第 33 卷 第 11 期 计 算 机 工 程 2007 年 6 月
Vol.33 No.11 Computer Engineering June 2007
·软件技术与数据库· 文章编号：1000—3428(2007)11—0037—02 文献标识码：A 中图分类号：TP311

基于目标的软件可信性需求规约方法研究

郭树行，兰雨晴，金茂忠
(北京航空航天大学计算机科学与技术系，北京 100083)

摘 要：高可信系统的软件规模不断扩大，其关键是分析并定义一致的可信需求描述，直接影响到需求规格说明的质量，进而影响到最终软件产品的质量。在目前公认的非功能需求规约框架的基础上，利用 B 抽象机理论，结合面向目标的规约方法，建立了一种可信性需求的分析与定义方法，即软件可信剖面。该方法可应用于 UML，利用 B 抽象机理论，为可信性需求模型的定理化证明奠定了基础。
关键词：可信剖面；面向目标；B 抽象机；需求规约

Research of Software Dependability Requirement Specification Method Based on Goal

GUO Shuhang, LAN Yuqing, JIN Maozhong
(Department of Computer Science and Technology, Beihang University, Beijing 100083)

【Abstract】 Analyzing and defining the consistent requirements of software dependability is critical to the development of complex dependable software systems. How to solve this problem directly influences the quality of requirements specification, as well as the final software production. Based on a widely-recognized management framework of NFR, this paper points out one requirement specification method of software dependability, which utilized the B AMN and thinking of goal-oriented theory. Such method can be named as the software profile of dependability. It may be applied in the UML area and also provides the formal input for the B proof though the B AMN.
【Key words】 Dependability profile; Goal oriented; B abstract machine; Requirement specification

软件系统的需求来自于人类对现实社会的知识和期望[1]，从有可能不一致的知识或期望中归结出来的软件需求也不可避免地存在不一致的可能性。不一致需求是普遍存在的这个观点目前已经得到广泛的共识[2~4]。同时复杂软件系统开发的一个关键问题是分析和处理可能存在的不一致性。这个问题影响到最终软件产品的质量。可信性需求对于安全关键软件系统是非常重要的软件规约要素，将可信性需求分解精化，及其转化成为软件行为的约束是定义与实现可信性需求的关键问题[5]。

1 可信性需求的精化问题

系统被划分为若干子系统的同时，可信性等系统需求也被分配到各子系统上，从而形成子系统的需求规格说明。高可信计算机系统的日趋复杂使分析设计工作也越来越复杂[5,6]，因此必须遵循严格的工程化分析设计过程。如何针对可信性质发现一种分而治之的策略从而控制复杂性，是进行面向可信性质的软件设计和验证的关键。其重要作用正在被人们所认识，这方面的研究业也越来越受到关注。

2 形式化抽象机及目标规约方法

2.1 B 方法抽象机

B方法用伪程序语言来描述需求模型，B AMN的机器装配机制以及需求目标元模型的语法和语义，可对需求中可信性软目标图进行转换映射。根据映射图中节点和节点间的连接关系的描述，对每个节点定义机器[5]。定义机器的方法如下：

MACHINE Soft-goal
SETS
SOFT-GOAL
VARIABLES
Soft-goales,
att1, att2,…, attn
INVARIANT
Soft-goales SOFT-GOAL
att1 ∈ Soft-goales→C1∧
att2 ∈ Soft-goales→C2∧
attn ∈ Soft-goales→Cn
OPERATIONS
END

如果软目标之间存在某些关系，那么 C1,C2,…,Cn 中的某些将涉及其他的软目标 Soft-goal2, Soft-goal3,…，这时可使用 USES 或 SEES 关系：

MACHINE Soft-goal
USES Soft-goal2, Soft-goal3,
END

如果在 Soft-goal 的不变式中只使用对象同软目标体集合 SOFT-GOAL2, SOFT-GOAL3,…，就是说，为一个 Soft-goal 连接提供一个范围软目标型，那么可以使用 SEES。如果要使用更具体的并且要使用已有的软目标集合 Soft-goales2 等作为不变式中的范围软目标型，就要使用 USES。同样的道理，如果 Soft-goal2 与 Soft-goal1 互斥，约束 Soft-goales2 ∩

作者简介：郭树行(1978－)，男，博士生，主研方向：可信软件过程；兰雨晴，博士生；金茂忠，教授、博导
收稿日期：2006-07-10 **E-mail：**guoshuhang@buaa.edu.cn

Soft-goales1 =Φ应该加入到不变式中。当使用机器对软目标的一个实例而不是实例变量集合 Soft-goales 建立模型时，可以使用 EXTENDS 结构化机制来表示继承关系。

利用B抽象机理论，可以验证与证明需求[7,8,9]：

(1)冲突：在一个领域*Dom*中，一组断言$A_1,\ldots,A_n$之间出现矛盾，当且仅当下列条件成立：

1){Dom,∧1≤i≤n Ai}存在 False(逻辑不一致)；

2)对任意的 i:{Dom,∧j≠i Aj}不存在 False(最小性)。

(2)偏差：在一个领域*Dom*中，一组断言$A_1,\ldots,A_n$之间出现分歧，当且仅当存在边界条件*B*，使得：

1){Dom,B,∧1≤i≤n Ai}存在 False(逻辑不一致)；

2)对任意的 i:{Dom,B,∧j≠i Aj}不存在 False(最小性)；

3)存在一个场景 S 和时间点 i 使得:(S,i) ⊢B(可行性)。

(3)竞争：是单个目标中分歧的一种特殊情况，由下列条件来刻画：

1)目标由形为(∀x:X)A[x]的断言表示；

2){Dom,B,∧i∈I A[xi]}存在 False(对某个 I)；

3){Dom,B,∧i∈J A[xi]}不存在 False(对任意 J⊂I)；

4)存在一个场景 S 和时间点 i 使得：(S,i) ⊢B。

(4)障碍：是在只涉及单个断言时分歧的一种边界情况：

1){*Dom*,*B*,*A*}存在 False；

2){*Dom*,*B*}不存在 False；

3)存在一个场景 *S* 和时间点 *i* 使得：(S,i) ⊢B。

2.2 面向目标的需求规约方法

面向目标的需求规约方法已经经过了几年的发展[10~12]，其中典型的KAOS[13]方法已经提供了一门需求规格说明语言、一种面向目标的软件需求规约模型及其有关的元知识。然而KAOS方法的语义网外层尚不支持需求模型的可视化建模，系统目标之间一般只是AND与OR关系；另外，掌握KAOS方法对于系统工程师有一定的复杂度。本文利用UML Profile 将语义网外层通过可视化方式进行定义；基于B方法抽象机方法[14]定义目标并提供有关的元知识，扩展了目标之间的AND与OR关系，提高了需求目标模型建模的灵活性，同时也为形式推导提供直接映射输入，为需求目标的形式化验证提供了基础。

3 可信软件 UML Profile

可信软件 UML Profile（trusted software UML profile, TSUP）是一种面向目标的方法。在此方法中，可以利用可信 Soft-goal 来表示系统需要满足的可信性需求。

3.1 UML Profile 概念元模型

基于 B 抽象机的目标需求规约元模型见图 1。

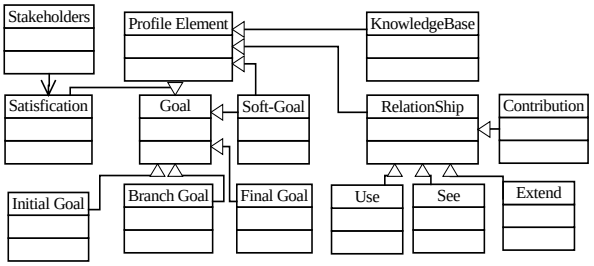

图 1 基于 B 抽象机的目标需求规约元模型

(1)目标可满足性（Satisfaction）：用于描述模型中节点可满足性，例如软目标，代表着不同用户对目标的满意度序列。

(2)贡献率（Contribution value）：定义节点间关系的关联（Edge）属性，表示当前子目标对于父目标的实现所起的贡献作用。

(3)元知识库（Knowledge base）：描述模型中节点或关系有向边的扩展属性，意味着目标分解为子目标的原理，或将此目标定义为父目标的子目标的原因，及为何将目标可信度及贡献率附加到模型节点与关系有向边上的原因。

3.2 目标规约的过程

需求规约模型的建模过程如图 2 所示。

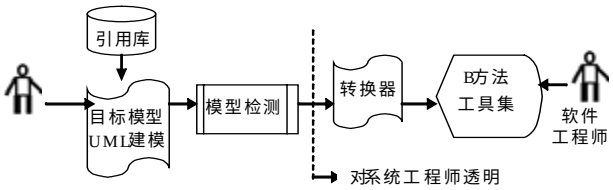

图 2 目标规约过程

(1)将系统相关人员（Stakeholders）的需求进行等价类划分，根据不同的等价类定义初始系统目标，初始目标（Initial Goal）覆盖用户的需求；

(2)根据规则(1)，针对每个父目标，按等价类划分将其分解并精化为分支子目标(Branch Goal)，直至目标不可分解并可操作化，这时不可再精化的目标成为叶子目标(Final Goal)。

(3)将模型转化为 B 抽象机，基于 B 语言抽象机检测并解决目标之间的冲突、偏差、竞争、障碍。

4 元模型在可信性需求规约中的应用

Web 系统易用性分析如图 3 所示。

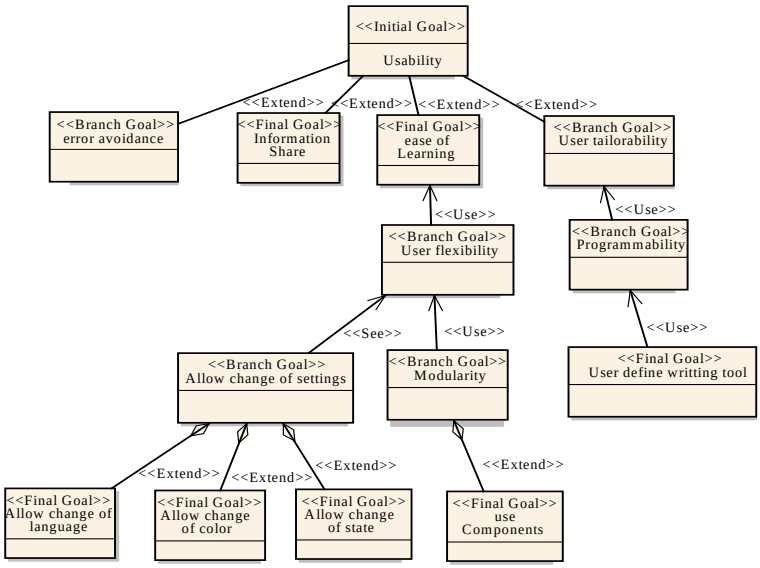

图 3 Web 系统易用性分析

下一步通过将 UML 模型转换成 B AMN 以后，就可以利用 Unix 或 Linux 下的 B 语言工具集，如 BToolKit，进行细化，实现以及验证。经过在 Redhat Linux 平台上的 BToolKit5.1.1 中对已有 UML 模型的转换运行，证明了本方法的可行性和有效性。

5 结束语

可信性需求的目标规约方法，依赖于其需求建模理念“目标”的语义。目标规约方法认为任何软件系统都是用来实现或达到一个或一组系统目标。通过 UML Profile 元模型，需

（下转第 41 页）