2019 届研究生博士学位论文

分类号：_____ 学校代码：10269

密　级：_____ 学　　号：52141500005

華東師範大學

East China Normal University

博 士 学 位 论 文

DOCTORAL'S DISSERTATION

论文题目：并发操作系统的自动化验证框架

院　　系:	计算机科学与软件工程学院
专 业 名 称:	软件工程
研 究 方 向:	可信计算
指 导 教 师:	何积丰教授
学位申请人:	朱晓冉

2019 年 5 月

Dissertation for doctoral degree in 2019 University Code: 10269

Student ID: 52141500005

EAST CHINA NORMAL UNIVERSITY

An Automated Verification Framework for Concurrent Operating Systems

Department:	School of Computer Science and Software Engineering
Major:	Software Engineering
Research direction:	Trustworthy Software
Supervisor:	Prof. He Jifeng
Candidate:	Zhu Xiaoran

2019. 05

华东师范大学学位论文原创性声明

郑重声明：本人呈交的学位论文《》，是在华东师范大学攻读硕士/博士（请勾选）学位期间，在导师的指导下进行的研究工作及取得的研究成果。除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确说明并表示谢意。

作者签名:_____ 日期: 年 月 日

华东师范大学学位论文著作权使用声明

《》系本人在华东师范大学攻读学位期间在导师指导下完成的硕士/博士（请勾选）学位论文，本论文的研究成果归华东师范大学所有。本人同意华东师范大学根据相关规定保留和使用此学位论文，并向主管部门和相关机构如国家图书馆、中信所和“知网”送交学位论文的印刷版和电子版；允许学位论文进入华东师范大学图书馆及数据库被查阅、借阅；同意学校将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于（请勾选）

（ ）1. 经华东师范大学相关部门审查核定的“内部”或“涉密”学位论文 *，于 年 月 日解密，解密后适用上述授权。

（ ）2. 不保密，适用上述授权。

导师签名:_____ 本人签名:_____

年 月 日

*“涉密”学位论文应是已经华东师范大学学位评定委员会办公室或保密委员会审定过的学位论文（需附获批的《华东师范大学研究生申请学位论文“涉密”审批表》方为有效），未经上述部门审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权）。

朱晓冉 博士学位论文答辩委员会成员名单

姓名	职称	单位	备注
		华东师范大学	主席
		华东师范大学	
		华东师范大学	

摘　要

软件可信性是建立在可靠性、安全性、可维护性等众多软件属性上，用于衡量软件运行过程与结果符合用户预期程度的综合属性。由于软件事故频发，人们对软件可信性的关注越来越多，如何准确高效的预测软件可信性是研究软件可信性的关键问题。相比于评估软件开发过程来度量软件可信性，对软件实体可信性的预测更加贴合用户实际需求。软件是由程序和文档构成的，其中程序是软件运行的主体。本文基于对软件源代码的可信性预测来反映软件可信性，使得度量结果更加准确高效。

首先，本文首先给出软件失信及程序中的失信证据的概念，从重大软件事故中收集典型的失信证据，并对失信证据进行分类。其次，借鉴基于属性的软件可信度量体系中可信性分级评估模型，给出适用于失信证据的可信分级模型，该模型确定了每条失信证据的可信度。

失信证据

接着，基于失信证据的可信度和失信证据对整个软件程序的影响，引入信息熵的概念，在信息熵模型基础上建立软件可信性预测模型。

再次，给出确定该预测模型中失信证据的特征参数的方法。

再次，基于失信证据和静态检测工具 CppCheck 进行二次开发，开发静态预测软件可信性工具。该工具不仅提供对 C/C++ 程序的典型缺陷检测，还提供对除缺陷以外的失信证据的检测，根据模型给出失信证据的可信度，并计算出当前软件的可信度，根据可信性分级模型给出当前软件的可信性。其中，检测出的失信证据和计算后的结果均可视化呈现。

最后，

关键词: 软件可信性，静态预测，失信证据，信息熵，CppCheck，缺陷检测

ABSTRACT

Space-Air-Ground integrated network (SAGIN) is a safety-critical system with a large interconnection of air, space, ground and sea nodes. This network is heterogenerous, whose reliability and dependability should be highly concerned. Earth observation mission is one of the most basic and important applications based on SAGIN. In order to ensure the reliability and dependability of the system, formal methods of modelling, simulation and verification should be applyed. Compared with other formal modelling languages, the Spatio-Temporal Consistency language (STeC) is more suitable to model earth observation missions of SAGIN applications, bacause the STeC stresses spatio-temporal information and the spatio-temporal consistency.

Firstly, this paper instantiates the specification language of real time systems – the STeC into the Domain-STeC, helping the Domain-STeC apply to SAGIN. Besides, the earth observation missions are modelled in two application scenarios.

Secondly, model checking techniques are used to verify some important properties of the system. One part of the verification is to do some preliminary model checking by the STeC tool, including lexical analysis, snytax analysis and spatio-temporal consistency checking. The other part is to verfiy properties in the UPPAAL tool after transforming STeC models to Timed Automata.

Thirdly, this paper develops a simulation and controlling tool of earth observation missions by re-developing the astronautics domain simulation software $STK(Satellite\,Tool\,Kit)$ with the Domain-STeC. This tool translates Domain-STeC statements to STK control commands, and controls STK. Consequently, Domain-

STeC statements are used to simulate system actions successfully, and processes of earth observation missions can be shown in STK dynamically.

Lastly, this paper introduces the concept of the spatio-temporal curve based on spatio-temporal points in the STeC, describing the region coverage problems related to the task scheduling in earth observation missions. In this paper, the mission scheduling problem is also discussed under three simple circumstances.

Keywords: Space-Air-Ground Integrated Network, Earth Observation, STeC, Modeling, Verification, Simulation

目录

第一章 绪 论 1
1.1 研究背景 1
1.2 研究现状 1
1.3 本文工作与主要贡献 1
1.4 组织结构 1
第二章 基本概念和预备知识 2
2.1 并发操作系统 2
2.2 可达性逻辑 2
2.3 精化关系定义 3
2.4 K 框架 3
2.5 AUTOSAR 规范 3
2.6 本章小结 3
第三章 基于多路径可达性分析的操作系统应用验证方法 4
3.1 多路径可达性分析方法 4
3.2 并发操作系统应用的操作语义定义 4
3.3 推理规则 4
3.4 案例分析 4
第四章 基于组合精化关系的操作系统内核验证方法 5
4.1 组合精化关系证明方法 5
4.2 组合精化关系在操作系统验证中的改进 5
4.3 组合精化关系自动化证明算法 5

4.4 案例分析 5
第五章 基于规范约束的操作系统内核测试用例生成方法 6
5.1 基于规范的约束提取方法 6
5.2 基于规范约束的测试用例生成方法 6
5.3 案例分析 6
5.4 本章小结 6
第六章 验证 AUTOSAR 操作系统 7
6.1 AUTOSAR 操作系统建模 7
6.2 AUTOSAR 操作系统应用的可达性检查 7
6.3 AUTOSAR 操作系统的实时性验证 7
6.4 AUTOSAR 操作系统内核的精化关系验证 7
6.5 符合 AUTOSAR 规范的测试用例自动生成 7
6.6 本章小结 7
第七章 总结与展望 8
7.1 本文总结 8
7.2 下一步工作 8
参考文献 9
致谢 9
发表论文和科研情况 10

插图

主要符号对照表

符号	英文含义	中文含义
Act	Action	动作
C	Control center	控制中心
Comp	Compute	计算
Conn	Connect	连接
h	Hour	时
HS	Handshake	握手
m	Minute	分
M	Message	消息
Obs	Observation	观测
P	Plane	飞机
$\mathcal{P}$	Process	进程
s	Second	秒
S	Satellite	卫星
Stat	State	状态
Store	Storage Capacity	存储空间
t	Time	时间

第一章　绪 论

1.1　研究背景

1.2　研究现状

1.3　本文工作与主要贡献

1.4　组织结构

第二章　基本概念和预备知识

2.1　并发操作系统

并发操作系统是指在只有一个处理器工作的情况下，同一时间段可以有多个进程在运行，但是任一时刻点最多只能有一个进程可以运行。并发操作系统的可以充分利用计算机的所有资源，像 cpu，外围设备、内存等。一个进程在执行时很大程度上在等待资源，而进程等待资源时，我们不希望它仍然占用 CPU，而是可以把 CPU 释放给其它可以运行的进程。

2.2　可达性逻辑

可达性逻辑（Reachability Logic）由美国伊利诺伊大学厄巴纳香槟分校 Grigore Rosu 教授所在的团队提出，其目的是：

- 构建了一套语言无关的用来验证系统可达性的证明系统；
- 所定义的语言操作语义可用作程序证明时所用的公理，从而减小做程序证明的工作量。

典型的，霍尔三元组

2.3 精化关系定义

2.4 K 框架

2.5 AUTOSAR 规范

2.6 本章小结

第三章　基于多路径可达性分析的操作系统应用验证方法

3.1　多路径可达性分析方法

3.2　并发操作系统应用的操作语义定义

3.3　推理规则

3.4　案例分析

第四章　基于组合精化关系的操作系统内核验证方法

4.1　组合精化关系证明方法

4.2　组合精化关系在操作系统验证中的改进

4.3　组合精化关系自动化证明算法

4.4　案例分析

第五章　基于规范约束的操作系统内核测试用例生成方法

5.1　基于规范的约束提取方法

5.2　基于规范约束的测试用例生成方法

5.3　案例分析

5.4　本章小结

第六章　验证 AUTOSAR 操作系统

6.1　AUTOSAR 操作系统建模

6.2　AUTOSAR 操作系统应用的可达性检查

6.3　AUTOSAR 操作系统的实时性验证

6.4　AUTOSAR 操作系统内核的精化关系验证

6.5　符合 AUTOSAR 规范的测试用例自动生成

6.6　本章小结

第七章　总结与展望

7.1　本文总结

7.2　下一步工作

致　　谢

“假如你初见一件东西，刚遇一个人，心里就隐隐有了离别的感伤的话，
那么，你已经爱上她了”

三年时光在不经意间悄然走过，逐渐接近尾声，离别的感伤也愈发突显。是的，我已经爱上了这里的一切，爱上了华东师大美丽的校园和成群结队的可爱妹子，爱上了有幸在这里遇到的每个人。在毕业论文完成之际，在不舍之余，还要献上我最诚挚的谢意。

首先感谢陈仪香老师，除了对本论文的指导之外，还要感谢这三年来陈老师给予我的做人、做事、做科学研究等各方面的教诲；陈老师知识的渊博让我深深折服，而他对待科学研究孜孜不倦的精神和严谨的态度更加让我敬佩。

感谢肖波老师在小论文的撰写上给予的指导；感谢给予过实验室指导和帮助的周勇老师，张敏老师，卜天明老师，张民老师。

感谢实验室已毕业的师兄师姐经常回来给我们分享科研和工作上的心得体会，我从中受益匪浅；感谢所有实验室的师兄弟姐妹的陪伴和帮助，他们是姚兴华，陈艳文，王娜，李慧勇，纪政，王保华，刘董倩，叶文斌，张元睿，何康力，张俊，周慧英，何佳，马煜婧，李岩，刘毅泽，李金洋，王士忠，方诚颖，李文婷；感谢实验室所有一起吃饭，吹牛，健身的同学们。

感谢辅导员叶林娟老师，张炜帆老师在学生工作方面给予的支持和帮助；感谢学院所有授课老师在课程上的教导和帮助。

感谢室友王中主，杨德城，翁海星，苏永浩，舒圣原，庞天泽在生活、学习等各方面给予的陪伴和帮助；感谢所有 2013 级研究生同学。

最后特别感谢我的父母，姐姐，女友一直以来对我无条件的关心、支持、鼓励和理解，你们是我最坚强的后盾。

杨志华

二〇一六年五月

攻读硕士学位期间发表论文和科研情况

■ 已公开发表论文或其他科研成果

[1] Yang Z, Xiao B, Chen Y. Modeling and Verification of Space-Air-Ground Integrated Networks on Requirement Level Using STeC[C]//Theoretical Aspects of Software Engineering (TASE), 2015 International Symposium on. IEEE, 2015: 131-134.(CCF-C)

[2] 软件著作权 1 项 (在申请)，基于 STeC 和 STK 的地球观测任务仿真控制工具.

■ 参加的科研项目

[1] 网络化信息物理计算基础研究，国家自然科学基金项目 (61202104)

[2] 具有时空一致性的软件形式化理论与方法研究，国家自然科学基金项目 (61370100)

[3] 上海市科委项目 (14511100400)

[4] 上海高校知识服务平台计划 (ZF1213)