

Model-Based Design for Safety-related Applications

Global Product Development Conference 2008 – Turin

Guido Sandmann

Automotive Marketing Manager, EMEA

The MathWorks GmbH

Guido.Sandmann@mathworks.de

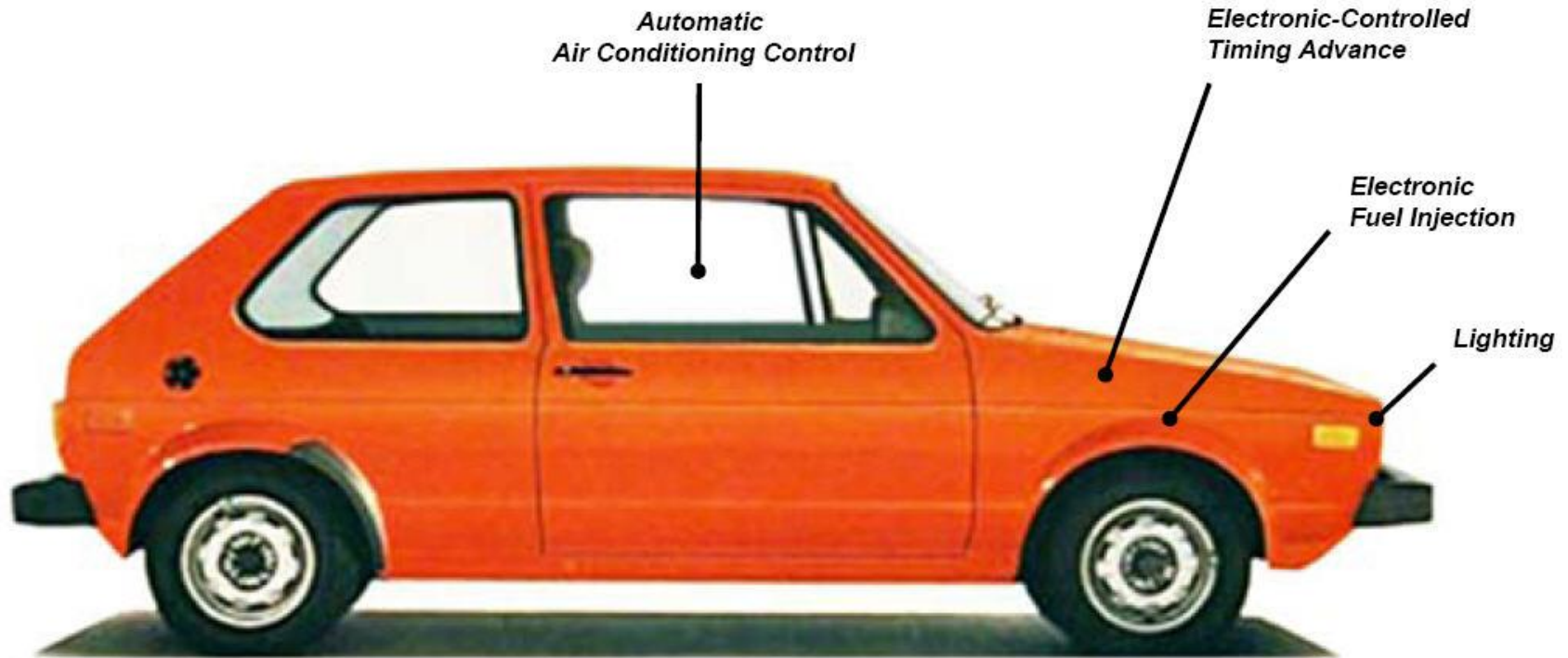
Agenda

- Introduction & Motivation
- IEC 61508 TÜV Certification of Real-Time Workshop Embedded Coder
 - IEC 61508 Workflow for Model-Based Design with MathWorks Products
- Automotive Code Validation Suite (AVS)
- Summary

Automotive Industry Trends & Challenges

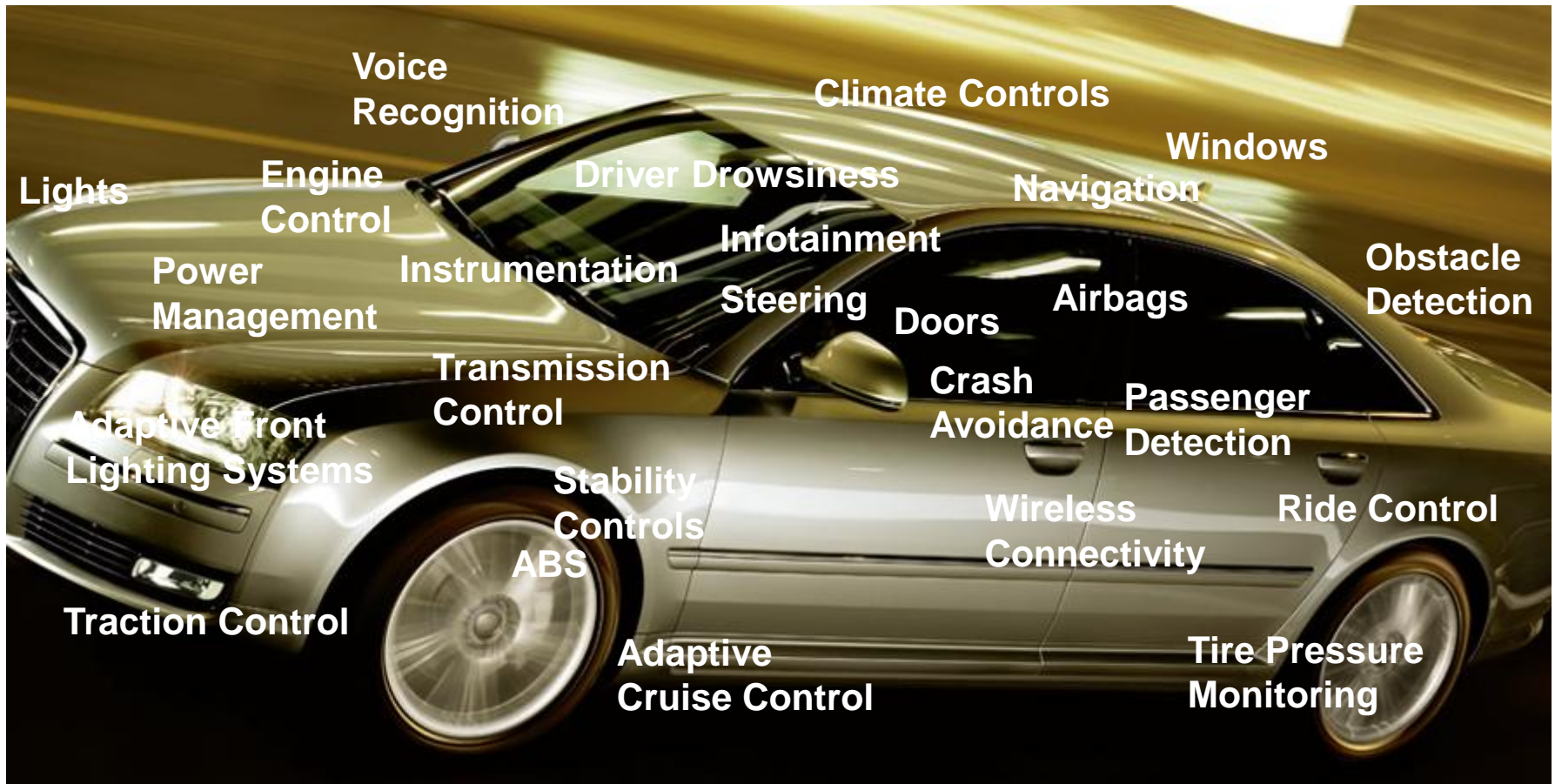


- 20 years ago:



Automotive Industry

Trends & Challenges today



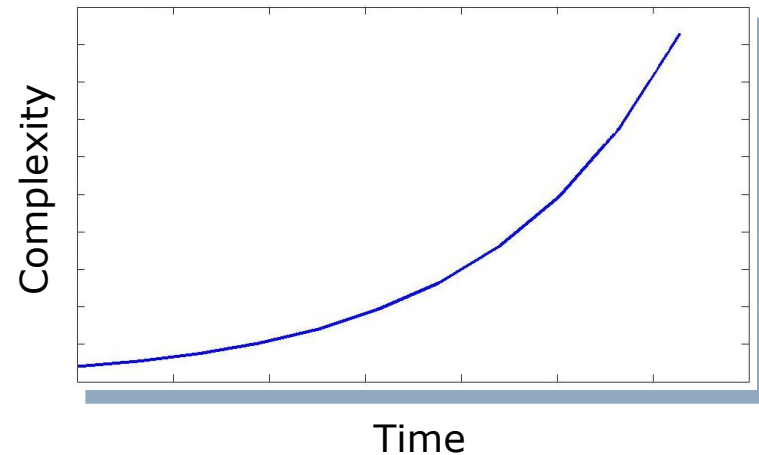
Automotive Industry

Trends & Challenges



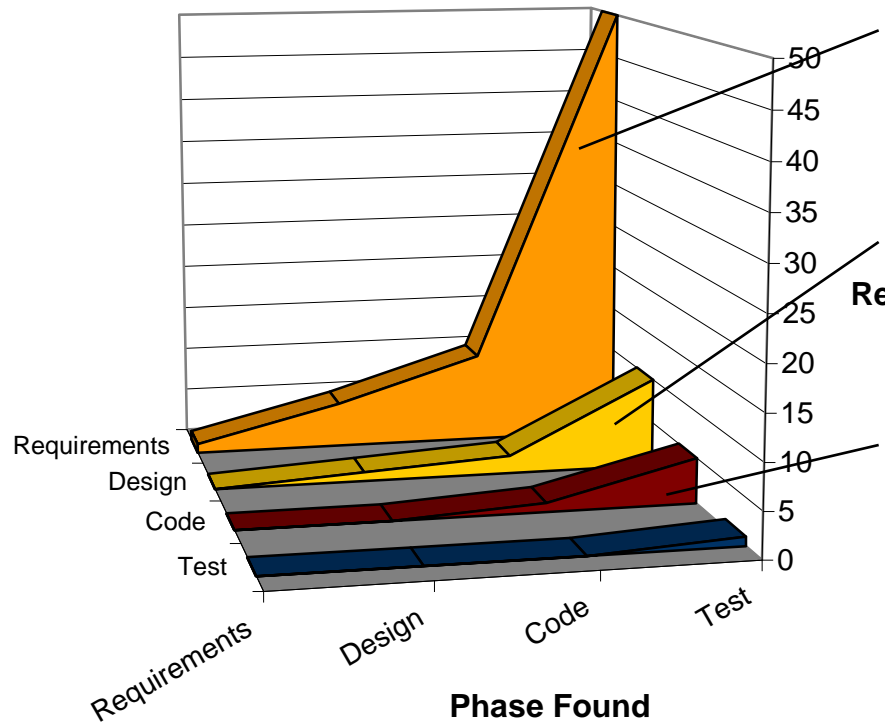
- Increasing Complexity
 - Increasing amount of Electronics leads to more Embedded Software

- Increasing Concerns with
 - Time to Market
 - Software Quality
 - Safety-related Applications



Embedded Software Fault Propagation

Relative Cost to Fix Defects per Phase Found



Engineers didn't get the problem (completely) !

Engineers got the problem but solution doesn't work!

The solution works but the implementation has faults!

■ Test ■ Code ■ Design ■ Requirements

Source: Return on Investment for Independent Verification & Validation, NASA, 2004.

Quality Issues of Electronic Systems and its Safety-related Consequences

BMW glitch locks Thai minister in

By Staff ZDNet Asia
Friday, May 16, 2003 10:13 AM

General Motors ACADIA Recall Feb 21, 2007

Recall Summary

The sensing and diagnostic module, which controls the function of front air bags, may not operated properly. As a result, the front air bags may fail to deploy in a frontal crash.

Consequence

In the event of crash, this condition could increase the risk of injury to occupants in the front seat.

...crawl out of his shattered windows of his ... sealed all exits.

...ault caused the problem, rather than a system ... mputer, as other reports have speculated.

...er, was on his way to address central bank ... -assigned BMW stalled, the Associated Press

...t down, the doors got locked and the windows

...all Sep 29, 2003

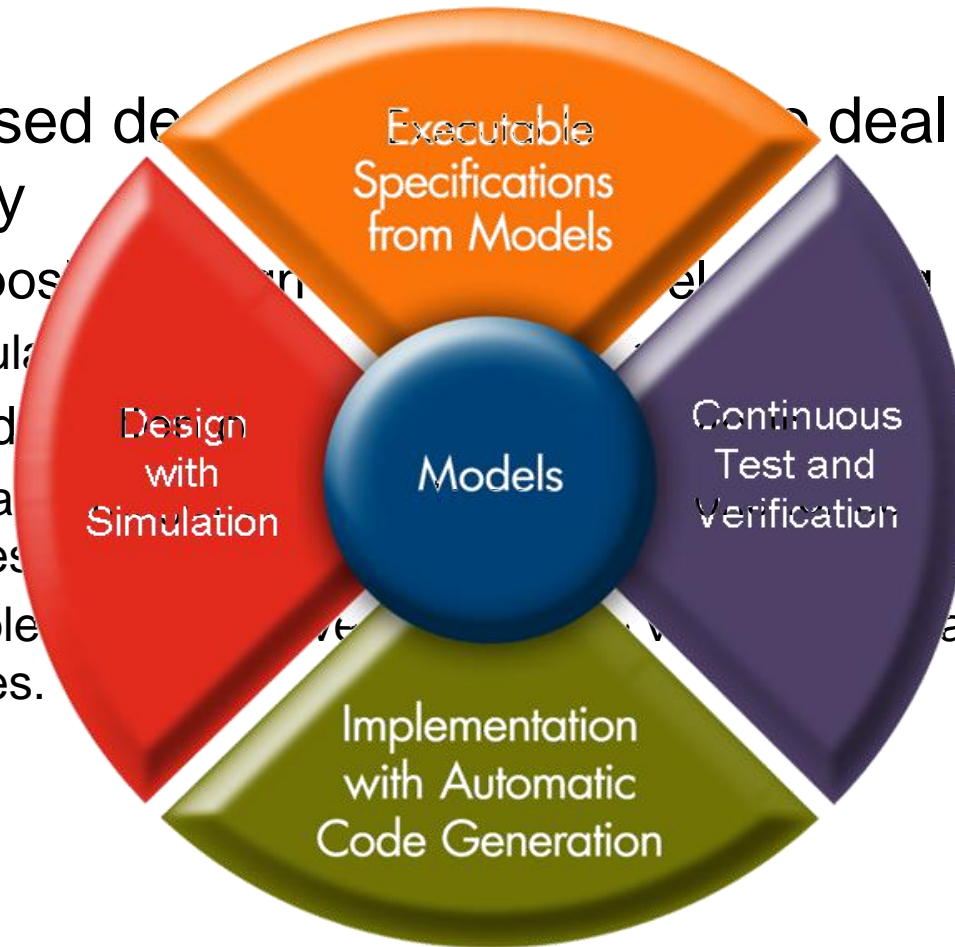
...nction of the passive ... em may become disabled.

Consequence

Should the PODS control unit malfunction, the air bag system in the vehicle will not work as designed and may not be able to properly protect occupants in a crash.

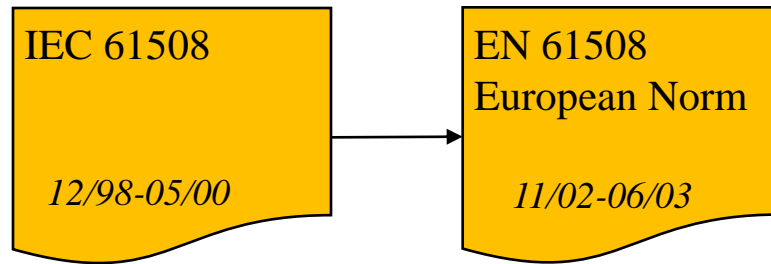
The Model-based Design Process

- Model-based design helps you deal with complexity
 - Decomposition into smaller models
 - Modular design
 - Formal design
 - Key analysis stages
 - Enable early development stages.

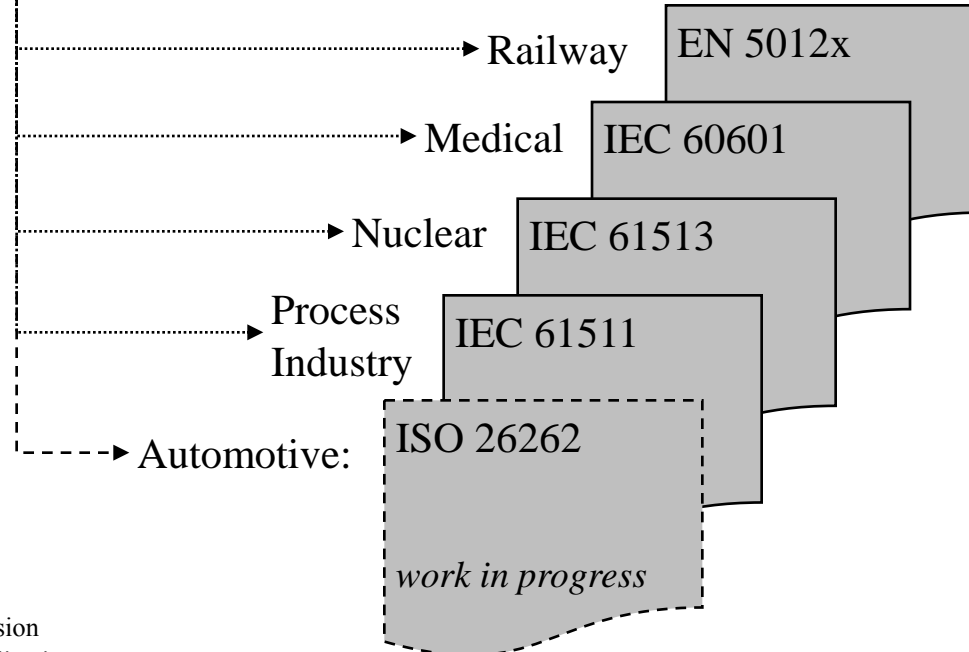


Safety Standards: IEC 61508 & the Derivates

Generic
Safety Standard



Sector / Product
Specific Derivates



IEC ... International Electrotechnical Commission
ISO ... International Organization for Standardization

IEC 61508 & Model-Based Design

IEC 61508 Functional safety of electrical/electronic/
programmable electronic safety-related systems*

* short: EE/PES

- 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 verification and validation) need to be mapped onto Model-Based Design processes and tools

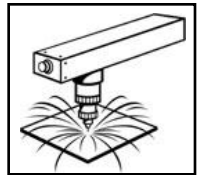
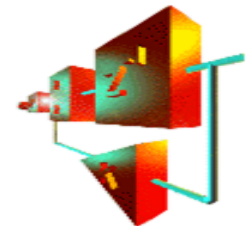


Table A.3 – Software design and development:
support tools and programming language (see 7.4.4)

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




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 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://tagteambdserver.mathworks.com/ttserverroot/Download/42572_IRSN_final.pdf

IEC 61508 and Certified Tools

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

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
...					
5a Certificated translator	C.4.3	R	HR	HR	HR
...					
Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.					

- IEC 61508-3 highly recommends the use of certified code generators for SIL 2 and above

IEC 61508 TÜV Certification of Real-Time Workshop Embedded Coder

- Real-Time Workshop Embedded Coder Version 5.1 (R2008a) was certified by TÜV SÜD for use in development processes which need to comply with IEC 61508.
- Note: Real-Time Workshop Embedded Coder was not developed using an IEC 61508 certified process.



MathWorks Announcement:

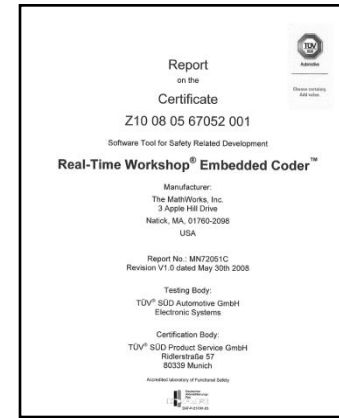
www.mathworks.com/company/pressroom/articles/article17790.html

TÜV SÜD certificate database:

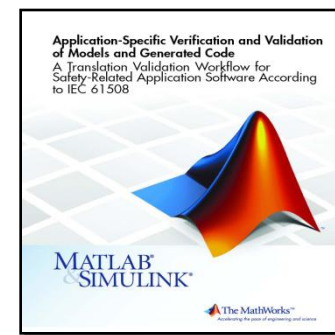
http://193.30.192.53:8080/CertDetail_eng.aspx?CertNo=Z10%2008%2005%2067052%20001&CertTyp=no

IEC 61508 TÜV Certification of Real-Time Workshop Embedded Coder

- Certificate based on:
 - Focused audit by TÜV of The MathWorks development and quality assurance processes for Real-Time Workshop Embedded Coder
 - Review by TÜV of MathWorks document describing example workflow for verification and validation of models and generated code



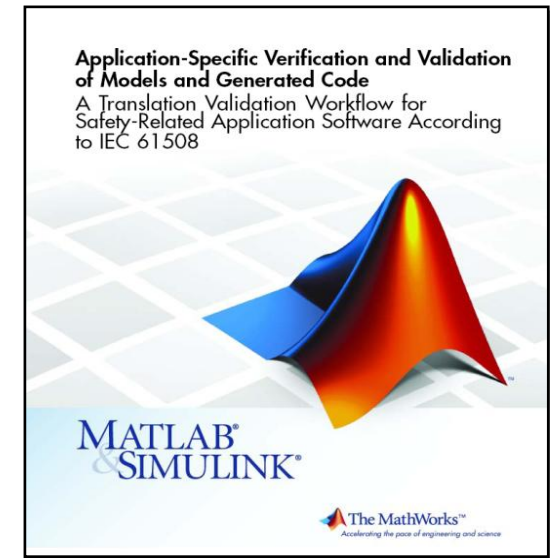
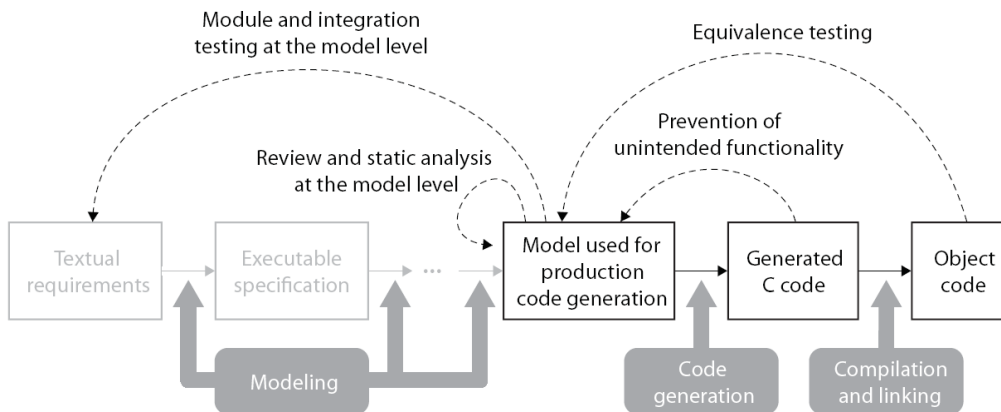
Certificate report



Workflow description

Workflow for Verification and Validation of Models and Generated Code

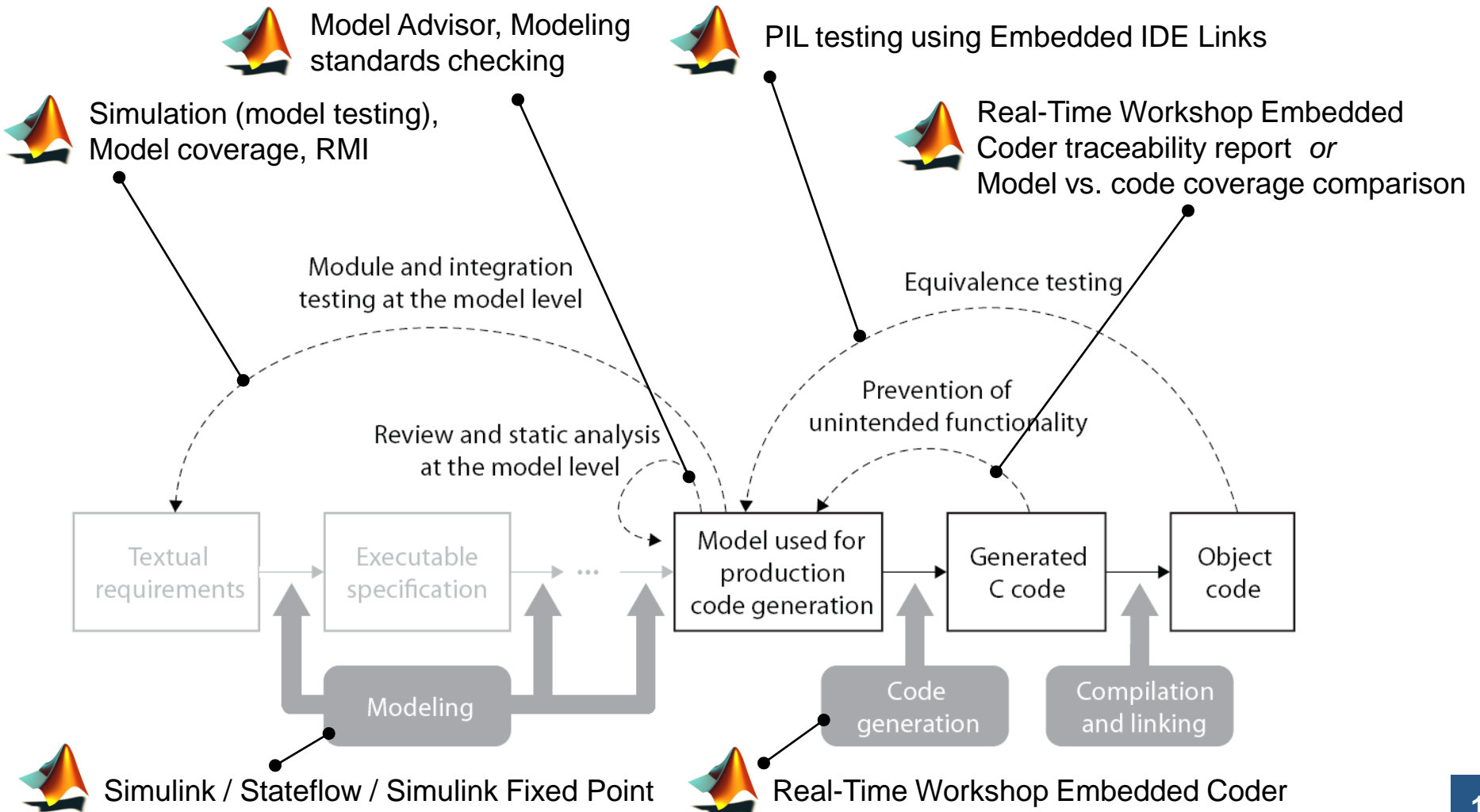
- Foundation of IEC 61508 certificate for Real-Time Workshop Embedded Coder



Workflow for Verification and Validation:

- Approved by TÜV SÜD
- Facilitates IEC 61508 compliant verification and validation
- Utilizes advantages of Model-Based Design
- Allows project-specific adaptations

Example IEC 61508 Workflow for Model-Based Design with MathWorks Products



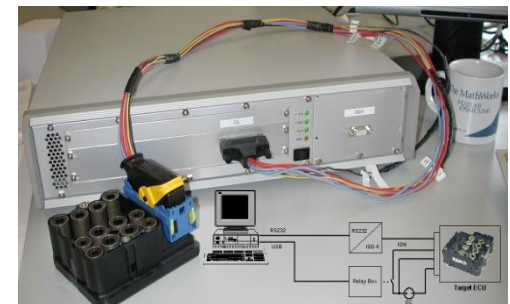
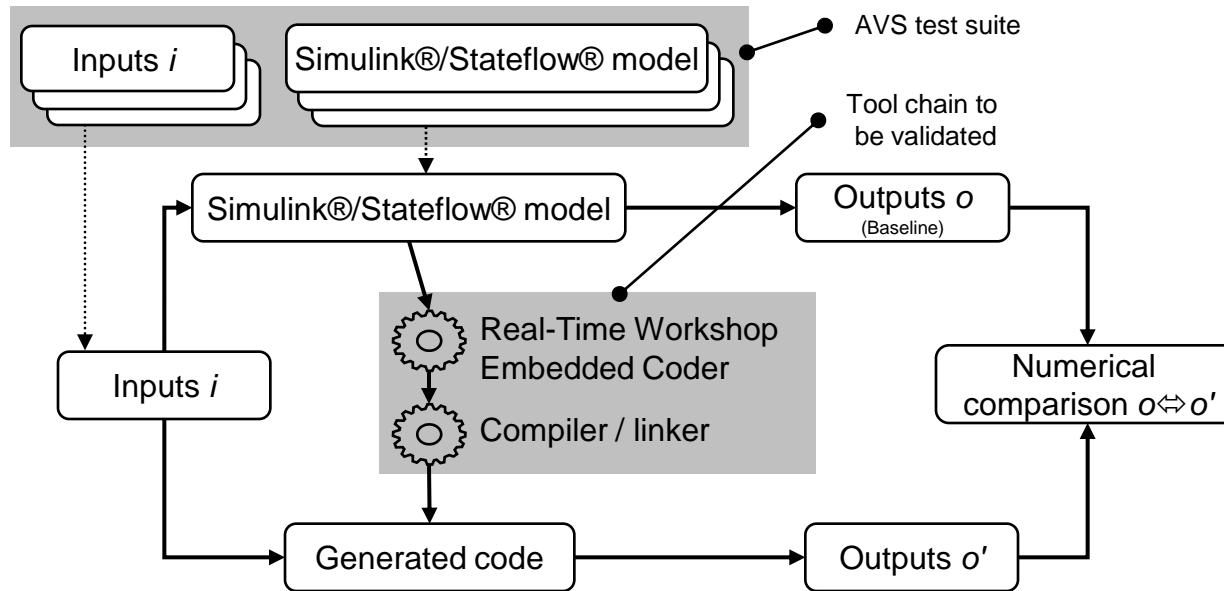
IEC 61508 TÜV Certification of Real-Time Workshop Embedded Coder

Benefits

- Offers V&V workflows options that can be tailored to your process
 - For example: prevention of unintended functionality can be verified by:
 - Comparing model and code structural coverage analysis
 - Moving reviews from code- to model- level
- Offers development options that can tailored to your process
 - For example: software optimizations are not explicitly prevented for coder and compiler tool chains
 - Real-Time Workshop Embedded Coder for source code generation
 - Third party compiler and linker tool chains for object code generation

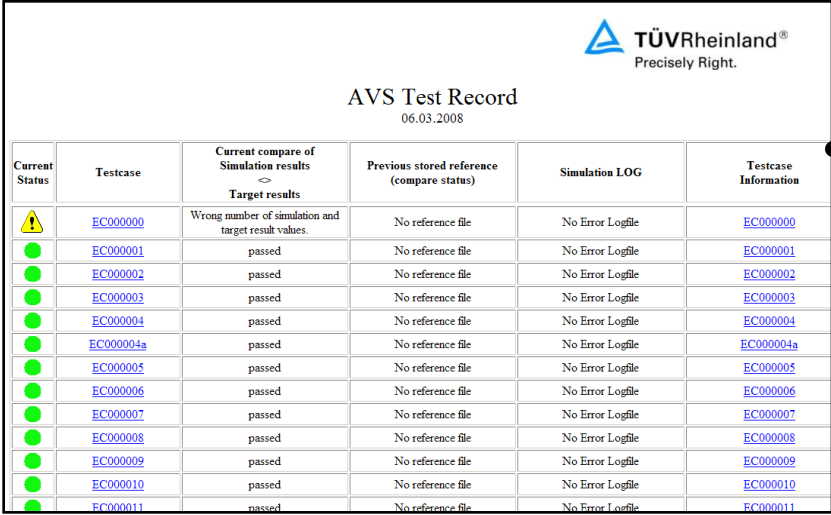
Automotive Code Validation Suite (AVS)

- Technology for end users to validate their Real-Time Workshop Embedded Coder / compiler / linker tool chain
- Independent test suite created by Ford, Continental, and TÜV Rheinland in 2002



AVS TÜV Validation of a Real-Time Workshop Embedded Coder / Compiler / Linker Tool Chain

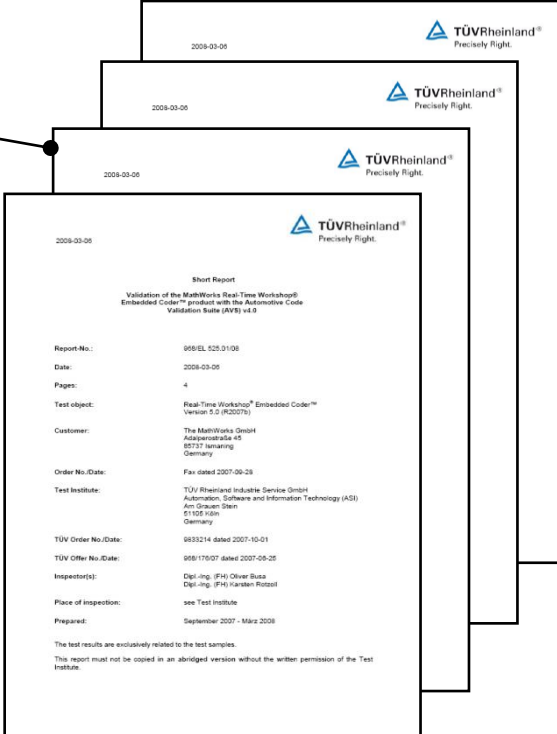
- TÜV Rheinland validated Real-Time Workshop Embedded Coder R2007b using a specific compiler / linker tool chain with AVS



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

Test report



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

Report No.: 9581EL 528.01/08
 Date: 2008-03-05
 Pages: 4
 Test object: Real-Time Workshop® Embedded Coder™ Version 5.0 (R2007b)
 Customer: The MathWorks GmbH, Ackermannstraße 65, 85737 Tirmming, Germany
 Order No./Date: Fax dated 2007-06-28
 Test Institute: TÜV Rheinland Industrie Service GmbH, Automation, Software and Information Technology (AS), Am Grauen Stein, 51105 Köln, Germany
 TÜV Order No./Date: 955214 dated 2007-10-01
 TÜV Offer No./Date: 958176/07 dated 2007-08-25
 Inspector(s): Dipl.-Ing. (FH) Oliver Busa, Dipl.-Ing. (FH) Jochen Rottst
 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.

AVS TÜV Validation of a Real-Time Workshop Embedded Coder / Compiler / Linker Tool Chain

- AVS technology can increase confidence in a specific code generation tool chain used for production applications

Benefits

- **Automated validation of the** code generator / compiler / linker tool chain
- **Enables reuse for re-validation** of project-specific tool versions / configuration sets
- **Recognized procedure** to validate a project-specific production code generation tool chain according to **IEC 61508-3** (clause 7.4.4)

Summary

① TÜV SÜD Certification

Activities:

- ❑ Use certified code generator as a means to increase IEC 61508 compliance
- ❑ Tailor and apply workflow for verification and validation of models and generated code for your project

Artifacts to submit for compliance demonstration:

- ❑ IEC 61508 certificate
- ❑ Completed compliance demonstration templates

② Automotive code Validation Suite (AVS)

- ❑ Use AVS technology to additionally validate your project-specific tool chain and configuration (*optional*)

- ❑ AVS test report

Key Takeaways

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

- ☑ **Can satisfy the objectives of automotive safety standards (IEC 61508, ISO 26262)**
- ☑ **Facilitates automated IEC 61508 compliant Verification & Validation**
- ☑ **Enables state-of-the-art production code generation reviewed by TÜV**
- ☑ **Eases compliance demonstration process**

The MathWorks



Change the world by

Accelerating the pace

of discovery, innovation, development, and learning

in engineering and science