Systems and Software Engineering Standards for the Automotive Domain

Joseph D'Ambrosio

Lab Group Manager

GM Research Laboratories

ISO 26262 Technical Expert

Outline

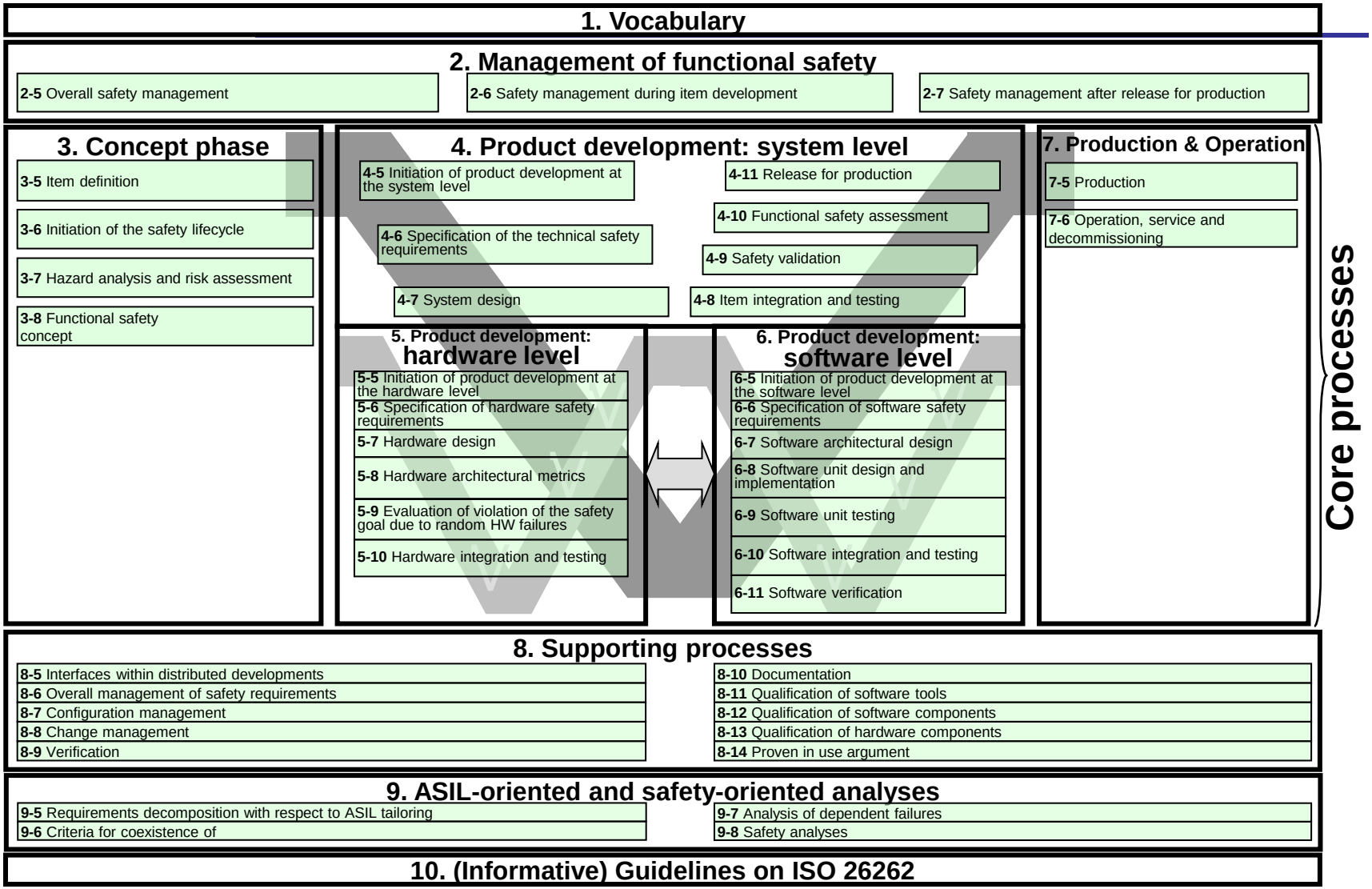
- ISO 26262
  - Certification & Initial Feedback
- MISRA C
- Mathworks Automotive Advisory Board Guidelines
- OMG Request for Information

What is ISO 26262?

- Adaptation of IEC 61508 to comply with the specific needs of E/E systems within road vehicles
  - Specifies a functional safety life-cycle for automotive products
  - Significant modifications vs. IEC 61508
- Applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic, and software components
- Is a standard, not a regulation
  - Broad industry participation in its development
  - Publication Date: Nov. 2011
- Key concept: Automotive Safety Integrity Level (ASIL)
  - Specify risk associated with a potential hazard
  - Dictate development requirements to achieve required integrity with respect to systematic and random hardware failures

ISO 26262
Road Vehicles
Functional Safety

ISO 26262 Overview



Source ISO/FDIS 26262

"Certification" Observations

- "Certification" is not required by standard, however …
  - Confirmation measures, including level of independence
- Two certification/confirmation perspectives
  - Integrated vehicle systems sold by automotive manufacturer
    - No current government regulations requiring the standard
    - Self confirmation: internal or external
  - Systems delivered by suppliers to manufacturer
    - Manufacturer must obtain confirmation of supplier systems
      - Approaches: manufacture internal, external; supplier internal, external
    - ISO 26262 distributed interface agreement applies
- Certification of products vs. process

ISO 26262 Certification Support

- Large ecosystem developing around ISO 26262
  - Certification, consulting, tools …

Volpe ISO 26262 Report: Industry's Views—Pro's

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation
Research and Innovative Technology Administration

- ISO 26262 is well regarded by industry and is seen as necessary.
- Many companies have at least tried it on pilot projects.
- GM has used it to ensure Volt's battery functional safety.
- Industry recognizes it is valuable to have safety standard to address the growing complexity of Cyber-Physical Systems.
- No discrepancy with mature product development process, and it is easy to implement.
- Aligns well with the model-based development process.

Source : Qi Van Eikema Hommes, "Assessment of the ISO 26262 Draft Road Vehicles - Functional Safety", http://www.sae.org/events/gim/presentations/2012/qi_volpe.pdf

Volpe ISO 26262 Report: Industry's Views--Cons

John A. Volpe National Transportation Systems Center
U.S. Department of Transportation
Research and Innovative Technology Administration

- Amount of documentation efforts
- Not convinced that the software development methods are sufficient to guarantee safety
- Since the standard is about the entire product life cycle, the effect of the standard will take some time to show.
- The concept phase is easy to implement, but there is difficulty to integrate a pilot project into the rest of the system that was not developed based on the standard.
- ASIL classification harmonization
- "Proven in use" argument is not useful
  - Takes too long to collect sufficient data
  - The definition in the standard makes it a step that will never be visited
- Qualification of software tools
  - The large number of software tools used in development
  - Comment: software tools are software. How will one quantify the probability of software making mistakes?

Source : Qi Van Eikema Hommes, "Assessment of the ISO 26262 Draft Road Vehicles - Functional Safety", http://www.sae.org/events/gim/presentations/2012/qi_volpe.pdf

Volpe Report: Summary of Recommendations

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation
Research and Innovative Technolo
Administration

1. Consider only using severity for ASIL assessment
2. Government may want to consider playing a role in ASIL standardization
   - However, the ASIL assessment must depend on the context and the design configuration of the system.
3. The standard may want to add a section to emphasize hazard elimination before detection and control
4. Research activities may want to investigate the effectiveness of system theory based hazard causal analysis in automotive complex cyber-physical systems
   - E.g. STAMP model and STPA.
5. Fundamental research is needed for the safety of complex software-intensive systems today, including those in the current automobiles:
   - The effect of complexity on safety is not well quantified
   - The effects of software engineering best practices on safety may be insufficient to ensure safety. New and different approaches may need to be developed.
6. Government may want to play a role in certifying software tools used for the development of safety critical systems
7. Government may want to consider regulating the safety of E/E systems after the vehicle is sold.

Source : Qi Van Eikema Hommes, “Assessment of the ISO 26262 Draft Road Vehicles - Functional Safety”, http://www.sae.org/events/gim/presentations/2012/qi_volpe.pdf

Outline

- ISO 26262
  - Certification & Initial Feedback
- MISRA C
- Mathworks Automotive Advisory Board Guidelines
- OMG Request for Information

The Motor Industry Software Reliability Association

- MISRA C:2004 (MISRA C2)
  - "Guidelines for the use of the C language in critical systems"
  - Restricted subset of C
- MISRA AC GMG / SLSF
  - Modeling design and style guidelines

MISRA C EXAMPLE

•**Rule 34 (required)**
•The operands of a logical && or || shall be primary expressions

Invalid

```
if ( x= = 0 && ishigh )
```

Valid

```
if ( ( x == 0 ) && ishigh )
```

Primary expressions are constants, a single identifier such as ishigh, or a parenthesized expression. Parentheses are important for readability and ensuring that the behavior is what the programmer intends.

Source: Electronic Design http://electronicdesign.com/article/embedded-software/misra-c-safer-is-better2824
http://www.misra.org.uk/misra-c/Activities/MISRAC/tabid/160/Default.aspx

Checking MISRA C:2004

- Static Code Analysis

Outline

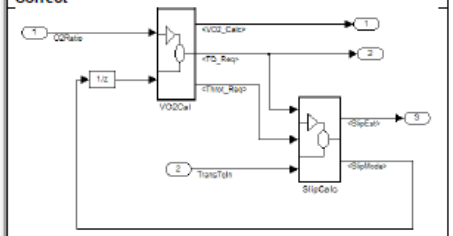
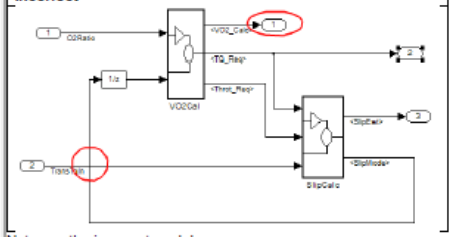
- ISO 26262
  - Certification & Initial Feedback
- MISRA C
- Mathworks Automotive Advisory Board Guidelines
- OMG Request for Information

Mathworks Modeling Guidelines

- Mathworks tools broadly used in automotive industry
- MAAB – Mathworks Automotive Association Board
  - Coordinate tool request and usage
- “Control Algorithm Modeling Guidelines Using Matlab, Simulink & Stateflow”
- Mathworks verification tools can check compliance

MathWorks

6.1.3. db_0042: Port block in Simulink models

ID: Title	**db_0042: Port block in Simulink models**
Priority	strongly recommended
Scope	MAAB
MATLAB Version	All
Prerequisites	
Description	In a Simulink model, the ports comply with the following rules: • Inports should be placed on the left side of the diagram, but they can be moved in to prevent signal crossings. • Outports should be placed on the right side, but they can be moved in to prevent signal crossings. • Duplicate Inports can be used at the subsystem level if required but should be avoided if possible. ○ Duplicate Inports cannot be used at the root level. **Correct**  **Incorrect**  Notes on the incorrect model • Inport 2 should be moved in so it does not cross the feed back loop lines. • Outport 1 should be moved to the right hand side of the diagram.
Rationale	☑ Readability ☐ Verification and Validation ☐ Workflow ☐ Code Generation ☐ Simulation
Last Change	V2.0

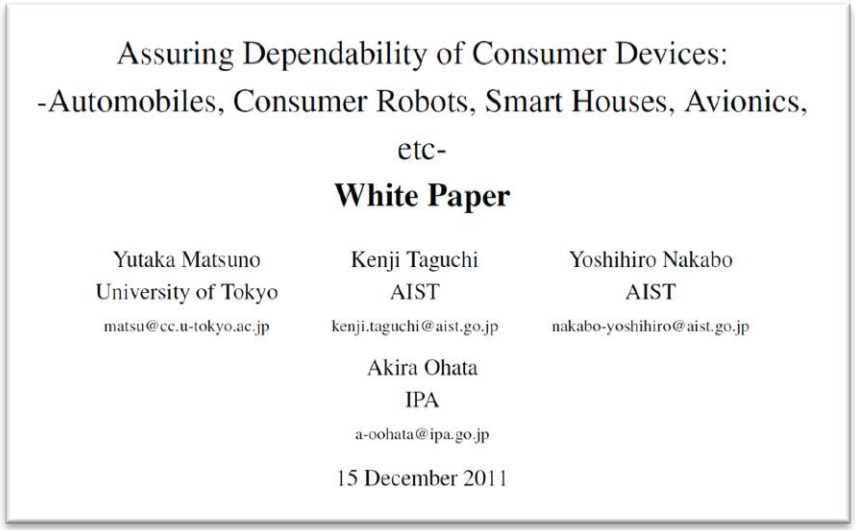
Source: http://www.mathworks.com/automotive/standards/maab.html

Outline

- ISO 26262
  - Certification & Initial Feedback
- MISRA C
- Mathworks Automotive Advisory Board Guidelines
- OMG Request for Information

OMG Dependability Request for Information

- OMG request for information for dependability standard
  - Due 5/20/2012
- References ISO 26262
- Key elements to address
  - Rapid development
    - Motivated by “unknown factors”
  - Model-based development
    - Controls & SW
  - Assurance cases
- Planning on 18 month development cycle



Assuring Dependability of Consumer Devices:
-Automobiles, Consumer Robots, Smart Houses, Avionics, etc-

White Paper

Yutaka Matsuno
University of Tokyo
matsu@cc.u-tokyo.ac.jp

Kenji Taguchi
AIST
kenji.taguchi@aist.go.jp

Yoshihiro Nakabo
AIST
nakabo-yoshihiro@aist.go.jp

Akira Ohata
IPA
a-oohata@ipa.go.jp

15 December 2011

Object Management Group

OBJECT MANAGEMENT GROUP

SysML

UML

MOF Meta-Object Facility

BPMN

DDS

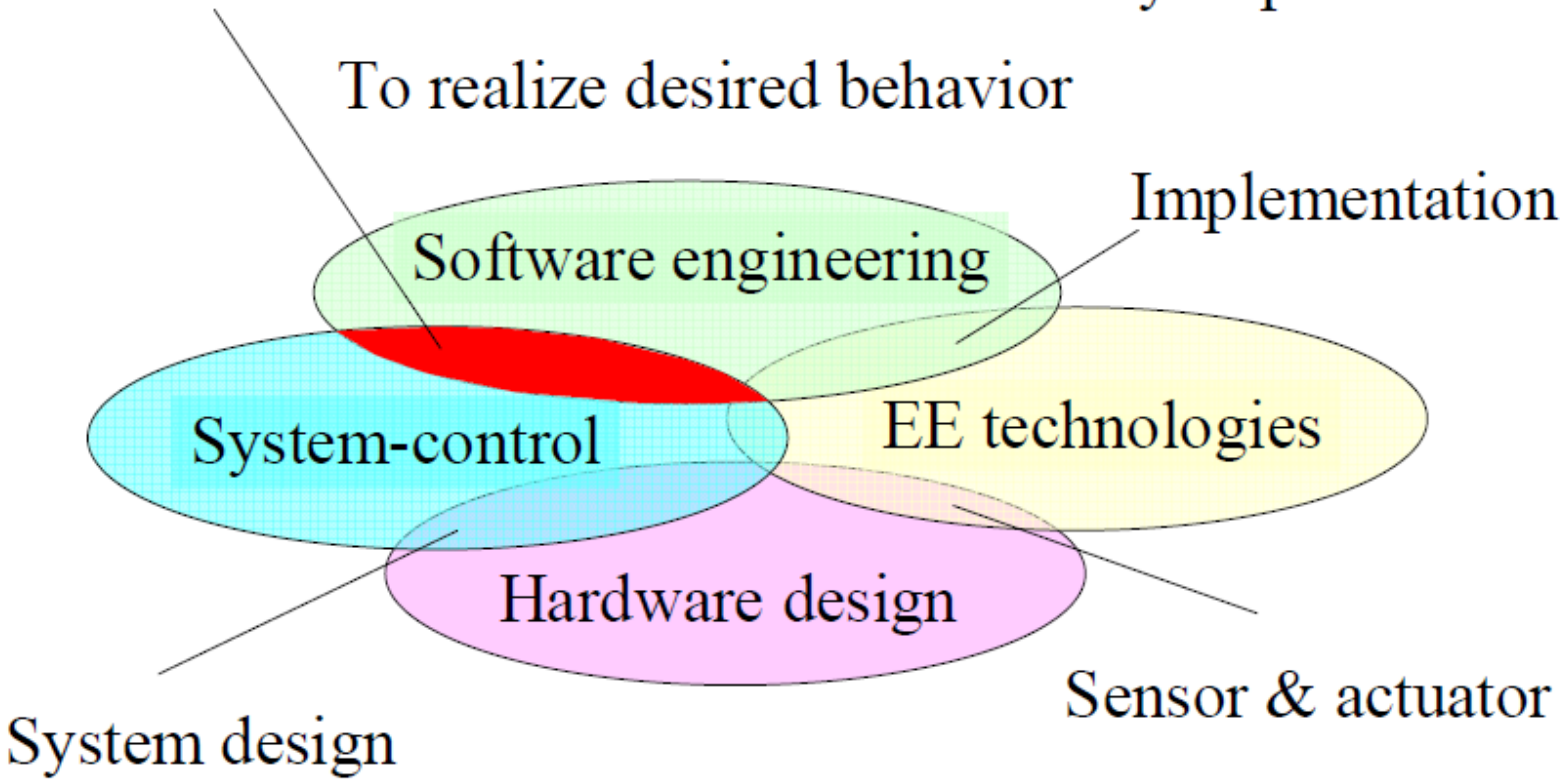
CORBA

UML MARTE

CWM

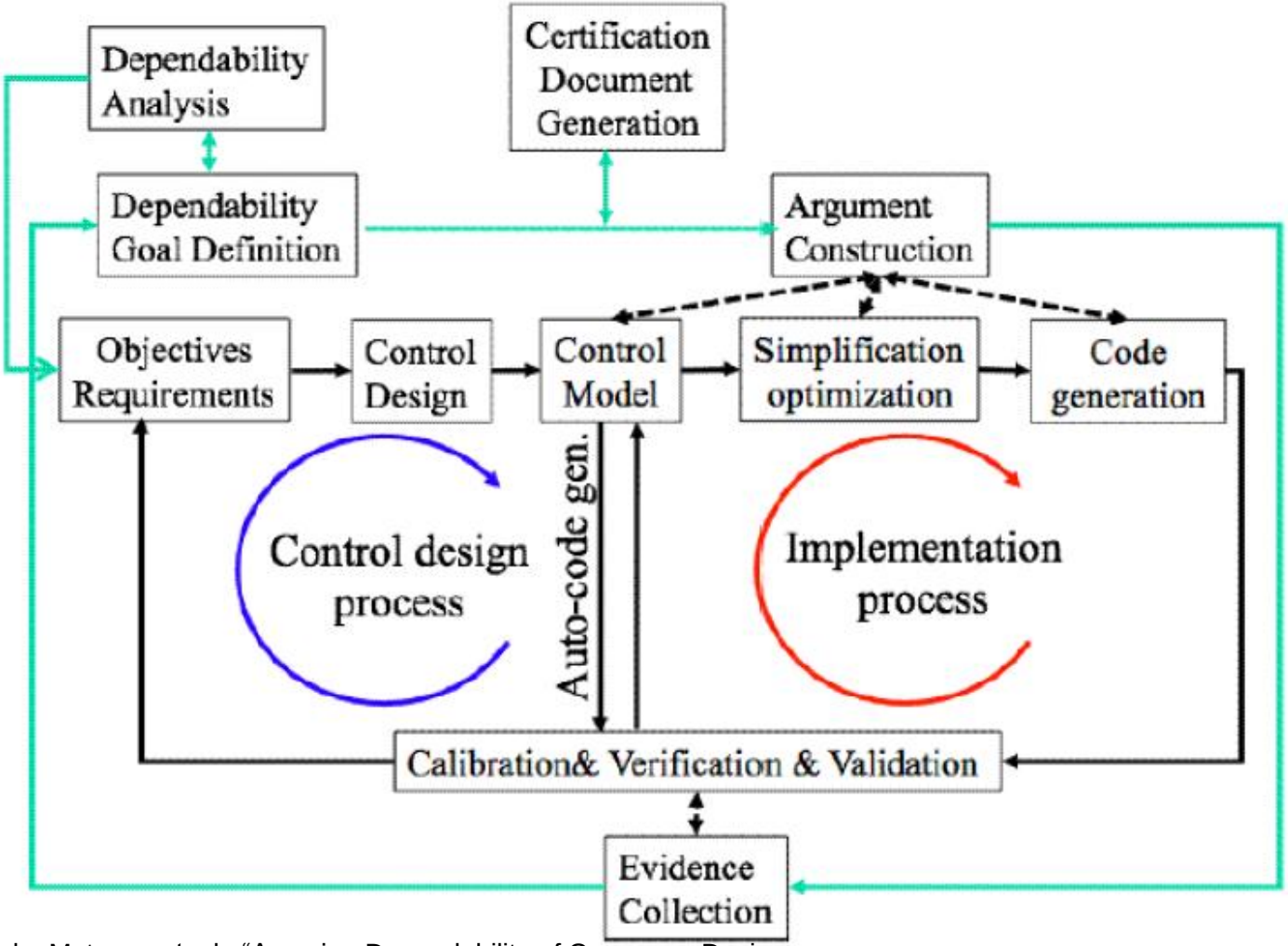
Integration of Software and System-Control Approaches

This collaboration has become extremely important.



Source: Yutaka Matsuno et. al., “Assuring Dependability of Consumer Devices: -Automobiles, Consumer Robots, Smart Houses, Avionics, etc-” White Paper, 12/15/2011.

Proposed Workflow



Source: Yutaka Matsuno et. al., “Assuring Dependability of Consumer Devices: -Automobiles, Consumer Robots, Smart Houses, Avionics, etc-” White Paper, 12/15/2011.

Summary

- Broadly applied automotive standards
  - ISO 26262, MISRA C coding guidelines

ISO 26262
Road Vehicles
Functional Safety

- Emerging automotive model-based standards & guidelines
  - MISRA GMG / SLSF, MAAB
  - OMG request for infomation