#### The AAMP5/AAMP-FV Project

Steven P. Miller Collins Commercial Avionics Rockwell International Cedar Rapids, IA 52498 USA spmiller@pobox.cca.rockwell.com N96-10027 6/
Project

Mandayam Srivas
Computer Science Laboratory
SPI International SRI International Menlo Park, CA 94025 USA srivas@csl.sri.com

Software and digital hardware are increasingly being used in situations where failure could be life threatening, such as aircraft, nuclear power plants, weapon systems, and medical instrumentation. Several authors have demonstrated the infeasibility of showing that such systems meet ultra-high reliability requirements through testing alone [1,2]. Formal methods are a promising approach for increasing our confidence in digital systems, but many questions remain on how it can be used effectively in an industrial setting.

This presentation describes a project, formal verification of the microcode in the AAMP5 microprocessor, conducted to explore how formal techniques for specification and verification could be introduced into an industrial process. Sponsored by the Systems Validation Branch of NASA Langley and by Collins Commercial Avionics, a division of Rockwell International, it was conducted by Collins and the SRI International Computer Science Laboratory. The project consisted of specifying in the PVS language developed by SRI [3] a portion of a Rockwell proprietary microprocessor, the AAMP5, at both the instruction set and register-transfer levels and using the PVS theorem prover to prove the microcode correct for a representative subset of instructions.

While this presentation includes a brief technical overview (see [4,5] for a detailed technical discussion), its emphasis is on the lessons learned in using PVS for an example of this size and the implications for using formal methods in an industrial setting. The central result of this project was to demonstrate the feasibility of formally specifying a commercial microprocessor and the use of mechanical proofs of correctness to verify microcode. This is particularly significant since the AAMP5 was not designed for formal verification, but to provide a more than three fold performance improvement, by pipelining instruction execution, while remaining object code compatible with the earlier AAMP2. As a consequence, the AAMP5 is one of the most complex microprocessors to which formal methods have been applied.

Another key result was the discovery of both actual and seeded errors. Two actual microcode errors were discovered and corrected during development of the formal specification, illustrating the value of simply creating a precise specification. Two seeded errors were systematically uncovered while doing correctness proofs. One of these was an actual error that had been discovered after first fabrication but left in the microcode provided to SRI. The other error was designed to be unlikely to be detected by walkthroughs, testing, or simulation.

Several other results emerged during the project, including the ease with which practicing engineers became comfortable with PVS, the need for libraries of general purpose theories, the usefulness of formal specification in revealing errors, the natural fit between formal specification and inspections, the difficulty of selecting the best style of specification for a new problem domain, the high level of assurance provided by proofs of correctness, and the need to engineer proof strategies for reuse.

Many of the costs of the AAMP5 project can be attributed to the overhead of applying an experimental method for the first time. To determine how much these costs can be reduced through reuse of the AAMP5 expertise. Collins, SRI, and NASA are conducting a follow-on project to verify the microcode in the AAMP-FV, a smaller microprocessor design similar to those actually used in autoland systems. A report on the status of this project is also presented.

- [1] Butler, R. and G. Finelli, The Infeasibility of Experimental Quantification of Life-Critical Software Reliability, Software Engineering Notes, Vol. 16, No.5, pg. 66-76, December 1991.
- [2] Littlewood, B. and L. Strigini, Validation of Ultra-High Dependability for Software-based Systems, Communications of the ACM, Vol. 36, No. 11, pg. 69-80, November 1993.
- [3] Owre, S., J. Rushby, and N. Shankar, PVS: A Prototype Verification System, In Deepak Kapur, Editor, 11th International Conference on Automated Deduction, (CADE), pg. 748-752, Saratoga, NY, June 1992, Vol. 607 of Lecture Notes in Artificial Intelligence, Springer-Verlag.
- [4] Srivas, M. and S. Miller, Formal Verification of the AAMP5: A Case Study in the Verification of a Commercial Microprocessor, to appear in Applications of Formal Methods, Michael G. Hinchey and Jonathan P. Bowen, Editors, Prentice-Hall International Series in Computer Science.
- [5] Srivas, M. and S. Miller, Formal Verification of an Avionics Microprocessor, to be submitted as a NASA Contractor Report.

## Rockwell Avionics

Formal Verification of the AAMP5 Microprocessor

Introduction

### Collins

## The AAMPS/AAMP-FV Project

Steven P. Miller

Mandayam Srivas

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

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

spmiller@pobox.cca.cr.rockwell.com

srivas@csl.sri.com

O Independent of Traditional Development and Verification Process of the AAMPS

O Specified Instruction Set (macro) Architecture in PVS (108 of 209 Instructions)

O Performed by SRI International and Collins (with Assistance from NASA)

O Funded by NASA Langley and Collins

Collaborative Effort

■ Formal Verification of the AAMPS Microcode

O Participated in the MCC Formal Methods Transition Study (1990-91) Assess the Feasibility of Formal Verification for Industrial Use

O Pilots using RAISE for Formal Specification (1992-93)

O Proved Microcode for 11 Instructions Correct using the PVS Theorem Prover

Shadow Project

Coffins

O Specified Register Transfer (micro) Architecture in PVS

A Rockness Acots
Collins

Formal Verification of the AAMPS Microprocessor

Overview of Presentation

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

### Background

### The AAMP Family of Microprocessors

CAPS-4	1974	CAPS-4 1974 Global Positioning System, General Development Model (GPS GDM)
CAPS-6 1977	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 Filght Instrumentation System (EFIS), Boeing 757, 767 Engine Instrumentation/Crew Alerting System (EICAS)
CAPS-7 1979	1979	Navstar Global Positioning System (GPS), Boeing 747-400 Integrated Display System (IDS),
CAPS-10 1979	1979	Boeing 747-400 Central Maintenance Computer (CMC), Boeing 737-300 Electronic Flight Instrumentation System (EFIS), Booing 73 - 300 Electronic Testimonal System Abusines System (EFIS),
AAMPI	1861	Air Transport Traffic Collision Avoidance System (TCAS), Air Transport Traffic Collision Avoidance System (TCAS), Air Transport TCAS Vertical Speed Indicator (TV I),
AAMP2	1987	Boeing 777 Flight Control Dackdrive, Commercial GPS: Navcore II, Navcore V
AAMP3	1992	Boeing 777 Standby Instruments
AAMPS	1993	AAMPS 1993 Global Positioning Systems, Upgrade for AAMP2

• Rockwell Adores
Collins

# 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 Real-Time Executive

O Notation Similar to Conventional Programming Languages O Sophisticated Type System O Higher Order Logic Pypechecker Interactive Theorem Prover O Automates Many of the Low Level Proof Steps	O Notation Similar to Conventional Programming Languages O Sophisticated Type System O Higher Order Logic Typechecker Interactive Theorem Prover O Automates Many of the Low Level Proof Steps

Dackground	AAMPS	Object Code Compatible with Earlier AAMP2	Uses Pipelining to Achieve 3x Performance of the AAMP2	-500,000 Transistors	<ul> <li>~20,000 Transistors in Other Formal Microprocessor Verification Efforts</li> <li>~3.1 Million Transistors in an Intel Pentium</li> </ul>	Performance Between Intel 386 and 486	Intended for Use in Avionics Displays and Global Positioning Systems	Arteria
		Object Code	Uses Pipelini	■ ~500,000 Tra	0 ~20,000 Ti 0 ~3.1 Milli	Performance	Intended for	A Rockwolf Atots

	Resolve Inspection Issues	Revision & Exercison	Initial Tevelopment	Specification of the Macro-Architecture	CA1 Few case inspected to the inspected	Education PVS Cource Specification of the Maintain Elemin of the ministration of the m
ī	£ 3 8	repection I or To Support Rev Ave Imspect	repection In n To Surper Revi Nee Inspec	Armion Inspection Reador Inspection Residue Inspection In Review To Surper Iton of the Micro-Architecture  Review Inspection In Residue Inspection Inspect	Development of Correctness Criterian Correctness Development of Proof Infrastructure	Collins 📰
Development	n To Supp Rev dve Inspec	repection I n To Suppo Rev Rev lave Inspec	repection I or To Supp Rev	ntruio Inspection Resolve Inspection Resolve Inspection In Revision To Support In Micro-Architecture responsed Inspection	Proofs of Correctness	
Proofs of Corr Development	Specification of the Micro-Architecture Initial Development Commission Revision Recolve Impaction Insuration Recolve Impaction Insuration Insur	Specification of the Micro-Architecture  Initial Development Recipion Recipion  Recipion Recipion  Recipion Recipion  Recipion Recipion  Recipion R	Revieton & Extension Inspection Investion Resolve Inspection Issues Revieton To Support Pools Specification of the Micro-Architecture Initial Development Revieton Revieton Revieton Inspection Recolve Inspection Issues	herection Resolution Resolution of the Micro-Architectic responses		
Proofs of Corr	Specification of the Micro-Architecture Initial Development Revision Revision Impaction Inspection	Inspection Resolve Inspection trusts Revision To Surport Prooft Specification of the Micro-Architecture Initial Development Revision Inspection	Revietor & Exemien Invection Resolve Inspection Insus Revietor Table Surgest Poole Specification of the Micro-Architecture Initial Excrepances	neration Inspection Research R	Resolve Inspection Issues	
Proofs of Corr	Specification of the Micro-Architecture	Inspection Resolve Inspection Insura Revistor To Support Proof Initial Development Revision Insuration Insurat	Revision & Exemin hyperion Reador Insusa Revision Profession of the Micro-Architecture Initial Development Revision Revision Revision	hepecision hepecision en Re Refile of the Micro-Architece	Inspection Comments	
Proofs of Corr	Specification of the Micro-Architecture	Inspection Resolve Inspection Insura Resolve Inspection Insura Specification of the Micro-Architecture Initial Development	Revision & Exercison Inspection Resolve Inspection Insurance Previous Revision To Surport Proof Specification of the Micro-Architecture Insist Development	herein Ingection Resident Resi		
Proofs of Corr	Revision To Support Proofs	Inspection Resolve Inspection Issues Revision To Suspent Proof	Revision & Estension Inspection Resolve Inspection Issues Revision To Support Proofs	skraion Inspection email	Micro-Architecture	Specification of the
pecification of the Micro-Architecturalist benchmark to the Micro-Architectural initial			Inspection	atrasion Inspection on	Revision To Support Proofs	
evien & Estention  evien & Estention  evien & Estention  Inspecification of the Micro-Architectur  finish Development  Proofs of Corr  Development	Specification of the Macro-Architecture Initial Perkion & Eakinion Perkion Perk	Specification of the Macro-Architecture	Specification of the Macro-Architecture			
cution of the Macro-Architecture cution & Estension Inspection Teach Respectification of the Micro-Architecture Initial Development  Proofs of Corr	Specification of the Macro-Architecture  Initial Peretonen  Revision & Estenton	PVS Course Specification of the Macro-Architecture Initial Psychogeners	PVS Course Course Specification of the Macro-Architecture			
ton  cetation of the Macro-Architecture eviden & Estension Inspection Teach  Respecification of the Micro-Architecture Initial Development  Proofs of Corr	Pducation PVS Course Specification of the Macro-Architecture Initial Psychome   Revision & Eatenton	Rducation PVS Course Specification of the Macro-Architecture Initial Developmen	Education  PVS Course   Specification of the Macro-Architecture			1eh Mar Apr
Iteh has Apr hay has Mars Sept Cat have for have for the Macro-Architecture evident & Estention   Inspection   Resolve Inspect   Resolve I	ish has age has he has see see cat has lon of the Macro-Architecture men Exension	In his age has he had see see the house of the Macro-Architecture	IT HE ME AR MAY IN IN AN SET ON INV.	1sh Mar Apr May Jan Jal Ang Sept CAI How		

## Formal Specification of the AAMP Macroarchitecture

Formal Specification of the AAMP Macroarchitecture

### ■ Initial Development Done by SRI

- O 1,595 Lines of PVS and Comments Organized into 25 Theories
  - Bit Vectors Library Taken Over by NASA Langley
- O Evolved into 2,030 Lines of PVS and Comments in 31 Theories

### Revised and Extended by Collins

- O Specified most of the Executive Service Routines
  - O Completed 108 of the AAMP's 209 Instructions
- O 2,550 Lines of PVS and Comments Organized into 48 Theories

## Performed 11 Inspections of the PVS Specifications

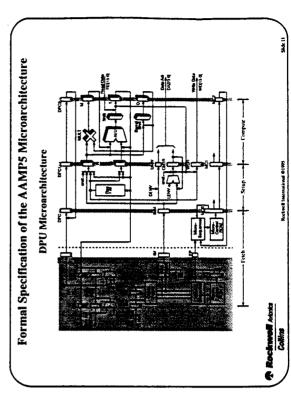
- O Practicing Electrical Engineers
- O Inspectors had Little Trouble Reading PVS
- O Average Preparation Rate of ~150 Lines of PVS and Comments/Hour
  - O Found 53 Minor (Style) Errors, 28 Major (Correctness) Errors

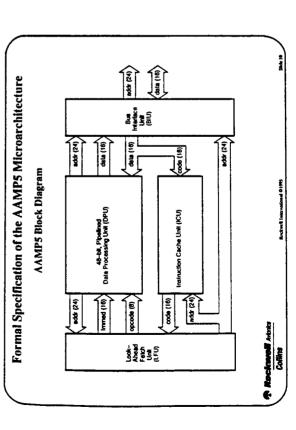
#### Rockmen Mar

Coffins

Rockwell International 01995

# ■ Discovered Two 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 Instruction Sequence and a Specific Instruction Sequence ■ Illustrates the Value of Simply Creating a Precise Specification





## Approach and Issues Maco Approach and Issues Maco Approach and Issues Maco Open Approach and Issues Communing Property

Proofs of Microcode Correctness Microcode Errors Found in This Phase

Pipelining

 Discovered by Collins While Running Application Code on an Early Prototype of the AAMP5
 Both Errors were Found by SRI While Doing the Proofs

O SRI Explained How to Correct Both Errors

O Discovery was Very Systematic

O Escaped Detection by Simulations and Walkthroughs

Seeded Two Errors in Microcode Provided to SRI

■ First was Designed to be Difficult to Detect

Second was an Actual Error

Autonomous Code and Data Access

■ Enhancements to Support Efficient Automation

O Buxlean Decision Diagram (BDD) Decision Procedures

O Optimizations to the PVS Rewriting Engine

Decomposition of Verification Approach to Facilitate Technology Transfer

lociment was

chueß Jakernational @1995

#### Summary

■ Specified 108 of the AAMP's 209 Instructions

Specified the AAMPS 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

Rockwell war

Rectived Internations

### Conclusions

Demonstrated the Technical Feasibility of

O Formally Specifying the AAMP5 at Instruction Set and Register Transfer Levels

O Formally Verifying the Microcode in the AAMPS

Benefits of Formal Specification

O Encourages Clean Abstractions and Interfaces

O Encourages "Looking in Comers"

■ PVS Specifications Successfully Used by Practicing Engineers

O Synergy between Specifications and Inspections was Key

O Acceptance of PVS by Engineers Varies Widely

O Difficult to Enforce the Discipline Needed to Ensure Quality Specifications

Could Achieve Dramatic Galns in Acceptance Through

O Notations that Fit a Specific Problem Domain

**Cociment** Arest

tree II International © 1995

63

### Conclusions

## Formal Verification, Done Correctly, Provides Very High Levels of Assurance

- O Does not Eliminate Good Process, Peer Reviews, Testing, Simulation, ... O May Facilitate or Lessen the Need for Some Traditional Practices

  - Expect Costs to be High the First Time in a New Problem Domain
- O Expertise
- O Reusable Theories and Proofs
- How Much Will Costs Drop on Subsequent Projects?

### AAMP-FV

### Collaborative Effort

- O Funded by NASA and Collins
- O Conducted by Collins and SRI
  - O Initiated in January, 1995
    - Smaller Microprocessor
- O Paper and Pencil Design
- O Similar to What We Would Use in an Autoland System
  - O ~100,000 Transistors

### Repeat AAMPS Experiment

- O Reuse Expertise and Theories
- O Demonstrate Cost Effectiveness
- Current Status
- O Specified Microarchitecture (50 Hours)
   O Nearly Completed the Proof of the First Instruction