

Pålitliga elektroniksystem: Ett nyckelområde för AB Volvo

Olle Bridal, Volvo Technology

CEDES Conference, 4 December 2008

Outline

- Outline
- Which systems and which hazards do I have in mind in this talk?
- The increasing importance of dependability in the automotive sector
- Dependability challenges for automotive electronics
- Some safety-related standards and guidelines
- Specific areas of interest
- Summary

CEDES
Cost Efficient Dependable Electronic Systems



Which systems and which hazards do I have in mind in this talk?

Systems

- Safety systems?
- ➔ Safety-critical systems?
- Safety-related systems?
- Safety-relevant systems?



Hazards

- ➔ Deviation from intended function?
- Deviations from specified function?
- ➔ Hazards associated with the intended function?

CEDES
Cost Efficient Dependable Electronic Systems



The increasing importance of dependability in the automotive sector

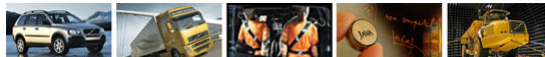
Why *increasing* importance? Hasn't dependability always been important?

- Increased amount of safety-critical systems
- Increased complexity of safety-critical systems
- Increased authority of safety-critical systems

Many new and future applications require very high dependability:

- Active safety systems: Radar/camera-based functions that influence the vehicle motion (acceleration, deceleration, turning)
- X-by-wire
- Hybrid powertrain (acceleration, deceleration, control of high voltage)

CEDES
Cost Efficient Dependable Electronic Systems



Dependability challenges for automotive electronics

- **Large production volumes** (anything that can happen will happen)
- **High dependability of conventional systems** (brakes, steering, etc)
- **Harsh environment** (temperature, moisture, vibrations, EMI)
- **Apparently random failures** (no "forewarn" by sound or feel)
- **Zero public acceptability for malfunctioning electronics** (tyre puncture, corrosion, metal fatigue are understood and "accepted")
- **Infrequent maintenance** (compared to avionics, railway, nuclear, etc)
- **Cost constraints** (compared to avionics, railway, nuclear, etc)

CEDES
Cost Efficient Dependable Electronic Systems



Some standards and guidelines for safety-critical electronics

Safety-specific standards

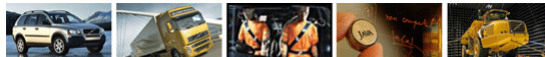
- IEC 61508 "Functional Safety of E/E/PE Systems" **1998-2000**
- ECE R13/R79 "Uniform Provisions for Braking/Steering Systems"
 - ▶ Annex on "Safety Aspects of Complex Electronic Vehicle Control Systems" **2002**
- MISRA Guidelines for safety analysis of vehicle based programmable systems **2007**
- ISO 15998 "Earth-moving machinery - Performance criteria and tests for functional safety" **2008**
- ISO 26262 "Functional Safety of Road Vehicles" (**2010**)

Some other standards and guidelines

- MISRA C **1998/2004**
- Automotive SPICE **2005**
- MISRA C++ **2008**



CEDES
Cost Efficient Dependable Electronic Systems



Specific areas of interest

CEDES has investigated several dependability issues of vital importance

- Development methodology
- Hazard identification
- Safety case
- Fault tolerance mechanisms
- Formal verification
- Error injection based on analysis of software
- Membership handling
- Aspect-oriented programming

Other areas of particular interest

- Model-based development
- Component-based development
- OEM/supplier relationship
- AUTOSAR
- FlexRay

CEDES
Cost Efficient Dependable Electronic Systems



Summary

- Dependability and safety are areas of increasing importance for automotive electronics..
- Achieving and ensuring the necessary level of safety for tomorrow's system is a not an easy task.
- In the last ten years, many new standards and guidelines concerned with safety-critical electronic systems have been published.
- The CEDES project has investigated many dependability-related topics of major importance for automotive electronic systems..

CEDES
Cost Efficient Dependable Electronic Systems

