第22卷 第8期
2012年8月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol. 22 No. 8
Aug. 2012

# 基于DO-254的航空集成电路设计保障研究

胡小婷,田 泽
(中国航空计算技术研究所,陕西 西安 710119)

**摘 要**:航空机载电子设备复杂度的不断提高,对于机载电子设备的基础——航空集成电路功能及性能的要求也不断提高,高集成度、高复杂度、高性能、低功耗、小型化已经成为了航空集成电路发展的必然趋势,而传统的设计和管理手段已经不能满足航空集成电路高安全性应用需求。探索并建立一个机载领域集成电路设计过程正确性保障体系,已成为迫切需要。DO-254标准代表了工业界、适航当局、机载领域硬件设计人员在内的大多数专家的一致意见,是机载电子硬件开发保证过程最好的实践经验的集合。文中将从集成电路硬件角度出发,研究并借鉴DO-254标准的需求管理和过程保证方法,将好的管理策略运用到集成电路系统设计和前端设计过程中,以提高航空集成电路硬件设计的安全等级,降低航空集成电路开发风险。

**关键词**:需求;确认;验证;配置管理;过程保证
**中图分类号**:TP39 **文献标识码**:A **文章编号**:1673-629X(2012)08-0189-03

# Research on Design Assurance for Aviation-integrated-circuit Based on DO-254

HU Xiao-ting, TIAN Ze
(Aeronautics Computing Technique Research Institute, Xi'an 710119, China)

**Abstract**: High complexity of integrated, high performance, low power dissipation and miniaturization have been considered as the inevitable tendency in aviation-IC while the requirement of function and performance had to be enhanced higher with increasingly complexity of aviation electronic devices. However, traditional design and management method could not satisfy developing demand of safety in aviation-integrated-circuit design field. It is definitely necessary to build a correctly and stably "procedure support system" for IC design in airborne implementation field. It is obviously that DO-254 standard could not doubt represent opinion of huge amount of experts in industry, airworthy department and IC designers of airborne field which DO-254 standard could be considered as the best and reliable standard in hardware design procedure of airborne implementation field. It focuses on research on requirement management and support process method of "DO-254 standard" standing on the view of hardware design, and then implement best manage strategy into system and front-end design in IC field in order to enhance safety level and decrease developing risk as possible as it could.

**Key words**: requirement; verification; velidation; configuration management; supporting processes

## 0 引 言

航空机载电子设备复杂度的不断提高,给航空集成电路的设计带来了巨大挑战,同时也引入了一些新的问题:需求遗漏、硬件设计错误难于管理、验证不全面等,传统的设计和管理手段已经不能满足航空集成电路高安全性应用需求。作为机载领域设计保证标准的DO-254[1]虽然定义了机载电子硬件开发的需求、设计、验证、确认、过程保证的目标及活动,但仍与航空集成电路开发有所不同。文中将结合DO-254标准中需求管理和过程支持的策略和方法,给出相应策略,确保航空集成电路硬件设计的可靠性[2]与安全性[3]。

**收稿日期**:2012-03-20;**修回日期**:2012-06-23
**基金项目**:装备预先研究项目(51308010601);武器装备预研基金项目(9140A08010712HK6101)
**作者简介**:胡小婷(1980-),女,陕西西安人,研究方向为集成电路设计与验证;田 泽,博士,研究员,中航工业集团首席技术专家,研究方向为SoC设计,嵌入式系统设计、VLSI设计。

## 1 DO-254体系概述

DO-254全称为"机载电子硬件设计保证指南"。该标准对硬件设计生命周期各阶段的目标、开展的设计保证活动以及产生的设计数据进行了详尽的阐述。图1为DO-254标准的内容框架。DO-254标准将硬件设计过程分为需求获取、概要设计、详细设计、实现与产品转换过程,这与传统的集成电路设计流程基本相同,不同的是,DO-254详细定义了支持过程,包括确认过程、验证过程、配置管理、过程保证以及审定联络,保证了硬件设计生命周期及其输出正确可控。

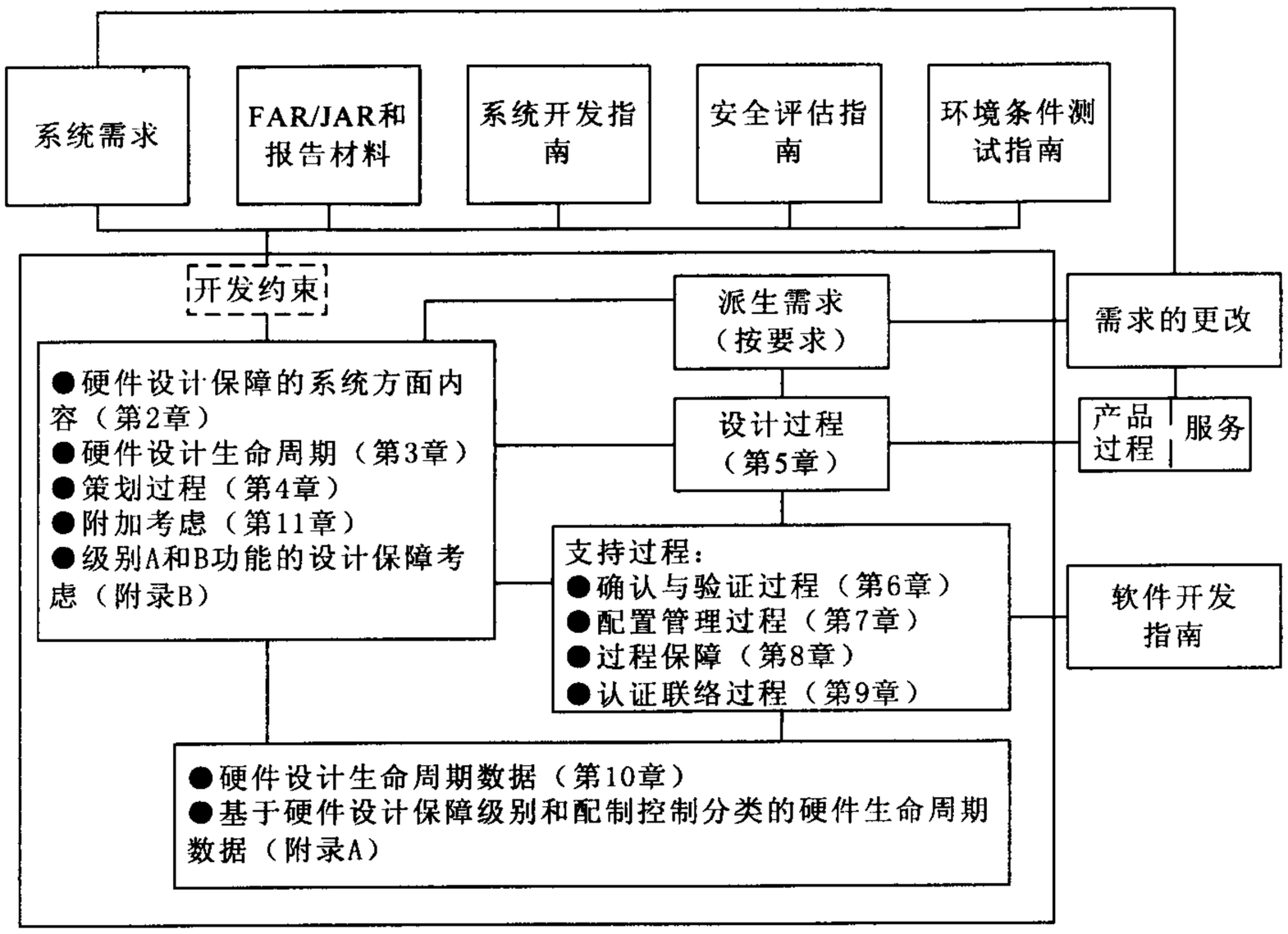


图 1 DO-254 标准的内容框架

确认过程是对硬件派生需求的正确性和完整性进行确认，并对派生需求进行安全性影响分析。

验证过程是保证硬件实体的实现满足其需求。验证包含验证计划中定义的评审、分析和测试过程。验证过程还包含对验证结果的评估，并建立硬件需求、实现与验证过程和结果之间的追溯关系。

配置管理过程的目的是为了唯一地标识并记录配置项，保证配置项复制的一致性和正确性，并提供标识和跟踪配置项更改的控制方法。

过程保证确保生命周期过程满足计划中确定的目标并完成相应的计划活动或者与计划的偏差得到处理。过程保证活动应独立完成，以保证生命周期过程评价、偏差识别以及纠正措施的客观性。

## 2 航空集成电路设计正确性保证策略

### 2.1 航空集成电路设计流程简介

集成电路设计流程划分为系统设计（需求获取、概要设计）、前端设计（详细设计）、物理实现和试制等几个阶段，与 DO-254 定义的生命周期基本相同，但在需求管理和过程控制方面，集成电路设计流程没有构建具体的需求追踪体系和详细的过程控制机制，随着航空集成电路设计规模与复杂度的不断增大，以目前的粗线条的管理手段已经不再适用。以下将基于 DO-254 标准与航空集成电路的系统设计[4,5]和前端设计[6]流程，给出如下基于需求的管理策略。

### 2.2 需求管理策略

#### 2.2.1 需求的确认

需求确认活动[7,8]用来保证需求是正确的和完整的。在需求确认阶段，所有的需求，包括派生需求，均应通过评审或分析等方法，进行确认；派生需求需要经过上层系统团队确认；需求与确认活动和确认结果之间应当建立追踪关系。

#### 2.2.2 需求追踪

应当建立需求与功能规范、概要设计、详细设计、验证规范、验证用例、验证报告之间的追踪关系。

#### 2.2.3 需求更改的管理

对于增加、删除、修改需求都应当做向上、向下的影响分析和回归性分析，并做好更改记录工作。比如，更改了一个需求，需要对验证程序进行修改，而这个验证程序可能覆盖了多个需求，所以验证程序的修改不仅要检查对更改的需求能否正确验证，还要检查是否保持了对其它需求的正确验证。

### 2.3 确认与验证策略

#### 2.3.1 确认策略

确认是对航空集成电路需求正确性、完整性和合理性的确认，可采用评审或分析的方法。确认活动应在集成电路设计的每个阶段进行，保证需求的正确性与完整性。确认过程是个反复迭代的过程，当在设计、验证及实现过程中发现有需求的错误、遗漏引起需求更改时，还需要重新确认复杂部件需求。系统设计和前端设计阶段的确认活动如图 2 所示。确认活动应当统计需求覆盖率，需求覆盖率应达到 100%，对于不能覆盖的需求应当给出理由。

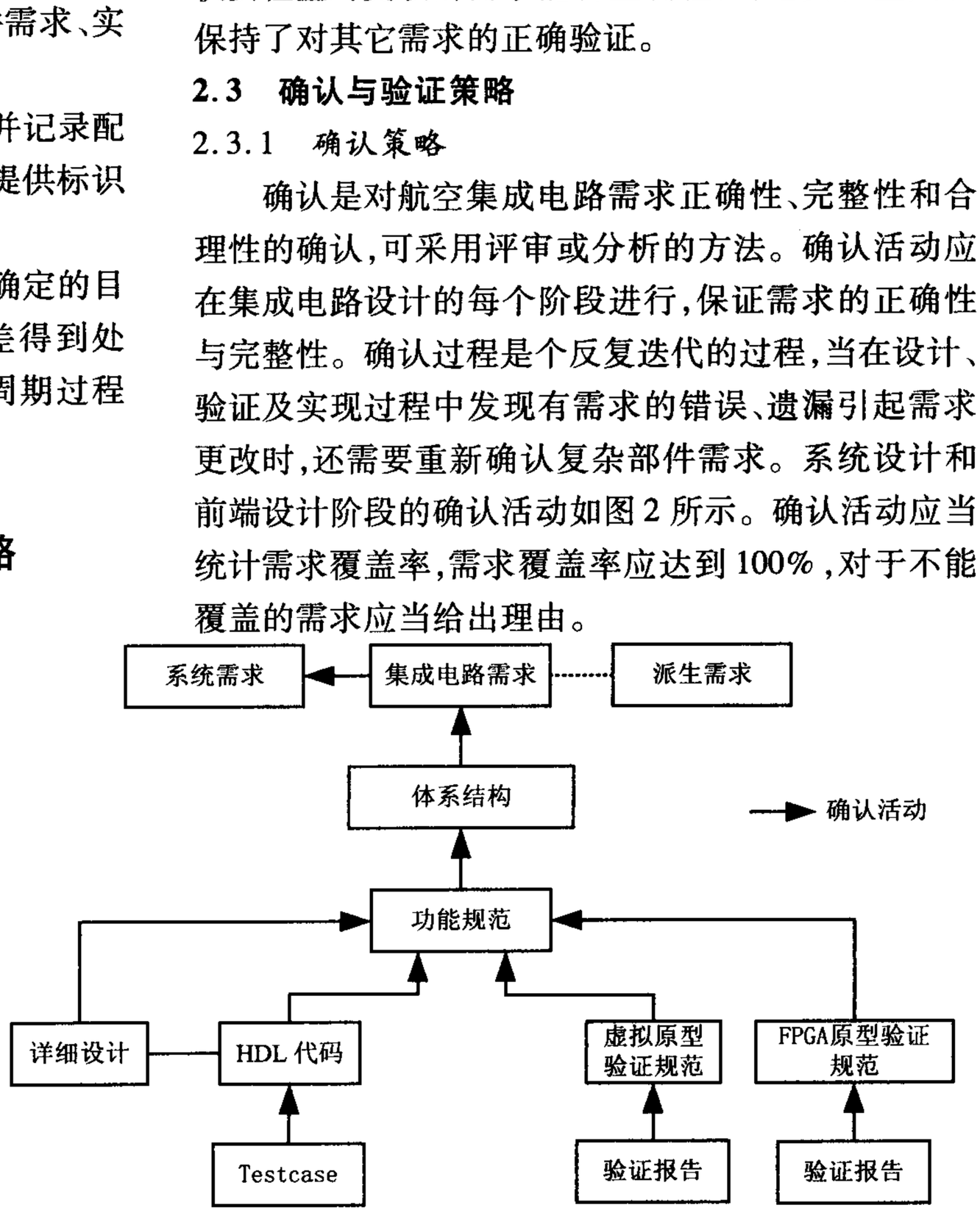


图 2 确认活动

#### 2.3.2　验证策略

代码检查及功能仿真采取自底而上的方式进行,即首先对各个模块自底向上进行代码检查和功能仿真,最后从设计顶层进行代码检查和功能仿真。

验证[9,10]是个需要回归的过程,当验证发现问题或不完善时,修改后需要重新回归验证。

当需求或设计发生更改时,应根据需求、设计、验证等之间追踪矩阵,进行影响分析,并确定需要重新验证的范围、内容,进行重新验证。

对于功能仿真[11]的需求覆盖率[12]应达到 100%,没有覆盖的应当给出理由;对于门级仿真,由于仿真运行时间过长,只进行典型测试用例的门级仿真,需求覆盖率应不小于 50%;采用分析方法来提供未覆盖部分的符合证据;对于时序仿真,由于仿真运行时间过长,只进行典型测试用例的后仿真,需求覆盖率应不小于 20%。采用分析方法来提供未覆盖部分的符合证据。物理测试应 100% 覆盖硬件需求。

### 2.4　配置管理策略

配置管理活动贯穿于航空集成电路设计的整个生命周期,完整的配置管理具备四个基本要素,分别为配置标识、配置控制、配置状态报告以及配置审查,其中配置控制是配置管理的核心,包括基线管理、配置库管理、配置变更控制等关键内容。配置管理活动体系结构如图 3 所示。

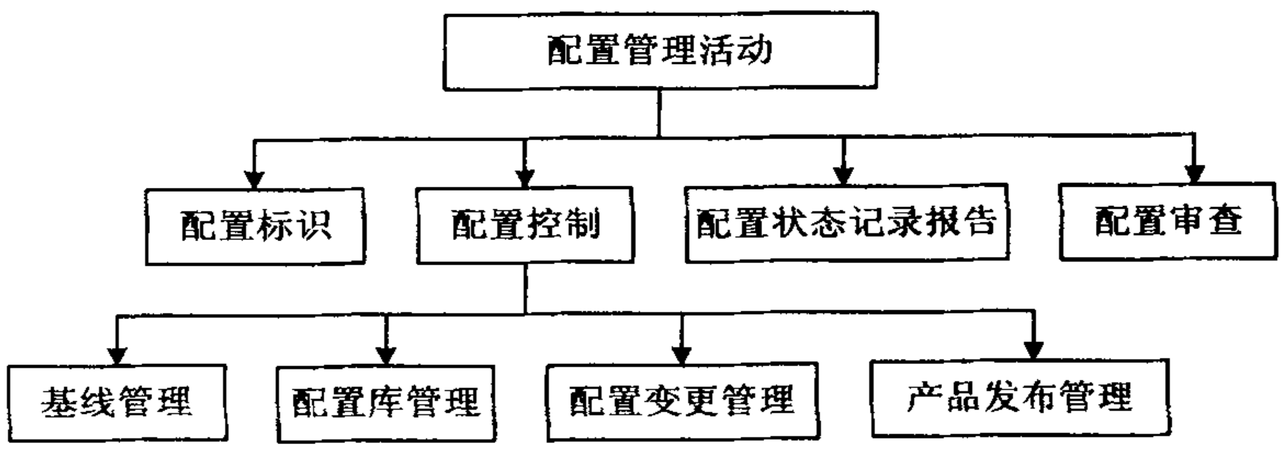


图 3　配置管理活动体系结构图

#### 2.4.1　配置标识管理

航空集成电路开发过程中产生或使用的配置项包括:文档、HDL 代码、开发包、开发工具、设计数据、确认与验证活动数据、配置管理活动数据、质量保证活动数据等。配置项标识定义为配置项的唯一标识,目的是清楚的为每一个配置项打上标识,以便为配置项的控制管理确定基准。

#### 2.4.2　基　线

基线是已经正式通过审核批准的规范文档或设计、生产数据,可作为项目进一步开发的基础,并且只能通过正式的配置变更控制过程实施改变,用于建立可控的配置项组合状态。每个基线应当具有唯一的基线名称和版本标识,当版本发生变化时,版本标识不允许后退,只能向上递增。

#### 2.4.3　配置库管理

在航空集成电路开发过程中,应当专门建立并维护一个配置管理仓库,实现数据的受控管理。对于配置库,可分为非基线状态和基线状态,非基线状态下配置库表现为版本受控,基线状态下配置库表现为更改受控。

#### 2.4.4　配置变更管理

航空集成电路开发过程中,对于配置项、基线以及发布版本的变更,都必须走更改控制流程,以保证所有变更都是可控的、可跟踪的、可重现的。配置变更控制流程应对整个处理流程进行详实的记录和问题跟踪。当配置变更实施过程中,中间工作成果需要变更实施人员提交开发库进行版本控制;配置变更实施后,经过变更确认后需要配置管理人员将变更实施后产生的工作成果重新提交受控库进行受控管理。对于非基线状态下的配置项而言,仅实施版本控制,不实施严格的变更控制。

### 2.5　质量保证策略

芯片开发过程中应指定一位质量工程师。质量工程师应独立于集成电路开发团队,以便客观地评价设计过程、识别偏离和确保纠正活动有效。质量工程师依据《质量保证计划》执行质量保证工作,对芯片投片前的各个活动进行评审、审计、监督和报告,以保证芯片的质量。质量工程师将对质量保证工作中发现的问题形成报告,并对这些问题进行记录、追踪、评估,对纠正措施进行批准。

## 3　结束语

DO-254 标准是对机载电子硬件领域最佳的工程实践总结,基于 DO-254 标准的航空集成电路硬件设计正确性保障策略可为集成电路设计带来更为彻底的验证、更高质量的项目管理、更好的进度管理,并为航空集成电路高安全性需求提供了有力保障。DO-254 标准基于需求的管理、确认和验证策略,配置管理和质量保障策略不仅仅应用于民用机载电子设备的研制,还应当广泛推广应用到军用机载电子设备的研制,这将对航空军事装备机载领域的长远发展产生重大意义。

**参考文献:**

[1] RTAC, DO-254. Design Assurance Guidance for Airborne Electronic Hardware[S/OL]. 2000. http://www.rtca.org/onlinecart/product.cfm? id=194.

[2] SAE, ARP 4754. Aerospace Recommended Practice 4754 Certification Considerations for Highly Integrated or Complex Air-

(下转第 195 页)

图 2 表示为一般洪泛算法与文中提出算法访问节点数目对比。可以看出当 TTL 值达到一定程度时,泛洪算法搜索将覆盖网络中大部分节点,文中提出算法覆盖率为 52%。因此说明在满足用户同等查询需求的条件下,基于兴趣相似度的搜索算法查找节点数目要小于一般洪泛算法。

图 3 表示了文中提出算法的搜索效率,大约在 55% 左右,比一般泛洪算法高。当 TTL 值大于 5,随着 TTL 值增加,泛洪算法效率越来越低,而文中算法波动不大。这是由于 TTL 值较大时,泛洪方法产生冗余消息数目逐渐增大,影响了查询效率,而本文算法基于节点兴趣相似度,只查询路由到相关节点上,因此不会随 TTL 值变化而波动。

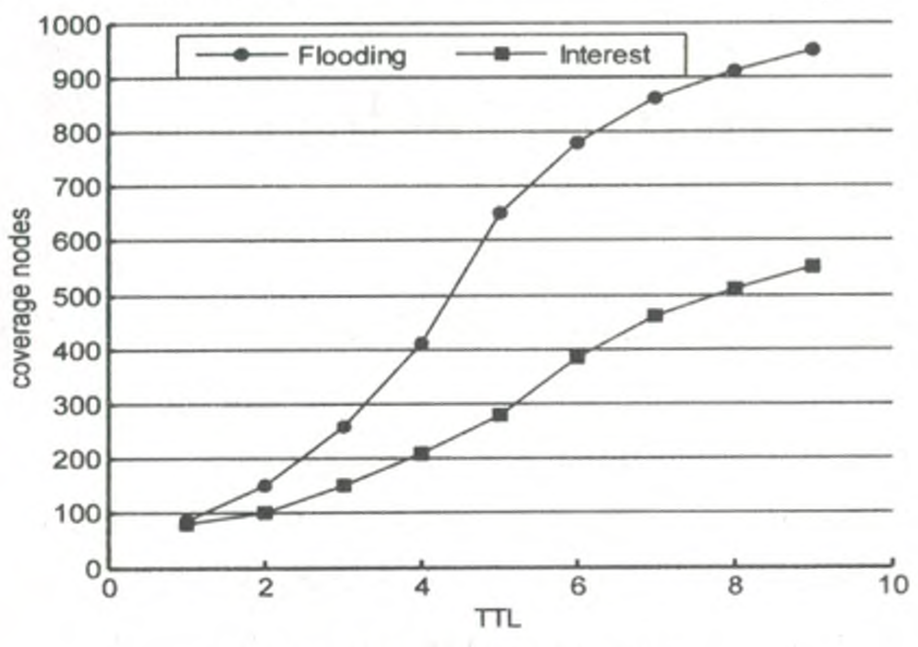


图 2　访问节点数目对比

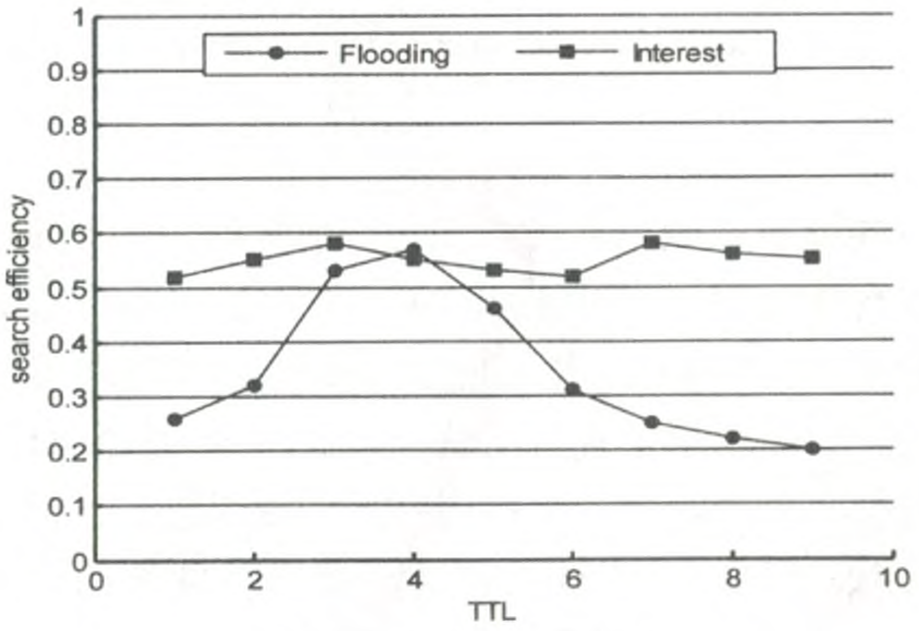


图 3　搜索效率对比

## 4　结束语

文中提出了一种基于兴趣域的 P2P 气象资料搜索算法,针对气象资料命名和属性特征具有一定规律性,通过采用了向量空间方法来将节点划分了不同兴趣域。实验证明该方法对于资源的搜索具有一定目标性,从而减少了访问节点数量,提高了查询效率。下一步将在文中基础上,对搜索算法进一步改进。

**参考文献:**

[1] 范会波,张新有. 基于 P2P 的文件共享系统的设计与实现[J]. 计算机技术与发展,2010,20(3):48-51.

[2] 张春红,裘晓峰,弭　伟,等. P2P 技术全面解析[M]. 北京:人民邮电出版社,2010.

[3] 谭义红,陈治平,林亚平. 基于兴趣挖掘的非结构化 P2P 搜索机制研究与实现[J]. 计算机应用,2006,26(5):1164-1166.

[4] 王国复,徐　枫,吴增祥. 气象元数据标准与信息发布技术研究[J]. 应用气象学报,2005,16(1):114-117.

[5] 廖华明,程伯羽,刘新周,等. 信息网格中元数据层次化结构模型的研究和应用[J]. 计算机研究与发展,2003,40(12):1694-1699.

[6] 饶文碧,柯慧燕,张　丽. 一种扩展的基于 VSM 的 Web 文本分类算法[J]. 计算机应用与软件,2006(10):113-116.

[7] 陈万勇,余日泰,万　健. 基于余弦相似度分组的 P2P 搜索机制[J]. 计算机通信,2009,35(12):92-94.

[8] Milgram S. The small world problem[J]. Psychology Today, 1967,67(1):60-67.

[9] 贾晓倩,刘方爱. 基于最近邻搜索算法分组式 P2P 网络拓扑模型[J]. 计算机技术与发展,2010,20(11):100-104.

[10] 陈香香,吴开贵,陈　明. 基于兴趣域的对等网络动态搜索机制[J]. 计算机应用研究,2011,28(1):226-229.

[11] Palmer C R,Steffan J G. Generating network topologies that obey power laws[C]//Proceedings of GLOBECOMM. [s. l.]: [s. n.],2000.

[12] Buckley C. Implementation of the SMART information retrieval system[R]. New York:Cornell University,1985.

(上接第 191 页)

craft Systems[S]. 1996.

[3] SAE, ARP 4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment[S]. 1996.

[4] 田　泽. 嵌入式系统开发与应用教程[M]. 北京:北京航空航天大学出版社,2004.

[5] 黄信兵,田　泽. Linux 在嵌入式系统中的应用与设计[J]. 计算机技术与发展,2006,16(10):216-218.

[6] Churiwala S, Garg S. Principles of VLSI RTL Design[M]. [s. l.]:Springer,2010.

[7] GJB 5000A-2008. 军用软件研制能力成熟度模型[S]. 总装备部军标出版发行部,2008.

[8] Lange M, Dewey T. Achieving Quality and Traceability in FPGA/ASIC Flows for DO-254 Aviation Projects[EB/OL]. 2006. http://www.mentor.com/.

[9] Glasser M. The Verification Cookbook[M]. 3rd ed. [s. l.]: Mentor Graphics Corporation,2007.

[10] Foster H D, Krolnik A C, Lacey D J. Assertion-based Design [M]. 2nd ed. Boston:Kluwer Academic Publishers,2004.

[11] Perry D L, Foster H D. Applied Formal Verification[M]. New York:McGraw-Hill,2005.

[12] Marriott P, Bailey S. Functional Coverage Using SystemVerilog [C]//Proc. of DVC on 2006. San Jose, CA, USA:[s. n.], 2006.

# 基于纹理特征的棒材自适应计数方法

作者：刘娜娜
作者单位：江苏科技大学计算机科学与工程学院,江苏镇江212003
刊名：计算机技术与发展
英文刊名：Computer Technology and Development
年，卷(期)：2012(8)

## 参考文献(12条)

1. RTAC,DO-254.Design Assurance Guidance for Airborne Electronic Hardware 2000
2. SAE Aerospace Recommended Practice 4754 Certification Considerations for Highly Integrated or Complex Air craft Systems 1996
3. SAE Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systens and E quipment 1996
4. 田泽 嵌入式系统开发与应用教程 2004
5. 黄信兵;田泽 Linux在嵌入式系统中的应用与设计 2006(10)
6. Churiwala S;Garg S Principles of VLSI RTL Design 2010
7. GJB 5000A-2008 军用软件研制能力成熟度模型 2008
8. Lange M;Dewey T Achieving Quality and Traceability in FP GA/ASIC Flows for DO-254 Aviation Projects 2006
9. Glasser M The Verification Cookbook 2007
10. Foster H D;Krolnik A C;Lacey D J Assertion-based Design 2004
11. Perry D L;Foster H D Applied Formal Verification 2005
12. Marriott P;Bailey S Functional Coverage Using System Verilog 2006