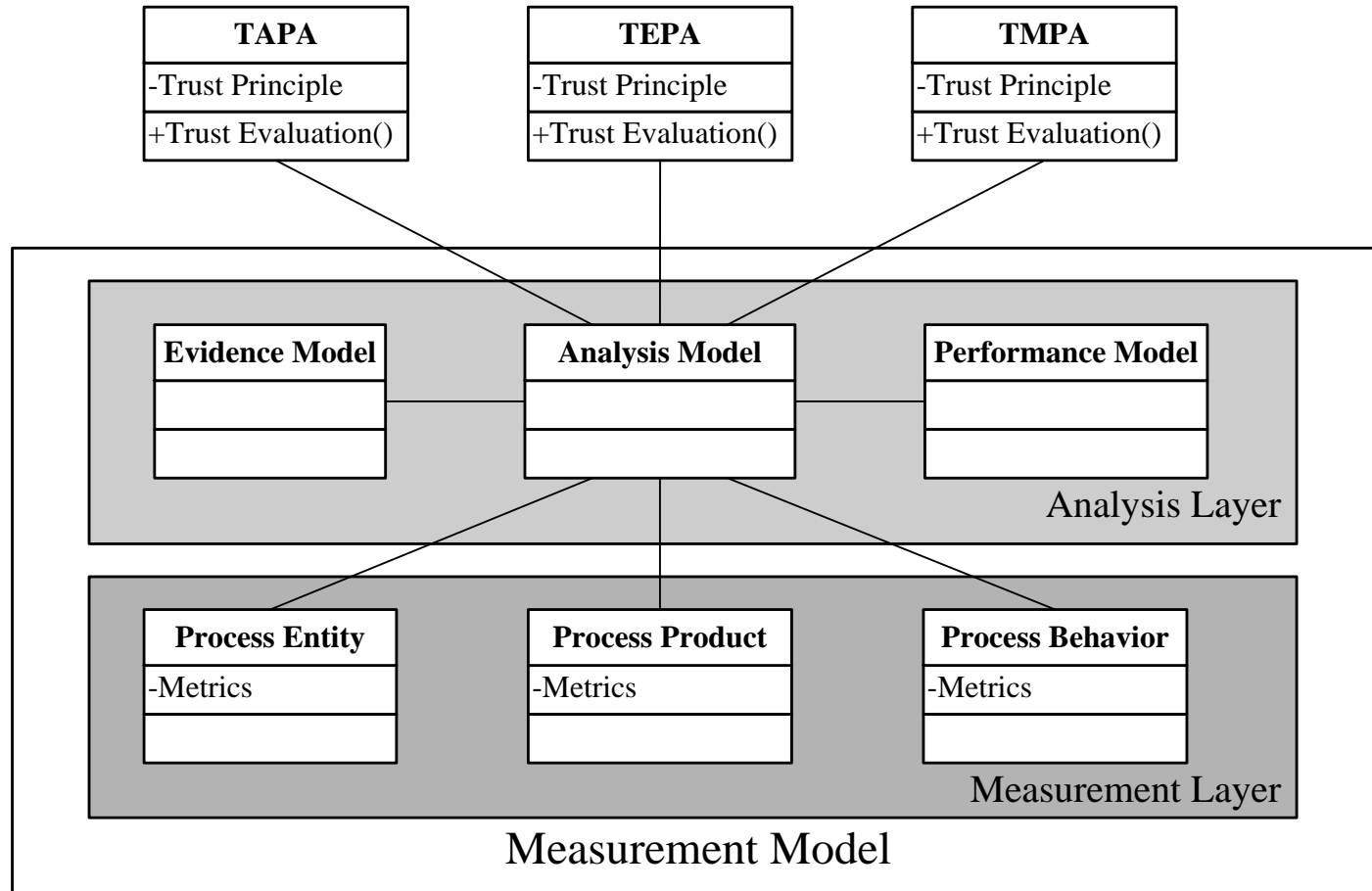
- Establish software process and product trustworthiness attributes and measurement model from three dimensions and three aspects respectively
- Reference
  - ISO 9126
  - PSM, COCOMO

Dimensions \ Aspects	Quality	Cost	Schedule
Process Entity	7	11	1
Process Behavior	33	17	11
Process Product	37	12	0

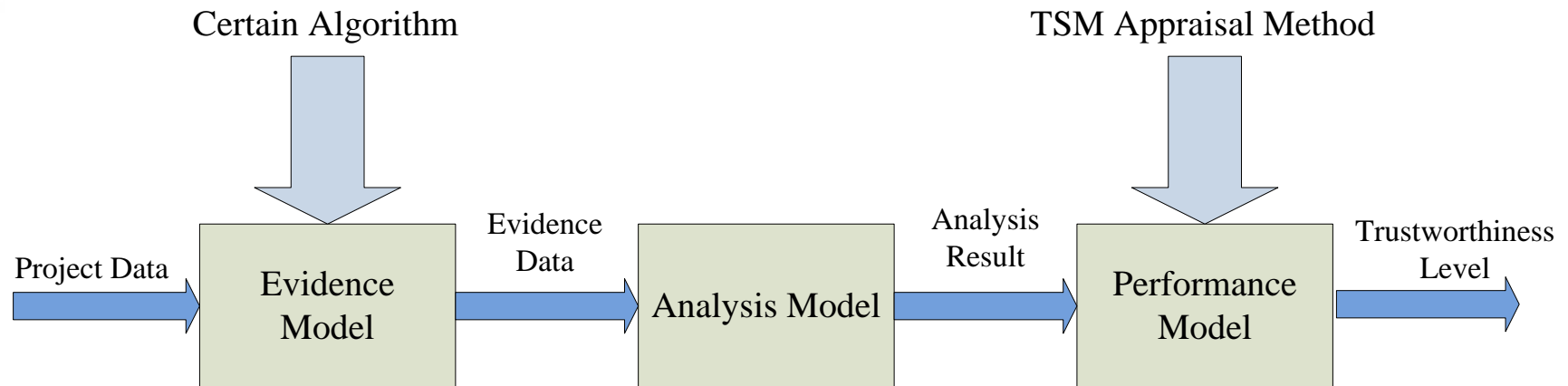
# Trustworthy Process Management Framework



# Trustworthiness Measurement Model



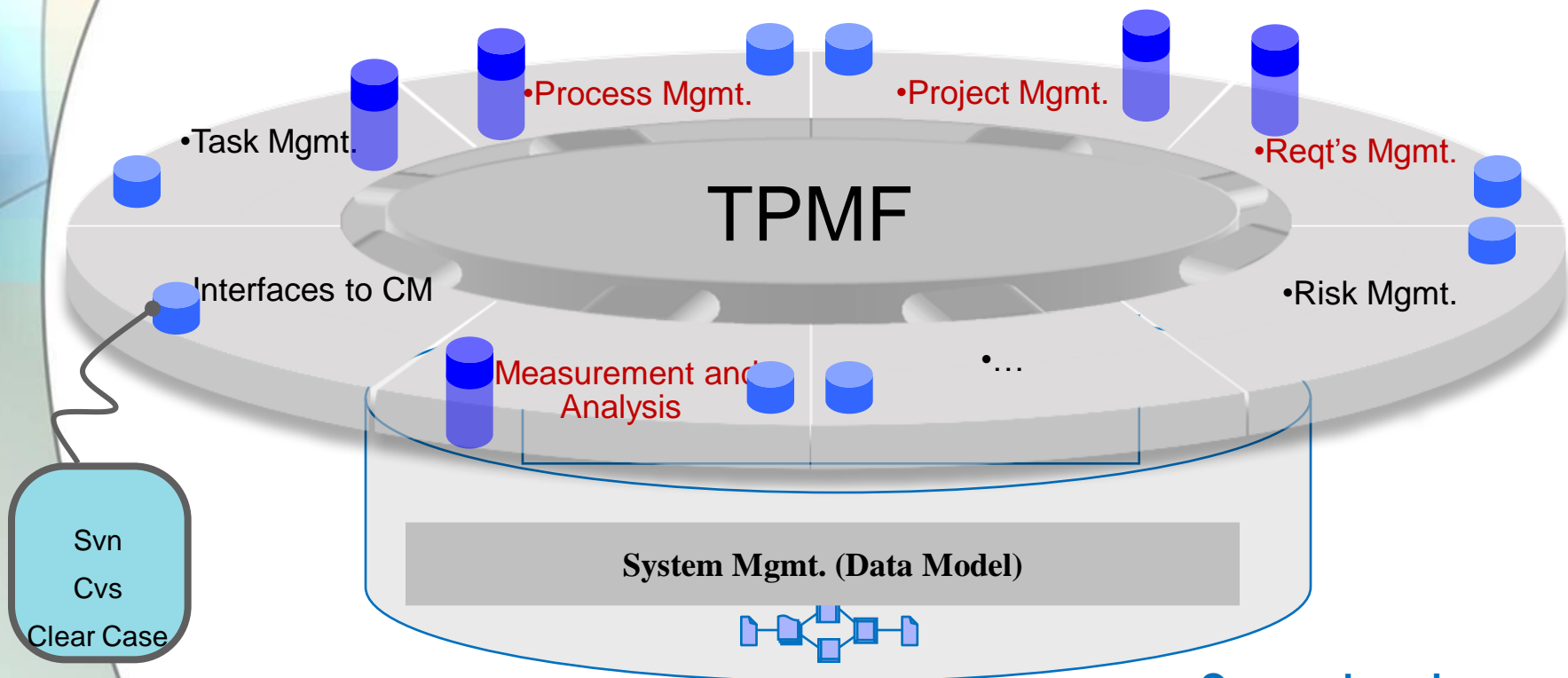
# Assessing Process Trustworthiness



# System Architecture of TPMF

Collaborative Environment

Rich Component Base



Open Interfaces

Comprehensive Data Model

# Tailoring the Measurement Model

度量指标体系				
列表格式 树形格式				
<input type="checkbox"/> 类别 <input type="checkbox"/> 工作量 <input type="checkbox"/> 层次 <input type="checkbox"/> 个人 <input type="button" value="查询"/> <input type="button" value="自定义指标"/> <input type="button" value="刷新"/>				
类别\层次	个人	任务	阶段	项目
工作量	<input checked="" type="checkbox"/> 各成员工作量偏差	<input checked="" type="checkbox"/> 各任务工作量偏差	<input checked="" type="checkbox"/> 各阶段投入相关项目工作量比率 <input checked="" type="checkbox"/> 各阶段工作量偏差 <input checked="" type="checkbox"/> 各阶段工作量比率 <input checked="" type="checkbox"/> 各阶段工作量按任务类型分布 <input checked="" type="checkbox"/> 各类型任务工作量按阶段分布	<input checked="" type="checkbox"/> 投入相关项目工作量比率 <input checked="" type="checkbox"/> 项目工作量偏差 <input checked="" type="checkbox"/> 相关项目投入工作量比率 <input checked="" type="checkbox"/> 各类型任务工作量偏差 <input checked="" type="checkbox"/> 各类型任务工作量比率
进度		<input checked="" type="checkbox"/> 任务进度偏差	<input checked="" type="checkbox"/> 阶段进度偏差 <input checked="" type="checkbox"/> 里程碑进度偏差	<input checked="" type="checkbox"/> 项目进度偏差
挣值		<input checked="" type="checkbox"/> 任务完成情况 <input checked="" type="checkbox"/> 成本/进度性能 <input checked="" type="checkbox"/> 成本/进度预测 <input checked="" type="checkbox"/> 挣值		
成本				<input checked="" type="checkbox"/> 项目成本偏差
生产率		<input checked="" type="checkbox"/> 任务生产率	<input checked="" type="checkbox"/> 阶段生产率	<input checked="" type="checkbox"/> 各类型工作产品生产率 <input checked="" type="checkbox"/> 项目平均生产率
评审缺陷	<input checked="" type="checkbox"/> 个人缺陷发现效率	<input checked="" type="checkbox"/> 各评审报告缺陷发现效率 <input checked="" type="checkbox"/> 各评审报告效率 <input checked="" type="checkbox"/> 各评审报告缺陷密度 <input checked="" type="checkbox"/> 各评审报告缺陷分类比率	<input checked="" type="checkbox"/> 各阶段评审缺陷分类比率 <input checked="" type="checkbox"/> 各阶段缺陷密度 <input checked="" type="checkbox"/> 各阶段评审缺陷平均关闭天数	<input checked="" type="checkbox"/> 评审效率 <input checked="" type="checkbox"/> 缺陷清除效率DRE <input checked="" type="checkbox"/> 评审缺陷发现效率 <input checked="" type="checkbox"/> 评审缺陷密度 <input checked="" type="checkbox"/> 评审缺陷平均关闭天数 <input checked="" type="checkbox"/> 评审缺陷分类比率
测试BUG	<input checked="" type="checkbox"/> 个人测试BUG发现效率	<input checked="" type="checkbox"/> 各测试报告效率 <input checked="" type="checkbox"/> 各测试报告BUG发现效率 <input checked="" type="checkbox"/> 各测试报告BUG分类比率 <input checked="" type="checkbox"/> 各测试报告BUG密度 <input checked="" type="checkbox"/> 各测试报告BUG发现趋势(报告期) <input checked="" type="checkbox"/> 各测试报告各严重程度BUG比率 <input checked="" type="checkbox"/> 各测试报告各严重程度的BUG关闭天数 <input checked="" type="checkbox"/> 各测试报告遗留BUG比率 <input checked="" type="checkbox"/> 各测试报告遗留BUG密度	<input checked="" type="checkbox"/> 各阶段测试效率 <input checked="" type="checkbox"/> 各阶段BUG分类比率 <input checked="" type="checkbox"/> 各阶段测试BUG密度 <input checked="" type="checkbox"/> 各阶段各严重程度BUG比率 <input checked="" type="checkbox"/> 各阶段BUG发现趋势 <input checked="" type="checkbox"/> 各阶段各严重程度的BUG关闭天数 <input checked="" type="checkbox"/> 各阶段BUG发现效率 <input checked="" type="checkbox"/> 各阶段遗留BUG比率 <input checked="" type="checkbox"/> 各阶段遗留BUG密度	<input checked="" type="checkbox"/> 测试效率 <input checked="" type="checkbox"/> 测试BUG发现效率 <input checked="" type="checkbox"/> 测试BUG分类比率 <input checked="" type="checkbox"/> BUG发现趋势 <input checked="" type="checkbox"/> 各严重程度BUG比率 <input checked="" type="checkbox"/> BUG发现趋势(日) <input checked="" type="checkbox"/> 测试BUG密度 <input checked="" type="checkbox"/> 遗留BUG比率 <input checked="" type="checkbox"/> 遗留BUG密度 <input checked="" type="checkbox"/> 各严重程度BUG关闭天数 <input checked="" type="checkbox"/> BUG关闭天数
需求			<input checked="" type="checkbox"/> 需求变更趋势(按阶段) <input checked="" type="checkbox"/> 各阶段需求变更频率	<input checked="" type="checkbox"/> 需求变更比率
过程符合性				<input checked="" type="checkbox"/> NC发生趋势(按报告期) <input checked="" type="checkbox"/> NC总数、关闭的NC数 <input checked="" type="checkbox"/> NC按所属过程分布 <input checked="" type="checkbox"/> NC增长趋势(按报告期) <input checked="" type="checkbox"/> NC按严重程度分布
规模		<input checked="" type="checkbox"/> 各工作产品规模偏差 <input checked="" type="checkbox"/> 自定义指标Affds	<input checked="" type="checkbox"/> 各阶段工作产品规模偏差	<input checked="" type="checkbox"/> 软件规模偏差 <input checked="" type="checkbox"/> 各类产品规模偏差
返工	<input checked="" type="checkbox"/> 个人各类BUG返工工作量比率 <input checked="" type="checkbox"/> 个人BUG修改效率		<input checked="" type="checkbox"/> 各阶段各类BUG修改效率 <input checked="" type="checkbox"/> 各阶段各类BUG解决工作量比率 <input checked="" type="checkbox"/> 各阶段BUG平均修改效率	<input checked="" type="checkbox"/> 返工工作量比率 <input checked="" type="checkbox"/> 各类BUG修改效率 <input checked="" type="checkbox"/> 各类BUG解决工作量比率 <input checked="" type="checkbox"/> BUG平均修改效率
任务	<input checked="" type="checkbox"/> 个人报告遗漏率	<input checked="" type="checkbox"/> 任务报告遗漏率 <input checked="" type="checkbox"/> 已完成任务比率 <input checked="" type="checkbox"/> 延期任务比率		

全选

# Measurement Analysis Results

度量报告

度量报告名称: QMP3.0测试总结报告 *	报告提交日期: 2007-05-19	度量时间段: 2007-03-10 到 2007-05-18
度量所处阶段: <input type="checkbox"/> 需求阶段 <input type="checkbox"/> 3.0版设计阶段 <input type="checkbox"/> 3.0版编码阶段 <input checked="" type="checkbox"/> 测试/debug <input type="checkbox"/> 3.1版策划 <input type="checkbox"/> 项目管理 <input type="checkbox"/> 技术支持和维护 <input type="checkbox"/> 2.0版		

度量指标名称	筛选条件	默认图表类型	CL	UCL	LCL
遗留BUG密度		表格			
遗留BUG比率		柱状图及折线图			
测试BUG密度		表格			

度量基线筛选: 0518用于制作QMP3.0测试过程及产品质里度量报告

测试BUG

遗留BUG密度  
 ... ..

遗留BUG比率  


测试BUG密度  
 ... ..

BUG发现趋势(日)  


各严重程度BUG比率  


问题分析与建议

附件 [增加附件](#)

带\*的数据项为必填项

打印

保存

刷新图形区

返回

# Process Performance Analysis

第七步：生成PCB

PCB报告名称: 生产率测试

说明: [ ]

项目特征类型: WEB开发类型项目 质量管理类型项目 底层系统软件 应用软件项目 客服销售类 研究型项目 其他项目 测试项目

度量指标: 各成员工作量偏差 控制图 XmR图

数据列为: 计划工作量(人时)

宽度: 1228 高度: 614 提交



# Conclusions

- We introduced an on-going research that may guide both researchers and industry practitioners to understand software trustworthiness in a clear and unified manner
- We also provided detailed structure that set up a common framework to describe and manage the various aspects for trustworthiness
- We are developing a toolkit to facilitate the management and assessment of process trustworthiness

Thank You!