3rd NASA Langley Formal Methods Workshop

Formal Methods Demonstration Project for Space Applications

May 11, 1995

John C. Kelly, Ph.D. and Ben DiVito, Ph.D.

- Joint NASA Code Q RTOP -

Jet Propulsion Laboratory*

Johnson Space Center

Langley Research Center

* The work described in this presentation was partially carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Contents

Overview of the Demonstration Project and the Guidebook - John C. Kelly

- The Software Requirements Problem
- Background Project Information
- Phases of the Project
- The NASA Formal Methods Specification and Verification Guidebook

Detailed look at applying Formal Methods to the Shuttle's GPS Upgrade Task - Ben DiVito

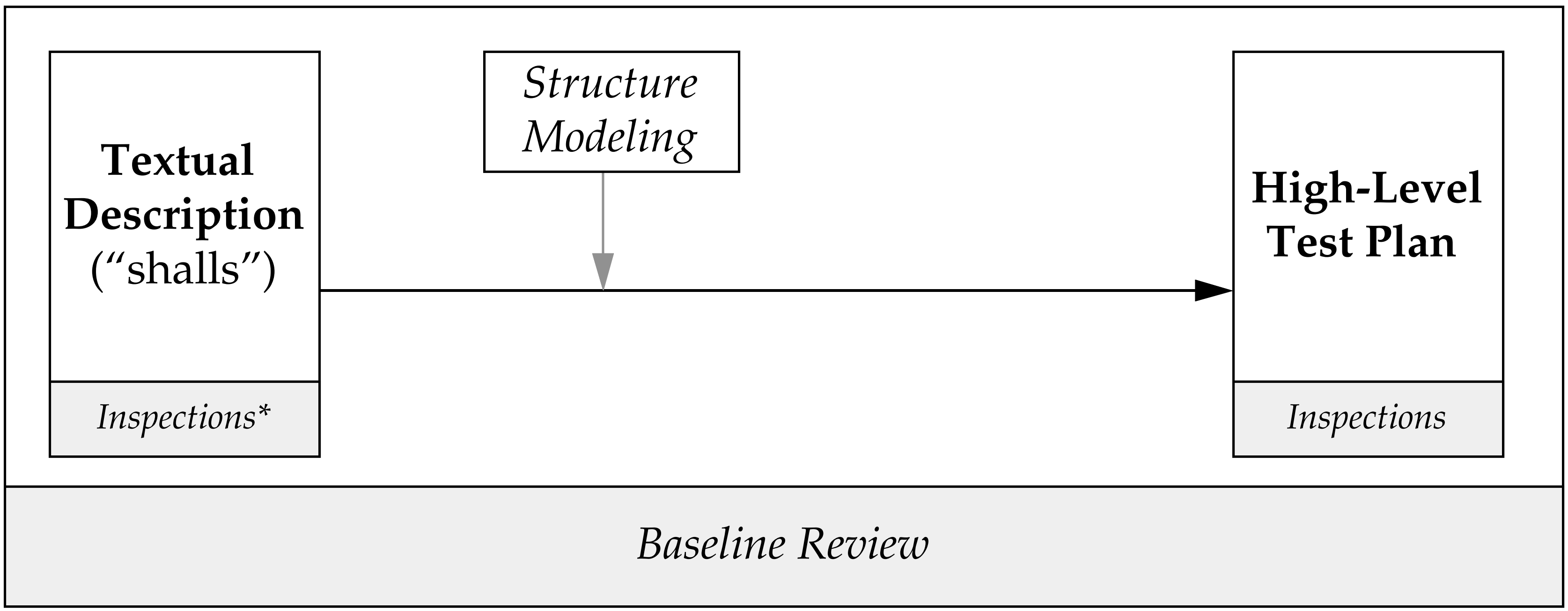
- Description of GPS CR Subset
- PVS Modeling of Principal Functions
- Receiver State Processing
- Results and Feedback
- Summary

The Requirements Problem in Engineering Software Subsystems

Requirements and design specifications are a high priority candidate for better software engineering techniques

- Most hazardous software safety errors found during system integration and test of two NASA spacecraft were the result of requirements discrepancies or interface specifications [Lutz93].
- The highest density of major defects found through the use of software inspections was during the requirements phase. This was 7 times higher than the density of major defects found in code inspections [Kelly92].
- Requirements errors are between 10 and 100 times more costly to fix at later phases of the software lifecycle than at the requirements phase itself [Basili84], [Boehm84], [Kelly92].

Current Requirements Process without Formal Methods



* Note: The word "inspection" is used differently in software than in manufacturing or hardware context . In software the term "inspection" refers to a structured peer review that uses a checklist and includes the collection of defect statistics. In software development, inspections are an upstream quality enhancement technique which support the principles of TQM (refer to NASA Standard 2202-93 or the two JPL Professional Development courses on this topic).

History of Formal Methods POP

Spring 1992	- JSC, JPL and LaRC submit independent Formal Methods proposals to NASA Code Q
Summer and Fall '92	- Code Q funds a Feasibility Study to derive a plan for how the 3 Centers could jointly do a Formal Methods RTOP
Winter '93	- Formal Methods Demonstration Project officially starts with a kick-off meeting at JSC
October '93	- Deliverables for Phase I completed (Formal Methods Specifications, Proofs, etc.)
December '93	- Phase I Report completed for demonstration of Formal Methods on an existing spacecraft
FY94	- Phase II Case Studies - Formal Methods Guidebook (Vol 1)
FY95	- Phase III Case Studies - Formal Methods Guidebook (Vol 2)

Purpose

- The Goal of this study is to demonstrate the applicability of Formal Methods techniques on critical NASA software subsystems
- Phase I Task: Demonstrate the Applicability of Formal Methods to Shuttle's On-Board Jet Select Software Subsystem (A highly critical, yet relatively stable set of requirements)
- Phase II Tasks: Demonstrate Formal Methods on several smaller projects which are currently developing critical software and provide guidance at the managerial level
- Phase III Tasks: Demonstrate Formal Methods on a large critical project in the early development stages, demonstrate at the design level, and provide guidance at the technical level

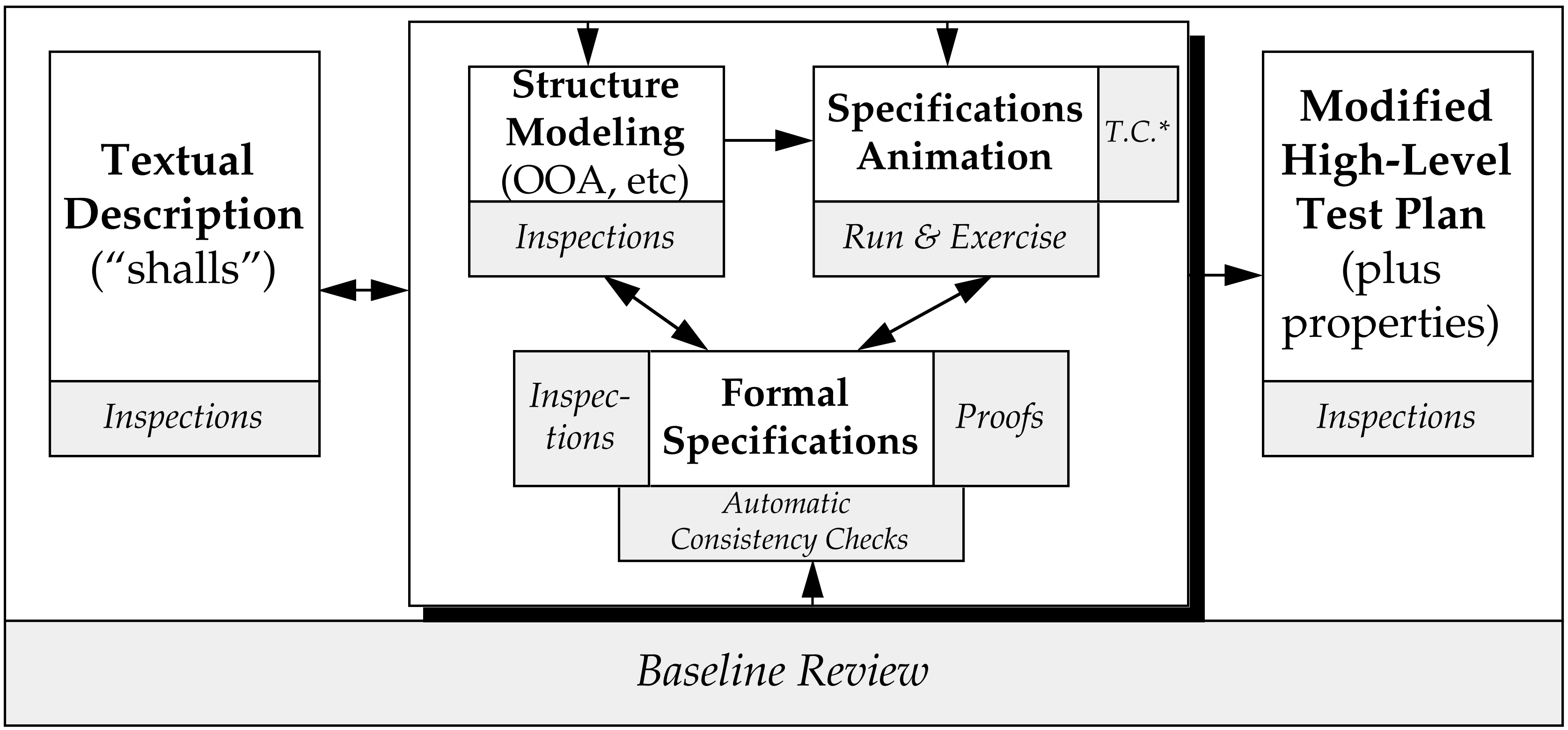
Introduction: Team Members

- **Jet Propulsion Laboratory**
  - **John Kelly, Ph.D., Rick Covington, Ph.D., Robyn Lutz, Ph.D., Ken Abernethy , Ph.D. (Furman U.)**
- **Johnson Space Center**
  - **Ernie Fridge, Dan Bowman (LORAL), Mike Beims (LORAL-Shuttle RA), Chris Hickey (LORAL-Shuttle RA)**
- **Langley Research Center**
  - **Ben DiVito, Ph.D. (VIGYAN), Judith Crow, Ph.D. (SRI), Rick Butler**
- **NASA HQ Sponsor: Alice Robinson**
- **Alumni**
  - **Betty Cheng, Ph.D. (MSU), Mori Khorrami (JPL), Doc Shankar, Ph.D. (IBM), Scott French (LORAL), Sally Johnson (LaRC), John Rushby, Ph.D. (SRI), Sam Owre (SRI), Al Nikora(JPL), Brent Auernheimer, Ph.D. (CSUF), Yoko Ampo (NEC), David Hamilton (HP)**

Generic approach for using Formal Methods to analyze requirements for Space Applications

- Select a portion of the requirements which is mission critical
- Model the selected requirement subset's structure using an informal approach (Object Modeling Techniques was used on some of the pilots)
- Develop Formal Specification for required functionality and state behavior (PVS was used for this on most of the pilots)
- Translate desired properties of the subsystem into a formal language then attempt to verify them against the Formal Specification with a theorem prover (PVS was used in most cases)
- Feedback lists of issues to Requirements Analysts and Development Engineers throughout this process

Integrated Formal Methods Process



* T.C. = Type Checking of formal specifications
** OOA = Object Oriented Analysis

Project Tasks and Deliverables

- Pre-project
  - Formal Methods Feasibility Study - October 1992
- Phase I: FY 1993
  - Shuttle's Jet Select Subsystem
    - 3 Levels of Formal Specifications
    - Ada emulator
  - Formal Methods Case Study Report
- Phase II: FY 1994
  - Shuttle's
    - MIR Docking Change Request
    - Orbit Digital Auto Pilot Model
    - Three Engine Out CR
    - Global Positioning System Change Request (ongoing)

Project Tasks and Deliverables (continued)

- Phase II: FY 1994 (continued)
  - Cassini Space Craft- Fault Protection (Requirements)
  - International□ Space Station Alpha FDIR (ongoing)
  - Formal Methods Guidebook - (development of Volume I)
- Phase III: FY 1995 (current)
  - Cassini Space Craft- Fault Protection (Design)
  - International□ Space Station Alpha FDIR
  - AP101S Assembler for Shuttle
  - Global Positioning System Change Request for Shuttle
  - Formal Methods Guidebook
    - Review Vol. I
    - Develop and Review Vol. 2

Overview of Results and Lessons Learned

- **Formal Methods uncovered significant issues in mature requirements**
- **Even in an unstable requirements environment, formal specifications were found to be beneficial**
- **Requirements Analysts and Developers were generally impressed by the thoroughness and insight of the *issues lists* produced by the pilot study team**
- **Object Modeling Technique provides a good road map before developing Formal Specification**
- **PVS is robust enough to be used for the practical application of Formal Methods to requirements**

Lesson Learned (continued)

- **Be willing to compromise and fill in the requirements analysis gaps with traditional techniques in addition to using Formal Methods**
- **Selecting portions of the requirements of large space application for which Formal Methods provides the greatest analysis leverage is nontrivial**
- **Formal Methods needs to be integrated with other V&V techniques (Fagan Inspections, Traceability Analysis, Hazards Analysis, etc.)**
  - **Automated Integration**
- **Formal Methods should be introduced on projects which already have in place good solid V&V procedures ("pick fertile ground")**

NASA GUIDEBOOK : FORMAL METHODS SPECIFICATION AND VERIFICATION

- Volume I
  - Written for project decision makers, including managers, engineers, and assurance personnel, who are considering the use of FM on their project
  - Easily understood overview of important management issues associated with the use of formal specifications
  - Useful guide to planning and implementing FM on a project
  - Available: June 1995

NASA GUIDEBOOK : FORMAL METHODS SPECIFICATION AND VERIFICATION

- **Volume II**
  - **Will contain detailed information for technical practitioners of FM**
  - **Will address the needs of engineers whose role it is to evaluate new technologies, to transfer those technologies into practice in their organization, and to help projects in planning, training, and implementation**
  - **Available: Fall 1995**

Key Issues for Next Steps (FY 96 and beyond)

- Integrate Formal Methods into a full set of verification, validation, modeling, and design techniques for critical software subsystems of space applications
- Act as a catalyst to transfer Formal Methods techniques to critical NASA Space projects
  - Developing a NASA technology transfer training package
  - Train starter groups of additional Formal Methods analysts from various NASA projects and centers
  - Act as advisors to NASA projects on the effective use Formal Methods
  - Be focal point for the maturation of applying Formal Methods to NASA Space Application projects