离散事件系统理论与软件可靠性设计

SY0303732

王鹏

内容

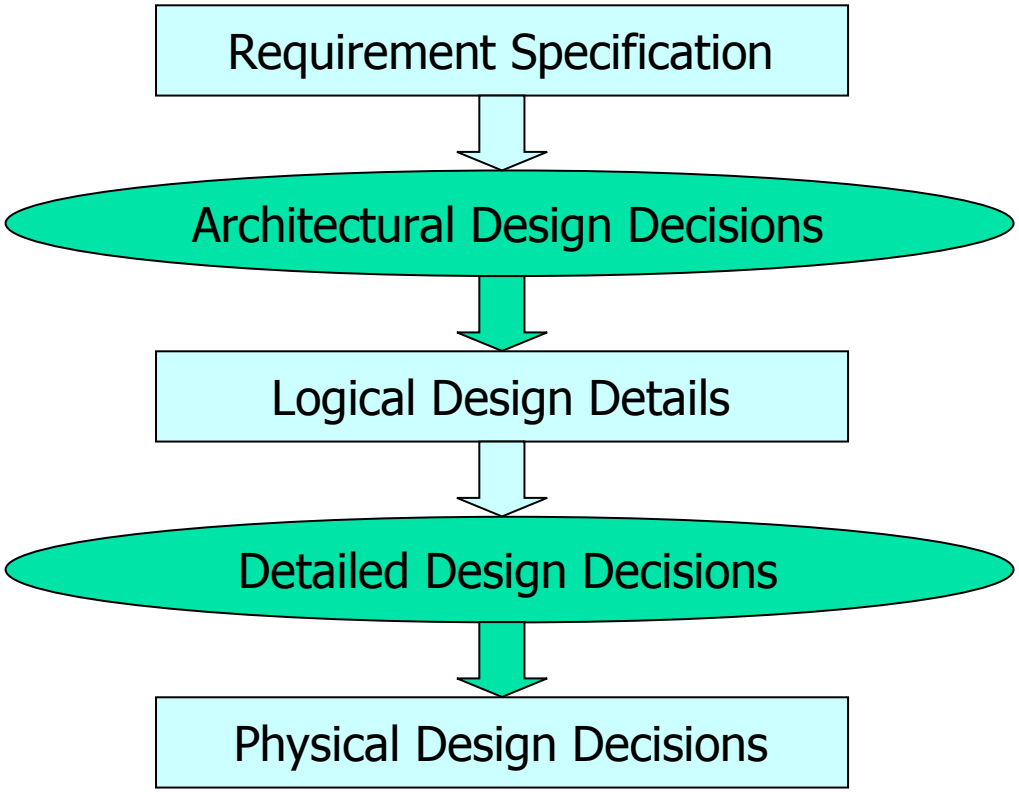
1. 研究综述
2. 研究内容
3. 可行性分析
4. 特色与创新之处

1. 综述
—软件设计与软件可靠性

- 软件是人造系统。
- 人造系统区别于自然系统。人对系统的设计决定人造系统的结构与行为。因此，系统设计在提高系统可靠性方面起着重要作用。
- 软件设计是软件开发过程中形成质量的关键地方。因此，研究软件的可靠性设计方法，对于提高软件可靠性有着重要意义。

1. 综述

—软件设计流程概述



1. 综述
—现有软件设计方法

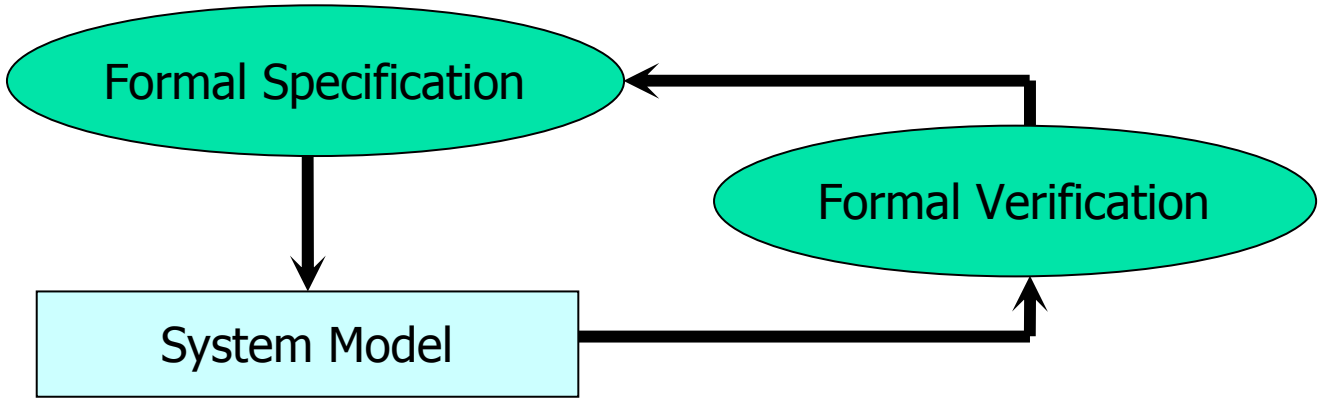
- 结构化方法（SASD）
- 面向数据结构的软件开发方法 (JSP)
- 面向对象的软件设计方法
- 基于构件的软件设计方法
- 形式化方法

1. 综述
—形式化方法的意义

- 形式化方法是一种基于数学的方法，由推理工具支持。它提供一种严格、有效的方法去建模，设计和分析计算机软件系统。
- 形式化方法的意义在于它能够依据数学原理，帮助我们去构建一个期望的系统，同时去验证系统是否满足期望的性质。
- 形式化方法有助于提高软件系统的可靠性，目前主要应用于安全关键系统（safety-critical system）的开发过程中。

1. 综述
—形式化方法的过程

- 形式规约描述（formal specification）
- 形式验证（formal verification）



1. 综述
—形式化规约描述

- 形式规约描述使用规约语言来描述系统。这种语言具有严格的语法和语义。被描述的系统特性包括静态的结构特性和动态的行为特性等。
- 形式规约语言按照描述系统的特性可以大致分为三类：
  - 描述顺序系统行为的形式规约方法，如Z、VDM等；
  - 描述并发系统行为的形式规约方法，如CSP、CCS、I/O自动机等；
  - 集成的形式规约方法，如SDL、RAISE等。

1. 综述
—形式化验证

- 形式化验证是指使用严格的数学方法来推理验证设计出的系统是否符合其全部或部分规约的过程。形式验证要求产品的规约和实现均需要有严格的形式描述。
- 目前，形式验证主要有两种方法：
  - 模型检验（model checking）
  - 定理证明（theorem proving）

1. 综述
—离散事件系统理论

- 软件是离散系统，其与离散类数学的关系是十分密切的。
- 离散事件系统 (Discrete Event System)理论的研究兴起于20世纪80年代。该时期，随着信息技术与计算机技术等的迅速发展，相继出现了一批新型的人造系统，如柔性生产线、大规模计算机和通讯网络、空中交通管理系统等。在这类人造系统中，驱动系统运动的是一批离散事件，运动所遵循的规律是一系列人为规则。基于对这类人造系统性能研究的需要，离散事件系统理论最终形成并发展。

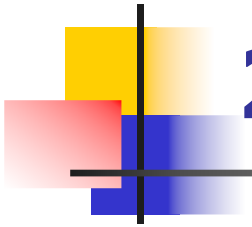
1. 综述

—离散事件系统的模型分类

	物理时间层面	*逻辑时序层面*
逻辑层次		形式语言与自动机、Petri网
代数层次	极大极小代数	
性能层次	排队网络、摄动分析、离散事件系统模拟	
	随机性→	*←确定性*

1. 综述
—离散事件系统的监控方法

- 由W. M. Wonham提出的监控理论（Supervisory control），是以形式语言与自动机为基本模型研究DES的一种方法。
- 该方法的基本思想：通过监督控制，来禁止某些被称为可控事件的事件发生，从而使系统的行为，即系统的运行轨迹，满足预先给定的行为规范。
- 监控机制可以在某种意义上理解为一种反馈控制机理，即根据系统已有的运动轨迹，即运动的历史信息，来监控系统现在和将来的运动方向。



2. 研究内容 —概述

以离散事件系统（DES）的形式语言与自动机的模型为基础，研究监控理论在软件设计中的应用问题，其研究目的是需找可行的形式化方法，以提高软件设计的可靠性。

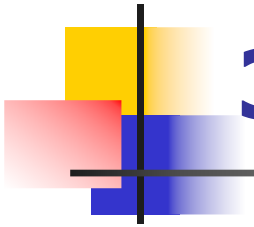
2. 研究内容
—实例研究（Case Study）

- 从软件实际中抽象出实例，应用DES有关理论，对其进行实例研究。

- 实例研究所依据的理论结果已在本实验室接收或投稿的论文中给出。

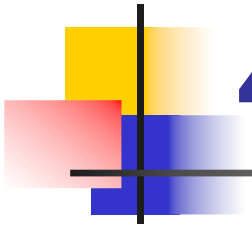
2. 研究内容
—实验工具开发

- 工具计划以有限确定性自动机（FDA）为基本计算模型，同时考虑多项式动态系统模型（PDS），借助计算机来完成对自动机的存贮与计算、以及对监控器的综合。
- 实验室博士创新性研究基金的课题内容



3. 可行性分析

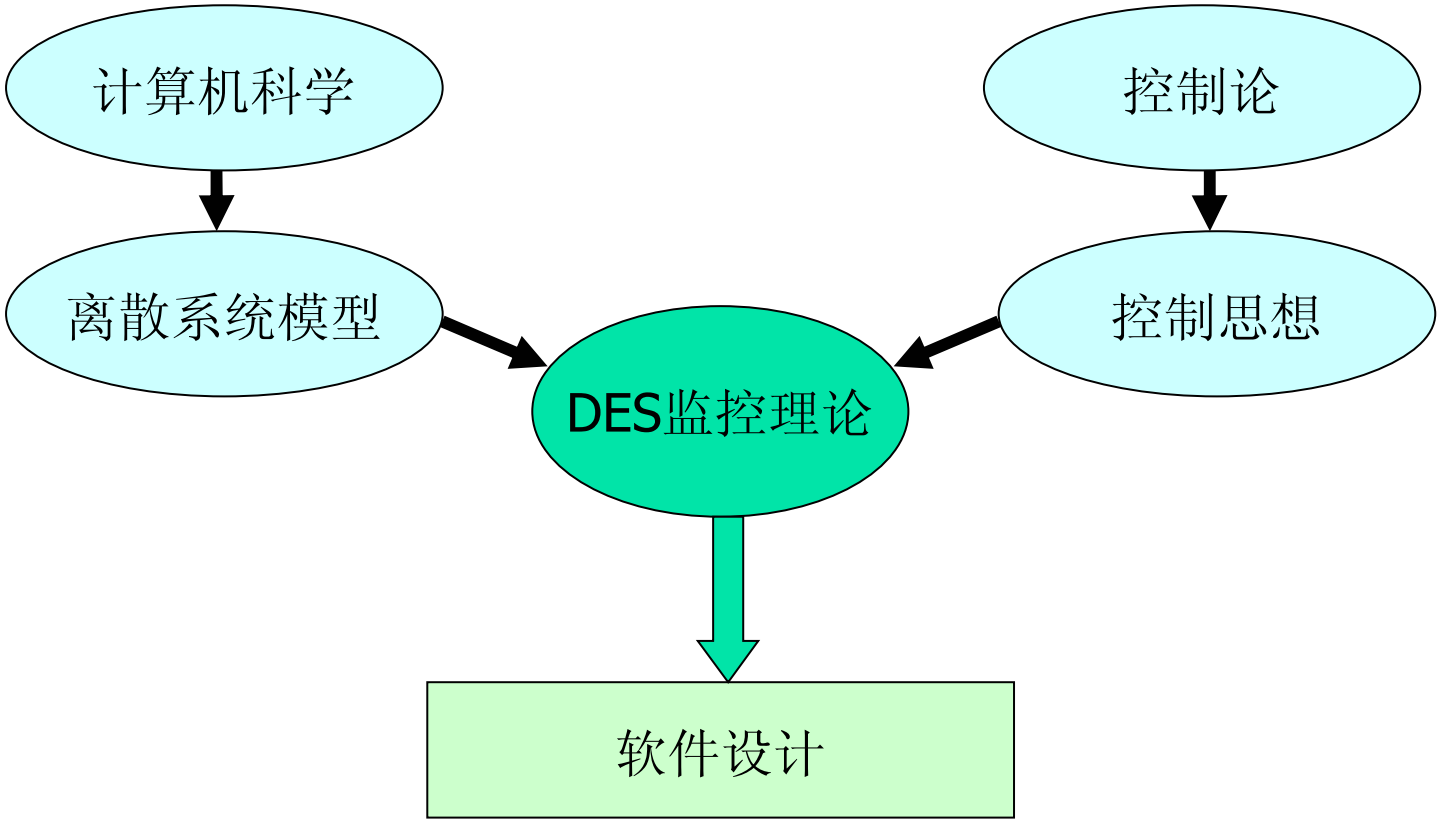
- 软件设计中对于状态机的应用是广泛的：
  - 软件体系结构：状态变迁结构
  - UML：状态转移图（state chart）
- 本实验室依据DES理论，利用PDS模型对软件设计的某些理论问题已进行探讨。目前，已接收论文一篇，投稿数篇。



4. 特色与创新之处

DES的监控理论中借鉴了控制论中的有益思想，我们将该理论应用于软件设计中，具有学科交叉的性质，同时为软件控制论的发展寻求新的方向。

4. 特色与创新之处



谢谢！