Verification of Avionics Systems

Dr. Steven P. Miller
Advanced Technology Center
Rockwell Collins

© Copyright 2011 Rockwell Collins, Inc.
All rights reserved.
Headquartered in Cedar Rapids, Iowa
20,000 Employees Worldwide
2010 Sales of $4.7 Billion
Focus on High Assurance Systems

- California
  - Carlsbad
  - Cypress
  - Irvine
  - Los Angeles
  - Pomona
  - Poway
  - San Francisco
  - San Jose
  - Tustin
- Florida
  - Melbourne
  - Miami
- Georgia
  - Atlanta
  - Warner Robins
- Hawaii
  - Honolulu
- Illinois
  - Chicago
- Iowa
  - Bellevue
  - Coralville
  - Decorah
  - Manchester
- Kansas
  - Wichita
- Maryland
  - White Marsh
- Massachusetts
  - Boston
- Michigan
  - Ann Arbor
  - Detroit

International

- Africa
  - Johannesburg, South Africa
- Asia
  - Bangkok, Thailand
  - Beijing, China
  - Hong Kong
  - Kuala Lumpur, Malaysia
  - Manila, Philippines
  - Moscow, Russia
  - Osaka, Japan
  - Shanghai, China
  - Singapore
  - Tokyo, Japan
- Australia
  - Melbourne, Australia
  - Sydney, Australia
- Canada
  - Montreal
  - Ottawa
- Europe
  - Amsterdam, Netherlands
  - Frankfurt, Germany
  - Heidelberg, Germany
  - London, England
  - Lyon, France
- South America
  - Santiago, Chile
  - Sao Jose dos Campos, Brazil
  - Sao Paulo, Brazil

© Copyright 2011 Rockwell Collins, Inc. All rights reserved.
Rockwell Collins’ core business is based on the delivery of High Assurance Systems

- Commercial/Military Avionics Systems
- Communications
- Navigation & Landing Systems
- Flight Control
- Displays

“Working together creating the most trusted source of communication and aviation electronic solutions”
Airborne Software Doubles Every Two Years

DoD software is growing in size and complexity

Total Onboard Computer Capacity (OFP)


Robert Gold, OSD
Software Aspects of Certification for Civil Aircraft

• Certification – Legal recognition by the certification authority that a product, service, organization or person complies with the requirements.

• Software is not actually certified, but certification of an aircraft does include the “software aspects” of certification.

• DO-178 – Software Considerations in Airborne Systems
  - DO-178A (1985) – 3 levels specified development & verification processes
  - DO-178B (1992) – 5 levels specified objectives, activities, and evidence
  - DO-178C (2012) – similar to DO-178B but with supplements for new technologies

© Copyright 2011 Rockwell Collins, Inc. All rights reserved.
DO-178C Formal Methods Supplement

- Calls Out Formal Methods as an Accepted Means of Compliance
  - Not just an alternate means of compliance as in DO-178B

- Defines Formal Methods
  - Mathematically-based techniques for the specification, development, and verification of software aspects of digital systems
  - Formal logic, discrete mathematics, and computer readable languages

- Allows Partial Use of Formal Methods
  - Enables evolutionary rather than revolutionary adoption

- Describes How Formal Methods Can be Used to Meet Objectives

- Formal Analysis Tools Must Satisfy Tool Qualification Supplement
  - Only if used to meet DO-178C objectives

- Clearly States that Testing Cannot be Completely Eliminated
  - Functional tests executed on target hardware are still required
  - Formal methods can be used to reduce amount of testing
ADGS-2100 Adaptive Display & Guidance System

Modeled in Simulink
Translated to NuSMV
4,295 Subsystems
16,117 Simulink Blocks
Over $10^{37}$ Reachable States

Example Requirement:
The Cursor Shall Never be Positioned on an Inactive Display

Counterexample Found in 5 Seconds

Checked 563 Properties - Found and Corrected 98 Errors in Early Design Models

© Copyright 2011 Rockwell Collins, Inc. All rights reserved.
ADGS-2100 Adaptive Display & Guidance System

System Requirements

A-2: 1, 2

High-Level Requirements

A-2: 3, 4, 5

Formal Properties

A-4.1 Compliance

A-4.2 Accuracy & Consistency

Software Architecture

A-4.8 Architecture Compatibility

A-4.9 Consistency

Design Description

Low-Level Requirements

Simulink Implementation

Source Code

A-2: 6

Object Code

A-2: 7

© Copyright 2011 Rockwell Collins, Inc. All rights reserved.
CerTA FCS Phase I

- Sponsored by the Air Force Research Labs
  - Air Vehicles (RB) Directorate - Wright Patterson

- Investigate Roles of Testing and Formal Verification
  - Can formal verification complement or replace some testing?

- Example Model – Lockheed Martin Adaptive UAV Flight Control System
  - Redundancy Management Logic in the Operational Flight Program (OFP)
  - Well suited for verification using the NuSMV model-checker

---

**Lockheed Martin Aero**

- Based on Testing
- Enhanced During CerTA FCS
  - Graphical Viewer of Test Cases
  - Support for XML/XSLT Test Cases
  - Added C++ Oracle Framework
- Developed Tests from Requirements
- Executed Tests Cases on Test Rig

---

**Rockwell Collins**

- Based on Model-Checking
- Enhanced During CerTA FCS
  - Support for Simulink blocks
  - Support for Stateflow
  - Support for Prover model-checker
- Developed Properties from Requirements
- Proved Properties using Model-Checking
## CerTA FCS Phase I – Errors Found

### Errors Found in Redundancy Manager

<table>
<thead>
<tr>
<th></th>
<th>Model Checking</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triplex Voter</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Failure Processing</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Reset Manager</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>12</strong></td>
<td><strong>0</strong></td>
</tr>
</tbody>
</table>

- Model-Checking Found 12 Errors that Testing Missed
- Spent More Time on Testing than Model-Checking
  - 60% of total on testing vs. 40% on model-checking

Model-checking was more **cost effective** than testing at finding **design** errors.

© Copyright 2011 Rockwell Collins, Inc.  
All rights reserved.
WPAFB 08-5183 RBO-08685 8/20/2008
CerTA FCS Phase I

System Requirements
A-2: 1, 2

High-Level Requirements
A-2: 3, 4, 5

Design Description
A-2: 6

Software Architecture
A-2: 7

Low-Level Requirements

Text Requirements

Formal Properties

Simulink Implementation

© Copyright 2011 Rockwell Collins, Inc.
All rights reserved.
Extending the Verification Domain

- **Theorem Provers**
  - Deal with arbitrary models
  - Concerns are ease of use and labor cost

- **Large Finite Systems (<10^{200} States)**
  - Implicit state (BDD) model checkers
  - Easy to use and very effective

- **Infinite State Systems**
  - SMT-Solvers
  - Large integers and reals
  - Limited to linear arithmetic
  - Ease of use is a concern

- **Floating Point Arithmetic**
  - Most modeling languages use floating point (not real) numbers
  - Decision procedures

- **Non-Linear Arithmetic**
  - Multiplication/division of real variables
  - Transcendental functions (trigonometric, ...)
  - Essential to navigation systems

© Copyright 2011 Rockwell Collins, Inc. All rights reserved.
System Architectural Modeling & Analysis

System Architecture Development
Conclusions

• Formal Methods Are Practical and Are Being Used
  – Model Based Development is the industrial face of formal methods
  – The engineers get to pick the modeling tools!
  – Semantics of some of the commercial tools could be improved

• Formal Verification Tools Are Being Used in Industry
  – Key is to verify the models the engineers are already building
  – Large portions of existing systems can be verified with model checkers
  – DO-178C Formal Methods Supplement opens up new opportunities
  – Tools will need to be qualified

• Directions for the Future Work
  – Making verification tools more powerful and easier to use
  – Floating point arithmetic and non-linear arithmetic
  – Addressing scalability through compositional verification
  – Tool qualification

© Copyright 2011 Rockwell Collins, Inc.
All rights reserved.