“Trends in CARS”
CARS Workshop (Valencia)

First Workshop on Critical Automotive applications: Robustness & Safety

VALENCIA, Spain
27 April 2010

Organised by: [Logos]
Sponsored by: [Logos]
In partnership with: [Logos]
Keynote on the ISO DIS 26262 Standard

ISO 26262 is applied to E/E safety-related systems installed in series production passenger cars, including Systems, Hardware & Software components

“Still on track for standard in mid-2011”

“The world will change after that”

“Considered published State of the Art”

Will be important for liability determination
What is included in 26262?

- 26262 is about hazards occurring caused by **malfunctioning** behavior of safety-related systems

- **Nominal performance** is excluded from 26262

- **Basic Software** is *not* excluded from 26262 – “unfortunately”
“Certification intentionally never mentioned in 26262”

Caution: we are not talking about safety **qualification** here, that is always required by 26262 (see Part 8)!

This statement created a discussion about the meaning and purpose of *certification*

“Useful for marketing purposes”

“A component could be certified but have inferior functionality”
Safety Element out of Context

- Safety Element Out of Context
- “The idea originated in FlexRay”
- “All AUTOSAR is a SEooC!”
“Is 26262 difficult to interpret?”

“No – it simply allows many solutions”

“61508 is prescriptive, 26262 is goal-oriented”

Example: no format prescribed for safety case

“A common language for interaction, not to provide solutions”

Technology is fast moving

This is where 26262 and AUTOSAR “meet” in their approaches: cooperate on standards, compete on solutions
There was heavy participation from the ATESTT2 project, co-funded by the EU.

The goal of ATESTT2 is to provide a method with the associated automotive architecture description language (EAST-ADL2) able to model EE Architecture in compliance with the ISO26262 functional safety standard.
The method developed in ATTEST2 includes an approach for **automatic allocation of Automotive Safety Integrity Levels** (ASILs), and consequently the associated safety requirements, to subsystems / components belonging to a complex EE safety related architecture

- “ASIL Algebra”

The ASIL automatic allocation approach is assisted by an automated safety analysis tool “Hip Hops”

- The process rationalizes complex risk allocation and leads to optimal/economic allocation of ASILs
- Deepens our understanding of ASIL decomposition and helps us understand how far tool support can be taken
Analysis of AUTOSAR Systems

“A Roadmap for Enabling Analysis of AUTOSAR Systems”

“The central issue in AUTOSAR: parallel development by multiple organisations”

“How to enable distributed responsibility”

ATTEST2 proposal: “contract based design”

A model based approach for specification
One Language for Spec and Architecture

- How to enable contract-based design?
- Introduce general specification concepts such as “constraint”
- Then construct domain models for types of constraints
  - Timing constraints
  - Safety constraints
- Give distributed developers a single language for both contract and development
Want to be really frightened?

http://www.autosec.org/publications.html
CarShark

- **Doomsday scenario**
- Transformed the instrument panel into a clock
- Countdown from 60 seconds to zero
- Final seconds: honking horn
- At zero: turn off the engine and lock the doors

“The computer systems used to control modern cars are very vulnerable to attack”
What are automotive control platforms currently missing?
- No support for trust/security in AUTOSAR
- Incorporate trust- and –security aware mechanisms into AUTOSAR Basic Software
  - Based on time and space partitioning – *but adoption is slow because increases costs*
“Plug & Safe” Systems?

- Fraunhofer IESE: *Conditional Safety Certificates in Open Systems*
  - Dynamic integration of devices and components into running systems
- The conditional safety certificate (ConSerts) is associated with the component
  - Dynamically checked at runtime to see whether it is conformant with its specification
- Move portions of the safety assurance process into runtime (!)
ConSerts – dynamic safety assurance

-Reactions:

-“There is enough trouble with static assurance”
-“The future is dynamic – this is the future”
AMBER Project – roadmap for 26262-directed research

- Emphasized four main points that could be pursued based upon the ISO 26262 standard:

  1. Methods allowing **extrapolation of measurements to prediction of system behavior**, in spite of differences between the system/environment where measurements were taken and the system/environment in operation

  2. Improving the **cost-effectiveness of methods for safety assessment** by developing techniques and tools that can be easily integrated into existing development methods and tool chains [**ASIL algebra, SEooC!**]

  3. **Argumentation processes** allowing the formulation of complex arguments, combining evidence from measurements with human judgment

  4. **Reference faultloads** (sets of faults) that are validated and representative of faults arising in the automotive domain, and practical injection tools to perform the evaluation
“After 30 years of advances in software engineering, why is the automotive industry [and also aerospace, others] still using plain-text requirements, still using typeless languages like C, etc.”?

Discussion: “Extremely cost-sensitive industry, progress is slow – but sure”