

面向可信软件的风险管理模型研究*

杨洁^{1,2}, 杨育¹, 王小磊^{1,3}

(1. 重庆大学机械工程学院, 重庆 400030; 2 重庆通信学院, 重庆 400035; 3 华北电力大学, 河北 保定 071003)

摘要: 进行了面向可信软件的风险管理模型的研究。首先采用贝叶斯信仰网络对影响软件可信性的风险进行了分析;其次,建立了基于约束满足的风险控制模型。该软件项目风险管理研究为提高软件质量,实现软件的可信性提供了新思路。

关键词: 软件可信性; 风险管理; 贝叶斯信仰网络; 约束满足

中图分类号: TP311 **文献标志码:** A **文章编号:** 1001-3695(2008)10-3010-02

Research for model of risk management oriented to reliability soft

YANG Jie^{1, 2}, YANG Yu¹, WANG Xiao-lei^{1, 3}

(1. College of Mechanical Engineering, Chongqing University, Chongqing 400030, China; 2 Chongqing Communication College, Chongqing 400035, China; 3. North China Electric Power University, Baoding Hebei 071003, China)

Abstract: This paper suggested a risk management model oriented to reliability soft. Firstly, used the Bayesian belief networks (BBN), the risks which had influenced the reliability of soft were analyzed. Secondly, established a risk control model based on constraint satisfaction. The research on soft project risk management provided a new method for improving the quality and reliability of soft.

Key words: soft reliability; risk management; Bayesian belief networks (BBN); constraint satisfaction

目前,软件质量还不能完全达到软件可信性的要求。可信软件的研究工作大多从安全性分析等技术方面保障和提高软件的可信性^[1]。但是,当软件开发规模大幅度增加,软件开发环境复杂化以及软件运行环境急剧恶化时,软件可信性面临着更加严峻的挑战,通过技术手段来提高软件的可信性变得非常困难。开发高质量可信软件的根本问题不仅在于是否使用新的技术,更在于开发过程中是否采用科学的风险管理标准^[1-3],尤其还需要解决可信软件开发过程中的风险管理 with 过程优化问题。因此,加强可信软件开发过程中的风险管理以提高软件质量与可信性是亟待解决的重要问题。

贝叶斯信仰网络

在不确定性的决策支持研究领域,BBN 近年来受到了极大的关注^[4,5]。BBN 的基本理论(如贝叶斯概率)已存在较长时间,而其算法和相关软件工具在近年来才被运用起来。贝叶斯信仰网络由具有一系列条件概率表的非周期性图表组成。BBN 中的节点代表随机变量,它的状态通常用离散数字或数据段来表示。弧代表变量之间的因果关系。条件概率表(CPT)与每个节点相联系,并表示出节点间的相互作用而对某个指标的影响概率。其中,如果变量 A 具有父节点 B_1, B_2, \dots, B_n ,在 CPT 中其节点将被赋值为 $P(A | B_1, B_2, \dots, B_n)$ 。同时可以利用专家的经验来填写 CPTs 中的数据。例如当 BBN 的根节点是未知数时,专家们通常对这些根节点均匀分配以分布概率。而不确定性决策支持过程中获得新数据时,将

新数据加入 BBN 网络,重新计算和更新节点数值,数值更新过程从父节点传递到子节点。并且,BBN 中的图表能扩充成 BBN 影响图,其最基本的形状分别用长方形和菱形表示。

以考虑影响软件可信性的风险为例,建立软件产品质量风险的 BBN 影响简图,如图 1 所示。在图中可以看出,管理者能力和开发者能力影响着软件产品的可信性质量;训练节点是决策节点,它与作为通用节点的训练成本节点相连。同时运用专家经验,得到软件产品质量的 CPT,如表 1 所示。BBN 能模拟网络构造者的信仰,基于该信仰,BBN 可提供软件开发项目中风险的相关数学运算、预测;BBN 也能用于支持可视和可重复的风险管理决策的制定以及复杂软件项目风险管理的度量。

表 1 软件产品质量的 CPT

管理者能力 开发者能力	高		低	
	高	低	高	低
概率(产品质量高)	0.9	0.85	0.35	0.15
概率(产品质量低)	0.1	0.15	0.65	0.85

基于 的软件项目风险管理系统框架

本文采用 BBN 来支持可信软件开发项目风险评估和风险控制策略的制定。建立基于 BBN 的风险管理系统框架,如图 2 所示。从该系统框架图中可以看出,运用 BBN 能分析风险并产生管理者的风险控制决策信息;同时管理者输入风险信息数据或管理决策数据到 BBN 中,以进行下一步的风险评估和预测^[6]。为实现动态可持续的风险管理,在风险管理系统中需要反馈环路,同时在反馈环路中使用 BBN。BBN 在每次迭代

收稿日期: 2007-12-14; 修回日期: 2008-03-12 基金项目: 国家自然科学基金资助项目(70601037); 重庆市科技攻关基金资助项目(CSTC, 2007AC2039); 重庆市自然科学基金资助项目(CSTC, 2007BB6106)

作者简介: 杨洁(1973-),女,博士研究生,主要研究方向为生产制造管理、风险管理(yangjie5581@163.com); 杨育(1971-),男,教授,博导,主要研究方向为系统建模与仿真、制造系统工程等。

构,四个视图模型从特定的不同方面描述软件的体系结构,忽略与此无关的实体。描述系统的功能需求采用逻辑视图,即系统提供给最终用户的服务;描述系统的运行特性采用进程视图,侧重关注非功能性的需求(如性能、可用性),该视图服务于系统集成人员,方便后续性能测试;硬件配置采用物理视图描述,该视图服务于系统工程人员,解决系统的拓扑结构、系统安装、通信等问题;软件模块的组织与管理采用开发视图描述,该视图服务于软件编程人员,方便后续的设计与实现;最后用场景视图刻画构件之间的相互关系。将四个视图有机地联系起来,场景视图不仅可以描述一个特定的视图内的构件关系,而且可以描述不同视图间的构件关系。在四个视图中,逻辑视图、开发视图主要用来描述系统的静态结构;进程视图、物理视图主要用来描述系统的动态结构。ATAM在实际运用中并非每个系统都必须将五个视图都画出来,而是各有侧重。

SAAM则提倡使用非常单纯的体系结构要素。对体系结构的静态描述一般都要区别数据的连接(数据在组件之间的传递)和控制连接(一个组件调用另一个组件执行某个功能);对软件体系结构的动态描述主要描述系统在各个不同时间的行为,给出软件的体系结构。软件体系结构的描述既可以用自然语言来描述系统的整体行为,又可以采用某种形式的结构化的描述,表述形式相对灵活。

结束语

SAAM与ATAM方法相比较,是一种相对简单的软件体系结构评价方法,进行培训和准备的工作量较少。尽管SAAM评估步骤及细节较少,但是涉及的内容更多,在评估中没有提供体系结构质量属性的清晰度量,评估过程过于依赖专家经验。总体评估时还需根据场景对系统功能的相对重要性设置权重,确定总体评价,权重的设置具有很强主观性,故SAAM方法适于体系结构的粗糙评价,用于边设计边评估的软件体系结构开发过程。

ATAM方法是目前被验证有效并广泛使用的一种体系结构评估方法,但没有对质量属性作深入分析,同样缺少定量数据来支持分析结果。ATAM方法尽管揭示了体系结构如何满

足特定的质量目标,而且还提供了这些质量是如何交互的,即它们之间如何权衡,但这些设计决策将影响整个软件生命周期,且软件实现后很难修改这些决策的影响。

目前对体系结构分析与评价大多采用基于场景的技术,这种技术存在着一定的不确定性。如何根据某质量特征使确立的场景更有代表性和完备性,如何为构造的场景确定合适的边界条件,即停止准则等。这些在具体应用中都有很大的主观性及经验性,而度量的评估方法在这方面做得较好,将定量的度量方法与定性场景结合是提高软件体系结构评估的有效途径。

参考文献:

- [1] BASS L, CLEMENTS P, KAZMAN R. Software architecture in practice [M]. Reading, Massachusetts: Addison-Wesley, 2002.
- [2] 张友生. 软件体系结构. [M]. 2版. 北京:清华大学出版社, 2006: 256-279.
- [3] 刘霞,李明树,王青,等. 软件体系结构分析与评价方法评述[J]. 计算机研究与发展, 2005, 42(7): 1247-1254.
- [4] 沈群力,刘渊. 微支付系统的解决方案研究[J]. 安徽大学学报, 2002, 26(3): 29-31.
- [5] 沈群力,唐思章,刘杰. 基于微支付的网络认证协议[J]. 上海商学院学报, 2006, 7(1): 27-30.
- [6] 沈群力. 信息系统分析与设计实验教学探讨[J]. 实验科学与技术, 2007, 5(2): 84-86.
- [7] GR MANA A, PEREZA M, MENDOZA L, *et al* Feature analysis for architectural evaluation methods[J]. The Journal of Systems and Software, 2006, 79(2): 871-888.
- [8] OLUMOFIN F G, MISD V B. A holistic architecture assessment method for software product lines [J]. Information and Software Technology, 2007, 49(4): 309-323.
- [9] LOPEZ M. Application of an evaluation framework for analyzing the architecture tradeoff analysis methodSM [J]. The Journal of Systems and Software, 2003, 68(12): 233-241.
- [10] ARES J, GARCIA R, JURISTO R, *et al* A more rigorous and comprehensive approach to software process assessment [J]. Software Process: Improvement and Practice, 2000, 5(1): 3-30.
- [11] CLEMENTS P, KAZMAN R. Valuating software architecture methods and case studies [M]. [S 1]: Addison-Wesley, 2002: 235-241.

(上接第 3011 页)关理论,对面向可信软件的风险管理模型进行研究。提出基于 BBN 的软件项目风险管理系统框架和影响软件可信性的风险因素 BBN 分析方法,采用 BBN 对影响软件可信性的风险进行分析评估。在风险分析、风险评价的基础上,建立基于多维约束满足的 HTOEP 风险控制模型,从环境、人因、技术、组织、过程多角度控制可信软件开发过程中的风险。通过面向可信软件的风险管理研究为软件产品质量的提高,软件可信性的实现提供新思路。

参考文献:

- [1] CARR M J, KONDA S, MONARCH I, *et al* Taxonomy based risk identification, Technical Report CMU/F93-TR-6 [R]. Pittsburgh, Pennsylvania: Software Engineering Institute, Carnegie Mellon University, 2002.
- [2] BOEHM B W. Software risk management: principles and practices [J]. IEEE Software, 1991, 8(1): 32-41.
- [3] CHARETTE R. Software engineering risk analysis and management

[M]. New York: McGraw Hill, 2005.

- [4] FRIEDMAN N. A Bayesian approach to structure discovery in Bayesian networks [J]. Machine Learning, 2003, 5(1-2): 95-125.
- [5] 冯楠,李敏强,寇纪淞,等. 基于贝叶斯网络的软件项目风险分析过程 [J]. 计算机工程与应用, 2006, 42(18): 16-18, 39.
- [6] HALL E M. Managing risk: methods for software system development [M]. [S 1]: Addison-Wesley, 2002: 89-99.
- [7] HOUSTON D X, MACKULAK G T, COLLOFELLO J S. Stochastic simulation of risk factor potential effects for software development risk management [J]. The Journal of Systems and Software, 2001, 59(3): 247-257.
- [8] HAN Wenming, HUANG Sun-jen. An empirical analysis of risk components and performance on software projects [J]. The Journal of Systems and Software, 2007, 80(1): 42-50.
- [9] OSMUNDSON J S, MICHAEL J B, MACHNIAK M J, *et al* Quality management metrics for software development [J]. Information & Management, 2003, 40(8): 799-812.