Rockwell Avionics

Collins

The AAMP5/AAMP−FV Project

Steven P. Miller

Collins Commercial Avionics
Rockwell International
400 Collins Road NE
Cedar Rapids, Iowa 52498 USA
(319) 337−5149

spmiller@pobox.cca.cr.rockwell.com

Mandayam Srivas

Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025 USA
(414) 859−6136

srivas@csl.sri.com

Rockwell International ©1995

Formal Verification of the AAMP5 Microprocessor

Introduction

- **Assess the Feasibility of Formal Verification for Industrial Use**
  - Participated in the MCC Formal Methods Transition Study (1990–91)
  - Pilots using RAISE for Formal Specification (1992–93)
- **Collaborative Effort**
  - Funded by NASA Langley and Collins
  - Performed by SRI International and Collins (with Assistance from NASA)
- **Formal Verification of the AAMP5 Microcode**
  - Specified Instruction Set (macro) Architecture in PVS (108 of 209 Instructions)
  - Specified Register Transfer (micro) Architecture in PVS
  - Proved Microcode for 11 Instructions Correct using the PVS Theorem Prover
- **Shadow Project**
  - Independent of Traditional Development and Verification Process of the AAMP5

Rockwell International ©1995

Formal Verification of the AAMP5 Microprocessor

Overview of Presentation

- **Background**
- **Project History**
- **Formal Specification of the AAMP Macroarchitecture**
- **Formal Specification of the AAMP5 Microarchitecture**
- **Proofs of Microcode Correctness**
- **Conclusions**

Rockwell International ©1995

Background

The AAMP Family of Microprocessors

CAPS–4	**1974**	**Global Positioning System, General Development Model (GPS GDM)**
CAPS–6	**1977**	**Boeing 757, 767 Autopilot Flight Director System (AFDS), Lockheed L–1011 Active Control System (ACS), Lockheed L–1011 Digital Flight Control System (DFCS), NASA Fault Tolerant Multiprocessor (FTMP)**
CAPS–8	**1979**	**Boeing 757, 767 Electronic Flight Instrumentation System (EFIS), Boeing 757, 767 Engine Instrumentation/Crew Alerting System (EICAS)**
CAPS–7	**1979**	**Navstar Global Positioning System (GPS), Boeing 747–400 Integrated Display System (IDS), Boeing 747–400 Central Maintenance Computer (CMC), Boeing 737–300 Electronic Flight Instrumentation System (EFIS), Boeing 737–300 Engine Instrumentation/Crew Alerting System (EICAS), Air Transport Traffic Collision Avoidance System (TCAS), Air Transport TCAS Vertical Speed Indicator (TVI), Boeing 777 Flight Control Backdrive, Commercial GPS: Navcore I, Navcore II, Navcore V**
CAPS–10	**1979**	
AAMP1	**1981**	
AAMP2	**1987**	
AAMP3	**1992**	**Boeing 777 Standby Instruments**
AAMP5	**1993**	**Global Positioning Systems, Upgrade for AAMP2**

Rockwell International ©1995

Background

AAMP Family of Microprocessors

- **Based on Stack Architecture**
- **Designed for Use in Embedded Systems with High–Level Languages (Ada)**
- **Multiple Addressing Modes**
- **Large, CISC–like Instruction Set**
- **Double Code Density of Most Microprocessors**
- **Provides Direct Hardware Support for Much of**
  - Run Time Environment
  - Real–Time Executive

Background

AAMP5

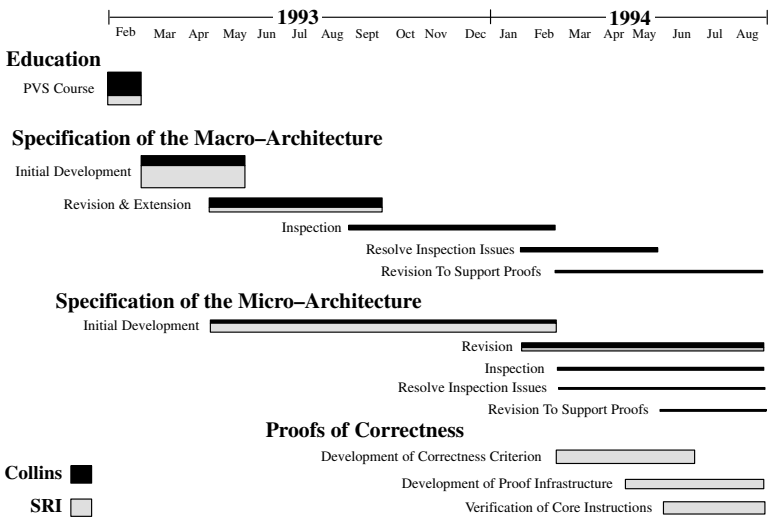
- **Object Code Compatible with Earlier AAMP2**
- **Uses Pipelining to Achieve 3x Performance of the AAMP2**
- **~500,000 Transistors**
  - ~20,000 Transistors in Other Formal Microprocessor Verification Efforts
  - ~3.1 Million Transistors in an Intel Pentium
- **Performance Between Intel 386 and 486**
- **Intended for Use in Avionics Displays and Global Positioning Systems**

Background

PVS

- **Environment for Formal Specification and Verification**
- **Developed by SRI International**
- **Expressive Specification Language**
  - Simple and Easy to Learn
  - Notation Similar to Conventional Programming Languages
  - Sophisticated Type System
  - Higher Order Logic
- **Typechecker**
- **Interactive Theorem Prover**
  - Automates Many of the Low Level Proof Steps

Project History



Formal Specification of the AAMP Macroarchitecture

- **Initial Development Done by SRI**
  - 1,595 Lines of PVS and Comments Organized into 25 Theories
- **Bit Vectors Library Taken Over by NASA Langley**
  - Evolved into 2,030 Lines of PVS and Comments in 31 Theories
- **Revised and Extended by Collins**
  - Specified most of the Executive Service Routines
  - Completed 108 of the AAMP's 209 Instructions
  - 2,550 Lines of PVS and Comments Organized into 48 Theories
- **Performed 11 Inspections of the PVS Specifications**
  - Practicing Electrical Engineers
  - Inspectors had Little Trouble Reading PVS
  - Average Preparation Rate of ~150 Lines of PVS and Comments/Hour
  - Found 53 Minor (Style) Errors, 28 Major (Correctness) Errors

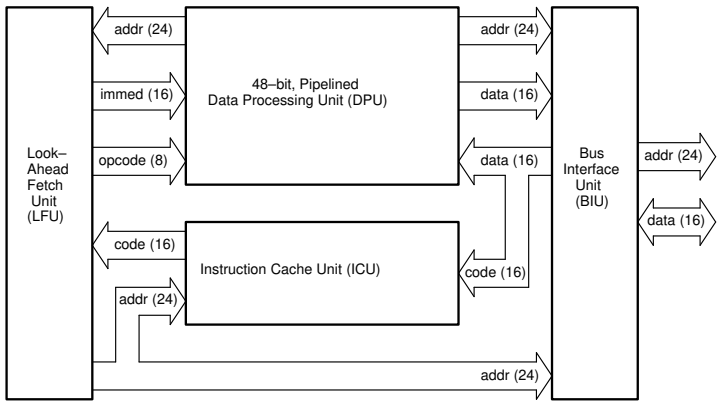
Formal Specification of the AAMP Macroarchitecture

Microcode Errors Found in This Phase

- **Discovered Two Microcode Errors**
  - Both Specific to the AAMP5
  - Both Corrected Before First Fabrication
  - Had Not Completed Traditional Verification Effort
- **Found While Specifying Behavior of the AAMP During Unusual Cases**
- **One was Due to a Missing Requirement**
  - Would Have Been Found During Ada Validation Testing
- **Other Was a Coding Error**
  - Required Specific Stack Configuration, an Improperly Sized Stack, and a Specific Instruction Sequence
- **Illustrates the Value of Simply Creating a Precise Specification**

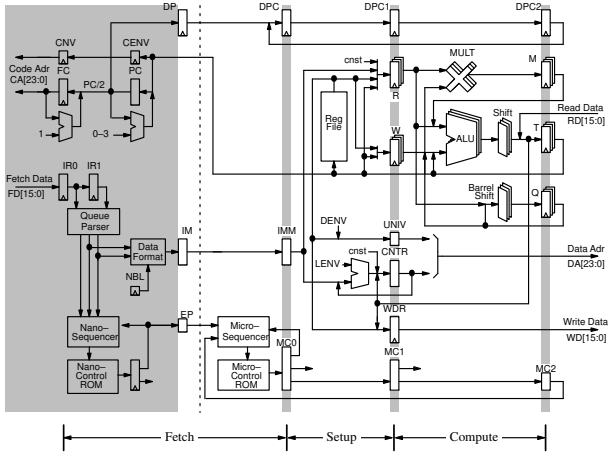
Formal Specification of the AAMP5 Microarchitecture

AAMP5 Block Diagram



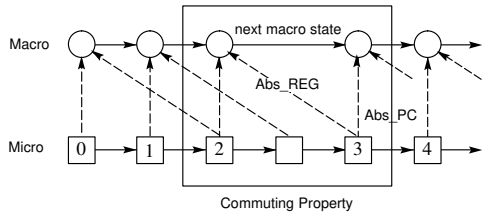
Formal Specification of the AAMP5 Microarchitecture

DPU Microarchitecture



Proofs of Microcode Correctness

Approach and Issues



- **Pipelining**
- **Autonomous Code and Data Access**
- **Enhancements to Support Efficient Automation**
  - Boolean Decision Diagram (BDD) Decision Procedures
  - Optimizations to the PVS Rewriting Engine
- **Decomposition of Verification Approach to Facilitate Technology Transfer**

Proofs of Microcode Correctness

Microcode Errors Found in This Phase

- **Seeded Two Errors in Microcode Provided to SRI**
- **First was Designed to be Difficult to Detect**
- **Second was an Actual Error**
  - Escaped Detection by Simulations and Walkthroughs
  - Discovered by Collins While Running Application Code on an Early Prototype of the AAMP5
- **Both Errors were Found by SRI While Doing the Proofs**
  - Discovery was Very Systematic
  - SRI Explained How to Correct Both Errors

Summary

- **Specified 108 of the AAMP's 209 Instructions**
- **Specified the AAMP5 at the Register Transfer Level**
- **Developed a Large, Reuseable Library of Bit Vector Properties**
- **Discovered Two Errors in AAMP5 Microcode During Specification**
- **Conducted Inspections of the PVS Specifications With Design Engineers**
- **Developed General Approach to Decomposing the Proofs of Correctness**
- **Automated these Strategies in the PVS Prover**
- **Formally Verified the Microcode in 11 Instructions**
- **Discovered Two Seeded Errors during Formal Verification**

Conclusions

- **Demonstrated the Technical Feasibility of**
  - Formally Specifying the AAMP5 at Instruction Set and Register Transfer Levels
  - Formally Verifying the Microcode in the AAMP5
- **Benefits of Formal Specification**
  - Encourages Clean Abstractions and Interfaces
  - Encourages "Looking in Corners"
- **PVS Specifications Successfully Used by Practicing Engineers**
  - Synergy between Specifications and Inspections was Key
  - Acceptance of PVS by Engineers Varies Widely
  - Difficult to Enforce the Discipline Needed to Ensure Quality Specifications
- **Could Achieve *Dramatic* Gains in Acceptance Through**
  - Notations that Fit a Specific Problem Domain

Conclusions

- **Formal Verification, Done Correctly, Provides Very High Levels of Assurance**
  - Does not Eliminate Good Process, Peer Reviews, Testing, Simulation, ...
  - May Facilitate or Lessen the Need for Some Traditional Practices
- **Expect Costs to be High the First Time in a New Problem Domain**
  - Expertise
  - Reusable Theories and Proofs
- **How Much Will Costs Drop on Subsequent Projects?**

AAMP–FV

- **Collaborative Effort**
  - Funded by NASA and Collins
  - Conducted by Collins and SRI
  - Initiated in January, 1995
- **Smaller Microprocessor**
  - Paper and Pencil Design
  - Similar to What We Would Use in an Autoland System
  - ~100,000 Transistors
- **Repeat AAMP5 Experiment**
  - Reuse Expertise and Theories
  - Demonstrate Cost Effectiveness
- **Current Status**
  - Specified Microarchitecture (50 Hours)
  - Nearly Completed the Proof of the First Instruction