The MathWorks™

MATLAB® & SIMULINK®

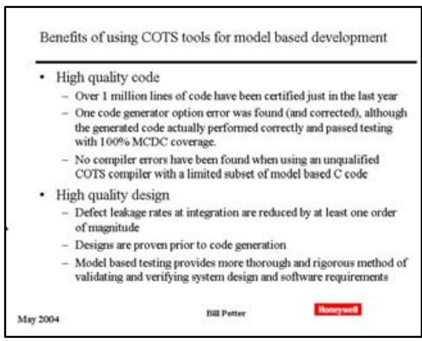
Model-Based Design for Safety Critical Automotive Applications

Mirko Conrad
Senior Team Lead
Simulink Certification and Standards

MathWorks Automotive Conference '08

Model-Based Design for Safety-Critical Applications Success Stories

- MathWorks tools **applied successfully to safety-critical applications** in different domains

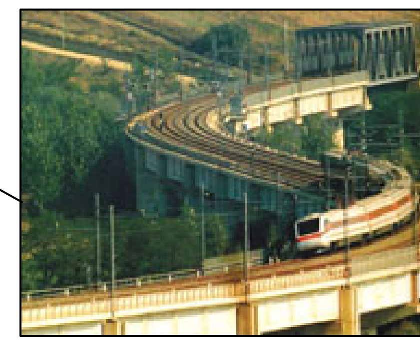


Benefits of using COTS tools for model based development

- High quality code
  - Over 1 million lines of code have been certified just in the last year
  - One code generator option error was found (and corrected), although the generated code actually performed correctly and passed testing with 100% MCDC coverage.
  - No compiler errors have been found when using an unqualified COTS compiler with a limited subset of model based C code
- High quality design
  - Defect leakage rates at integration are reduced by at least one order of magnitude
  - Designs are proven prior to code generation
  - Model based testing provides more thorough and rigorous method of validating and verifying system design and software requirements

May 2004 Bill Potter Honeywell

Honeywell generated flight control code certified to DO178-B Level A
www.mathworks.com/industries/aerospace/miadc05/presentations/potter.pdf
faculty.erau.edu/korn/ToolForum/Potter_files/frame.htm



Alstom generated code for safety-critical power converter control systems
www.mathworks.com/products/rtwembedded/userstories.html?file=10591

Institute for Radiological Protection and Nuclear Safety verified nuclear safety software with PolySpace products
https://tagteamdbserver.mathworks.com/ttserverroot/Download/42572_IRSN_final.pdf

Model-Based Design for Safety-Critical Automotive Applications

Customer's "list of presents"

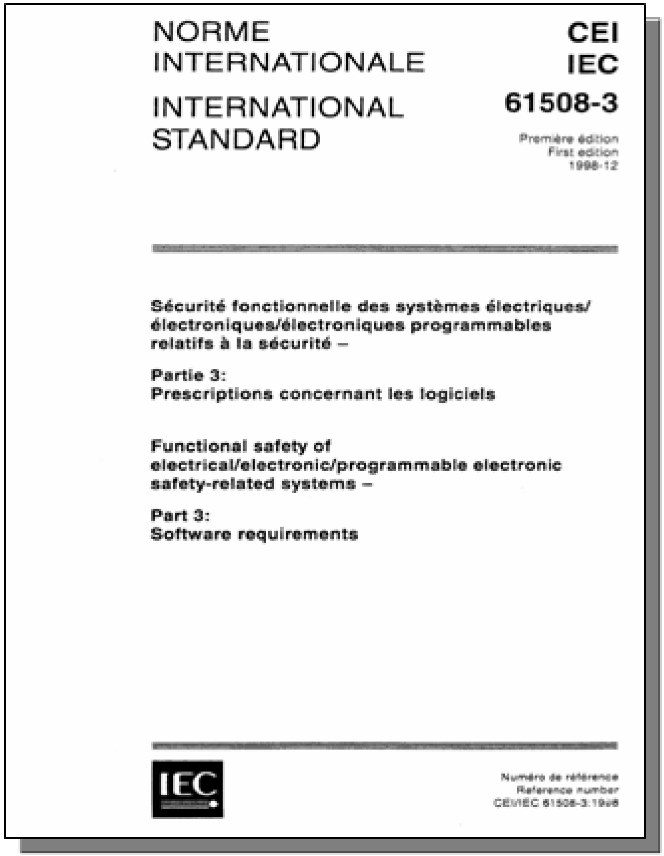
1. Leverage advantages of Model-Based Design and state-of-the-art code generation

2. Eased compliance demonstration

3. Validated / certified tools

IEC 61508 in the Automotive Industry

- Generic Safety Standard
- Defines safety life cycle
- Constrains software development, verification, and validation processes
- Increasingly relevant for automotive companies
  - Voluntary adherence across Europe (state-of-the-art)
  - Also applicable to noncritical applications (best practices)



NORME INTERNATIONALE
INTERNATIONAL STANDARD

CEI
IEC
61508-3

Première édition
First edition
1998-12

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –

Partie 3:
Prescriptions concernant les logiciels

Functional safety of electrical/electronic/programmable electronic safety-related systems –

Part 3:
Software requirements

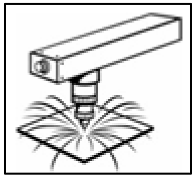
IEC

Numéro de référence
Reference number
CEI/IEC 61508-3:1998

Model-Based Design for IEC 61508

- Standard was established in late 1990s:
  No notion of Model-Based Design, code generation, etc.

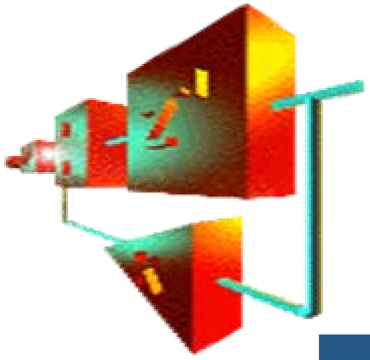
- Origin in the process and automation industries:
  Industry-specific adaptations; subject to interpretation



- Processes, measures, and techniques (especially in the verification and validation area) need to be mapped onto Model-Based Design processes and tools

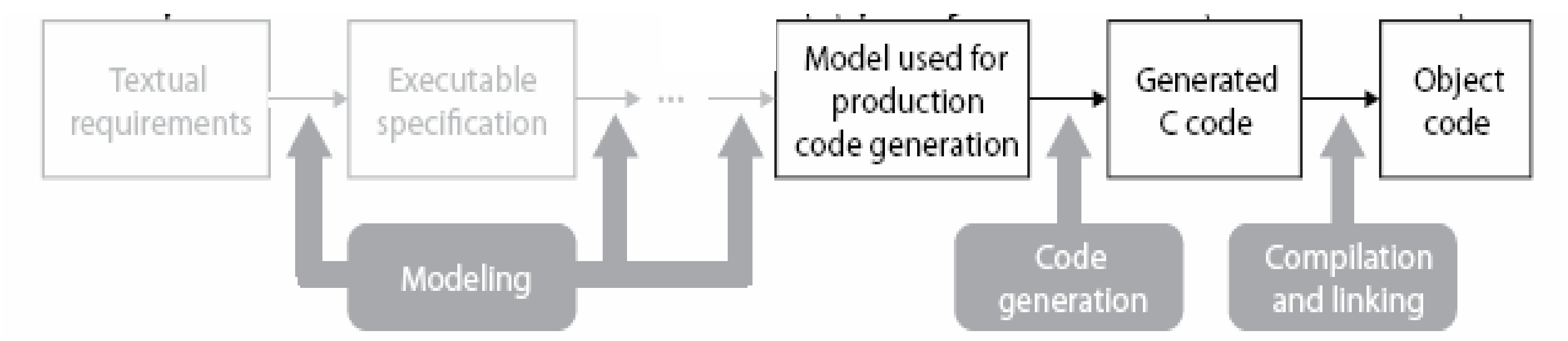
Table A.3 – Software design and development:
support tools and programming language (see 7.4.4)

	Technique/Measure*	Ref	SIL1	SIL2	SIL3	SIL4
1	Suitable programming language	C.4.6	HR	HR	HR	HR
2	Strongly typed programming language	C.4.1	HR	HR	HR	HR
3	Language subset	C.4.2	---	---	HR	HR



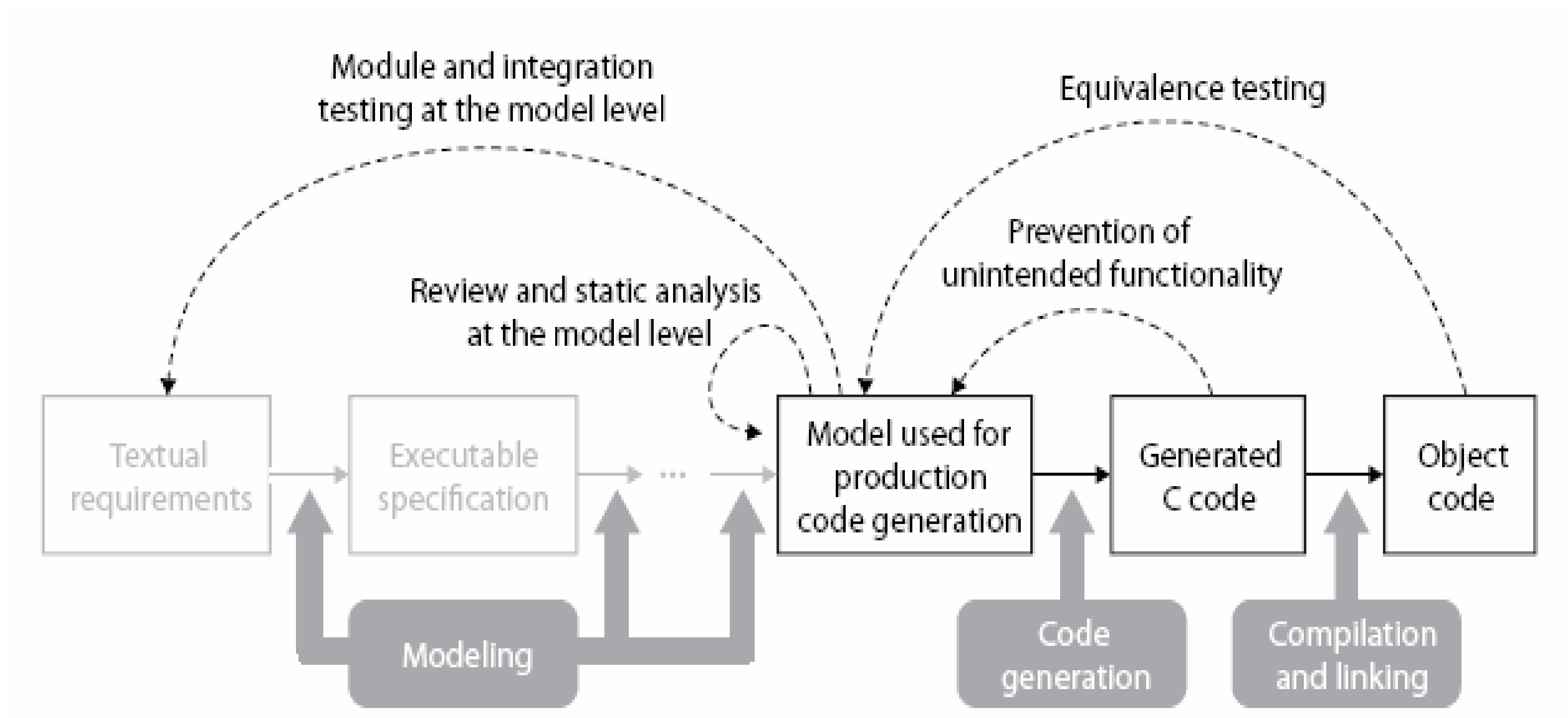
IEC 61508 Compliant Verification and Validation

- TÜV approved reference workflow



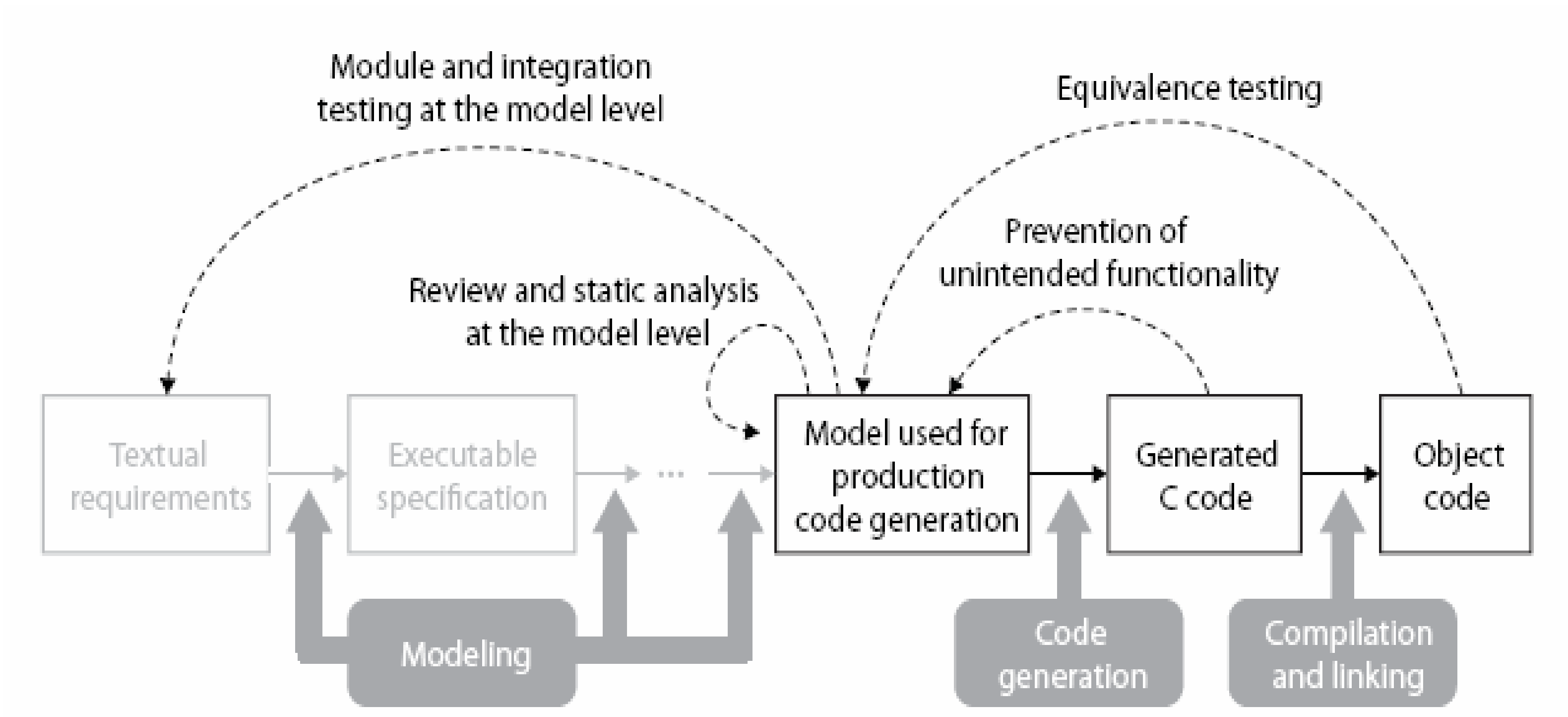
IEC 61508 Compliant Verification and Validation

- TÜV approved reference workflow

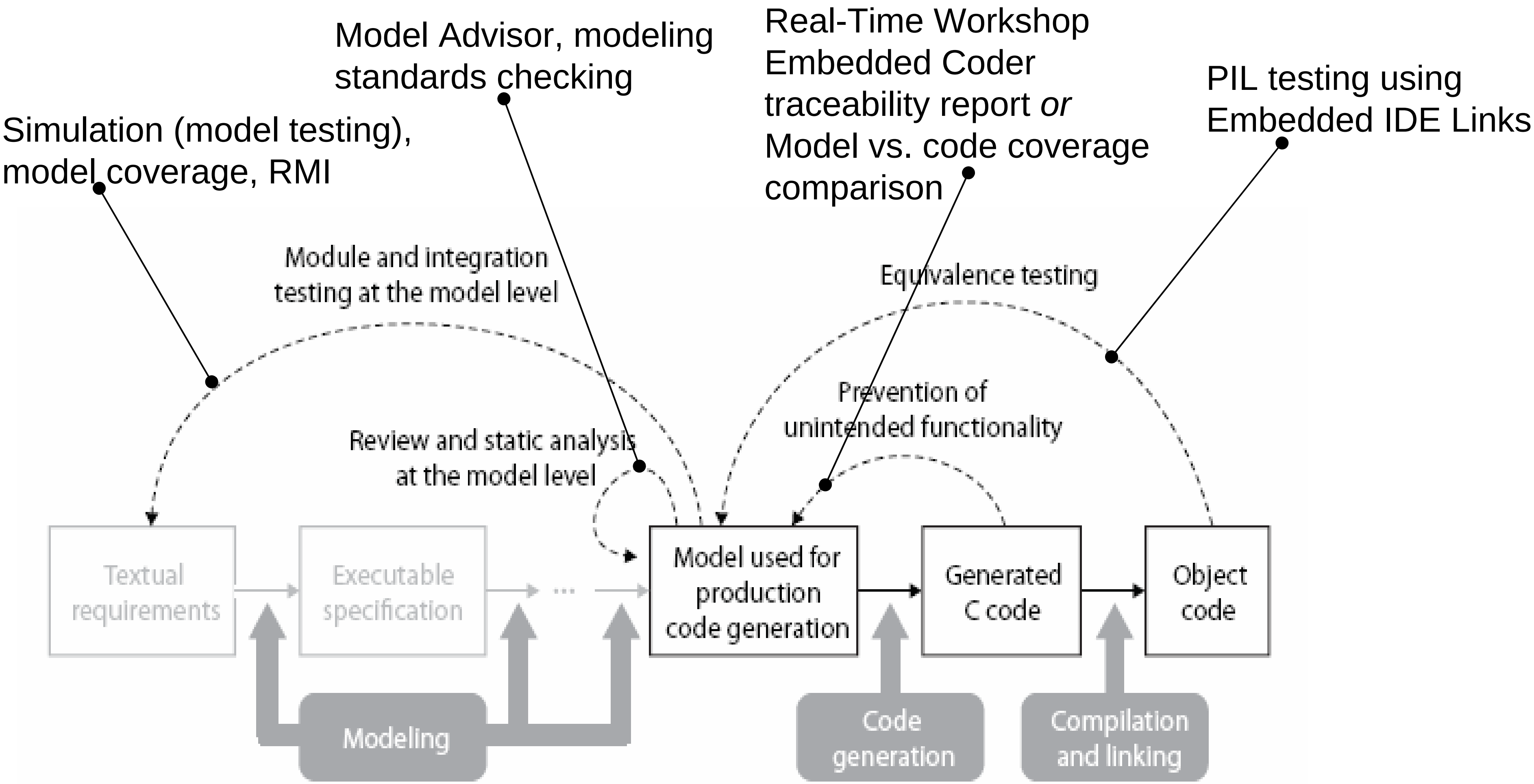


IEC 61508 Compliant Verification and Validation

- TÜV approved reference workflow

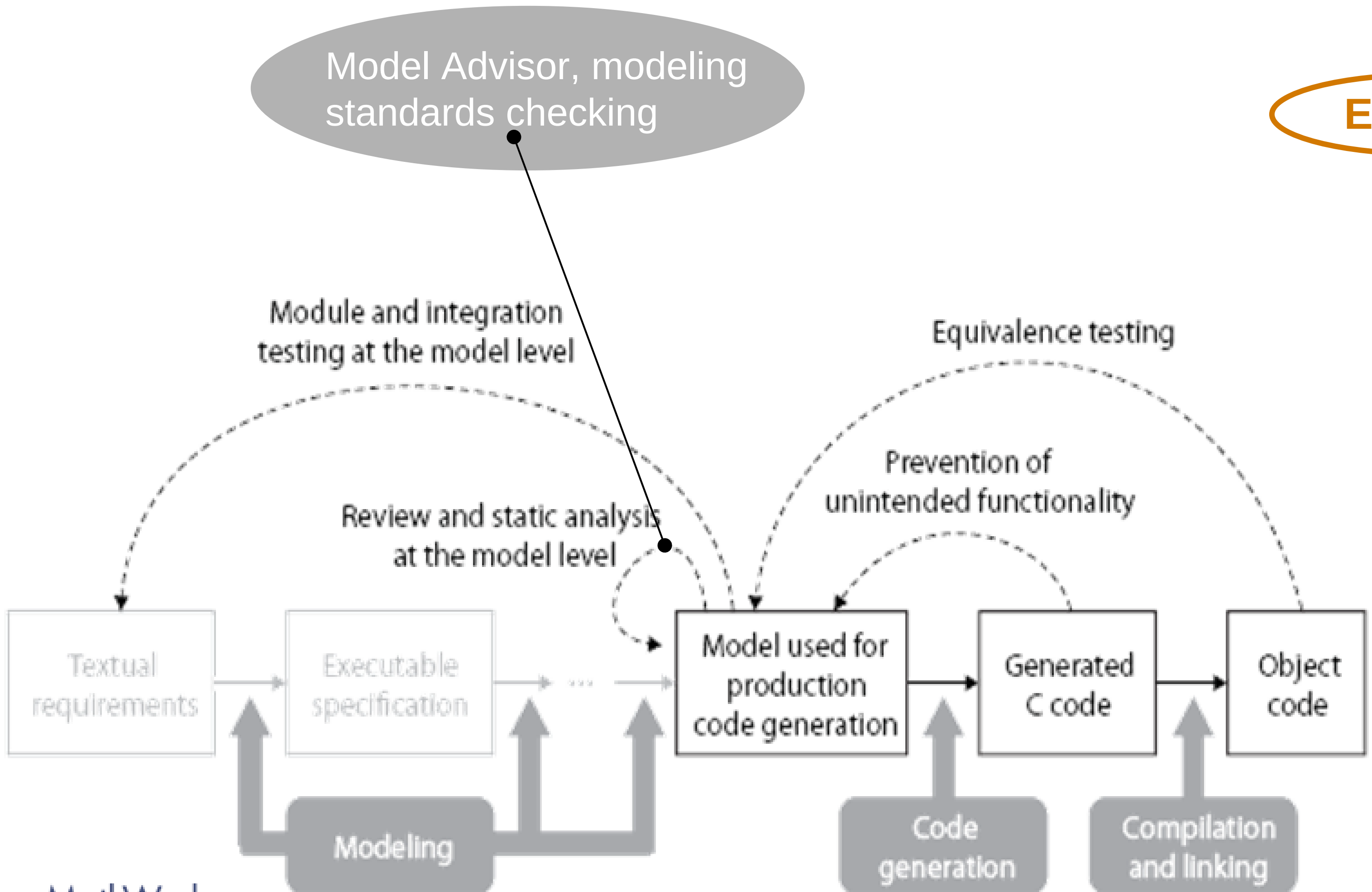


IEC 61508 Compliant Verification and Validation with MathWorks Products



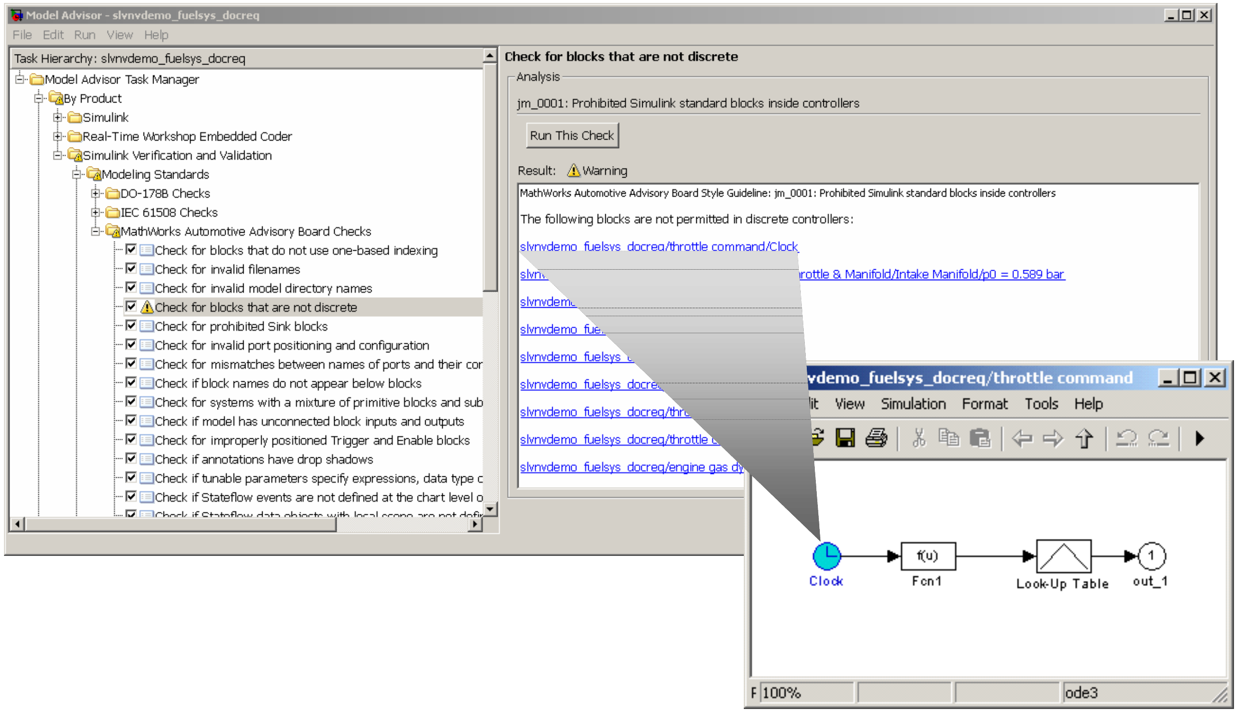
IEC 61508 Compliant Verification and Validation with MathWorks Products

Example



Model Advisor

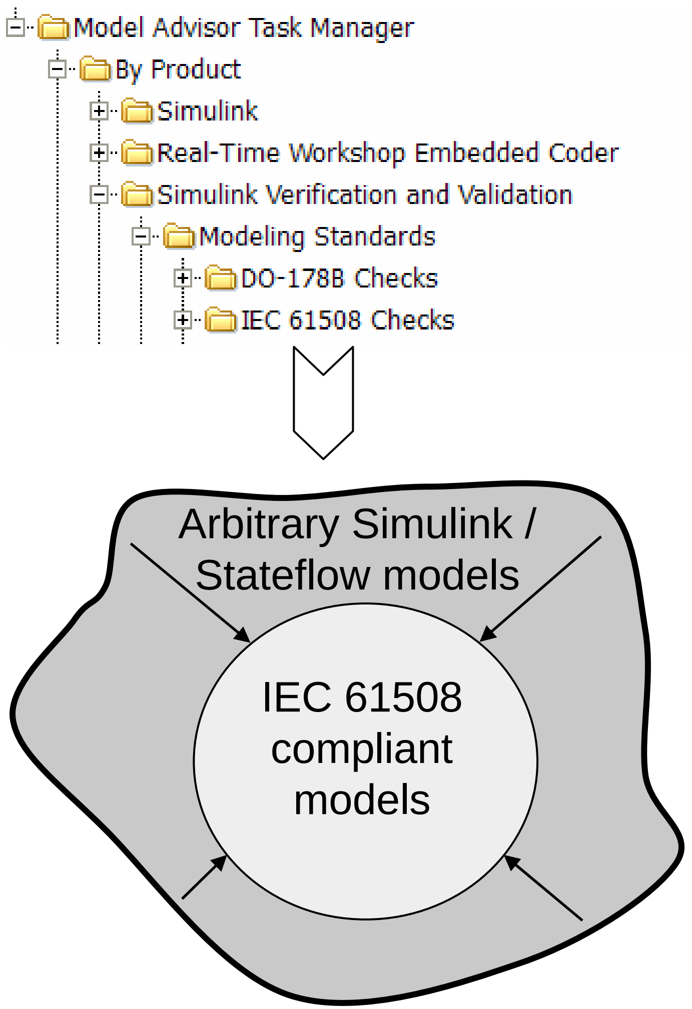
- **Static analysis of models** against a set of checks
  - Simulation
    (Simulink)
  - Code generation
    (RTW-EC)
  - Requirements consistency
    (Simulink V&V)
  - Modeling standards
    (Simulink V&V)
    - MAAB
    - IEC 61508
    - DO178B



- API to create custom checks and groups (Simulink V&V)

Modeling Standards Checking IEC 61508

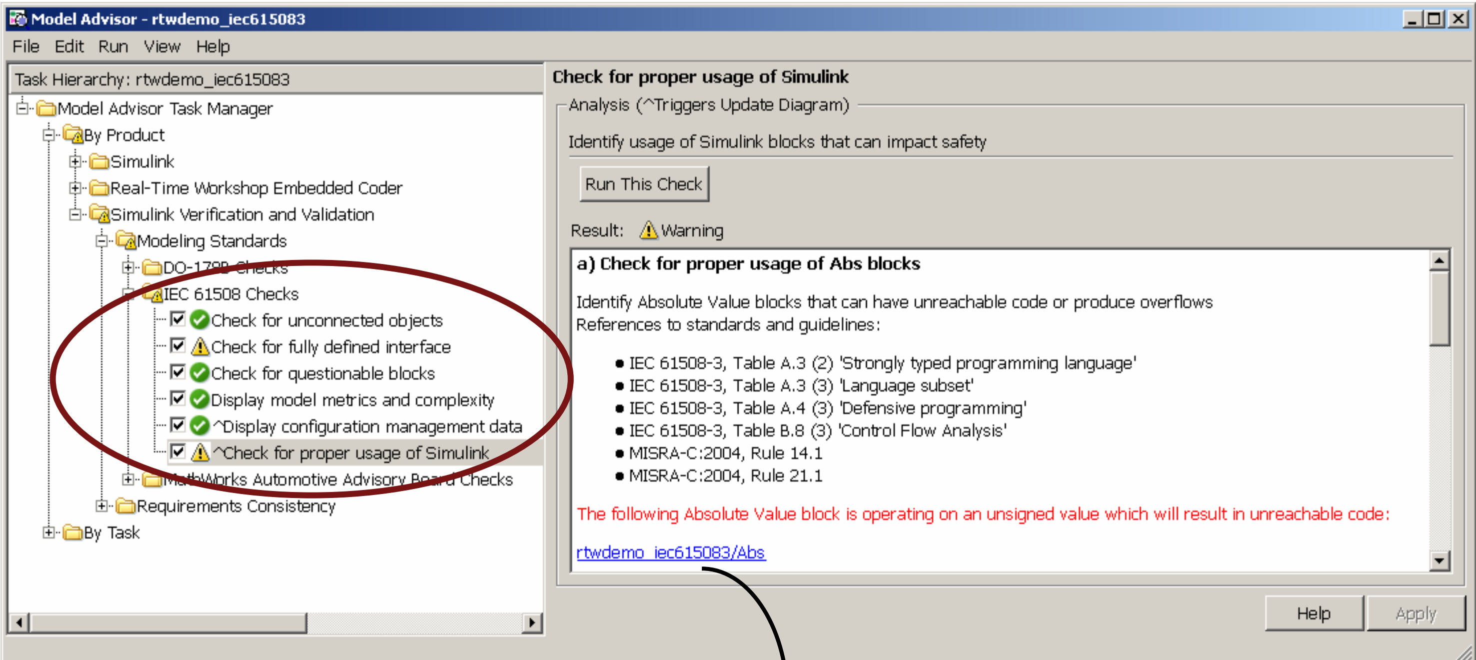
- Quickly **identify issues** at the model level **that impede deployment in IEC 61508 applications** or limit traceability



Benefits

- Automated design reviews
- Enhanced traceability
- Seamless use of Real-Time Workshop Embedded Coder and V&V products

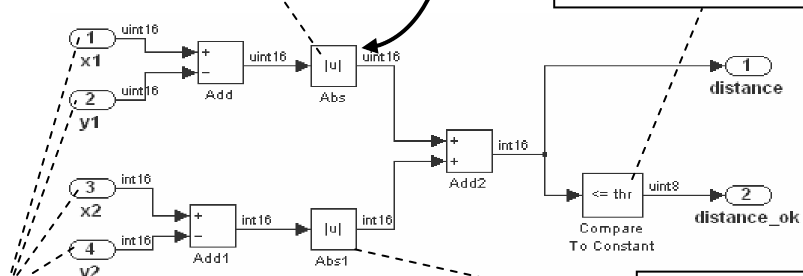
Modeling Standards Checking IEC 61508



Demo

This Absolute Value block is operating on an unsigned value which may result in unreachable code.

This relational operator block is not outputting a boolean data type which can lead to unpredictable results in the generated code.



These root-level Inport blocks have undefined attributes.

This Absolute Value block is operating on a signed integer value but saturate on integer overflow is not set, which can lead to incorrect results in the generated code.

www.mathworks.com/support/solutions/data/1-5WGFYT.html

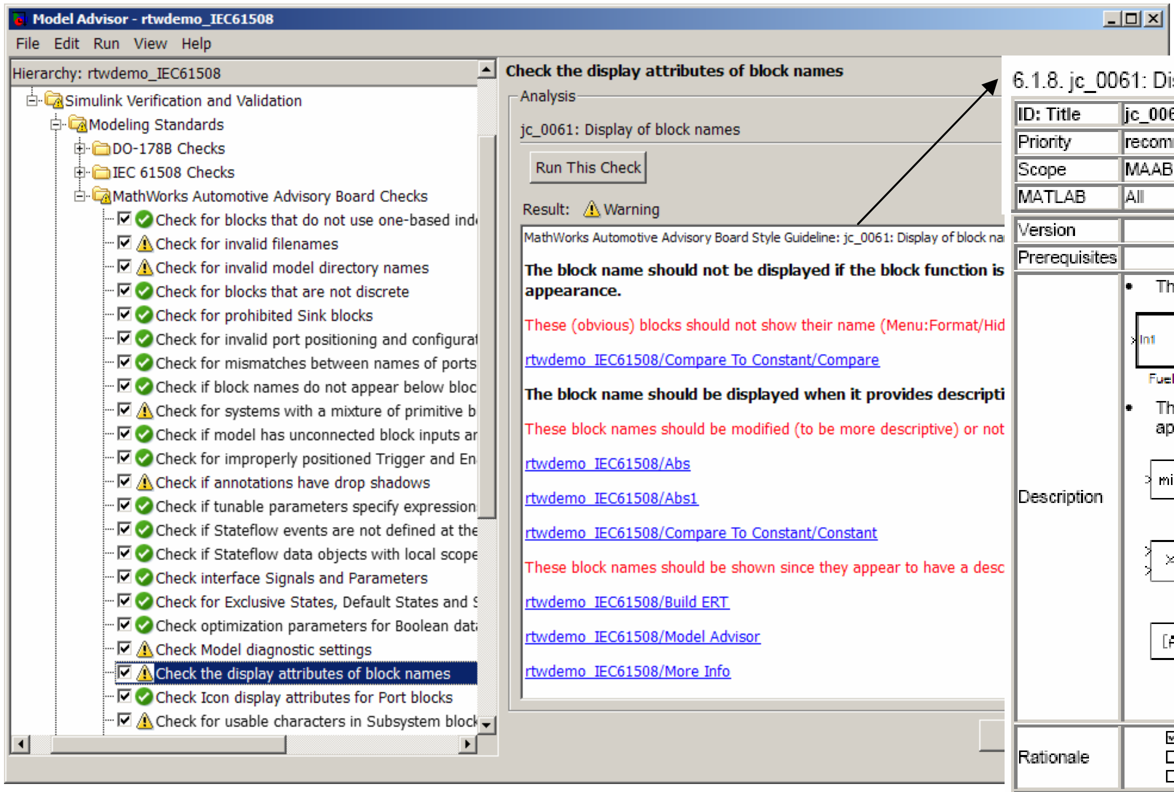
Modeling Standards Checking MAAB

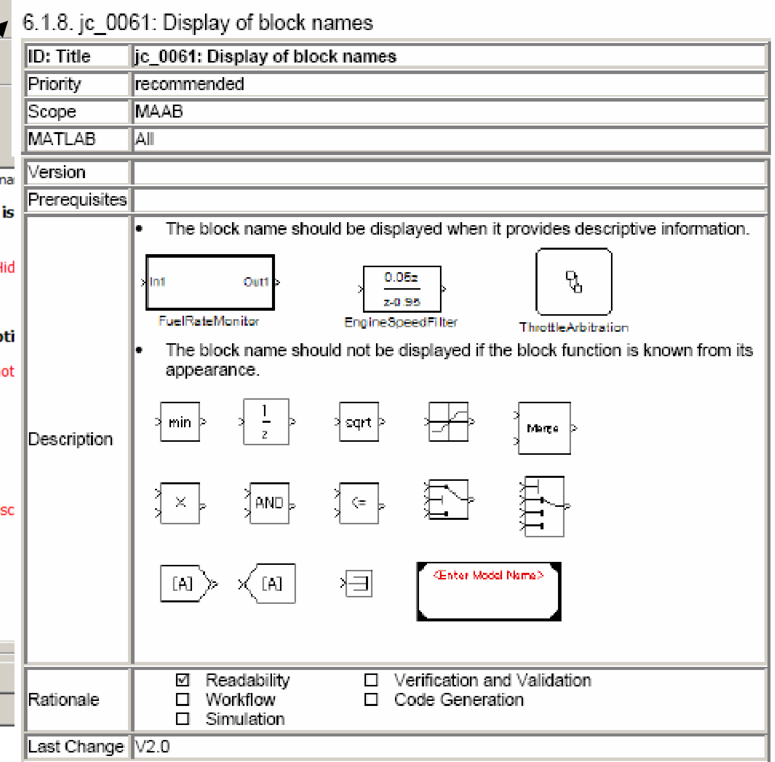
- Automated rule checking
  for 30+ MAAB V2.0 guidelines

CONTROL ALGORITHM MODELING GUIDELINES USING MATLAB®, Simulink®, and Stateflow®
Version 2.0

MathWorks Automotive Advisory Board (MAAB)
July 27th, 2007

www.mathworks.com/industries/auto/maab.html




6.1.8. jc_0061: Display of block names

ID: Title	jc_0061: Display of block names
Priority	recommended
Scope	MAAB
MATLAB	All
Version	
Prerequisites	
Description	• The block name should be displayed when it provides descriptive information. FuelRateMonitor, EngineSpeedFilter, ThrottleArbitration • The block name should not be displayed if the block function is known from its appearance.
Rationale	☑ Readability ☐ Workflow ☐ Simulation ☐ Verification and Validation ☐ Code Generation
Last Change	V2.0

Model-Based Design for Safety-Critical Automotive Applications

Customer's "list of presents"

1. Leverage advantages of Model-Based Design and state-of-the-art code generation
   - **Tool-supported IEC 61508 compliant verification and validation**
2. Eased compliance demonstration
3. Validated / certified tools

IEC 61508 Compliance Documentation

"To conform to this standard it shall be demonstrated that the requirements have been satisfied to the required criteria specified and therefore, for each clause or sub-clause, all the objectives have been met"

- Often involves listing all IEC 61508 requirements with an explanation of how each requirement has been met

61508-3 © IEC:1998 – 79 –

Table A.3 – Software design and development: support tools and programming language (see 7.4.4)

	Technique/Measure*	Ref	SIL1	SIL2	SIL3	SIL4	Interpretation in this Application
1	Suitable programming language	C.4.6	HR	HR	HR	HR	?
2	Strongly typed programming language	C.4.1	HR	HR	HR	HR	?
3	Language subset	C.4.2	---	---	HR	HR	?
4a	Certificated tools	C.4.3	R	HR	HR	HR	?
4b	Tools: increased confidence from use	C.4.4	HR	HR	HR	HR	?
5a	Certificated translator	C.4.3	R	HR	HR	HR	?
5b	Translator: increased confidence from use	C.4.4	HR	HR	HR	HR	?
6	Library of trusted/verified software modules and components	C.4.5	R	HR	HR	HR	?

IEC 61508 Compliance Documentation
with MathWorks Products

61508-3 © IEC:1998 – 79 –

Table A.3 – Software design and development:
support tools and programming language (see 7.4.4)

	Technique/Measure*	Ref	SIL1	SIL2	SIL3	SIL4	Interpretation in this Application
1	Suitable programming language	C.4.6	HR	HR	HR	HR	?
2	Strongly typed programming language	C.4.1	HR	HR	HR	HR	?
3	Language subset	C.4.2	---	---	HR	HR	
4a	Certificated tools	C.4.3	R	HR	HR	HR	?
4b	Tools: increased confidence from use	C.4.4	HR	HR	HR	HR	?
5a	Certificated translator	C.4.3	R	HR	HR	HR	?
5b	Translator: increased confidence from use	C.4.4	HR	HR	HR	HR	?
6	Library of trusted/verified software modules and components	C.4.5	R	HR	HR	HR	?

The MAAB Style Guides and/or organization specific modeling guidelines can be used to define a subset of the modeling language.

The Stateflow language can be restricted to Stateflow charts that implement pure Mealy or Moore semantics.

The Simulink Block Data Type Support table lists the blocks that can be used for code generation with Real-Time Workshop Embedded Coder.

Simulink - Model Advisor can be used to partially enforce restricted language subsets.

Model reviews based on reports generated by Simulink Report Generator can be conducted to check language subset considerations on model level.

Model reviews based on reports generated by Simulink Report Generator – Web View can be conducted to check language subset considerations on model level.

Code Reviews based on Real-Time Workshop Embedded Coder – Code Generation Reports can be conducted to check language subset considerations on code level.

Configuration Sets can be customized to enforce specific settings of the involved Model-Based Design Tools, e.g. diagnostics and optimization settings.

MISRA-C and/or organization specific coding guidelines can be used to define a subset of the implementation language.

Third-party products, such as the TASKING compiler tool chain (for Infineon, ARM, and other devices), supported by Link for TASKING®, facilitate MISRA-C compliance checking of generated code.

Third-party products, such as PolySpace Desktop, facilitate MISRA-C compliance checking of generated code.

Third-party products, such as PolySpace Desktop, can be used to check language subset considerations within the generated code.

- Maps IEC 61508-3 objectives onto Model-Based Design and production code generation
- Provides detailed suggestions for 100+ techniques and measures

www.mathworks.com/products/rtwembedded/technicalliterature.html

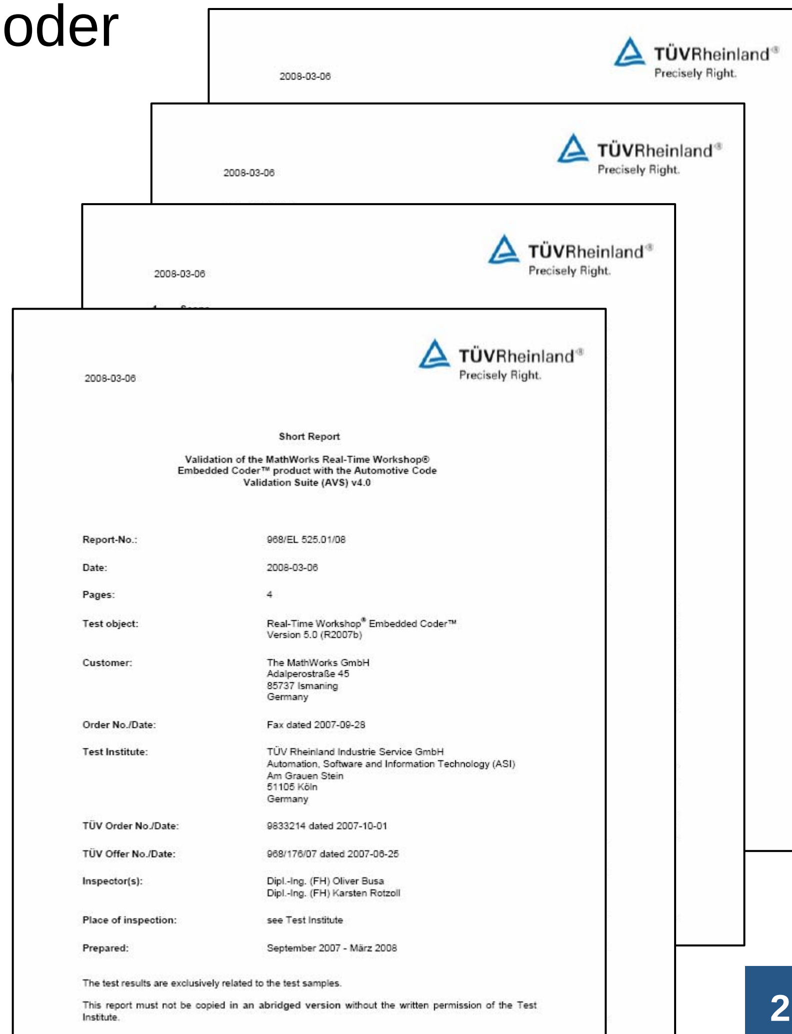
Model-Based Design for Safety-Critical Automotive Applications

Customer's "list of presents"

1. Leverage advantages of Model-Based Design and state-of-the-art code generation
   - ➢ **Tool-supported IEC 61508 compliant verification and validation**
2. Eased compliance demonstration
   - ➢ **IEC 61508 compliance documentation**
3. Validated / certified tools

Automotive Code Validation Suite (AVS)

- **Independent test suite** to validate Real-Time Workshop Embedded Coder and the compiler / linker tool chain
- Initiated by Ford, Conti, and TÜV Rheinland
- **Real-Time Workshop Embedded Coder** v4.2 (R14sp2) and v5.0 (R2007b) **sucessfully passed AVS**
- Validation indicates that Real-Time Workshop Embedded Coder and the target compiler* can be seen as **trusted processes**



2008-03-06

TÜVRheinland®
Precisely Right.

Short Report

Validation of the MathWorks Real-Time Workshop® Embedded Coder™ product with the Automotive Code Validation Suite (AVS) v4.0

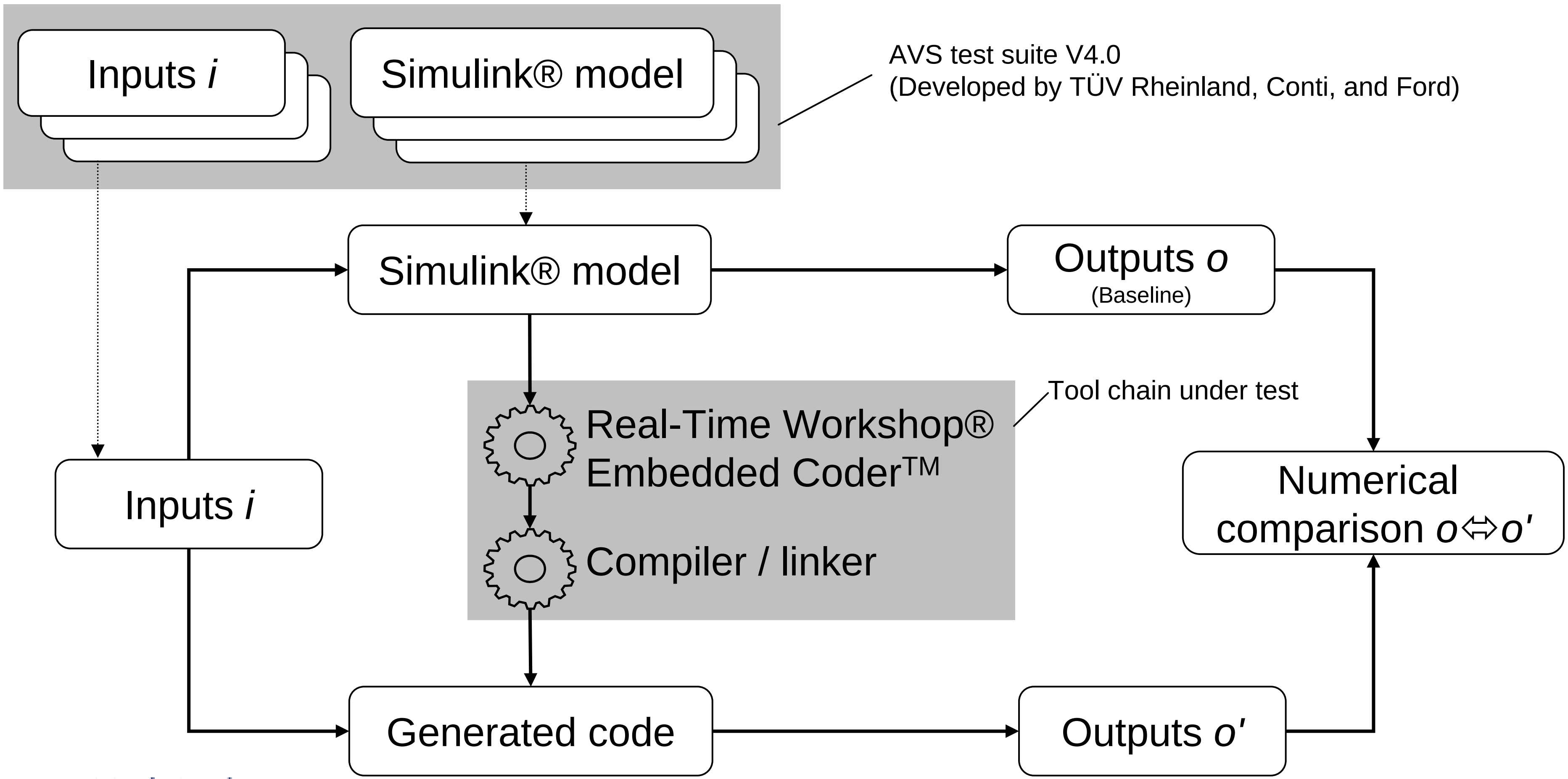
Report-No.:	968/EL 525.01/08
Date:	2008-03-06
Pages:	4
Test object:	Real-Time Workshop® Embedded Coder™ Version 5.0 (R2007b)
Customer:	The MathWorks GmbH Adalperostraße 45 85737 Ismaning Germany
Order No./Date:	Fax dated 2007-09-28
Test Institute:	TÜV Rheinland Industrie Service GmbH Automation, Software and Information Technology (ASI) Am Grauen Stein 51105 Köln Germany
TÜV Order No./Date:	9833214 dated 2007-10-01
TÜV Offer No./Date:	968/176/07 dated 2007-06-25
Inspector(s):	Dipl.-Ing. (FH) Oliver Busa Dipl.-Ing. (FH) Karsten Rotzoll
Place of inspection:	see Test Institute
Prepared:	September 2007 - März 2008

The test results are exclusively related to the test samples.

This report must not be copied in an abridged version without the written permission of the Test Institute.

* based on a fixed Real-Time Workshop Embedded Coder, Simulink, compiler, and linker configuration and limited number of test cases

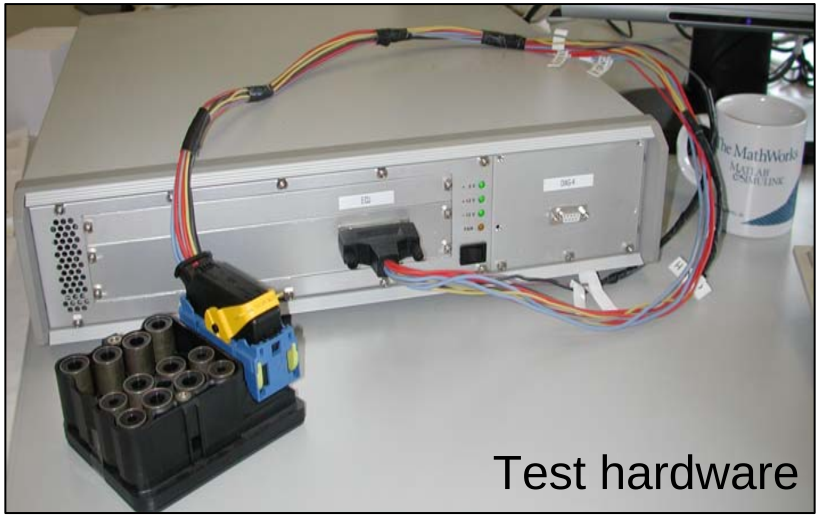
AVS for Real-Time Workshop® Embedded Coder™



Validation carried out by TÜV Rheinland Industrie Service, ASI

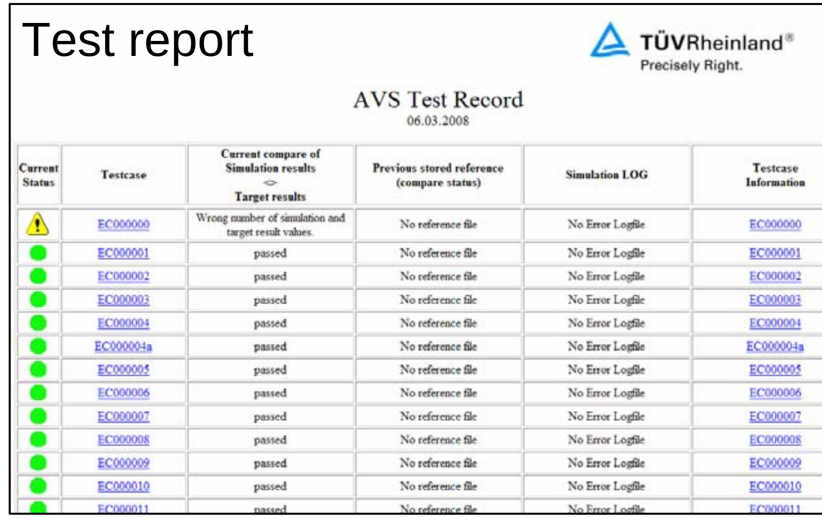
AVS for Real-Time Workshop® Embedded Coder™

Demo



Test hardware

Test report



AVS Test Record

06.03.2008

Current Status	Testcase	Current compare of Simulation results <> Target results	Previous stored reference (compare status)	Simulation LOG	Testcase Information
⚠	EC000000	Wrong number of simulation and target result values.	No reference file	No Error Logfile	EC000000
●	EC000001	passed	No reference file	No Error Logfile	EC000001
●	EC000002	passed	No reference file	No Error Logfile	EC000002
●	EC000003	passed	No reference file	No Error Logfile	EC000003
●	EC000004	passed	No reference file	No Error Logfile	EC000004
●	EC000004a	passed	No reference file	No Error Logfile	EC000004a
●	EC000005	passed	No reference file	No Error Logfile	EC000005
●	EC000006	passed	No reference file	No Error Logfile	EC000006
●	EC000007	passed	No reference file	No Error Logfile	EC000007
●	EC000008	passed	No reference file	No Error Logfile	EC000008
●	EC000009	passed	No reference file	No Error Logfile	EC000009
●	EC000010	passed	No reference file	No Error Logfile	EC000010
●	EC000011	passed	No reference file	No Error Logfile	EC000011

Benefits

- **Fully automated validation of the entire** code generator / compiler / linker **tool chain**
- **Easy re-validation** of project-specific tool versions / config sets

AVS for Real-Time Workshop® Embedded Coder™

- Press Release

The MathWorks

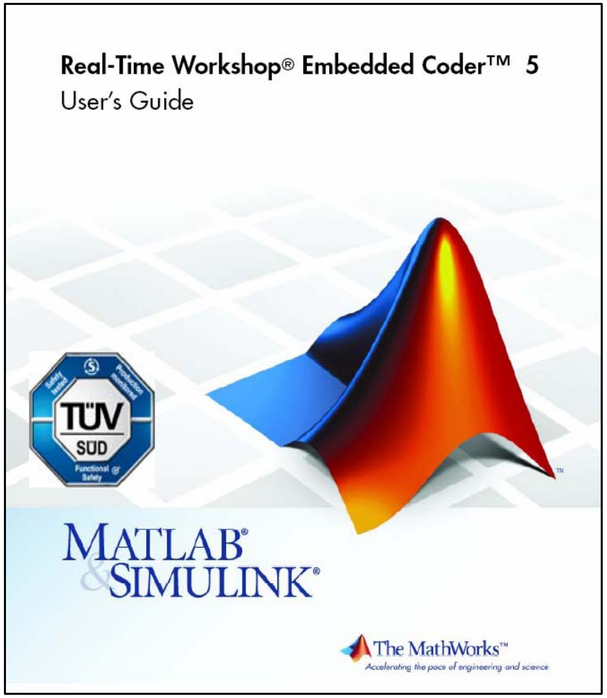
THE MATHWORKS REAL-TIME WORKSHOP EMBEDDED CODER VALIDATED BY TÜV RHEINLAND

TÜV Rheinland Successfully Applied the Automotive Code Validation Suite to Real-Time Workshop Embedded Coder

NATICK, Mass. – June 3, 2008 – The MathWorks today announced that its Real-Time Workshop Embedded Coder product successfully passed the Automotive Code Validation Suite (AVS). AVS provides an independent test suite for validating embedded code generators . According to the TÜV Rheinland report, "A successful validation using AVS shall be considered as proof of validation to a recognized procedure according to IEC 61508-3:1998, clause 7.4.4."

Certified Code Generation with Real-Time Workshop® Embedded Coder™

- Version 5.1 (R2008a) certified **fit for purpose to develop safety related software according to IEC 61508**



ZERTIFIKAT ◆ CERTIFICATE ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE
No. Z10 08 05 67052 001

Holder of Certificate: **The MathWorks, Inc.**
3 Apple Hill Drive
Natick MA 01760-2098
USA

Factory(ies): 67052

Certification Mark:

Product: **Software Tool for Safety Related Development**

Model(s): **Real-Time Workshop® Embedded Coder™**

Parameters: The code generator is fit for purpose to develop safety related software according to IEC 61508.

The report MN72051C is a mandatory part of this certificate.

Tested according to: IEC 61508-3:1998 (Fitness for Purpose)

The listed product was tested on a voluntary basis and complies with the relating standards or directives. The certification mark shown above can be affixed on the product. The certification mark must not be altered in any way. See also notes overleaf.

Test report no.: MN 72051 C

Peter G. Weiß

Date, 2008-05-29
Page 1 of 1

280329

A1 / 02.06

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

Certified Code Generation with Real-Time Workshop® Embedded Coder™

Benefits

- Satisfies IEC 61508-3 clause 7.4.4.3 / Table A.3 (5a)

> 7.4.4.3 To the extent required by the safety integrity level, the programming language selected shall:
>
> a) have a translator/compiler which has either a certificate of validation to a recognised national or international standard, or it shall be assessed to establish its fitness for purpose;

☑

- Eases certification of generated code
  - Large portion of the **test and review activities can be shifted** from the code level **to the model level**
- **Facilitates optimizations**

Model-Based Design for Safety-Critical Automotive Applications

<u>Customer's "list of presents"</u>

1. Leverage advantages of Model-Based Design and state-of-the-art code generation
   - **Tool-supported IEC 61508 compliant verification and validation**
2. Eased compliance demonstration
   - **IEC 61508 compliance documentation**
3. Validated / certified tools
   - **IEC 61508 certification and AVS validation of Real-Time Workshop Embedded Coder**

Key Takeaways

Model-Based Design with Simulink® and Real-Time Workshop® Embedded Coder™

- ☑ **Applied successfully to safety-critical applications in multiple domains**
- ☑ **Can satisfy the objectives of automotive safety standards (IEC 61508, ISO 26262)**
- ☑ **Facilitates highly automated IEC 61508 compliant verification and validation**
- ☑ **Provides certified state-of-the-art code generation**