GSN是一种可以明确说明任一论证过程中存在的元素机器相互关系的图形化论证符号语言。运用GSN语言来表述论证过程可以有助于形象、具体、合理地说明系统、运营肌组织的安全性能。运用GSN语言完成的论证模型主要是用来表述安全子目标是如何支持顶层的安全目标的，下一层的安全子目标又是如何支持该层安全子目标的。

采用一种生命周期数据进行配置管理检验的方法。即给出一种软件配置管理过程的动态模型，通过将生成的生命周期数据输入该模型，模型能够对整个软件生命周期进行一次模拟管理，并通过比较软件配置管理记录与各个标识项是否吻合、生命周期数据的改变是否符合相关目标要求的方法对配置管理目标进行验证，可以用于审定过程，也可以用于开发过程期间的检查等。

技术方案（如图 5）：

1. 研究配置管理记录。从庞大的生命数据周期数据中找到与配置管理中变更控制相关的管理记录数据。
2. 研究标识项的文档属性。问了能够对变更情况进行跟踪，必须对标识项数据的属性进行提取。关键要素是角色、创建时间、更改时间、更改的数据元或数据项。
3. 研究选定建模方法。具体建模方法见关键技术与难点。
4. 变更控制目标模型化。



图 5 技术方案

3.2.3审定辅助工具

基于完成的配置管理过程的模型实现审定辅助工具。审定辅助工具的作用是能够通过输入已生成生命周期数据，对软件在开发过程中是否实现了配置管理相关目标进行验证。

3.2.3.1审定工具的功能

审定辅助工具是一个配置管理环境的模拟，每次从生命周期数据中读取一条配置管理记录，通过这条管理记录对生命周期数据中相关配置项进行检查，判断是否相互矛盾，同时根据配置记录内容改变当前的虚拟配置管理环境的状态，再输入另一条配置管理记录，依次循环直至配置管理记录全部读取完毕（如图 6）。

## 

## 完成的工作内容一

## 对do178标准和现状的研究和学习

对整个证据管理现状的调查研究显示，

在适航软件 符合do178c标准，配置管理方面，国内的大部分研究集中在具体实践中配置管理方案的制定。

从对软件的适航进行安全认证的角度看，国外部分专家

## 完成的工作内容二

## do178c配置管理过程目标和过程的分解。

面向适航审定中对于配置管理过程的审查。

证据：通过生命周期数据来体现

证据+专家现场审查 可以证明符合do178c标准

基于清单进行review ，但清单基于分解问题的考虑，不考虑审定的自动化怎样实现。

核查人员与审查人员应该进行的工作内容是区别不大的，主要区别在于进行review的人员不同。

审查方不应对研发方干涉太多，但按审定经验来说，现阶段采取最多的也是最有效的方法即使提前规定好证据的规格。

利用GSN方法将目标与过程 进行分解，直到分解出最小证据（能够直接通过生命周期数据识别）。

证据将分为两类，一、由计算机进行检查

二、由专家进行检查

证据列表：

细分为以下证据

2.3.3.1适航软件开发中关于配置管理的目标

在Do178c标准的71个目标中，以下6个是与配置管理相对应的目标。

1. 标识构型项（A-8.1）
2. 建立基线和可追溯性（A-8.2）
3. 建立问题报告，变更控制，变更评审和构型状态纪实机制（A-8.3）
4. 建立归档、检索和发布机制（A-8.4）
5. 建立软件加载控制机制（A-8.5）
6. 建立软件生命周期环境控制（A-8.6）

必须注意的是，这些目标都是比较笼统的，无法直接应用于开发与审查的实践，在对目标进行验证时，对于每个目标在研发实践中如何保证需要更加细致的了解，同时必须考虑到隐形目标的存在。

Do178c规定的目标，过程要求。结合变更管理的基本要求，符合配置管理的控制类别cc2.

|  |  |  |
| --- | --- | --- |
| SCM进程活动 | CC1 | CC2 |
| 配置鉴定 | ● | ● |
| 基线 | ● |  |
| 可追溯性 | ● | ● |
| 问题报告 | ● |  |
| 变更控制-完整性和鉴定 | ● | ● |
| 变更控制-跟踪 | ● |  |
| 变更审查 | ● |  |
| 配置状态统计 | ● |  |
| 恢复 | ● | ● |
| 已批准变更的保护 | ● | ● |
| 媒体选择，刷新，复制 | ● |  |
| 释放 | ● |  |
| 数据保留 | ● | ● |

|  |  |
| --- | --- |
| 数据项内容 | 原子性数据项 |
| a.1软件配置索引 |  |
| a.2需要变更的基线 | a.2.1基线的受控软件库  a.2.2基线.pre  a.2.3基线.next |
| a.3变更完成后的基线 | a.3.1基线的受控软件库  a.3.2基线.pre |
| a.4配置项库 |  |
| a.5变更申请单 | a.5.1变更影响分析（包含受变化影响的生命周期数据）  a.5.2受影响的配置项或数据元列表（变更对象）  a.5.3软件发生错误的起始处（如果是需求变更则需求处）  a.5.4变更和行动 ） |
| a.6变更审批单 | a.6.1变更影响分析 （包含受变化影响的生命周期数据）  a.6.2受影响的配置项或数据元列表（变更对象）  a.6.3软件发生错误的起始处（如果是需求变更则需求处）  a.6.4变更和行动 ） |
| a.7问题报告 | a.7.1变更影响分析 （包含受变化影响的生命周期数据）  a.7.2受影响的配置项或数据元列表（变更对象）  a.7.3软件发生错误的起始处（如果是需求变更则需求处）  a.7.4变更和行动 ）  a.7.5问题描述  a.7.6问题报告的批准、关闭情况。 |

|  |  |  |
| --- | --- | --- |
| 7.2.2基线和可追溯性 | 应为配置项建立基线供认证信誉（certification credit）使用 | 通过生命周期中基线建立、变更情况以及软件配置索引中的基线记录确保变更控制被正确全面的落实。 |
| 应为软件产品建立软件产品基线 |
| 软件产品基线应定义在软件配置索引中 |
| 基线控制应建立受控软件库，无论是物理的，电子的或其他，以确保其完整性。 | 联合检查受控软件库和软件配置索引。 |
| 基线一旦建立，其更改应该收到保护。 | 未经变更程序或基线建立，不会建立基线。对基线建立，变更程序和基线库中存在的基线进行检查 |
| 变更控制活动应从已建立的基线发展出一个衍生的基线 | 检查a.2.3 |
| 基线应可追溯它是从哪个基线衍生出来的 | 检查 a.2.2 a.3.2 |
| 一个配置项应该可追溯至它是从哪个配置项派生出来的 | 检查 a.4 |
| 7.2.3问题报告，跟踪和纠正措施 | 一个问题报告应准备好描述进程不按计划执行，输出的不足，或软件异常行为数据项 | 检查a.7.5 |
| 问题报告应采取纠正措施 | 检查a.7.4 |
| 问题的报告应提供受影响的配置项或受影响的活动过程的配置标识 | 检查a.7.2 |
| 问题报告的status报告 | 问题报告的状态 |
| 问题报告的批准与关闭情况。 | 检查a.7.6 |
| 若问题报告需要对软件产品或软件生命周期过程的输出采取纠正行动，应调用变更控制活动。 | 不需要变更的都直接关闭了，其它都调用了变更。 |
| 7.2.4变更控制 | 变更控制应通过对配置项和基线的变化提供保护 来保证他们的完整性。 A | 通过生命周期中基线建立、变更情况以及软件配置索引中的基线记录确保变更控制被正确全面的落实。 |
| 变更控制应确保任何一个配置项的变化，都需要改变其配置标识。 | 通过生命周期中基线建立、变更情况以及软件配置索引中的基线记录确保变更控制被正确全面的落实。同时配置项改变但配置标识未改变的无法直接发现，由专家结合其他活动发现。 |
| 对处于变更控制下的基线和配置项的变更，应被记录、批准、并进行跟踪。 | 通过对比变更前后的基线受控软件库的变化， 并结合检查数据项 a.5.3 a.6.3 a7.3的人工检查 |
| 软件的变化应当追溯到源头。 | 检查数据项 a.5.3 a.6.3 a7.3 是否追溯到源头 |
| 软件生命周期过程应当从(变化会影响它们的输出的地方）重新开始。 | 检查a.5.3,a.6.3,a.7.3 |
| 在整个变更活动中，受变化影响的软件生命周期数据应该更新 | 直接检查数据项 a.5.1 a.6.1 a7.1 ，若无数据项，可从数据项 a.5.2 a.6.2 a.7.2与软件生命周期数据的包含关系中取得受变化影响的软件生命周期数据。 |
| 变更控制活动的记录应保存。 | 数据存在且无明显造假 |
| 7.2.5变更审查 | 评估问题或提议的系统需求变化的影响。应为系统过程提供反馈，包括系统安全评估过程，系统过程的任何反应都应被评估。 | 检查数据项 a.5.1 a.6.1 a7.1 |
| 评估问题或提议的软件生命周期数据变化的影响. | 检查数据项a.6.1 |
| 确定 将要做出的变更和采取的行动。 | 检查a.5.4 |
| 确认受影响的配置项已经被标识。 | 由假设7.2.1已达到。 |
| 对问题报告或变化的影响进行反馈并作出决定（影响那些过程） | 检查 a.6.4 |

概念

Issue论点 假设、

变更管理过程 目标和过程分解成目标还是过程？

将配置管理相关目标相关的生命周期数据的数据项抽取出来

核心思想：研发方在制订计划时应尽量满足这些条件，使配置项能够

生命周期数据

证据的状态：1.不存在 2.不全面 3.不符合其他证据 4.

将一次变更作为研究对象。

本研究不对具体生命周期数据做出规定，而是通过提供 关键数据项，以供审查人员参考，审查人员可以据此 适当干预开发方制定配置管理计划，从而有效指导生命周期生成，便于审查工作。

是否需要考虑两次变更间互相影响，**独立性，并更需要锁定受控库**，如何实现。

从哪一过程开始锁定受控库，检出？开始审核时是否已经需要锁定。考虑基线的状态，当某基线处于可能改变时，不能对此基线进行其他变更，变更申请delay。

充分参考过程要求，目标要求，以及一般变更管理的要求，为了满足过程要求，有一些必须实现的证据，这些证据是 存在关联关系的。

**某证据存在是另一证据可能存在的基础。**

在过程要求中产生的证据 是存在**先后之分**的，A证据可能是B证据的基础，所以

## 完成的工作内容三

## 适航审定中的变更管理进行建模。

建模的考虑：1.对变更管理的过程，设计到开发的整个过程，而这个过程不是孤立的，涉及到了人员和时间的关系，建立模型后有利于理解和开发。

2.建立模型是对过程进行分析的一种方法，有利于理解。

更好的理解证据间关系。时间关系、人员关系。对变更管理利用uml进行建模。

关键技术或难点

1. 目标研究。

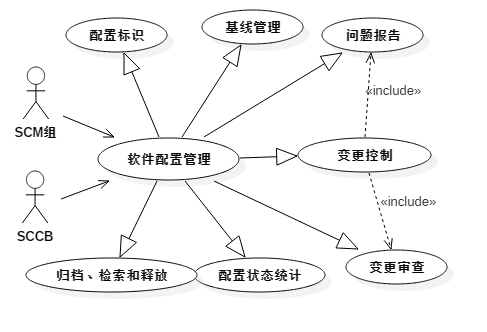
有隐形目标，设计到普通的变更管理的内容，也有do178c的要求，同时要考虑生命周期要素如人员、活动时间等关系。

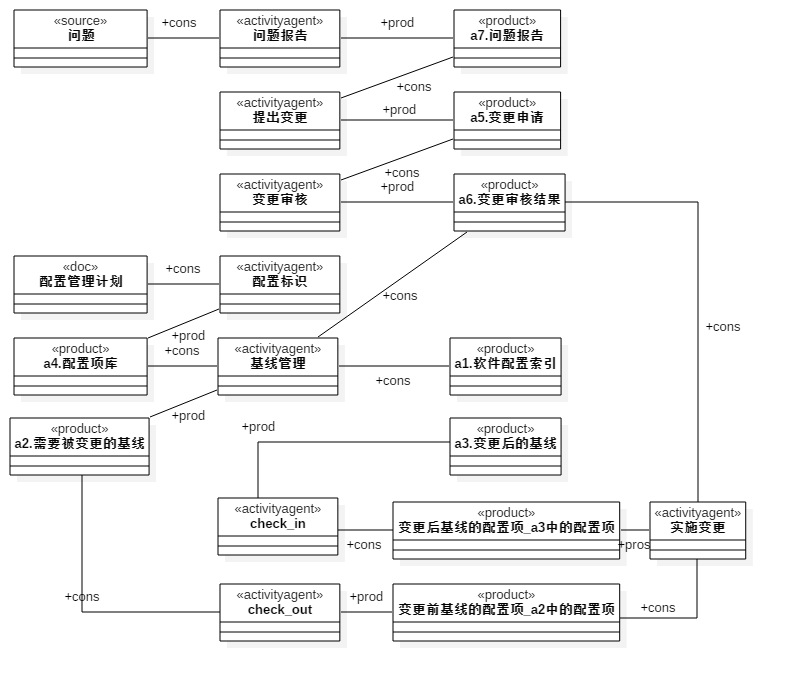
技术方案：

建模（别人的方法）+ gsn方法。同时考虑的 gQM等方法，

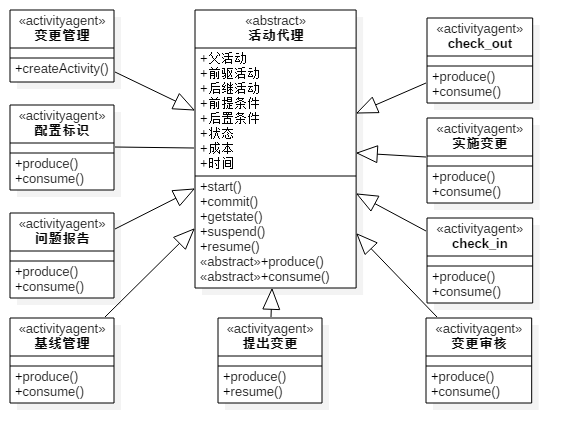
1. 建模的方法和角度

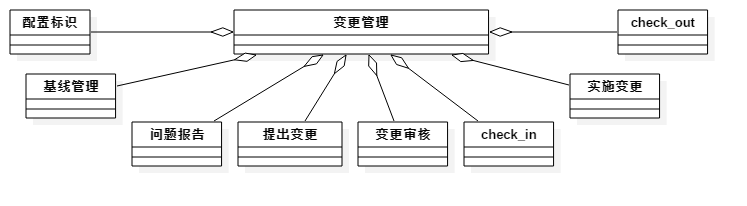
流程图

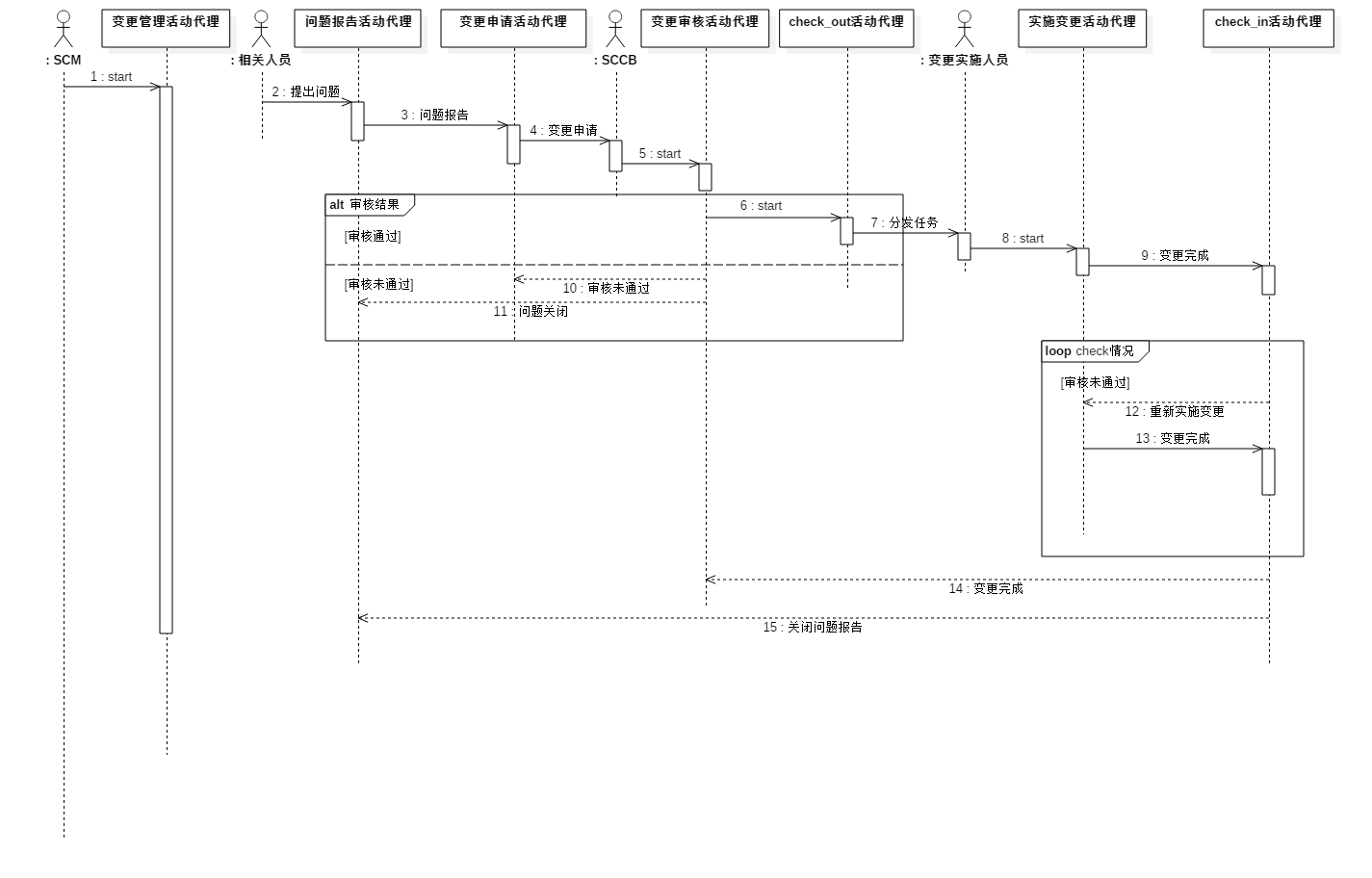
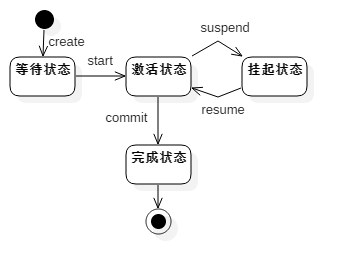
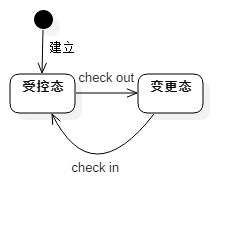












关键技术与难点

## 4.1.目标的验证

根据2.3.3.1，由于目标的模糊性和不全面性，对目标进行审定既要考虑实践工作中各种情况，还要考虑隐形目标的实现，怎样将目标的验证转化为模型是一个难点，为解决此问题，

4.2配置管理过程建模方法的选取

由于所建立模型的过程、数据与目标间的复杂关系，选择一种适用于此次建模的方法是一个难点。

由于过程建模是对软件过程活动的再工程,涉及到软件产品的开发与维护、软件项目管理、过程管理与过程改善等各个方面,涉及到过程活动、角色、产品、资源和约束等各种过程成分,还涉及到建模所用的形式化方法,加之软件过程本身具有的复杂性,使得构造过程模型的方法也是多种多样的。

* 以**过程所涉及的各种成分**(如活动、角色、产品、资源和约束等)为出发点来考虑过程建模。主要有四种不同方法：

1. 以活动为中心的建模方法
2. 以角色为中心的建模方法
3. 以产品为中心的建模方法
4. 基于过程模板的建模方法

* 以软件过程模型侧重于描述**功能目标**还是侧重于描述**活动行为**。主要考虑过程模型是否支持软件过程的动态性进行分类

1. 面向活动的过程建模方法
2. 面向目标的建模方法
3. 面向活动和面向目标的建模方法的结合。

* 按照过程建模所采用的不同形式化方法的分类。

1. 过程程序设计方法
2. 多功能分解方法
3. 基于计划的建模方法
4. 基于Petri网的建模方法
5. 基于规则的建模方法
6. 基于逻辑的建模方法
7. 基于知识的建模方法
8. 混合风格的建模方法

# 下一阶段工作计划

尚未完成的工作内容：

模型的验证

工具的开发

论文撰写

为解决的关键技术问题，下一步解决这些问题的思路

问题1：缺乏软件开发经验，具有挑战性，开发辅助工具可能费事费力

前期话费一些时间学习了mvc的相关知识，目前能够开展工作，在工作中还会遇到更多的问题

问题2：生命周期数据的获取和标准化

难以直接获得，后期开发出的辅助工具由于数据的非格式，可能只有极少部分能够又工具自动审定，使用工具可能更多的作为证据管理的作用。

技术思路或措施：一是要尽量找先关的生命周期数据，进行分析，最好能够找到将其进行预处理的方法；二是本研究的目的之一也在于 本研究不对具体生命周期数据做出规定，而是通过提供 关键数据项，以供审查人员参考，审查人员可以据此 适当干预开发方制定配置管理计划，从而有效指导生命周期生成，便于审查工作。 相信对我国适航软件的开发及审定技术也会有推动作用。

1. 民航局令第207号, 关于修订《航空发动机适航规定》的说明
2. 民航局令第207号, 航空发动机适航规定 尉询楷，杨立，刘芳，战立光，冯悦.
3. AC 20-115C. AirBorne Software Assurance,dated July 19,2013.
4. AB 20-115B. RTCA,Inc,Document RTCA/DO-178B, dated January 11, 1993.
5. 沈小明等. 机载软件研制流程最佳实践. 上海交通大学出版社，2013
6. SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems, 2010.12.
7. SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996.12.
8. RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification, dated December 13, 2011.
9. RTCA DO-330, Software Tool Qualification Considerations, dated December 13,2011.
10. RTCA DO-331, Model-Based Development and Verification Supplement to DO-178C and DO-278A, dated December 13, 2011.
11. RTCA DO-332, Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A, dated December 13, 2011.
12. RTCA DO-333, Formal Methods Supplement to DO-178C and DO-278A, dated December 13, 2011. Tong M,Thurman D R,Guynn M D. Conceptual design study of an advanced technology open-rotor propulsion system[R]. ISABE-2011-1311,2011.
13. SEI. CMMI for Development, Version 1.2-Improving Processes for Better Products. SEI, CMU, 2006.
14. Kitchenham BA, Mendes E, Travassos GH. Cross versus within-company cost estimation studies: A systematic review. IEEE Trans. on Software Engineering, 2007,33(5):316−329.
15. Jorgensen M, Shepperd M. A systematic review of software development cost estimation studies. IEEE Trans. on Software Engineering, 2007,33(1):33−53.
16. 王长元，赵莉，王淑蓉.软件工程与建模[M].西安交通大学出版署，2010.
17. 李明树，杨秋松，翟健.软件过程建模方法研究[J].软件学报，2009
18. 范玉顺.面向对象的Petri网方法及其在软件工程中的应用[J].计算机应用，1998
19. 乐晓波，汪琳.面向对象的Petri网建模技术的研究[J].计算机工程，2002
20. Lee S, Shim J, Wu C. A meta model approach using UML for task assignment policy in software process. In: Proc. of the 9th Asia-Pacific Software Engineering Conf. on APSEC 2002. IEEE Computer Society, 2002. 376−382.、
21. Bendraou R, Combemale B, Cregut X, Gervais MP. Definition of an Executable SPEM 2.0. In: Proc. of the 14th Asia-Pacific Software Engineering Conf. on APSEC 2007. IEEE Computer Society, 2007. 390−397.
22. Park S, Choi K, Yoon K, Bae DH. Deriving software process simulation model from SPEM-based software process model. In: Choi K, ed. Proc. of the Asia-Pacific Software Engineering Conf. on APSEC 2007. 2007. 382−389.
23. 陈迎欣.小组软件过程的仿真建模方法的研究[D],哈尔滨工程大学博士论文，2006
24. J.Peterson.Petri net theory and the modeling of systems[M].中国矿业大学出版社
25. 张绍阳.基于性能分析的一种OOPN关联矩阵建立方法[J].西北大学学报.
26. Atkinson DC, Weeks DC, Noll J. The design of evolutionary process modeling languages. In: Weeks DC, ed. Proc. of the Software Engineering Conf. on 2004 11th Asia-Pacific. Washington: IEEE Computer Society, 2004. 73−82.
27. Franch X, Ribó JM. A structured approach to software process modelling. In: Proc. of the 24th Conf. on EUROMICRO. IEEE Computer Society, 1998. 753−762.
28. Bhuta J, Boehm BW, Meyers S. Process elements: Components of software process architectures. In: Proc. of the Int’l Software Process Workshop (SPW 2005). LNCS 3840, Springer-Verlag, 2005. 332−346.
29. Min SY, Lee HD, Bae DH. Soft PM: A software process management system reconciling formalism with easiness. Information and Software Technology, 2000,42(1):1−16.
30. Henderson-Sellers B, Gonzalez-Perez C. A comparison of four process metamodels and the creation of a new generic standard. Information and Software Technology, 2005,47(1):49−65.
31. 李思广，林子禹，胡 峰，潘小劲.基于UML的软件过程建模方法研究，计算机工程与应用，2003
32. [张璇](http://epub.cnki.net/kns/popup/knetsearchNew.aspx?sdb=CJFD&sfield=%e4%bd%9c%e8%80%85&skey=%e5%bc%a0%e7%92%87&scode=21832615%3b09324537%3b09337460%3b17304744%3b24411866%3b27362069%3b); [李彤](http://epub.cnki.net/kns/popup/knetsearchNew.aspx?sdb=CJFD&sfield=%e4%bd%9c%e8%80%85&skey=%e6%9d%8e%e5%bd%a4&scode=21832615%3b09324537%3b09337460%3b17304744%3b24411866%3b27362069%3b); [王旭](http://epub.cnki.net/kns/popup/knetsearchNew.aspx?sdb=CJFD&sfield=%e4%bd%9c%e8%80%85&skey=%e7%8e%8b%e6%97%ad&scode=21832615%3b09324537%3b09337460%3b17304744%3b24411866%3b27362069%3b); [代飞](http://epub.cnki.net/kns/popup/knetsearchNew.aspx?sdb=CJFD&sfield=%e4%bd%9c%e8%80%85&skey=%e4%bb%a3%e9%a3%9e&scode=21832615%3b09324537%3b09337460%3b17304744%3b24411866%3b27362069%3b); [谢仲文](http://epub.cnki.net/kns/popup/knetsearchNew.aspx?sdb=CJFD&sfield=%e4%bd%9c%e8%80%85&skey=%e8%b0%a2%e4%bb%b2%e6%96%87&scode=21832615%3b09324537%3b09337460%3b17304744%3b24411866%3b27362069%3b); [于倩](http://epub.cnki.net/kns/popup/knetsearchNew.aspx?sdb=CJFD&sfield=%e4%bd%9c%e8%80%85&skey=%e4%ba%8e%e5%80%a9&scode=21832615%3b09324537%3b09337460%3b17304744%3b24411866%3b27362069%3b)，[面向软件非功能需求的软件过程建模方法](http://epub.cnki.net/kns/detail/detail.aspx?QueryID=4&CurRec=12&FileName=JFYZ201607018&DbName=CJFDLAST2016&DbCode=CJFQ&pr=)[M] 计算机研究与发展