Model-Based Design for High Integrity Software Development

Mike Anthony
Senior Application Engineer
MathWorks
Tucson, AZ USA
Model-Based Design for High Integrity Software Development

Agenda

Development and V&V of the Model

- Building a Model from Requirements
  - Introduction to Simulink

- Traceability of a Model to Requirements
  - Using the Requirements Management Interface
  - The Requirements Report

- Conformance to Modeling Standards
  - Using the Model Advisor
  - Customizing the Model Advisor
  - Model Advisor Report

- Verification of the Model against Requirements
  - Requirements-Based Testing & Report Generation
  - Formal Methods Verification

Development and V&V of the Code

- Production Code Generation
  - Creating Data Objects
  - Function Prototype Control

- Traceability of the Generated Code to the Model
  - Code-to-Model Linking
  - Model-to-Code Linking
  - Traceability Report & Traceability Matrix

- Conformance to Coding Standards & Code Verification
  - PolySpace
    - MISRA-C Compliance
    - Proving the Absence of Runtime Errors

- Verification of the Source Code
  - Automating Code Reviews with Simulink Code Inspector

- Verification of the Object Code
  - Test Case reuse
  - SIL/PIL Testing
  - Code Coverage
Why did we miss our deadline?

Reasons for late projects, as reported by Venture Development Corporation. 
Source: Embedded Software Strategic Market Intelligence report, Volume 4, December 2007, VDC. 
Note: Percentages sum to over 100% due to multiple responses.
Minimize Costs by Detecting Errors Earlier

“…each delay in the detection and correction of a design problem makes it an order of magnitude more expensive to fix…”

Clive Maxfield and Kuhoo Goyal
“EDA: Where Electronics Begins”
TechBites Interactive, October 1, 2001
ISBN: 0971406308
62% Cost Savings

- Total Savings: $3,720,000
- Total Investments: $592,000
- ROI: 528%

Bar chart showing savings and investments across different stages: Requirements, Design, Coding, Analysis, Testing.
Methods for Verification and Validation

Verification: Did I do the design right?
Validation: Did I do the right design?

- **Traceability**
  - Requirements to model and code
  - Model to code

- **Modeling and Coding Standards**
  - Modeling standards checking
  - Coding standards checking

- **Testing**
  - Model testing in simulation
  - Processor In the loop

- **Proving**
  - Proving design properties
  - Proving code correctness
Workflow Example

- **Validate**
  - **Requirements**
  - **Design**
    - **Source Code**
      - **Object Code**

- **Trace**
  - Between **Requirements** and **Design**
  - Between **Design** and **Source Code**
  - Between **Source Code** and **Object Code**

- **Conformance**
  - From **Requirements** to **Design**
  - From **Design** to **Source Code**
  - From **Source Code** to **Object Code**

- **Verify**
  - From **Requirements** to **Object Code**
  - From **Design** to **Object Code**
  - From **Source Code** to **Object Code**
**Workflow Example**

### Verify
- **EC:** PIL
  - Simulink Report Generator
  - PS Code Prover*

### Validate
- Embedded Coder
  - Simulink Code Inspector*

### Trace
- **SLVNV:** RMI
  - SLRG: SDD*

- **SLVNV:** DO-178C/DO-331 Checks*

- **PS Bug Finder:** MISRA-C Checks*

- **SLDNV:** Model Coverage*

- **Simulink Design Verifier**

- **Simulink Code Inspector**
  - PS Bug Finder*
  - PS Code Prover*

---

**Abbreviations**
- SL: Simulink
- SLVNV: Simulink Verification and Validation
- RMI: Requirements Management Interface
- SDD: System Design Description
- SLDV: Simulink Design Verifier
- SLRG: Simulink Report Generator
- PS: Polyspace
- RTE: Run-Time Error
- EC: Embedded Coder
- PIL: Processor-in-the-Loop

* DO-178C Qualifiable Tool
Model-Based Design Maturity

Requirements-Based V&V
(requirements-based algorithm development and testing, requirements modeling)

Model Verification & Validation
(simulation-based analysis of requirements)

System Verification & Validation
(re-use of requirements-based tests and results comparisons between simulation and real-time environments)

Fully-leveraged Model-Based Design
(requirements-based design, development, and deployment of production hardware/software)

System Simulation
(algorithm models and plant models)

System Modeling
(closed-loop simulation of algorithms and plant models)

System Prototyping
(real-time closed-loop system simulation with production algorithms on target hardware)

Model-Based Development
(requirements-based design, development, and deployment of production hardware/software)

Algorithm Modeling
(algorithm models, no plant models)

Design Modeling
(open-loop simulation of algorithms)

Design Prototyping
(real-time open-loop simulation of algorithms)

Model-Based Programming
(automatic production code generation from algorithm models)

Simulation Real-Time Testing Production

Modeling & Simulation Adoption

Code Generation Adoption

MAXIMIZE ROI
Septentrio Streamlines DO-178B Certification with MATLAB and Simulink

**Challenge**
Obtain DO-178B certification for a GNSS-based landing system for precision aviation applications

**Solution**
Use Model-Based Design with MATLAB and Simulink to trace requirements, architect system components, simulate the design, and generate and verify source code

**Results**
- Design test cases reused on generated C source code
- Models verified via simulation, ensuring virtually bug-free code
- Key SOI-1 certification milestone achieved

“Model-Based Design enabled us to streamline the certification process by tracking requirements, verifying the design using simulation, and maintaining the system model as the single source of truth throughout development.”
Jan D’Espallier
Septentrio

Link to article
Challenge
Speed the development, validation, and verification of DO-178B certified helicopter flight software

Solution
Use Model-Based Design to model the system design and software design, and to generate flight code

Results
- Software testing time cut by two-thirds
- Requirements stabilized earlier
- Certified flight software automatically generated

“We use our system design model in Simulink for ARP4754 to establish stable, objective requirements. We save time by using the model as the basis for our software design model for DO-178—from which we generate flight code—and reusing validation tests for software verification.”

Ronald Blanrue
Eurocopter

Link to user story
Airbus Develops Fuel Management System for the A380 Using Model-Based Design

**Challenge**
Develop a controller for the Airbus A380 fuel management system

**Solution**
Use MATLAB, Simulink, and Stateflow for Model-Based Design to model and simulate the control logic, communicate the functional specification, and accelerate the development of simulators

**Results**
- Months of development time eliminated
- Models reused throughout development
- Additional complexity handled without staff increases

“Model-Based Design gave us advanced visibility into the functional design of the system. We also completed requirements validation earlier than was previously possible and simulated multiple simultaneous component failures, so we know what will happen and have confidence that the control logic will manage it.”

Christopher Slack
Airbus

Link to user story
MathWorks Services & Support
Support and Community

The MathWorks Connections Program

The MathWorks Consulting Services

MATLAB® CENTRAL

The MathWorks Training Services

The MathWorks Book Program
MATLAB Central

- Open exchange for the MATLAB and Simulink user community
- 662,000 visits per month
- File Exchange
  - Upload/download free files including MATLAB code, Simulink models, and documents
  - Rate files, comment, and ask questions
  - More than 9,000 contributed files, 400 submissions per month, 25,500 downloads per day
- Newsgroup
  - Web forum and newsgroup for technical discussions about MATLAB and Simulink
  - 200 posts per day
- Blogs
  - Read posts from key MathWorks developers who design and build the products
  - Join the conversation at blogs.mathworks.com

Based on February 2009 data
Technical Support

Resources

- Over 100 support engineers
  - All with MS degrees (EE, ME, CS)
  - Local support in North America, Europe, and Asia
- Comprehensive, product-specific Web support resources

High customer satisfaction

- 95% of calls answered within three minutes
- 70% of issues resolved within 24 hours
- 80% of customers surveyed rate satisfaction at 80-100%

www.mathworks.com/support
Training

- Three ways to get training
  - Public training
    - Offered throughout the world
    - Schedule and course information at www.mathworks.com/training
  - Onsite training
    - Bring training to your site, with course customization available
  - Web-based training
    - Instructor-led e-learning
    - Train at work or at home, with flexible dates and times

- Example course topics
  - Introductory and intermediate training on MATLAB, Simulink, Stateflow, and Real-Time Workshop
  - Specialized courses in control design, signal processing, parallel computing, code generation, communications, financial analysis, and other areas
Consulting

- Engineering expertise and deep product knowledge, specializing in:
  - Application development using MATLAB
  - Model-Based Design using Simulink and Stateflow
  - Embedded systems development
  - Enterprise-wide integration of MathWorks products into engineering process and systems
  - Jumpstart services for a fast, smooth transition to MathWorks products

- Project-based services for a growing number of industries, including aerospace and defense, automotive, communications, power and marine, and financial services
Partner Program

More than 300 add-on products and services that complement and extend MathWorks products:

- Specialized third-party toolboxes for MATLAB
- Interfaces to third-party software and hardware products
- Specialized training courses and consulting services
- System integrators and suppliers that incorporate MathWorks products
We want to hear from you – demonstrate how MathWorks products support innovation and improve development process within your organization

We host dozens of events annually

If you would like to
- Present at a MathWorks seminar or symposium
- Write a white paper
- Develop a user story

Sign up
At the registration table
Fill out form