Using MathWorks Products to Generate Code for DO-178B Applications

Presenter: Bill Potter

Date: June 15, 2006

The MathWorks
Aerospace & Defense Conference | 2006

Frequently Asked Question

Do MathWorks products generate DO-178B certified code?

This is not a valid question, because code does not get certified.

What is certification?

- Certification applies to (ARP-4754/DO-178B):
    - A Product
    - A Service
    - An Organization
    - A Person
- Certification involves (ARP-4754/DO-178B):
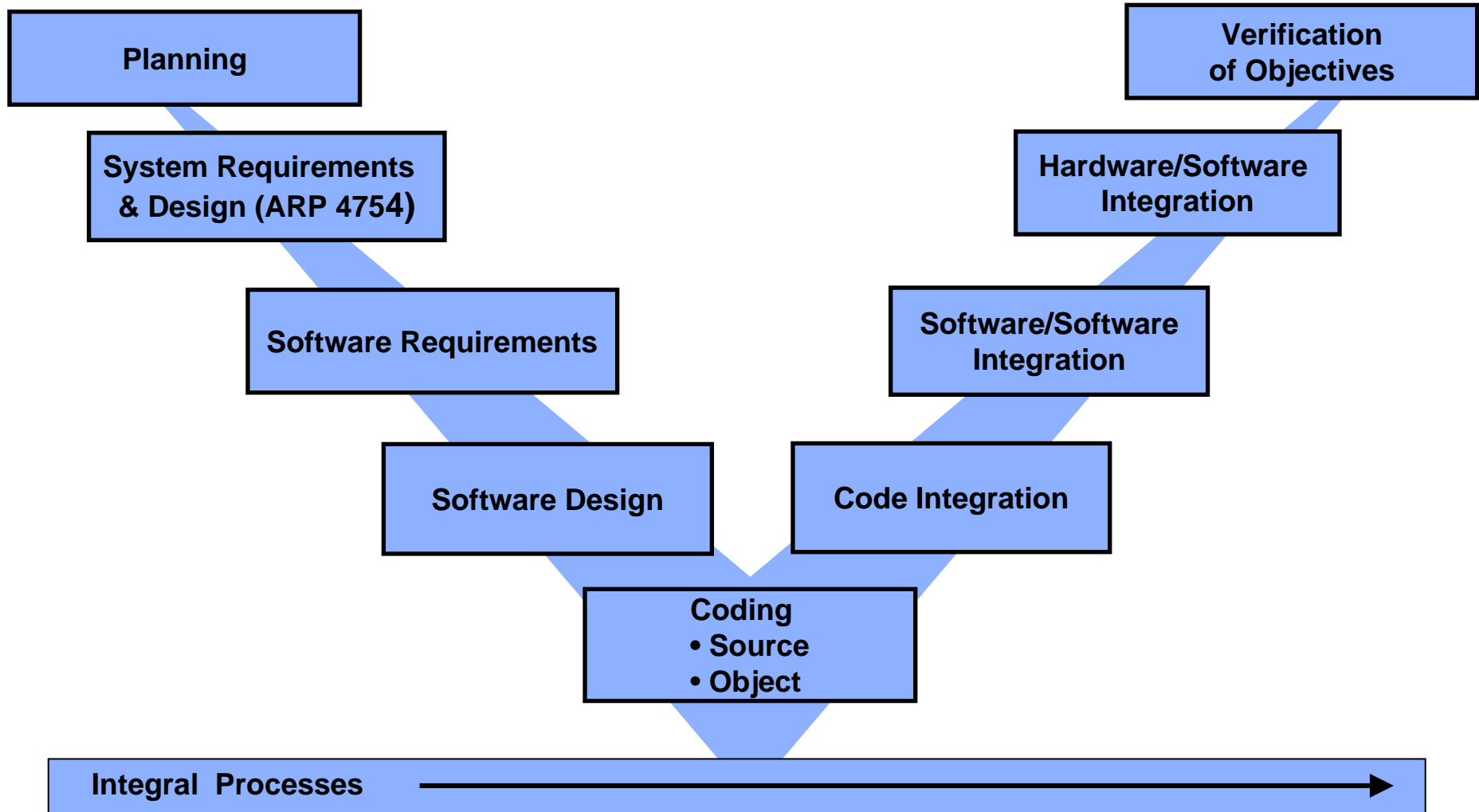   - Compliance demonstration

Demonstrating DO-178B Compliance

- Planning process (7 objectives)

- Software development process (7 objectives)

- Verification of requirements process (7 objectives)

- Verification of design process (13 objectives)

- Verification of coding and integration process (7 objectives)

- Testing of outputs of integration process (5 objectives)

- Verification of verification process results (8 objectives)

- Integral processes (12 objectives)

The Bottom Line

- Total objectives = 66

- Source code objectives = 7

- Must address the entire software lifecycle, not just source code

DO-178B Development Process

Planning

System Requirements & Design (ARP 4754)

Software Requirements

Software Design

Coding
• Source
• Object

Code Integration

Software/Software Integration

Hardware/Software Integration

Verification of Objectives

Integral Processes

Planning Process for Model-Based Design

- Model standards and guidelines

- Mapping to DO-178B
    – High-level requirements?
    – Low-level requirements?
- Configuration management
- Traceability
    – Models trace to higher-level requirements
    – Source code traces to models
- Testing independence
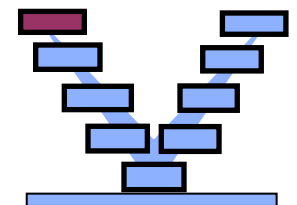
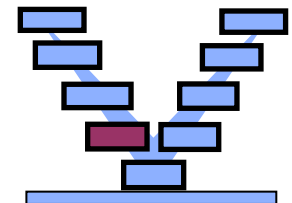# Requirements Process for Model-Based Design

- Functional, operational, and safety requirements
  - Exist one level above the model
  - May be systems requirements or high level software requirements
  - Models trace to these using Simulink® Verification and Validation - Requirements Management Interface
- Requirements validation
  - Prove requirements are complete and correct
 - Modeling is a validation technique using Simulink and Stateflow®
- Examples
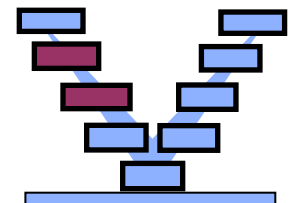
Design Process for Model-Based Design

- Model-Based Design
  - Simulink and Stateflow used to create the design
  - Simulink® Report Generator used to document the design
- Traceability
  - Design traces to requirements using Simulink® Verification and Validation - Requirements Management Interface
- Example

Coding Process for Model-Based Design

- Automatic code generation
    - Source code is generated from model using Real-Time Workshop® Embedded Coder
- Traceability
    - Source code is traceable to model using HTML Code Report generated by Real-Time Workshop Embedded Coder
- Example
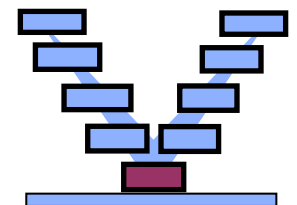
Integration Process for Model-Based Design

- Executable object code generation
  - Source code is compiled, linked, and loaded using third party tools
  - Real-Time Workshop Embedded Coder may be used to generate a makefile for use in the build process
  - Run-time libraries are supplied with Real-Time Workshop Embedded Coder for use with generated code
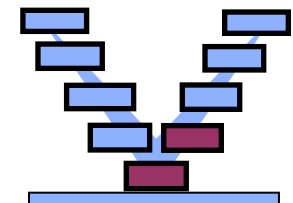
Verification Process for Model-Based Design

- Design verification
  - Design complies with standards using manual reviews and Simulink Verification and Validation - Model Advisor
  - Design complies with requirements using Simulink Verification and Validation, SystemTest, and Simulink Report Generator

- Source code verification
  - Source code complies with standards using third party tools such as PolySpace MISRA-C Checker
  - Source code complies with design using manual reviews

- Executable object code verification
  - Reuse test cases from design verification produced by Simulink Verification and Validation and SystemTest for PIL testing
  - Eliminate traditional software unit testing

- Examples
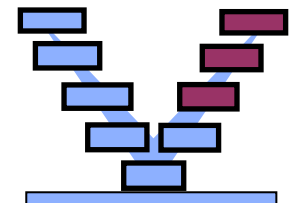
MathWorks products can assist with:

- Planning and integral processes: 1 out of 7 objectives
- Software development process: 6 out of 7 objectives
- Verification of requirements process: 7 out of 7 objectives
- Verification of design process: 12 out of 13 objectives
- Verification of coding and integration process: 1 out of 7 objectives
- Testing of outputs of integration process: 5 out of 5 objectives
- Verification of verification process results: 7 out of 8 objectives
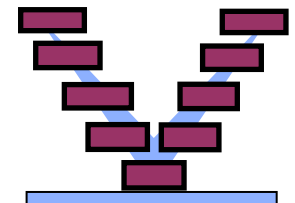
Conclusion

- MathWorks products can be used to accelerate software development for products that must comply with the DO-178B guidelines for certification.

- MathWorks products can assist in satisfying 38 of the 47 development and verification objectives required by DO-178B (ignoring the 19 Planning and Integral Process objectives).

- Third-party tools can be used to address additional objectives.