Automotive SPIN

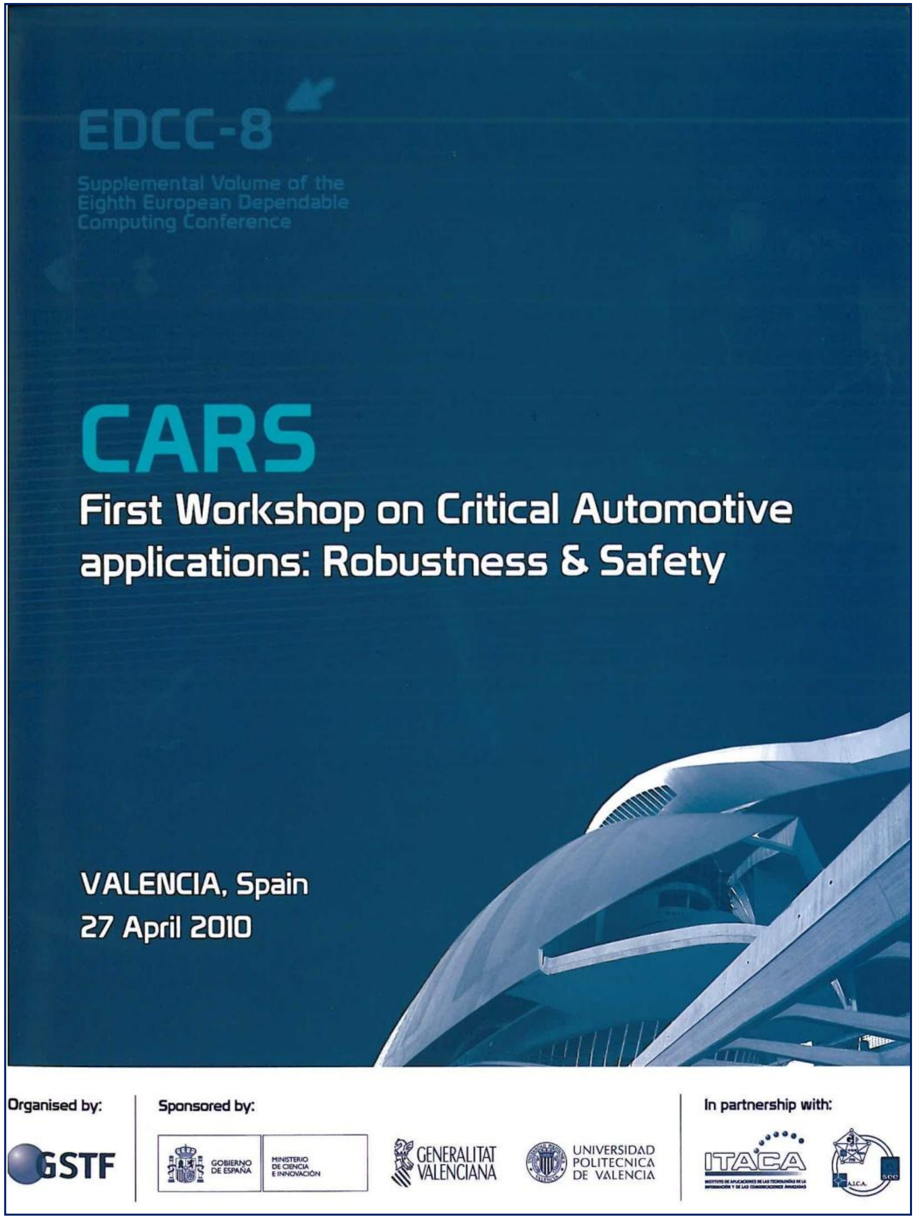
Pisa – 21 May 2010

“Trends in CARS”

John Favaro
Intecs SpA

Fulvio Tagliabò
CRF

CARS Workshop (Valencia)



EDCC-8

Supplemental Volume of the Eighth European Dependable Computing Conference

CARS

First Workshop on Critical Automotive applications: Robustness & Safety

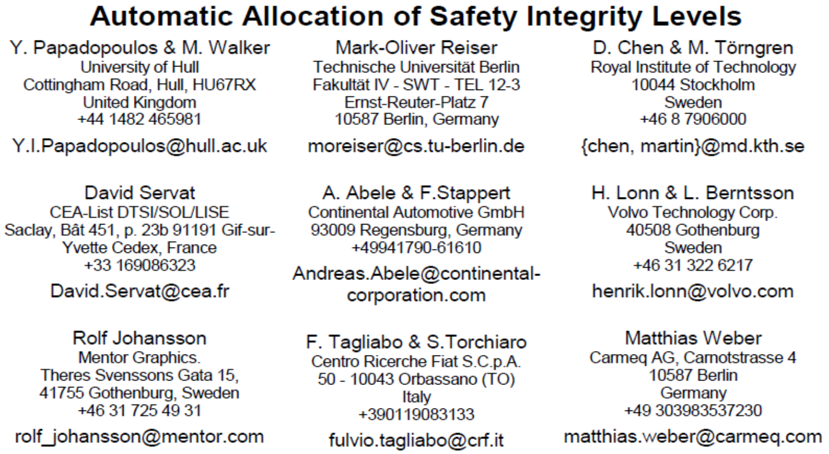
VALENCIA, Spain

27 April 2010

Organised by: GSTF

Sponsored by: GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA E INNOVACIÓN · GENERALITAT VALENCIANA · UNIVERSIDAD POLITECNICA DE VALENCIA

In partnership with: ITACA · A.I.CA



Automatic Allocation of Safety Integrity Levels

Y. Papadopoulos & M. Walker
University of Hull
Cottingham Road, Hull, HU67RX
United Kingdom
+44 1482 465981
Y.I.Papadopoulos@hull.ac.uk

Mark-Oliver Reiser
Technische Universität Berlin
Fakultät IV - SWT - TEL 12-3
Ernst-Reuter-Platz 7
10587 Berlin, Germany
moreiser@cs.tu-berlin.de

D. Chen & M. Törngren
Royal Institute of Technology
10044 Stockholm
Sweden
+46 8 7906000
{chen, martin}@md.kth.se

David Servat
CEA-List DTSI/SOL/LISE
Saclay, Bât 451, p. 23b 91191 Gif-sur-Yvette Cedex, France
+33 169086323
David.Servat@cea.fr

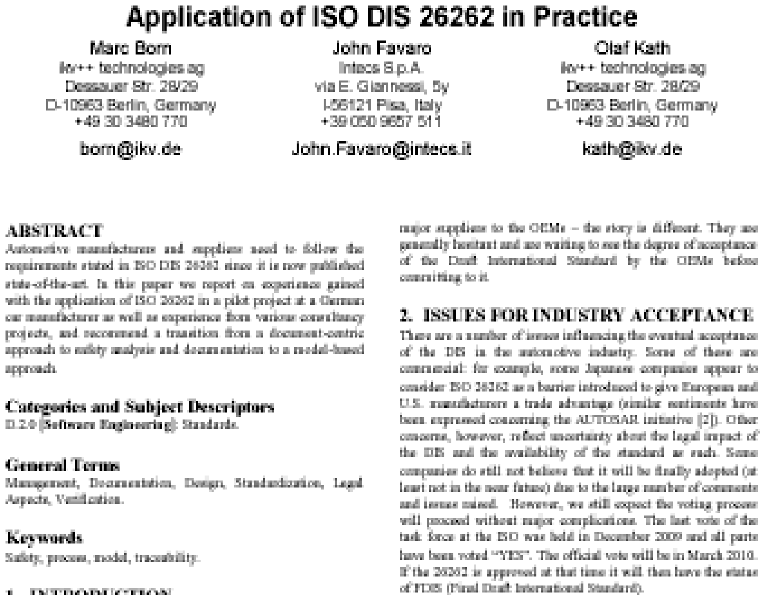
A. Abele & F.Stappert
Continental Automotive GmbH
93009 Regensburg, Germany
+49941790-61610
Andreas.Abele@continental-corporation.com

H. Lonn & L. Berntsson
Volvo Technology Corp.
40508 Gothenburg
Sweden
+46 31 322 6217
henrik.lonn@volvo.com

Rolf Johansson
Mentor Graphics.
Theres Svenssons Gata 15,
41755 Gothenburg, Sweden
+46 31 725 49 31
rolf_johansson@mentor.com

F. Tagliabo & S.Torchiaro
Centro Ricerche Fiat S.C.p.A.
50 - 10043 Orbassano (TO)
Italy
+390119083133
fulvio.tagliabo@crf.it

Matthias Weber
Carmeq AG, Carnotstrasse 4
10587 Berlin
Germany
+49 303983537230
matthias.weber@carmeq.com



Application of ISO DIS 26262 in Practice

Marc Born
ikv++ technologies ag
Dessauer Str. 28/29
D-10963 Berlin, Germany
+49 30 3480 770
born@ikv.de

John Favaro
Intecs S.p.A.
via E. Giannessi, 5y
I-56121 Pisa, Italy
+39 050 9657 511
John.Favaro@intecs.it

Olaf Kath
ikv++ technologies ag
Dessauer Str. 28/29
D-10963 Berlin, Germany
+49 30 3480 770
kath@ikv.de

ABSTRACT

Automotive manufacturers and suppliers need to follow the requirements stated in ISO DIS 26262 since it is now published state-of-the-art. In this paper we report on experience gained with the application of ISO 26262 in a pilot project at a German car manufacturer as well as experience from various consultancy projects, and recommend a transition from a document-centric approach to safety analysis and documentation to a model-based approach.

Categories and Subject Descriptors

D.2.0 [**Software Engineering**]: Standards.

General Terms

Management, Documentation, Design, Standardization, Legal Aspects, Verification.

Keywords

Safety, process, model, traceability.

major suppliers to the OEMs – the story is different. They are generally hesitant and are waiting to see the degree of acceptance of the Draft International Standard by the OEMs before committing to it.

2. ISSUES FOR INDUSTRY ACCEPTANCE

There are a number of issues influencing the eventual acceptance of the DIS in the automotive industry. Some of these are commercial: for example, some Japanese companies appear to consider ISO 26262 as a barrier introduced to give European and U.S. manufacturers a trade advantage (similar sentiments have been expressed concerning the AUTOSAR initiative [2]). Other concerns, however, reflect uncertainty about the legal impact of the DIS and the availability of the standard as such. Some companies do still not believe that it will be finally adopted (at least not in the near future) due to the large number of comments and issues raised. However, we still expect the voting process will proceed without major complications. The last vote of the task force at the ISO was held in December 2009 and all parts have been voted "YES". The official vote will be in March 2010. If the 26262 is approved at that time it will then have the status of FDIS (Final Draft International Standard).

ISO DIS 26262

- 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”

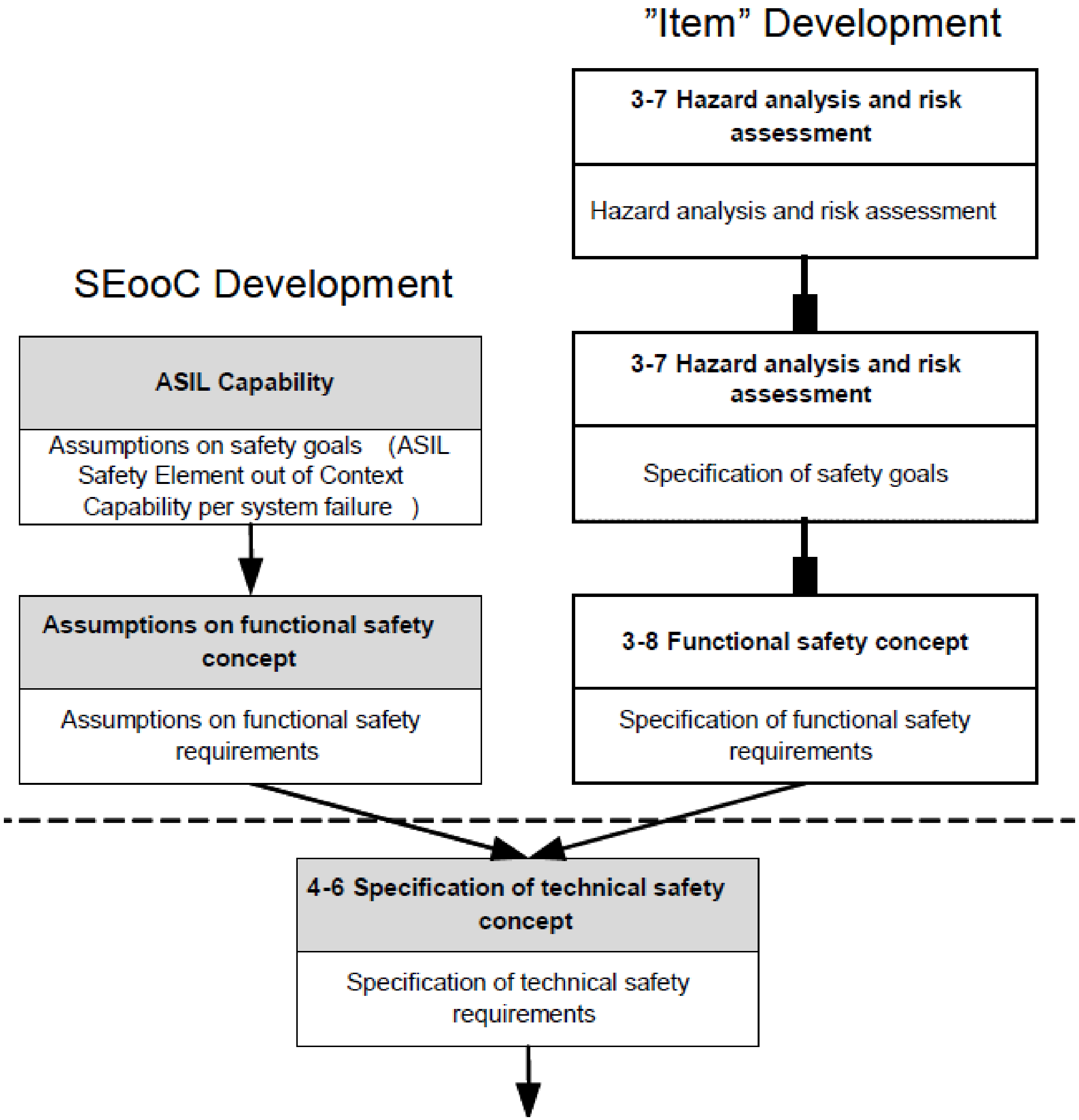
ISO 26262 and Certification?

- “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!”


"Item" Development
3-7 Hazard analysis and risk assessment
Hazard analysis and risk assessment
SEooC Development
ASIL Capability
Assumptions on safety goals (ASIL Safety Element out of Context Capability per system failure)
3-7 Hazard analysis and risk assessment
Specification of safety goals
Assumptions on functional safety concept
Assumptions on functional safety requirements
3-8 Functional safety concept
Specification of functional safety requirements
4-6 Specification of technical safety concept
Specification of technical safety requirements

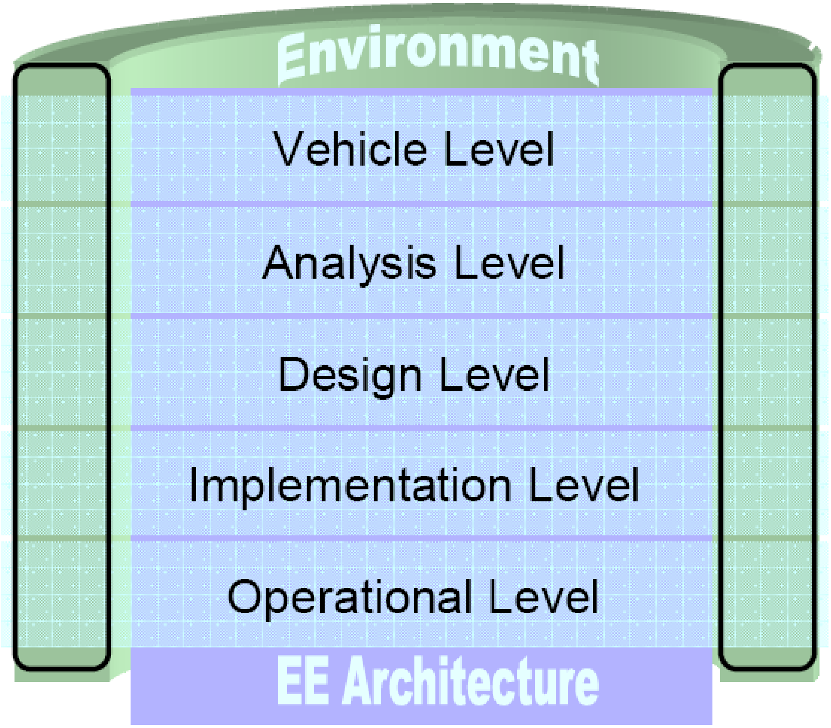
“A Common Language?”

- “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

ATESST2 and EAST-ADL2

ATESST

- There was heavy participation from the **ATESST2** project, co-funded by the EU
  - The goal of ATESST2 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



Automatic ASIL Allocation

- 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

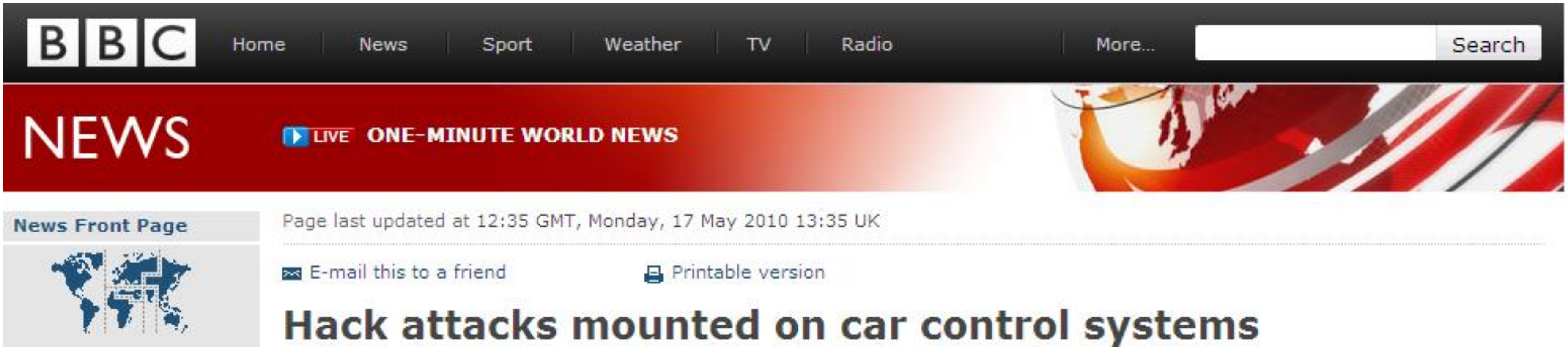
Analysis of AUTOSAR Systems

- “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?



Page last updated at 12:35 GMT, Monday, 17 May 2010 13:35 UK

E-mail this to a friend

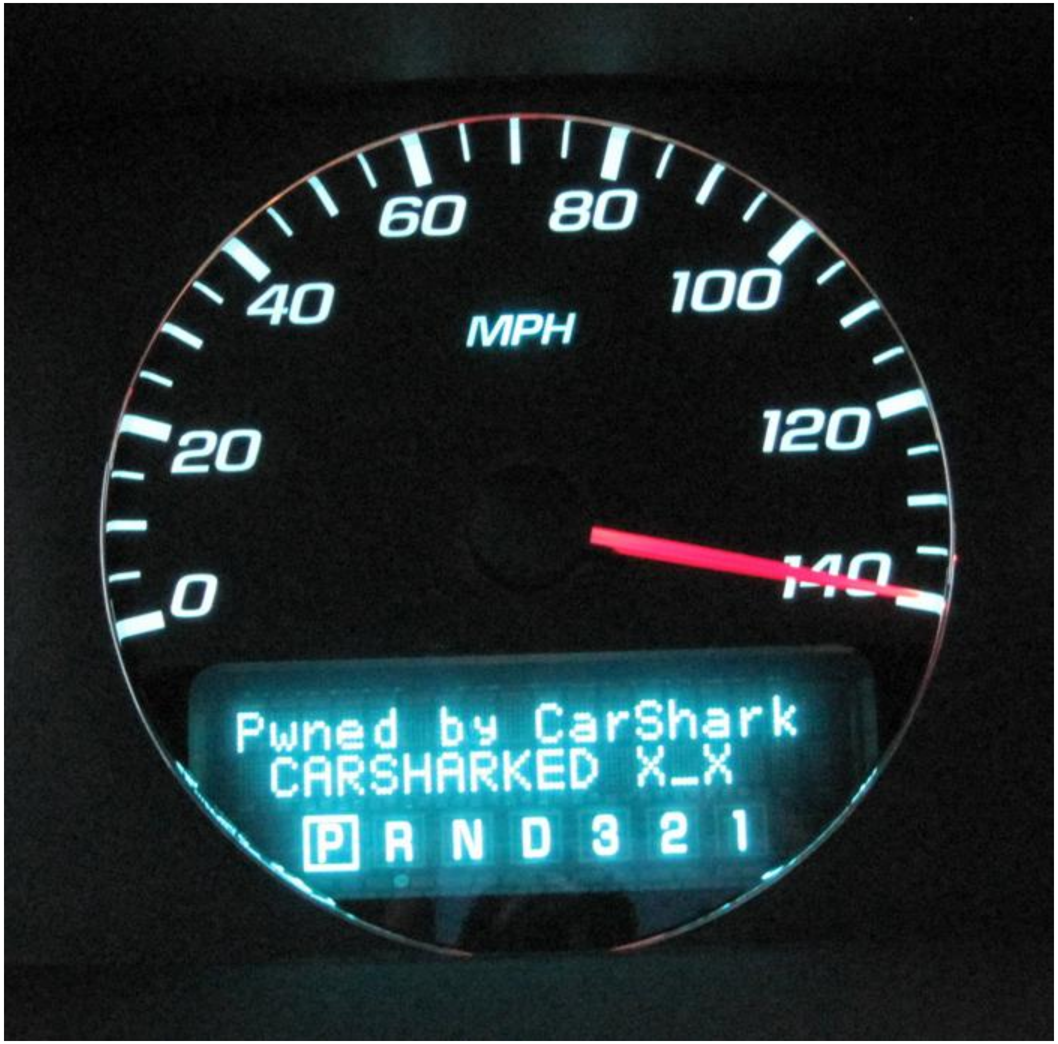
Printable version

Hack attacks mounted on car control systems

CENTER FOR AUTOMOTIVE EMBEDDED SYSTEMS SECURITY

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"

Trusted AUTOSAR Systems?

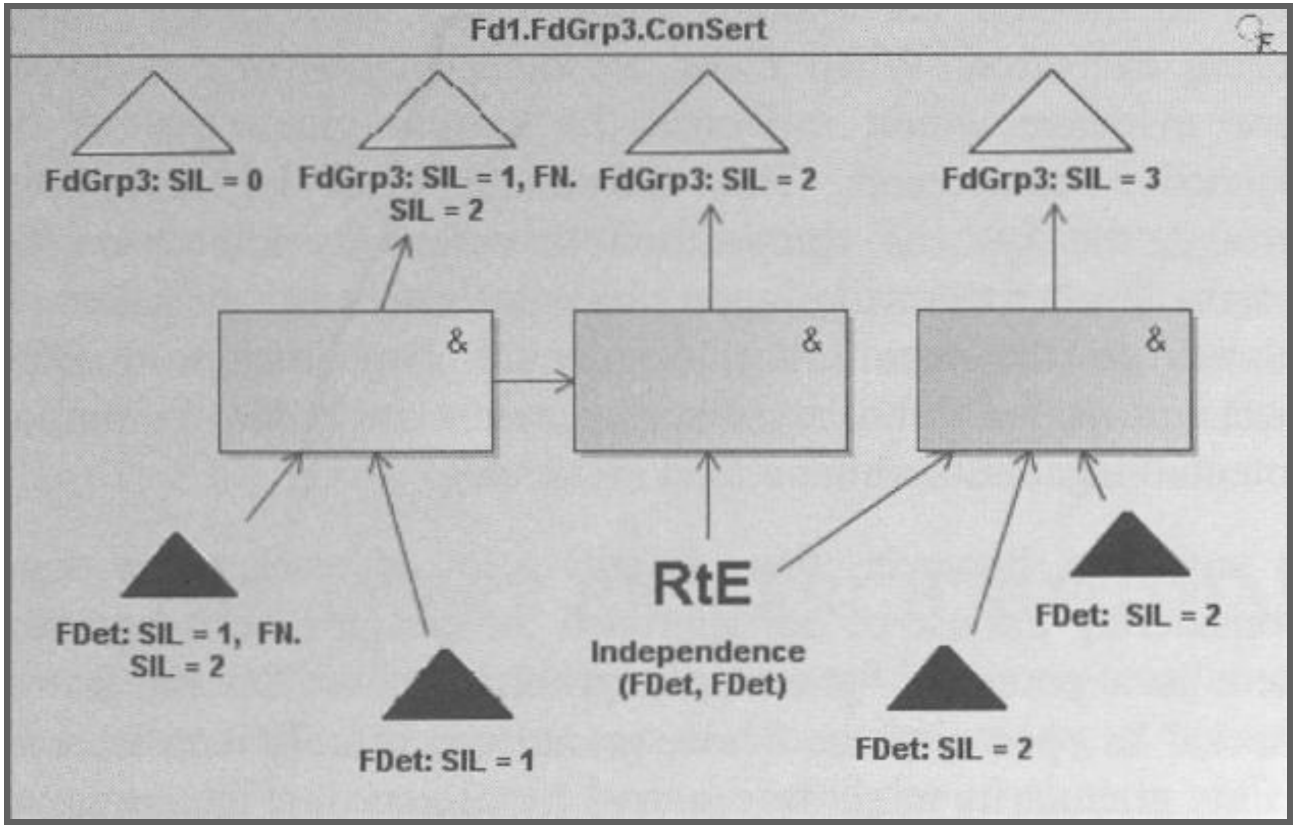
- What are automotive control platforms currently missing?
  - No support for trust/security in AUTOSAR
- Incorporate trust- and –security aware mechanisms into AUTOSAR Basic Software
  - Based on time and space partitioning – **but adoption is slow because increases costs**

“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”



26262 Research Roadmap?

amber Assessing, Measuring and Benchmarking Resilience

- 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

Why Have We Not Progressed Further?

- "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"