第五讲 可信需求分析

高可信软件工程

5.1 可信需求分析

5.2 需求工程

5.3 安全需求工程

5.1可信需求分析

- 5.1.1 可信需求的相关研究
- 5.1.2 可信需求的分类
- 5.1.3 可信需求的内涵及定义
- 5.1.4 可信需求的特征
- 5.1.5 可信需求的全生命周期管理框架及其实现方法

5.1.1可信需求的相关研究

- 美国《国家软件发展战略（2006-2015）》将开发高可信软件放在首位，提出了下一代软件工程的构想。
- 美国国土安全部2006年启动了Software Assurance Program，目的是改进可信软件产品的开发与部署。
- 美国政府的“网络与信息技术研究发展技术NITRD”中，提出了8个重点领域，有4个与“可信软件”密切相关，在“高可信软件与系统”领域，NITRD在2006年投入约1.34亿美元，其中，美国自然科学基金会投入0.41亿美元；在 2007 年投入预算 1.45 亿美元，其中 NSF 投入预算 0.53 亿美元。NSF 近 3 年（2006-2008）在可信软件研究领域投入 1.52 亿美元。

5.1.1可信需求的相关研究

在我国，为了引导并支持可信软件的研究：

- 国务院发布的《国家长期科学和技术发展规划纲要（2006-2020）》将支持可信软件产业的高效能可信计算机列入了重点领域及其优先主题；
- 国家科学技术部启动了 863 高技术研究发展计划重点项目“高可信软件生产工具及集成环境”；
- 国家自然科学基金委员会启动了“可信软件重大研究计划”(2008)。

5.1.2 可信软件需求的分类

- 一般来说，软件系统的需求分成三个类型：业务需求、用户需求、功能需求(Hashim and Khairuddin, 2009)。

➢ 业务需求说明了提供给用户和软件开发方的新系统的最初利益，反映了组织机构或用户方对系统、产品高层次的目标要求，它们在项目视图与范围文档中予以说明；

➢ 用户需求文档描述了用户使用产品必须要完成的任务，这在使用实例文档或方案脚本说明中予以说明；

➢ 功能需求定义了开发人员必须实现的软件功能，使得用户能完成他们的任务，从而满足业务需求。

上述被业界普通所接受的软件的需求分类，其实存在片面性和不完整性，并不完全适用于可信软件需求的表达与分类。

5.1.2 可信软件需求的分类

- 可信软件开发过程中，需求管理的第一步就是获取各种需求。

➢ 首先经过调研等方法获得**业务需求**，写出项目范围视图文档；

➢ 接着结合用户要求和用户所从事的行业规范文档得到**用户需求**；

➢ 然后从用户需求中分离出**功能需求**和**质量需求**。

质量需求定义了对可信软件包括快捷、简易、直观性、用户友好、健壮性、可靠性、可用性和安全性等方面的需求，它对系统的总体架构形成起关键性作用。对于**普通软件**，由于其软件系统规模较小，复杂度不高，其质量需求往往被用户所忽略，用户比较偏重软件的功能需求。

但对于**可信软件**，由于软件系统规模较大、复杂程度高、专业人员操作，并且其应用范围主要是面向航空航天、金融、电力等国民经济高科技领域，因此，用户除了关注可信软件的功能需求外，往往更加关注如可用性、可靠性、安全性和可生存性等可信需求，这就使得可信软件的质量需求往往体现为可信需求。

5.1.2 可信软件需求的分类

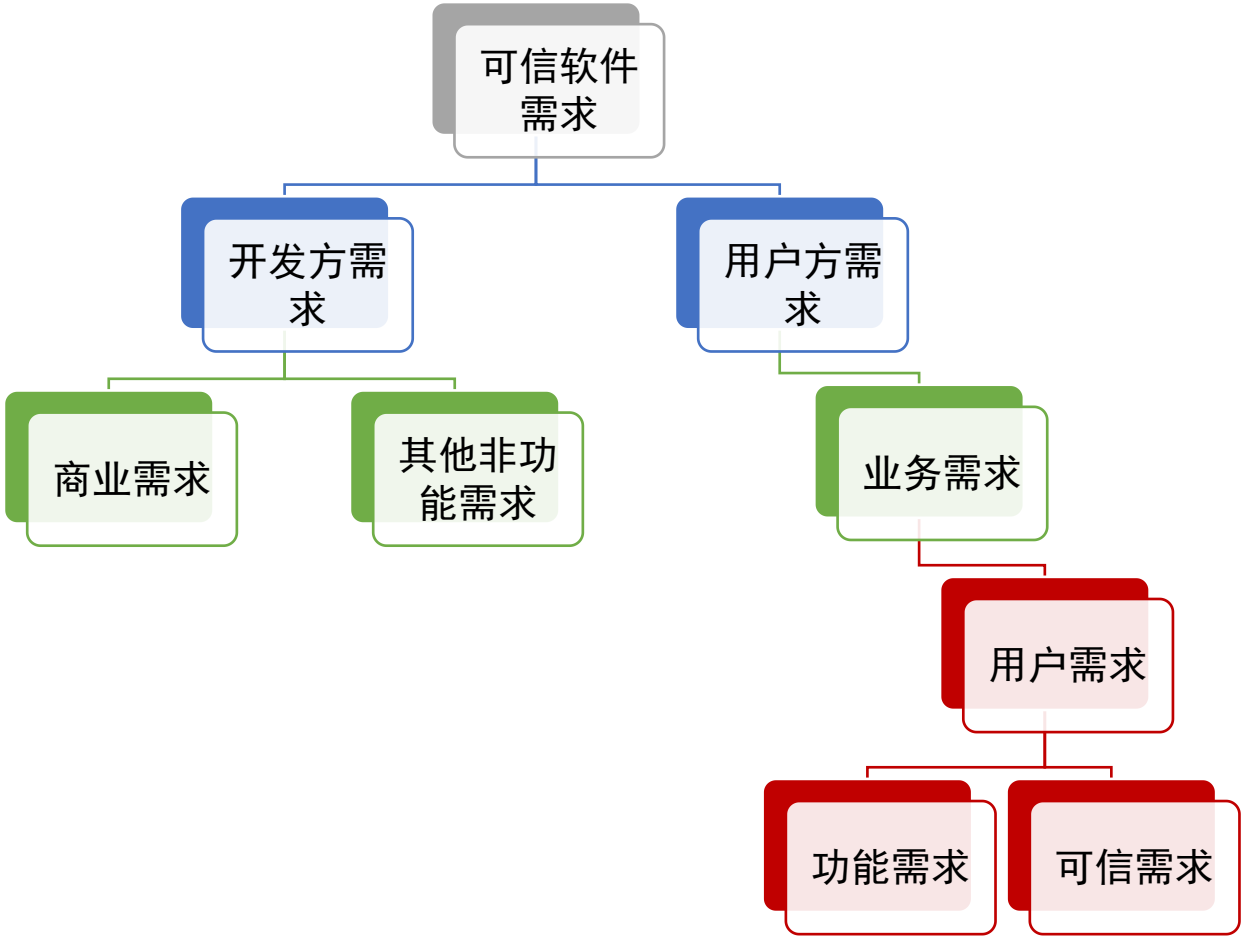
- 另一方面，从软件开发方的角度出发，针对具体的项目或产品形成其它的两类需求：商业需求和其它非功能需求。

➢商业需求是从开发方的开发成本、开发时间、开发风险等因素考虑的。

➢其它非功能需求是指软件开发方考虑到架构、控件、模块、类库等的重用性而需考虑的需求。

5.1.2 可信软件需求的分类

- 通过上述对可信软件需求类型的分析，可以得到可信软件需求分类二叉树，如图所示。



从上图所示的可信软件需求分类二叉树可以看出，其叶子结点包括功能需求、可信需求、商业需求和其它非功能需求。实际上，从可信软件开发的角度，商业需求和其它非功能需求可以理解为可信软件功能需求和可信需求实现的限制性约束条件，这样可信需求和功能需求就成为可信软件的两大类核心需求。

5.1.3 可信需求的内涵及定义

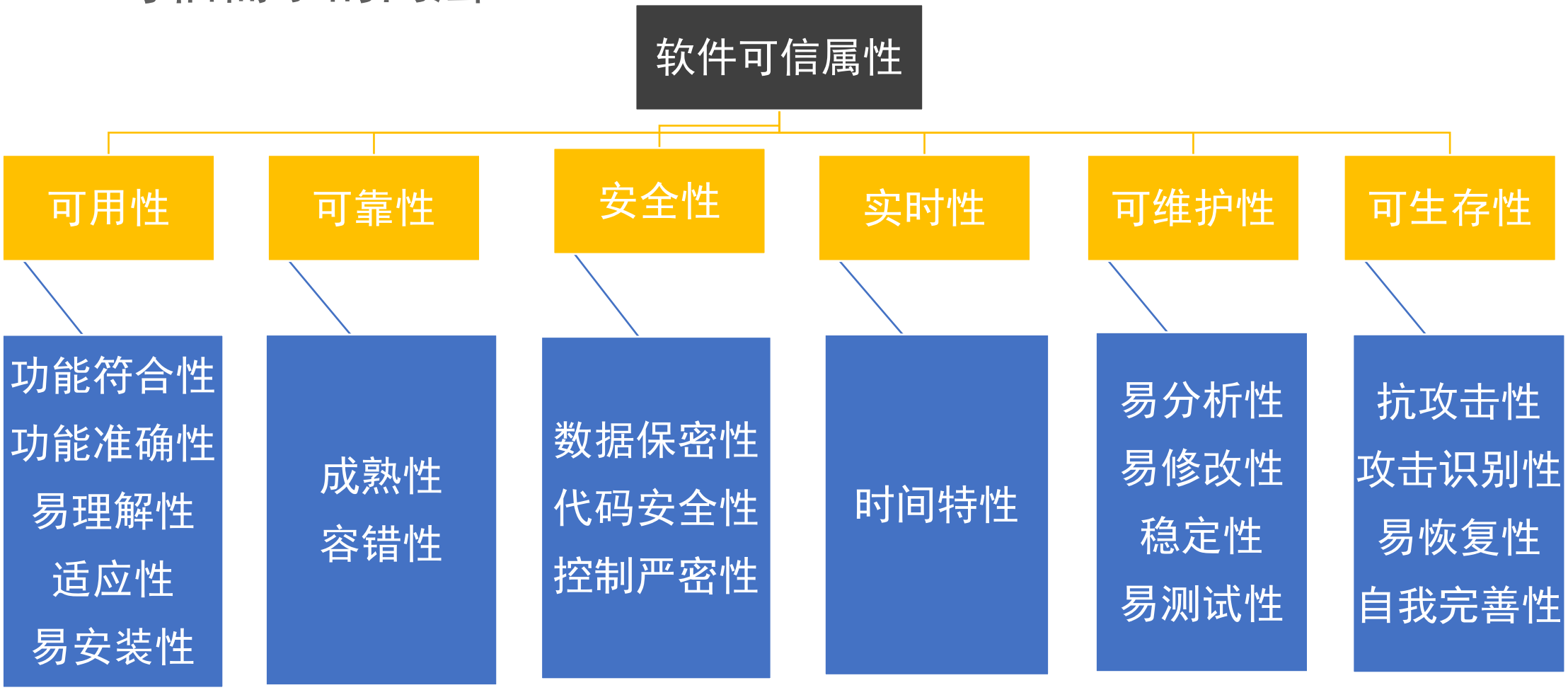
- 可信需求的内涵

可信需求是用户对软件系统的可信性要求，是一种特殊的质量需求，是一种需要分解精化的全局性软件行为的约束，它由可靠性、安全性、时效性、可用性、可生存性和可维护性等可信属性组成。

将软件可信级别分为6个等级，并提出了软件可信属性模型，指出软件的可信性，即软件系统的可信需求包括可用性（Availability）、可靠性（Reliability）、安全性（Security）、实时性（Real Time）、可维护性（Maintainability）和可生存性（Survivability）等6个可信属性，这几个可信属性又由若干个可信子属性构成，这些属性从不同层次、不同粒度展现了软件可信需求的内涵，如图所示。

5.1.3 可信需求的内涵及定义

- 可信需求的内涵



5.1.4可信需求的特征

可信需求是用户对软件系统的可信性要求，是一种特殊的质量需求，是一种需要分解精化的全局性软件行为的约束，它用可靠性、安全性、时效性、可用性、可生存性和可维护性等多个可信属性来表征，具有如下特征：

- 由于软件类型、应用环境和应用范围的不同，用户和软件开发方在知识结构和专业领域的差异，用户和软件开发方对软件的可信需求的理解往往不一致；

➢ 可信需求，是在正确性、可靠性、安全性、时效性、完整性、可用性、可预测性、生存性、可控性等概念的基础上发展起来的概念。

5.1.4可信需求的特征

- 可信需求属于软件系统高层次的质量需求，根据软件类型、应用环境和应用范围的不同，可信需求往往表现出不同的可信性要求。
- 由于用户和软件开发方在知识结构和专业领域存在较大的差异，用户和软件开发方往往对很难达成对可信需求内涵的一致性理解，这就增加了用户完整、无歧义表达可信需求的难度，也增加了软件开发方获取可信需求的难度，因此，在可信需求获取过程中需要用户和软件开发方充分的交流。

- 表征可信需求的各可信属性之间存在复杂的相互影响和依赖关系

- 可信需求包含的可信属性之间存在复杂的相互影响和依赖关系，例如，可用性、可靠性及用户和环境的安全性等可信属性与完整性存在依赖关系，系统完整性的变化直接影响并制约软件的可用性、可靠性及用户和环境的安全性。

5.1.4可信需求的特征

- 同样，可信属性可靠性的好坏将直接影响软件的可维护性和可生存性等可信属性，而软件的可信属性可生存性与系统的正确性、实时性、可靠性、用户和环境安全性等可信属性也密切相关。由于可信软件的规模比较大，复杂程度比较高，这就使得用户的可信需求往往多而复杂，因此，软件开发方在实现用户的可信需求时，其需求实现次序就必须考虑可信属性之间的相互影响和依赖关系，也就是说可信需求优先级的设定必须考虑可信属性之间本身所要求的实现次序，以降低可信需求实现的复杂度。
- 此外，可信需求的变化管理也必须考虑可信属性之间复杂的相互影响和依赖关系。

5.1.4可信需求的特征

- 在基于构件的软件体系结构下，软件系统整体的可信需求可分解到各构件，形成各构件的可信需求。

软件可简单的认为是组成系统的若干构件以及构件与构件之间交互作用关系的高度抽象(Huang, 2008)，这样软件系统整体的可信需求就表现为组成软件的各个构件的可信需求，就意味着各个构件用一系列的可信属性来表达其可信需求。

5.1.4可信需求的特征

定义1 （构件可信需求）构件的可信需求是指构件的可信能力，它用一组相互影响和依赖的可信属性来表示。由于构件在实现目标和用户期望可信性要求的不同，描述和评价其可信需求的各构件的可信属性往往存在差异。

定义2 （软件可信需求）软件可信需求是指整个软件系统的可信能力，它可用一组构件可信需求来表示，各构件可信需求之间的相互影响和依赖是通过可信属性之间的作用机制来体现。

根据上面的定义，软件可信需求实质上就高度抽象为组成系统的若干构件的可信属性和各可信属性之间的依赖关系。这样，整个软件可信需求的实现和可信需求的变化管理就体现为各构件可信需求的实现和各构件可信需求的变化管理。

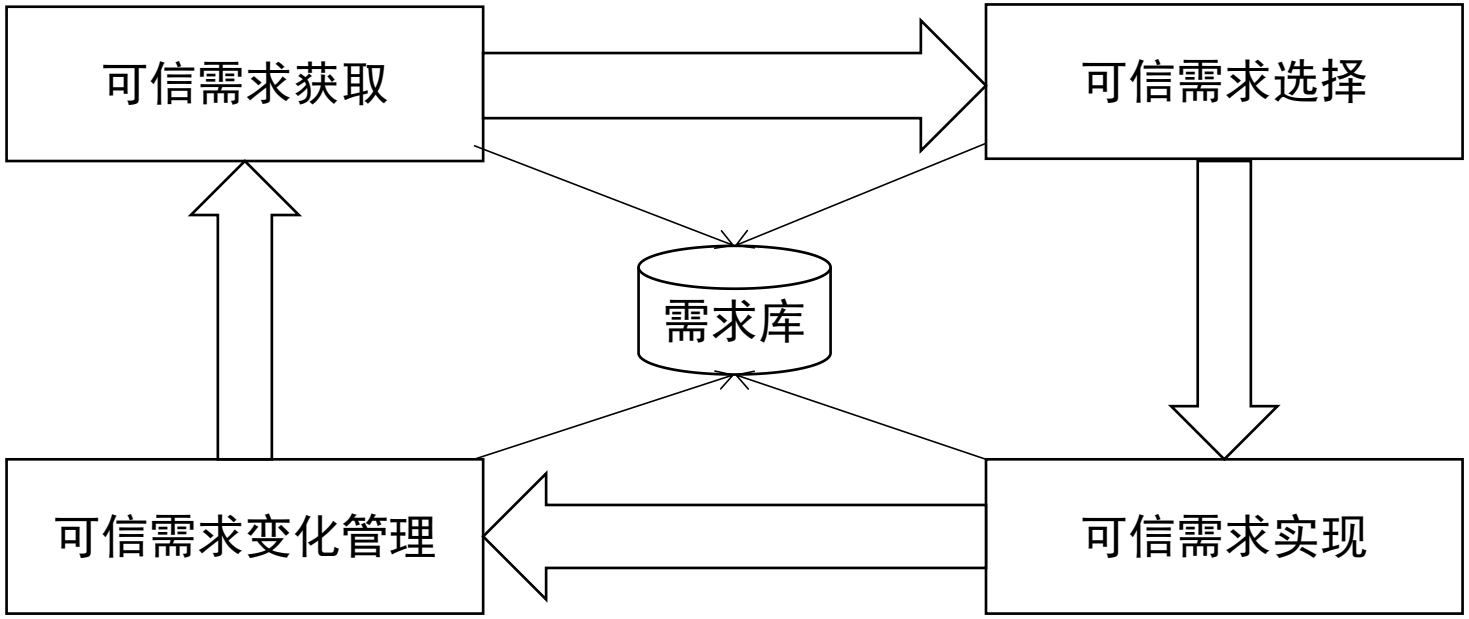
5.1.5 全生命周期管理框架及其实现方法选择

- 可信需求全生命周期管理框架
- 可信需求管理实现方法

5.1.5 全生命周期管理框架及其实现方法选择

- 可信需求全生命周期管理框架

根据需求管理的生命周期，可信需求管理包括可信需求获取、可信需求选择、可信需求实现和可信需求变化管理等过程，可以得到如图示的可信需求全生命周期管理框架。



5.1.5 全生命周期管理框架及其实现方法选择

- 可信需求全生命周期管理框架

从上图所示的可信需求全生命周期管理框架可知，该管理框架覆盖了可信需求获取、可信需求选择、可信需求实现、可信需求变化管理等四个过程的可信需求的全生命周期管理，各过程自成体系又有机形成一个闭环的可信需求循环管理。在可信软件开发过程中，这四个部分是一个交替循环的过程，可信需求获取后，首先是选择，然后是实现，最后是作变化管理，如果这时用户提出新的可信需求，则重新迭代这四个过程，这四个过程中产生的文档保存在需求库中。

5.1.5 全生命周期管理框架及其实现方法选择

- 可信需求管理实现方法

下面根据上图所示的可信需求管理框架，分别阐述可信需求管理的四个过程，并结合可信需求的特征提出相应的实现方法。

- **可信需求获取：**可信需求获取是软件开发方从用户 (软件需求方)通过相互交流得到可信需求的过程。可信需求获取将注意力放在系统可信性要求的描述上。软件开发方和软件需求方共同标识了一个问题域，定义了解决这一问题域的系统。这类定义称为需求规格说明，可用于软件开发方和软件需求方之间的沟通。

5.1.5 全生命周期管理框架及其实现方法选择

- 可信需求管理实现方法

  - **可信需求选择：**软件开发方不但要与用户方进行沟通，尽可能全面地了解用户的可信性要求，提出相对完整的可信需求分析报告，但是更要考虑由于表征可信需求的各可信属性之间存在复杂的相互影响和依赖关系，其需求的实现次序会对系统的开发复杂程度产生较大的影响，这就是可信需求的选择问题。通常，不合理的可信需求实现次序会加大软件开发的复杂度，延长开发时间，甚至影响软件的质量，因此，必须对众多的可信需求选择一个合理的顺序，对其进行有序的实现，这对可信软件的开发才是一个比较实际的开发策略。

5.1.5 全生命周期管理框架及其实现方法选择

- 可信需求管理实现方法

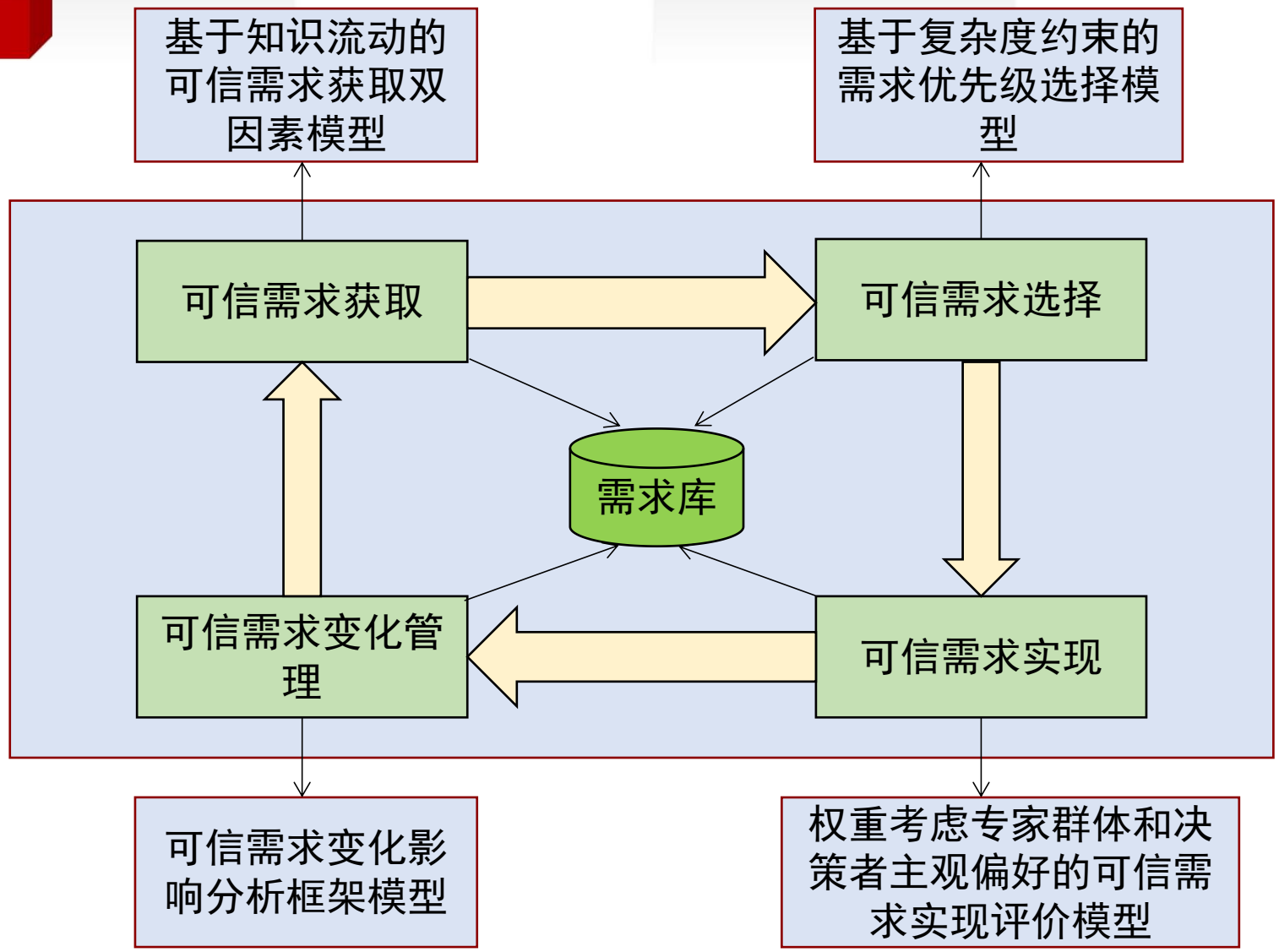
  - **可信需求实现：**软件开发完成之后，软件是否实现了可信需求、实现程度如何成为了用户和软件开发商都关注的重要问题之一。由于可信需求是一种表示软件可信性的特殊的质量需求，对于可信需求的实现，用户的可信性要求往往体现为软件的整体性可信性要求或某关键子系统的可信性要求。软件可视为构件的组装，这样软件系统整体的可信需求也可理解为各构件的可信需求的综合。

5.1.5 全生命周期管理框架及其实现方法选择

- 可信需求管理实现方法

➢ 可信需求变化管理：在可信需求管理的生命周期中，最大的问题是可信需求不断的变化（包括需求的变更或演化），这是可信软件开发之所以困难的主要根源，因此对可信需求实施有效的变化管理是项目成功的基础。可信需求变化贯穿了软件的整个生命周期，从软件的立项、研发到维护，用户的可信需求有可能增加也有可能减少，也有可能要求程度发生变化，这些都使软件的可信需求需要不断的完善。

基于上面对可信需求获取、可信需求选择、可信需求实现和可信需求变化管理内容的阐述及其实现方法的选择，可以得到如下图所示的可信需求全生命周期管理框架及其实现方法选择图。



在图中，可信需求全生命周期管理是通过四个模型来实现的，

- 基于知识流动的可信需求获取“双因素”模型实现可信需求的获取，
- 基于复杂度约束的选择优先级模型实现可信需求的选择管理，
- 权重考虑专家群体和决策者主观偏好的可信需求实现评价模型完成可信需求的实现。
- 可信需求变化影响分析框架模型实现可信需求变化管理。

在这四个模型的制导下，可以实现对可信需求的全生命周期管理。

该部分参考《基于需求特征的软件可信需求全生命周期管理研究》，重庆大学博士学位论文，学生程平，刘伟教授

5.2 需求工程

- 5.2.1　需求工程基本内容
- 5.2.2　需求工程方法
- 5.2.3　需求工程技术

5.2.1 需求工程基本内容

➢什么是需求工程

需求工程是指应用已证实有效的技术、方法进行需求分析，确定客户需求，帮助分析人员理解问题并定义目标系统的所有外部特征的一门学科。需求工程通过合适的工具和记号系统地描述待开发系统及其行为特征和相关约束，形成需求文档，并对用户不断变化的需求演进给予支持。

➢需求工程的概述

需求工程是随着计算机的发展而发展的，在计算机发展的初期，软件规模不大，软件开发所关注的是代码编写，需求分析很少受到重视。后来软件开发引入了生命周期的概念，需求分析成为其第一阶段。随着软件系统规模的扩大，需求分析与定义在整个软件开发与维护过程中越来越重要，直接关系到软件的成功与否。人们逐渐认识到需求分析活动不再仅限于软件开发的最初阶段，它贯穿于系统开发的整个生命周期。80年代中期，形成了软件工程的子领域——需求工程(requirement engineering, RE)。进入90年代以来，需求工程成为研究的热点之一。

5.2.1 需求工程基本内容

- 需求工程的概述
- 从1993年起每两年举办一次需求工程国际研讨会(ISRE)，自1994年起每两年举办一次需求工程国际会议(ICRE)，在1996年Springer-Verlag发行了一新的刊物——《Requirements Engineering》。一些关于需求工程的工作小组也相继成立，如欧洲的RENOIR(Requirements Engineering Network of International Cooperating Research Groups)，并开始开展工作。
- 需求分析是介于系统分析和软件设计阶段之间的桥梁。一方面，需求分析以系统规格说明和项目规划作为分析活动的基本出发点，并从软件角度对它们进行检查与调整；另一方面，需求规格说明又是软件设计、实现、测试直至维护的主要基础。良好的分析活动有助于避免或尽早剔除早期错误，从而提高软件生产率，降低开发成本，改进软件质量。

5.2.1 需求工程基本内容

- 需求工程的定义

➢需求工程是指应用已证实有效的技术、方法进行需求分析，确定客户需求，帮助分析人员理解问题并定义目标系统的所有外部特征的一门学科。它通过合适的工具和记号系统地描述待开发系统及其行为特征和相关约束，形成需求文档，并对用户不断变化的需求演进给予支持。

➢需求工程是一个不断反复的需求定义、文档记录、需求演进的过程，并最终在验证的基础上冻结需求。80年代，Herb Krasner定义了需求工程的五阶段生命周期：需求定义和分析、需求决策、形成需求规格、需求实现与验证、需求演进管理。近来，Matthias Jarke和Klaus Pohl提出了三阶段周期的说法：获取、表示和验证。

5.2.1 需求工程基本内容

- 需求工程的分类

需求工程(RE)可分为

1.系统需求工程（如果是针对由软硬件共同组成的整个系统）

2.软件需求工程（如果仅是专门针对纯软件部分）。

软件需求工程是一门分析并记录软件需求的学科，它把系统需求分解成一些主要的子系统和任务，把这些子系统或任务分配给软件，并通过一系列重复的分析、设计、比较研究、原型开发过程把这些系统需求转换成软件的需求描述和一些性能参数。

5.2.1 需求工程基本内容

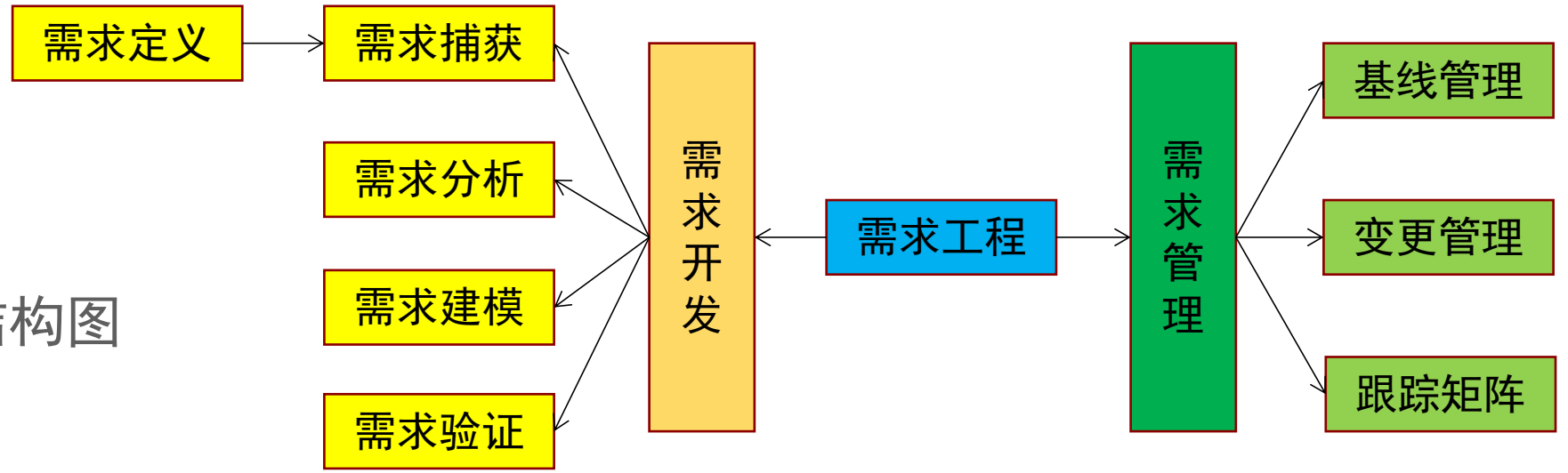
- 需求工程结构图

需求工程包括需求开发和需求管理两大范畴。

需求开发是收集、分析、整理、编写、验证需求的全过程。其重点在于整理出高质量的需求规格说明书。

需求管理则对需求的实现、变化进行追踪的全过程。重点在于确保开发的软件“不走样”。

结构图



5.2.2 需求工程方法

- 需求工程的方法

需求工程包括需求开发和管理，而需求开发又包括这几个过程：需求获取，需求分析，需求规格说明和需求验证。

- 需求获取和分析包括发现，分类和组织需求、需求的优先级排序、协商需求以及形成需求文档。
- 需求验证的方法包括评价需求、原型设计和生成测试用例。

在需求开发之前，还需要有一知识培训的过程，需求工程也是一个项目工程，因此也包括了项目的管理。对于这些过程，有以下方法可以采用。

5.2.2 需求工程方法

- 需求工程的方法——知识培训

➢ 需求分析员培训：需求分析员应该具有良好的交流沟通能力，同时理解产品，并掌握了需求工程的技能。

➢ 用户培训：用户也应该接受需求工程知识的培训，让他们理解需求的重要性，知道如何准确的描述需求，需求的风险性等。

➢ 开发人员培训：开发人员应该对用户的应用领域有一个基础的了解，明白客户的业务活动，术语，产品目标等。

5.2.2 需求工程方法

- 需求工程的方法——需求获取

需求包括业务需求，用户需求和功能需求以及非功能需求，在需求开发之前，需要先定义好需求开发的过程，形成文档，内容包括：需求开发的步骤，每一个步骤如何实现，如何处理意外情况，如何规划开发资源等。

需求获取包括以下方法和技能：

项目范围确定：需求开发前期，应该获取用户的业务需求，定义好项目的范围，使得所有的涉众对项目有一个共同的理解。

用户确定：确定用户群和分类，对用户组进行详细描述，包括使用产品频率，所使用的功能，优先级别，熟练程度等等。对每一个用户组确定用户的代言人。对于大型项目，需要先确定中心客户组，中心客户组的需求具有高级别的优先级，需要先实现的核心功能。

5.2.2 需求工程方法

- 需求工程的方法——需求获取

用例确定：与用户代表沟通，了解他们需要完成的任务，得到用例模型。同时根据用例导出功能需求。用例描述应该采用标准模板。

系统事件和响应：业务事件可能触发用例，系统事件包括系统内部的事件以及从外部接受到信息，数据等等，或者一个突发的任务。

获取方法：召开需求讨论会议，观察用户的工作过程，采用问答式对话，采用诱发式需求诱导等等。检查完善：问题报告和补充需求建议。

5.2.2 需求工程方法

- 需求工程的方法——需求分析

需求分析是对用户的需求获取之后的一个粗加工过程，需要对需求进行推敲和润色以使所有涉众都能准确理解需求。

首先，需要对需求进行检查，以保证需求的正确性和完备性，然后将高层需求分解成具体的细节，创建开发原型，完成需求从需求获取人员到开发人员的过渡。

绘制关联图：关联图确定系统和外部的交互。划分了系统的范围和界限，构建了系统对外的接口。

原型开发：对于敏捷方法，推荐完成一个界面的原型，一个初步的系统实现，通过原型，让所有涉众对开发的项目有了一个初步的映像，同时可以提供对需求的检验。

5.2.2 需求工程方法

- 需求工程的方法——需求分析

需求优先级别：采用分析的方法确定产品的功能，用例和单项需求的优先级别，以优先级为基础，确定各项功能和需求都包括在哪个版本中，在项目开发过程中，需求的优先级别根据实际情况进行调整。

需求建模：图形分析模型对需求描述更加抽象。主要可以采用UML的建模分析。

数据字典创建：建立系统中所用到的数据项和结构的定义，数据字典可以使参与项目开发的每一个人都使用统一的定义。

子系统：建立系统的结构，同时将需求分配到各个子系统和模块中。

5.2.3 需求工程技术

- 需求工程的基本活动及其各个阶段的技术：
  - 抽取需求；
  - 模拟和分析需求；
  - 传递需求；
  - 认可需求；
  - 进化需求。

5.2.3 需求工程技术

- 需求工程的基本活动及其各个阶段的技术：

➢ 抽取需求；

需求抽取的方法一般有问卷法、面谈法、数据采集法、用况法、情景实例法、组织会议法以及基于目标的方法等，还有知识工程方法，如：场记分析法、卡片分类法、分类表格技术和基于模型的知识获取等。

5.2.2 需求工程技术

- 需求工程的基本活动及其各个阶段的技术：

➢ 模拟和分析需求

需求工程的第二个阶段是模拟和分析需求，目前有许多工作都以此为目标进行。

需求分析和模拟又包含三个层次的工作。首先是需求建模。需求模型的表现形式有自然语言、半形式化（如图、表、结构化英语等）和形式化表示等三种。

✓ 自然语言形式具有表达能力强的特点，但它不利于捕获模型的语义，一般只用于需求抽取或标记模型。

✓ 半形式化表示可以捕获结构和一定的语义，也可以实施一定的推理和一致性检查。

✓形式化表示具有精确的语义和推理能力，但要构造一个完整的形式化模型，需要较长时间和对问题领域的深层次理解。

5.2.2 需求工程技术

- 需求工程的基本活动及其各个阶段的技术：

➢ 传递需求

传递需求的主要任务是书写软件需求规格说明，其目的是：

✓传达对需求的理解；

✓作为软件开发项目的一份契约；

✓作为评价后续工作的基线；

✓作为控制需求进化的基线。

对需求规格说明感兴趣的群体包括：用户、客户；系统分析员、需求分析员；软件开发者、程序员；测试员；项目管理者。

5.2.2 需求工程技术

- 需求工程的基本活动及其各个阶段的技术：

➢ 认可需求

认可需求就是让上述人员对需求规格说明达成一致，其主要任务是冲突求解，包括定义冲突和冲突求解两方面。常用的冲突求解方法有：协商、竞争、仲裁、强制、教育等，其中有些只能用人的因素去控制。

➢ 进化需求

进化需求的必要性是明显的，因为客户的需要总是不断（连续）增长的，但是一般的软件开发又总是落后于客户需求的增长，如何管理需求的进化（变化）就成为软件进化的首要问题。对传统的变化管理过程来说，其基本成分包括软件配置、软件基线和变化审查小组。当前的发展是软件家族法，即产品线方法。多视点方法也是管理需求变化的一种新方法，它可以用于管理不一致性并进行关于变化的推理。

5.3 安全需求工程

5.3.1 安全需求工程的起源与发展

5.3.2 安全需求工程的研究现状

5.3.3 安全需求工程研究存在的不足

5.3.1 安全需求工程的起源与发展

- 安全需求工程的发展史

在安全需求工程发展的前期，大多数安全需求工程师无法区分系统的安全需求与安全需求的实现手段，他们仅仅针对某个单独的安全目标进行分析，并提出相应的解决方案。

自1999 年12 月Common Criteria(CC) 2．1 正式版成为信息安全技术国际标准以来，软件工程研究者将CC 整合到软件开发周期中，并在此基础上提出基于特定框架的安全需求模型。

2005 年Nancy R． Mead 等人提出安全质量需求工程Security Quality Requirements Engineering (SQUARE) ，这个过程围绕着需求工程师和一个IT 项目的涉众之间的交互展开，由统一定义，识别安全目标，开发工件，执行风险评估，选择获取技术，获取安全需求，对需求分类，优化需求，需求检测等9 个步骤组成。

5.3.1 安全需求工程的起源与发展

纵观安全需求发展过程，安全问题从最初的软件设计完之后考虑到在需求阶段就引进相关的安全机制，再到利用已经存在建模框架进行安全需求建模，逐步发展成为以面向组织层面建模的潮流，划分了面向组织的模型框架与传统的面向系统的模型框架的界限。安全需求的发展在安全需求工程实践中发挥了重要的指导作用。

5.3.1 安全需求工程的起源与发展

- 安全需求的主要研究方向

基于框架的安全需求建模方法成为目前建立软件系统安全性行为的流行方法，使软件系统的安全需求与实现这些需求的手段日趋明显，

如何描述，获取，分析，建模安全需求?

如何验证一个安全需求是否符合期望的系统需求?

如何基于安全需求建模框架开发实例化的软件系统?

是安全需求工程中必须研究和解决的核心问题。根据现有的安全需求工程的研究活动，

主要包括如下几个方面:

1) 安全需求描述语言　　2) 安全需求的获取与分析

3) 安全需求的建模　　4) 安全需求的模型检测

5) 安全需求的系统支持工具　　6) 软件系统的安全风险评估

5.3.2 安全需求工程的研究现状

1. 安全需求工程的有关定义
2. 安全需求工程研究的不同思路
3. 安全需求工程的主要内容与进展

5.3.2 安全需求工程的研究现状

1. 安全需求工程的有关定义：

安全需求工程是一门涉及到需求工程和信息安全的交叉学科。

需求工程是指应用已证实的有效的技术、方法进行需求分析，确定客户需求，帮助分析人员理解问题并定义目标系统的所有外部特征的一门学科;

信息安全是通过实施一组控制而达到的，包括策略、措施、过程，组织结构及软件功能，是对机密性、完整性和可用性保护的一种特性。

因此，将信息系统的安全属性整合到主流的需求工程中则产生了安全需求工程这门新兴学科。

5.3.2 安全需求工程的研究现状

2. 安全需求工程研究的不同思路

实践表明: 一个好的安全需求获取、分析与建模方法是系统开发成功的重要因素。但由于对软件系统的安全需求和实现这些需求的手段的不同理解，安全需求工程可以分为典型的两种派别: 学院派与实用派。

学院派研究者侧重于安全需求工程的形式化理论研究，主要是对安全需求分析的早期阶段进行分析、建模。

而实用派则是从具体的一些方面对安全需求进行分析，找出一种有效的方法和防范机制来解决安全问题。如需求: 身份识别需求、认证需求、授权需求、免疫需求、完整性需求、入侵检测需求、不可否定性需求、隐私需求、安全审查需求、系统可生存性需求、物理防护需求、系统的安全维护需求，并对这些需求给出了相应的解决方案。

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

目前，安全需求工程研究的活动主要集中在以下几个领域:

(1) 安全需求描述语言

(2) 安全需求的获取与分析

(3) 安全需求建模

(4) 安全需求模型检测

(5) 安全需求的系统支持工具

(6) 软件系统的安全风险评估

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(1) 安全需求描述语言

为了保证需求工程师和涉众对安全需求进行有效和清晰的交流，需要使用一致的安全术语。SWEBOK， IEEE 和Wikipedia等相关组织制定的标准已经对需求工程中可能使用的公共安全术语进行了定义。

同时，研究者们还提出了若干适用于特定领域的安全需求描述语言，主要有: SDL(Scenario Description Language)，一种基于安全评估标准的场景片段织入型安全需求描述语言，通过SDL 描述的与安全相关的特定场景片段能够通过织入技术自动定位、插入到相关主成功场景，从而实现安全需求的自动织入。

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(2) 安全需求的获取与分析

使用合适的安全需求获取技术是成功获取安全需求的首要条件。除了面谈、头脑风暴等非结构化的需求获取方法外，目前结构化需求获取技术主要有误用例法MC、软系统法SSM、控制需求表达法CORE、问题分析法IBIS、联合应用开发法JAD、面向特征领域分析法FODA、关键步骤分析法CDA 和加速需求获取法ARM 等。

安全需求的获取实际上是一个对用户意图不断进行揭示和判断的过程。当用户在对信息系统自身的状况和可能遇到的安全危险并不太了解的情况下，只能提出一些较为抽象的安全需求。安全危险性分析的目标就是对各种危险信息进行全面地收集和充分地分析，以使用户能够进一步地明确系统的脆弱点和可能遭受的安全威胁，从而能够提出详细的、准确的安全需求。

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(2) 安全需求的获取与分析

当前安全需求分析技术有很多，主要从两方面分析系统安全需求。

一类是非形式化分析方法，分析系统可能遭受的安全威胁。例如，软件故障树分析(SFTA) 法，以一种逆推的方式对一个已知的入侵行为进行建模分析。

另一类是形式化分析方法，从身份识别、权限管理、密码保护、信任评估等方面分析系统应满足的安全需求。

这些方法都是从系统层面或使用系统的组织机构层面来定性的分析安全需求。

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(3) 安全需求建模

针对安全需求工程中的概念和研究理论的不同，提出了相应的安全需求建模方法。最具代表性的是: Giorgini 等人以Tropos/i* 框架为基础；

另有一些人提出了面向系统的安全需求建模方法，是对访问控制策略建模和怎样把这些策略整合到模型驱动的软件开发过程中。比如， 提出了一种扩展的统一建模语言(UML) ，即UMLsec，对诸如机密性和访问控制等安全相关的特征进行建模；

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(3) 安全需求建模

也有一些人提出了从反面通过诱导，对攻击者的行为进行安全需求建模的方法。典型的有：采用用例(用例描述了系统允许的一个功能) 来获取和分析安全需求，并引进了反用例模型(通过对系统的不受限制和约束的任意使用，来增加系统的危险性) 。

通过对以上各种安全需求建模方法的分析，可以预测，未来的发展将会继续以已经存在的建模框架为基础，把安全相关的因素整合到框架中，并将CC融入到安全需求模型中，从而使安全需求建模方法更加完善，更加有效。

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(4) 安全需求模型检测

目前的安全需求分析技术主要分为形式化和非形式化两大类。

非形式化方法一般通过如攻击树等手段分析系统可能遭受的安全威胁;

形式化方法则主要通过将安全需求转化为形式化验证工具所能支持的表述形式进行验证。

需求检测在创造一个准确和可验证的安全需求中是关键因素，模型检测技术已经成为安全需求工程研究领域中的关键技术。

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(5) 安全需求的系统支持工具

基于安全需求工程中的各种建模框架，开发出相应的支持工具：

例如Giorgini 等人开发出的图形工具ST-Tool［30］，由ST-Tool内核和外部解析器两部分组成，能支持Tropos 框架中提出的所有新特征。

此外，最新开发出的si* -tool，也能对Security Tropos 进行建模，它与ST-Tool 具有相同的功能，并作为一种插件嵌入到主流的eclipse 开发平台中，使用XML 作为它的文档格式。

5.3.2 安全需求工程的研究现状

3. 安全需求工程的主要内容与进展

(6) 软件系统的安全风险评估

软件系统的安全风险评估主要是识别系统面临的脆弱性和威胁性。

安全风险是由于某种不希望事件的发生，从而对系统造成影响的可能性。根据系统安全工程能力成熟度模型(SSECMM)中的理论，能够成为风险的事件有三个重要的组成部分：安全威胁、系统脆弱点和事件造成的影响，一般而言，这三个因素必须同时存在才能构成安全风险。

目前，主要有以下风险评估技术: 政府问责办公室风险评估模型(GAO model)，美国标准技术研究所风险评估模型(NIST model)， INFOSEC 评估法，RFRM 模型，可生存系统分析法。

5.3.3 安全需求工程研究存在的不足

目前，尽管在安全需求工程领域取得了上述的若干成果，但在理论上，安全需求工程的研究方法还不够成熟，对安全需求工程相关概念的理解都比较模糊; 在应用方面，不能有效地指导软件工程实践、为开发出安全软件提供一个好的指导原则，安全需求工程还有若干问题需要解决。

总结对安全需求工程的研究，主要存在以下不足：

(1) 缺乏统一的安全需求概念，导致安全需求工程的研究范畴模糊。比如，学院派研究者着重考虑从理论上对安全需求建模，而实用派则主要对安全需求的实现手段进行需求建模，概念的不统一导致设计人员交流上的困难，不利于支持工具的开发，也不利于软件系统的应用。

5.3.3 安全需求工程研究存在的不足

(2) 对安全术语还没有形成统一的标准化定义，例如在Tropos方法中可以引进本体技术对安全需求相关概念进行描述，建模。

(3) 在需求阶段，没有把时间等相关因素考虑进去(比如安全的时效性) ，无法保证开发出的产品安全相关因素的存活期。

(4) 对于模型检测技术仅仅从形式化方法进行描述，未开发出可视化的检测工具。

(5) 目前的安全需求风险评估系统还不完善，安全风险度量理论还不成熟，不能有效的平衡系统的功能与开发系统时的经济花销。

安全需求工程结语

目前的安全需求工程研究的理论方法以ISO-15408 和ISO-17799 安全管理策略为基础，特别是在形式化分析技术中逐渐改正并完善自己的理论、方法。

针对安全需求工程未来的发展趋势，主要是基于本体对安全需求中所涉及的概念进行描述; 以面向领域的安全需求获取与分析方法作为建模的先决条件，开发出能直接映射成可运行代码的框架，实现真正的理论应用于实践。

谢谢大家！