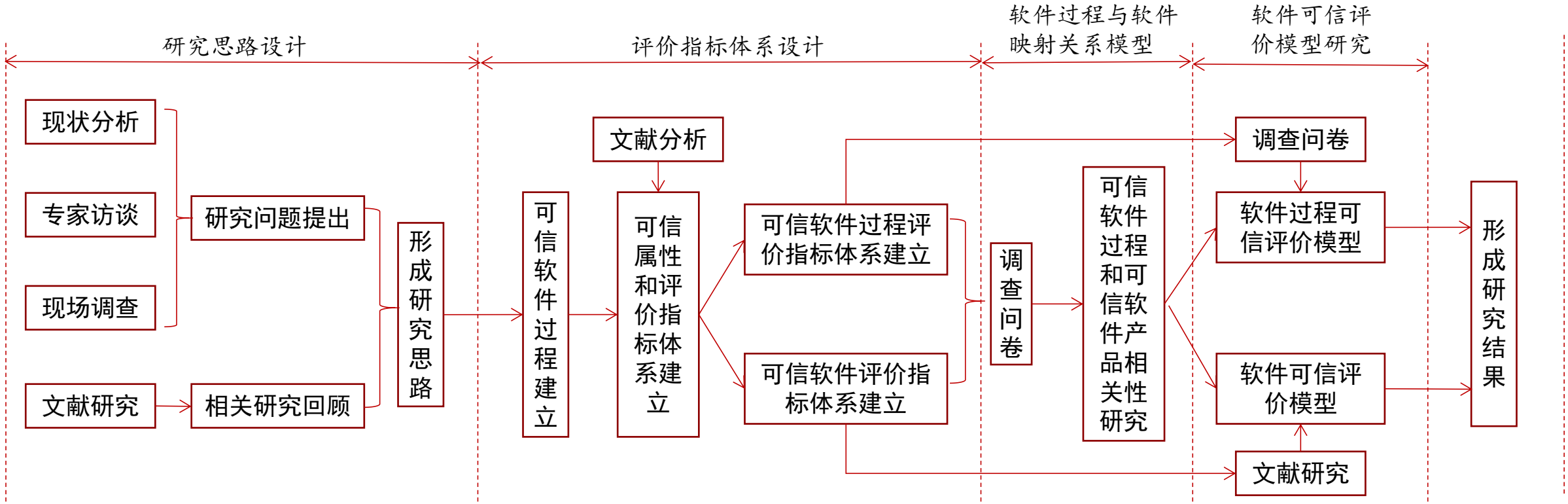
第二讲 可信软件相关研究

高可信软件工程

2.1 可信软件评价研究框架



2.2 可信软件过程研究

• 2.2.1可信软件过程定义

可信软件过程是在约定的成本和进度计划的前提下，软件过程实体通过合理的软件过程行为，有效的识别规避软件项目风险，通过生成可信的软件过程阶段性产品，最终完成可信软件产品开发任务的一系列软件开发活动及可信软件过程，过程的可信性即过程的有效性。

2.2 可信软件过程研究

• 2.2.2可信软件过程风险管理

软件过程风险是在软件开发过程中可能会影响软件产品可信的任何因素。

风险管理是指监控风险与在风险发生之前，分析、发现、控制、规避或转移风险的持续不断的软件开发活动，是可信软件项目过程管理的必要组成部分。成功的软件项目开发团队应努力在风险发生之前发现风险，并实施合理的风险规避策略，达到防患于未然的目的。

软件开发过程风险是导致软件不可信的主要原因

2.2 可信软件过程研究

- 风险管理模型
  - **瀑布模型与软件风险**

    对于需求变化频繁的软件风险极大
  - **原型模型与软件风险**

    适合需求变化大的情况，但缺乏严格的分析、设计和系统性，易造成低质量软件

    对于复杂大型软件系统构建原型较为困难

    原型需反复修改，用户不耐心
  - **演化软件过程模型与软件风险**

    是经过多次过程而演化出来的，是一种迭代的方法

    有：增量模型，螺旋模型，构建组装模型，并行开发模型
  - **面向对象方法与软件风险**

    与人类思维方式一致，产品稳定性好，易于测试维护

    需高级软件环境和开发工具支持

    不适宜大型、对象多、关系复杂的软件开发

2.2 可信软件过程研究

⑩ 统一软件开发过程与软件风险

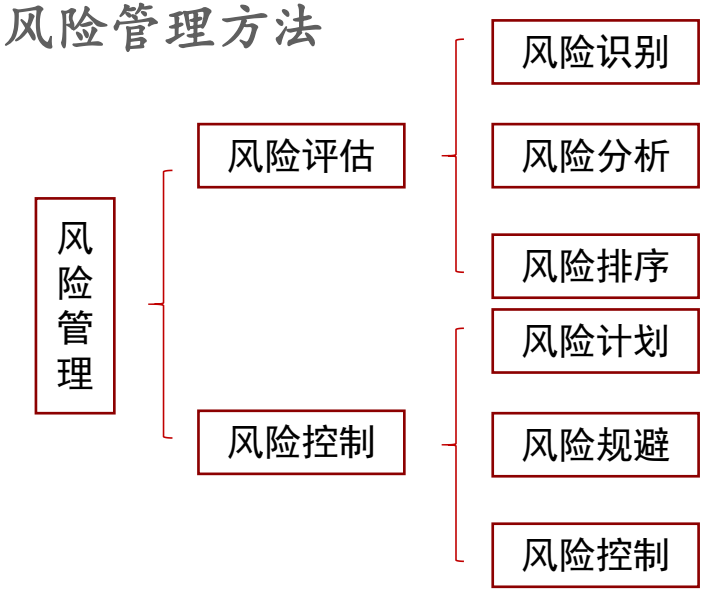
使用UML构建软件蓝图

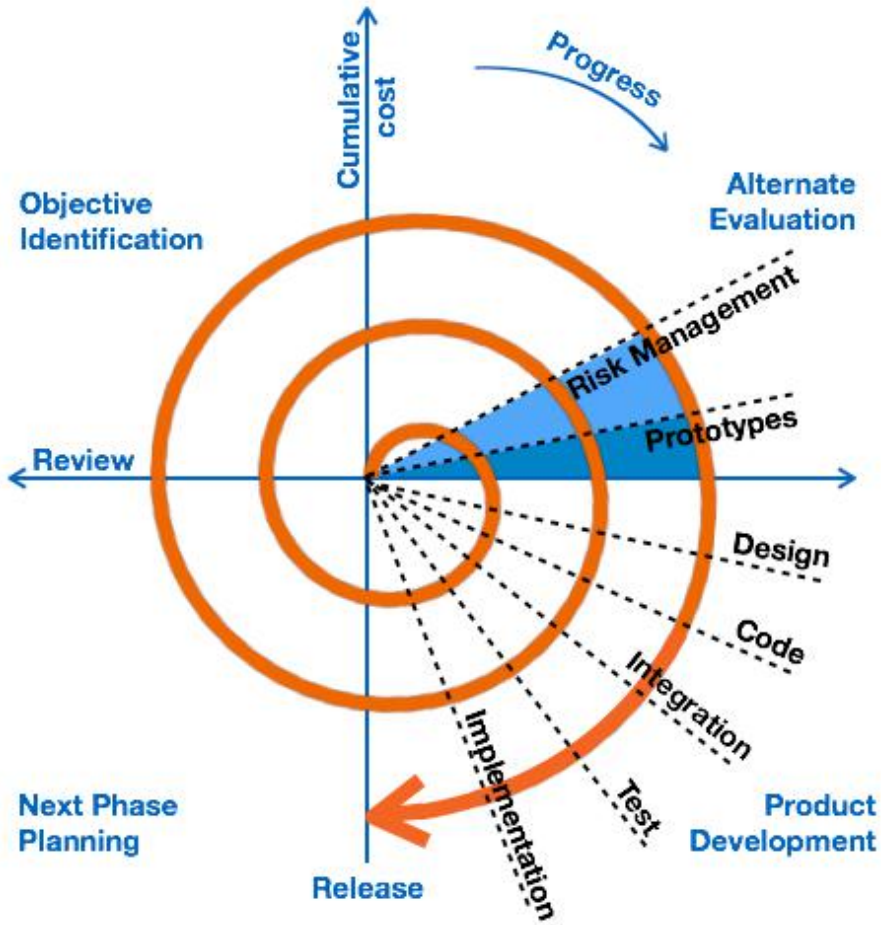
用例驱动、以架构为中心、迭代和增量的开发过程

➢ Barry Boehm的风险管理理论

螺旋模型将风险管理带入软件开发过程

风险管理方法

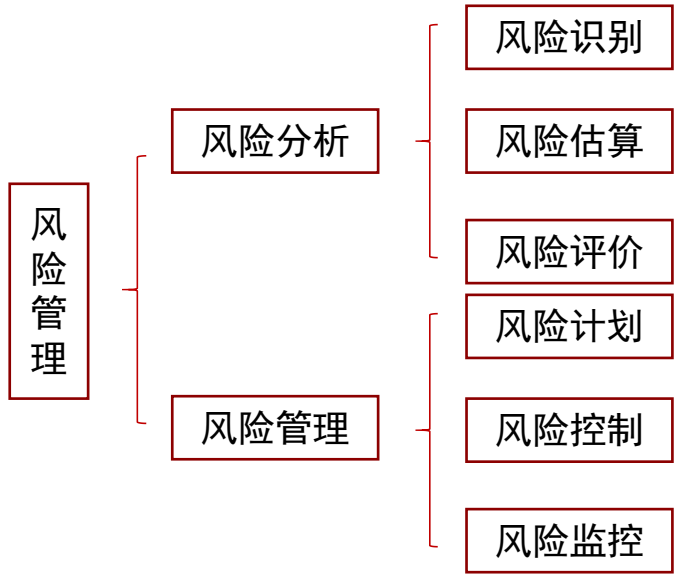




2.2 可信软件过程研究

⑩ Chartette风险管理框架

与Barry Boehm理论非常相似。使用UML构建软件蓝图，用例驱动、以架构为中心、迭代和增量的开发过程。将风险管理分为两个部分



➢ SEI的风险管理方法

包括三个部分：

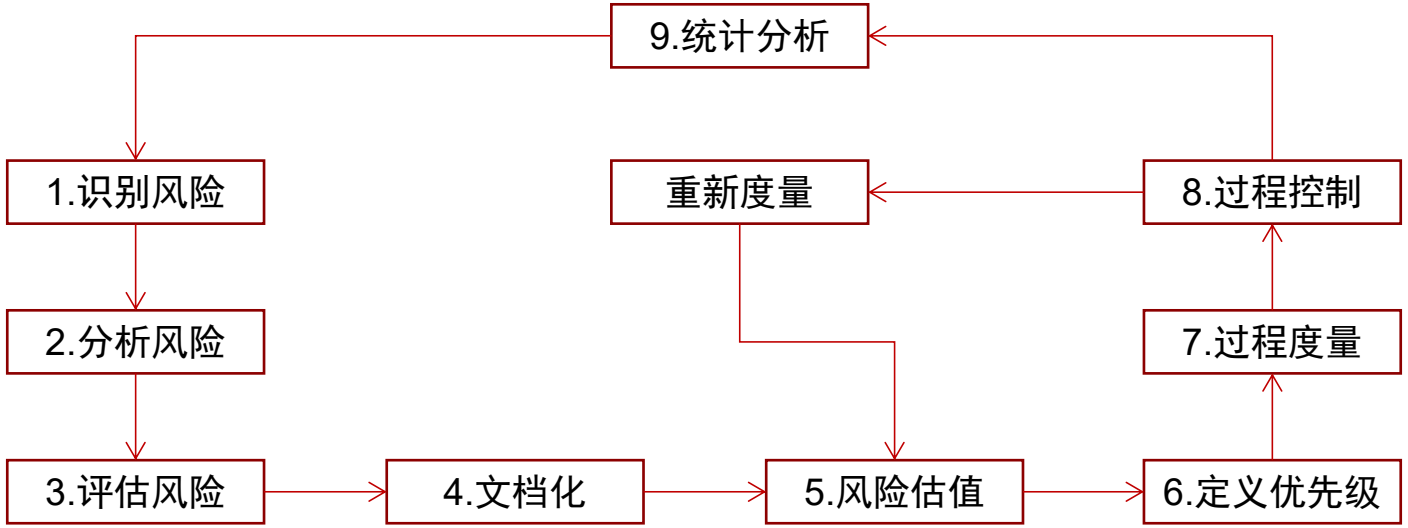
- 风险评估SRE：识别、分析、交流和缓解软件技术风险的方法
- 持续风险管理CRM：核心是风险交流
- 团队风险管理TRM：开发的沟通交流（理念核心）

2.2 可信软件过程研究

- **Riskit方法**

旨在对软件风险的来源、触发事件和影响等进行完整的体现和管理，并使用合理的步骤评估风险

⑩ **Softrisk法**



2.2 可信软件过程研究

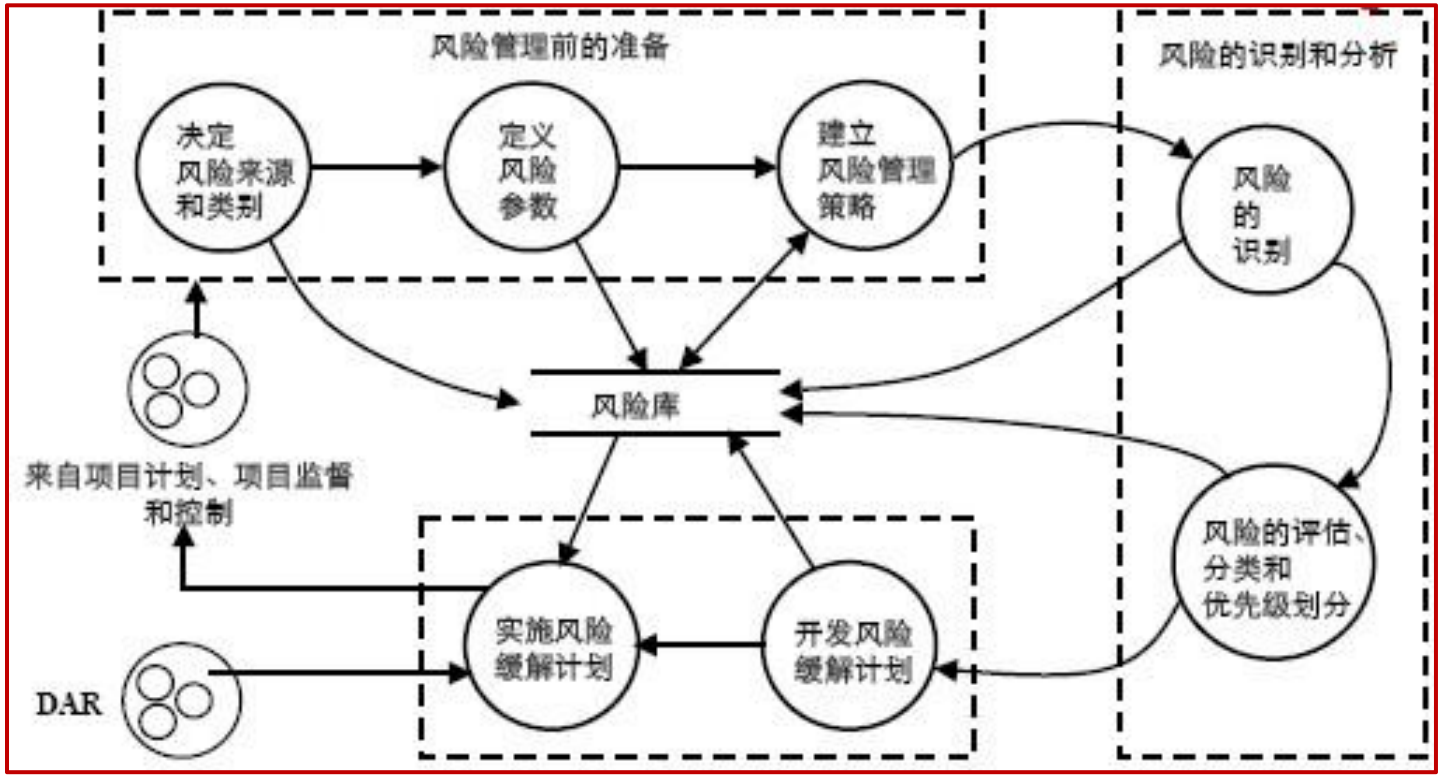
CMMI风险管理过程域

软件能力成熟度模型集合(Capability Maturity Model Integration),其中的风险管理过程域将风险管理分成三个目标:

1风险管理准备

2识别和分析风险

3缓解风险



风险管理的核心是风险库的构建与管理，所有的实践活动都围绕风险库展开。

2.2 可信软件过程研究

- **IEEE的风险管理标准**

IEEE提出关于软件风险管理的标准16085.该标准定义了整个软件开发生命周期内持续的风险管理过程，包括计划和实施项目风险管理、管理项目风险库、风险分析、风险监控、风险处理、评估风险等管理过程或活动

- **MSF法**

微软的MSF风险管理模型有一个基本理念和四条基本原则：

MSF理念：必须主动实施项目风险管理

四条原则：持续地、敏捷地实施风险管理；鼓励风险管理开放交流；不停的从风险管理中学习；责任分担与明晰风险管理责任

2.2 可信软件过程研究

- 2.2.3软件过程管理方法

软件过程管理DPM：是指成功地对软件产品和强化软件系统的开发、维护和支持工作进程进行管理。成功的软件过程管理，使软件过程生产的产品和服务完全符合用户的需求，并且达到软件组织对生产软件产品的商业目的。

软件过程管理模型：

- CMMI软件过程能力成熟度评估模型
- PSP/TSP个体软件过程/团队软件过程
- 软件能力成熟度模型（SJ/T 11235），我国实施的评估标准
- 软件过程能力评估模型（SJ/T 11234），我国实施的评估标准
- ISO/IEC 15504软件过程评估的国际标准
- ISO 9001标准
- Bootstrap模型，欧洲标准
- TQM全面质量管理
- 6SIGMA
- Taguchi method

2.2 可信软件过程研究

软件过程管理方法比较

方法	来源	层次	目的	支持度	分级方法	评估认证方式	成本
CMMI	美国	组织级	软件过程改进与评估	高 模型&指导	阶段模型+连续模型	内部评估+外部评审	很高
SJ/T 11234	中国	组织级	软件过程改进与评估	高 模型&指导	22个过程+5个成熟等级	外部评审	很高
SJ/T 11235	中国	组织级	软件过程改进与评估	高 模型&指导	22个过程+6个评估等级	内部评估	很高
PSP	美国	个人级	提高个人过程能力和技能训练	低 模型&指导	结构化框架+方法	培训与实践	很低
TSP	美国	项目级	提高团队性能	低 指导	指导方法：TSP原则	培训与实践	低
ISO/IEC 15504	国际标准	组织级	过程改进和能力确定	高 评估需求&申请指导指导	2维模型框架+6个能力等级+9个能力属性	内部评估+外部评审	高
TQM	美国	组织级	用于内部质量控制改进	一般 模型&指导	EFQM卓越模型+MBNQA模型	不提供认证，内部使用	高
ISO 9001	国际	项目级	软件过程改进质量管理	低 指导	二元模型	外部评审	一般
Bootstrap	欧洲	组织级	过程评估质量管理和改进	一般 模型&指导	成熟度算法+CMM5个成熟度等级	外部的调查评估	高
6SIGMA	美国	项目级	质量管理与交互过程改进	高 模型&指导	5个管理人员组织结构等级+DMAIC模型	内部评估	一般
田口方法	日本	组织级	质量改进	一般 模型&指导	质量损失函数+三次设计法	内部评估	高

2.3可信平台研究

• 2.3.1可信计算平台

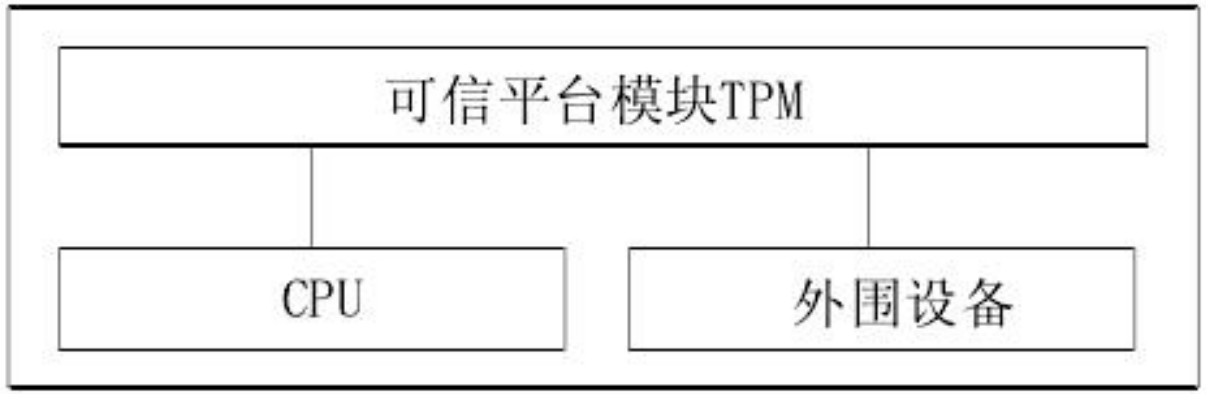
- 平台是一种能向用户发布信息或从用户那里接收信息的实体。把引入安全芯片架构的平台称之为**可信平台**,**可信计算平台(Trusted ComPuting Platform,TCP)**是一种能够提供可信计算服务并可以确保系统可靠性的计算机软硬件实体。

- 可信计算平台实现可信的基本思路是利用可信计算的核心技术——**可信平台模块(Trusted Platform Model,TPM)**建立可信计算平台的信任根,再把该信任根作为信任的起点,在可信软件的协助下,建立一条信任链。在建立信任链的过程中,系统把这种底层可靠的信任关系扩展到整个计算机系统,从而确保整个计算机系统的可信。

2.3可信平台研究

可信平台体系结构

可信平台的发展经历了从简单到复杂的过程。早期的可信平台相对比较简单，一般就只有 TPM（TCM）模块、CPU、外围设备纯硬件组成。



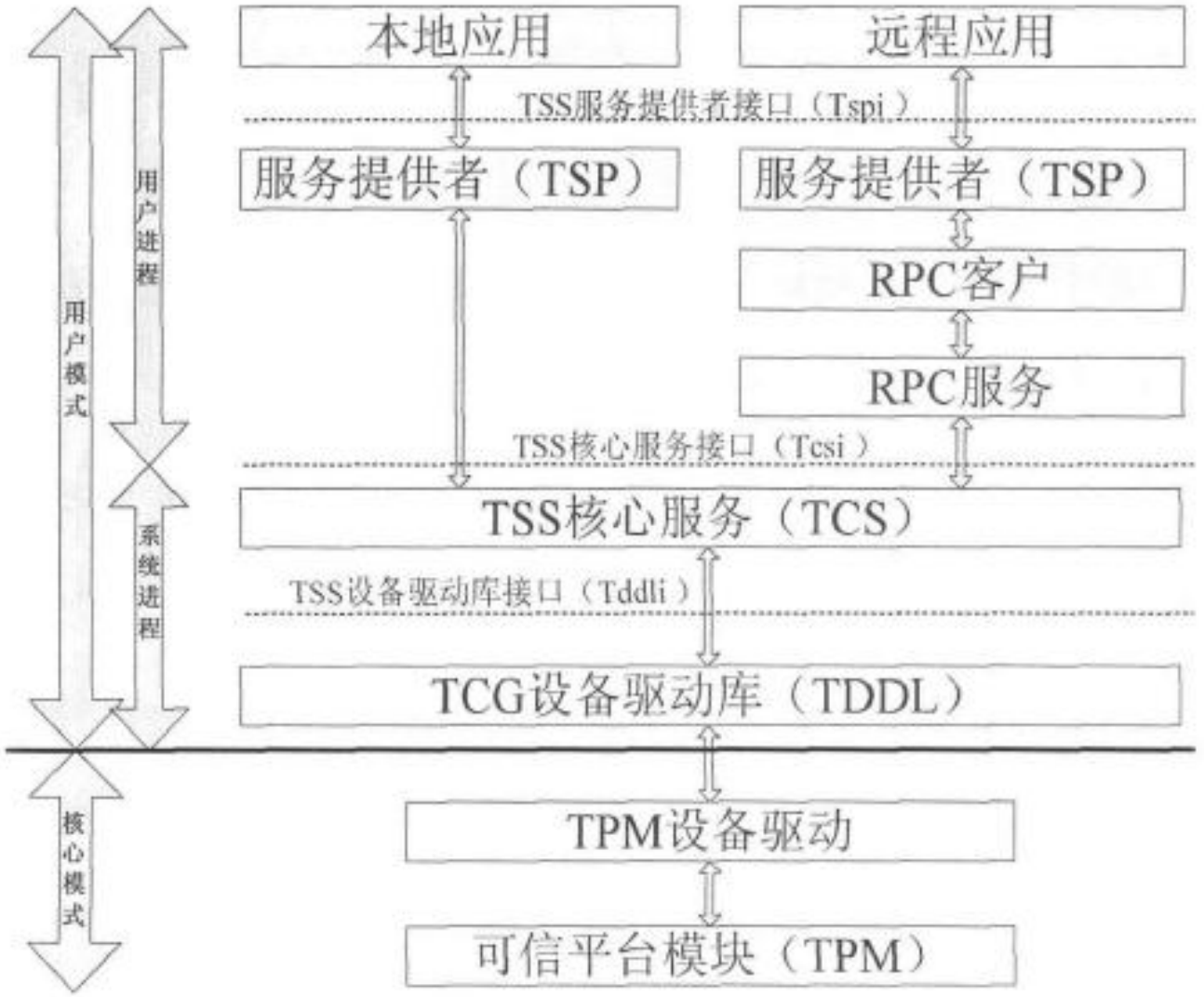
随着可信计算技术的发展，可信计算模型和可信计算平台也是不断地变化，逐渐趋于完善，在硬件平台方面可信计算方面技术逐渐成熟。

2.3可信平台研究

可信计算技术着重从硬件和操作系统等方面着手，希望建立一个完整、可信、可靠的信任平台。

一个典型的可信计算平台上的体系结构主要由以下三层组成：可信平台模块（TPM），可信软件栈(TCGSoftwareStaek,TSS)和应用软件。

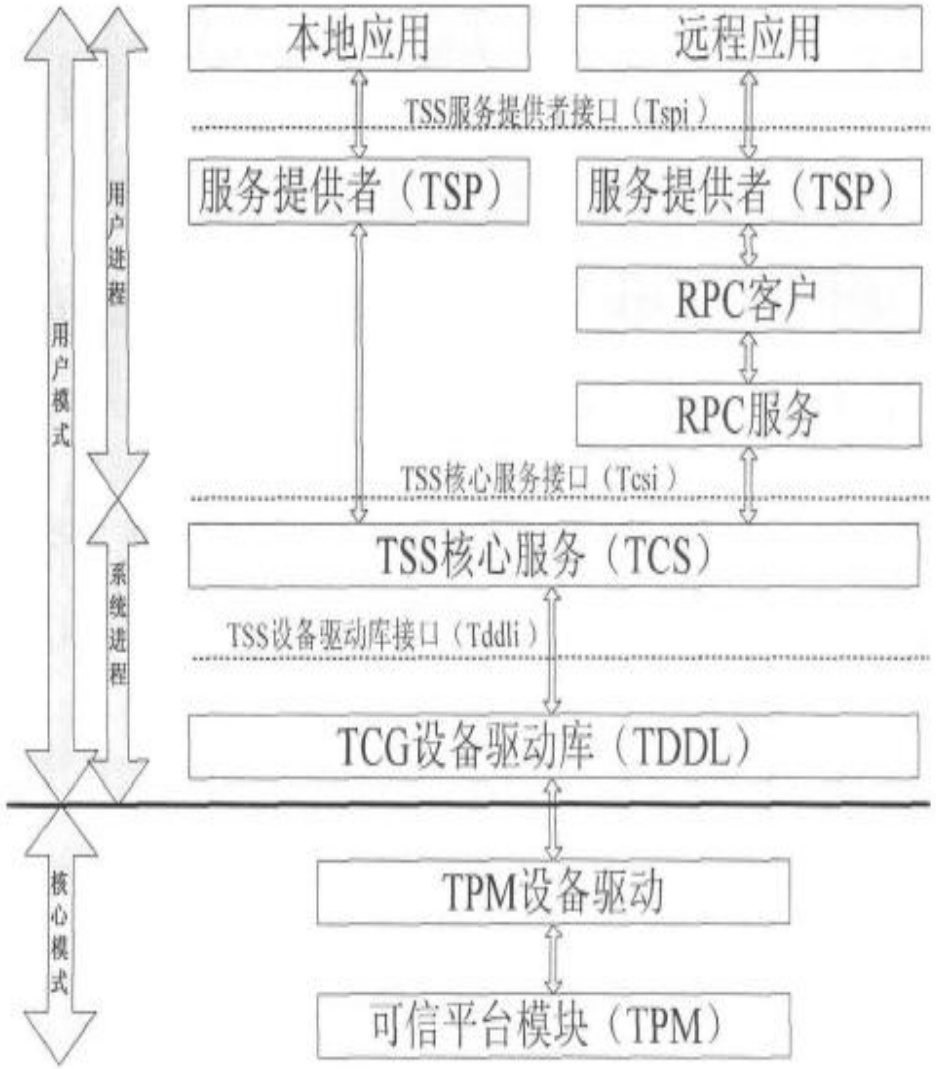
可信平台模块(含TPM设备驱动)属于核心模式,TSS和应用软件属于用户模式。TSS位于TPM和应用软件之间。TSS为应用程序提供可信平台模块的接口。



2.3可信平台研究

TSS从结构上可以分为三层，自下而上分别为TCG设备驱动库(TDDL)、TSS核心服务(TCS)和TSS服务提供者(TSP)，其中TDDL和TCS属于系统进程，TSP连同上层应用软件属于用户进程。

- TDDL是存在于TCS和内核模式TPM设备驱动(TDD)之间的一个中间模块，是用户状态和核心状态的过度，提供了用户模式的开放接口。
- TCS是用户模式的系统进程，为用户提供一组标准平台服务接口，通常以系统服务的形式存在，它向上可以给多个TSP提供服务，向下可以通过TDDL与TPM直接进行通信。
- 位于TSS协议栈最上层的TSP为用户模式的用户进程，它为可信平台系统上层的应用程序不仅提供了丰富的面向对象接口，而且还提供了上下文管理和密码功能等服务，使上层应用程序能够更加直接、方便地利用TPM提供的功能来构建平台所需的安全特性



2.3可信平台研究

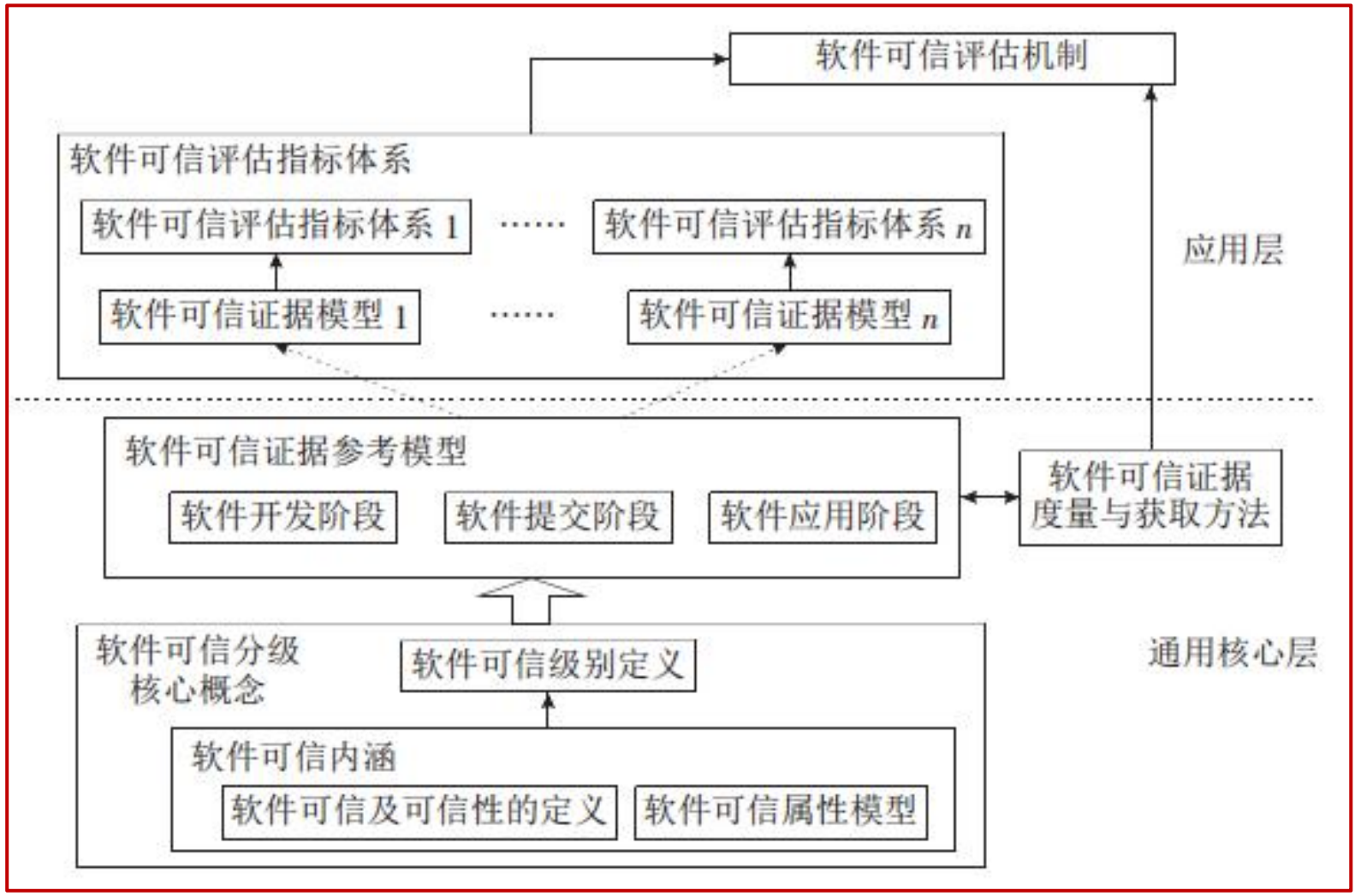
可信平台功能

对于一个可信计算平台，要实现可信的目标，必须至少具备三个最基本的功能：安全存储（数据加密）、认证机制及平台完整性度量、存储和报告

- 安全存储是为了确保敏感数据的机密性和完整性
- 可信计算平台证明机制是用来确认来自主机的信息是否真实的过程。通过可信计算平台证明机制，可以实现对网络通信实体的身份进行认证。
- 完整性度量就是对当前平台运行状态的收集，完整性度量的过程也是信任链的建立过程；完整性存储除了将度量摘要通过扩展的方式存储起来；完整性度量和存储是完整性报告的基础和前提。完整性报告则是终端向外部实体（服务器）证明完整性度量和存储的过程，展示保护区域中完整性度量值的存储，依靠可信平台的鉴定能力证明存储值的完整性。

2.3其他相关研究

- 2.3.2软件可信分级模型



2.3其他相关研究

- 软件可信级别定义

软件可信级别是一个软件可信性的量化标度。可依据软件对用户所期望的可信属性的满足程度，以及软件所具有的可信证据对软件可信的支持程度，将软件可信性分为6个级别，并分别命名为：未知级、可用级、 证实级、 实用级、 评估级和证明级。各级别的定义如下：

第 0 级——未知级

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软件可信属性的期望，软件的可信等级定义为未知级。

第 1 级——可用级

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基本期望。 软件的可信等级定义为可用级。

第 2 级——证实级

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发布软件可信属性声明，该声明可通过软件可信性分析、 测试或验证工具以及其他可信评估机制进行确认，表明该软件能满足用户对该类别软件可信属性的普遍期望，且用户期望的可信属性均得到了确认。软件的可信等级定义为证实级

2.3其他相关研究

第 3 级——实用级

在证实级的基础上，软件已在相关应用领域得到应用，并且有可证实的成功应用案例，隐含表明该软件能满足用户对该类别软件可信属性的普遍期望，且得到实际应用的证实。软件的可信等级定义为实用级。

第 4 级——评估级

在实用级的基础上，软件的可信性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，表明该软件能满足用户对该类软件可信属性的较高期望，且用户期望的可信属性均得到了权威机构的评估保证。 软件的可信等级定义为评估级。

第 5 级——证明级

在评估级的基础上，所提交的软件可信性属性都是可被严格证明的，软件的可信等级定义为证明级。证明级是最高的可信级别。

谢谢大家！