

The logo for CEDES, consisting of the word "CEDES" in a bold, yellow, sans-serif font.

Cost Efficient Dependable Electronic Systems

The logo for IVSS, featuring three vertical yellow bars of varying heights to the left of the letters "IVSS" in a bold, grey, sans-serif font.

Intelligent Vehicle Safety Systems

Cost Efficient Dependable Electronic Systems

Håkan Edler

SP Swedish National Testing and Research Institute

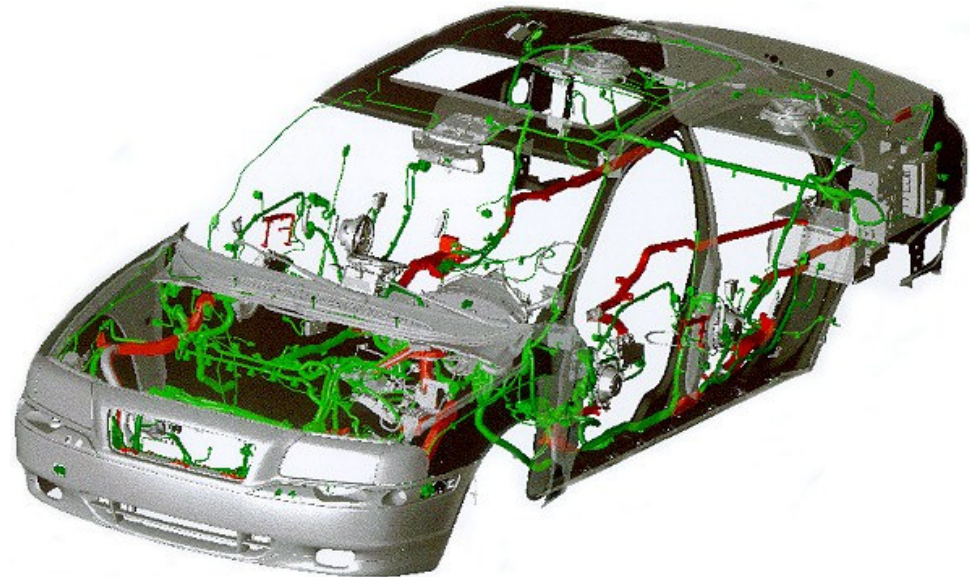
7 October 2006

hakan.edler@sp.se

www.cedes.se

A conventional car

The cable harness is one of the most expensive parts of a car

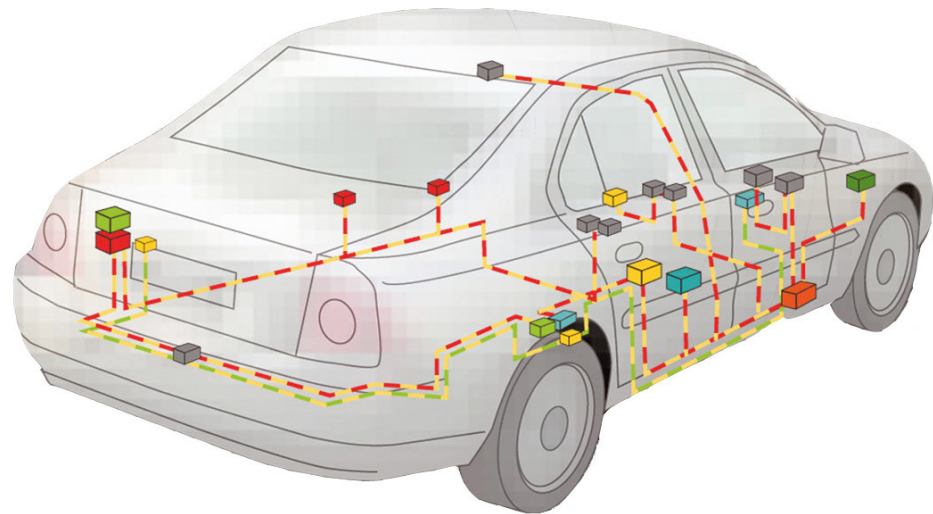


A modern car is a computer on wheels

Many functions are performed by computers

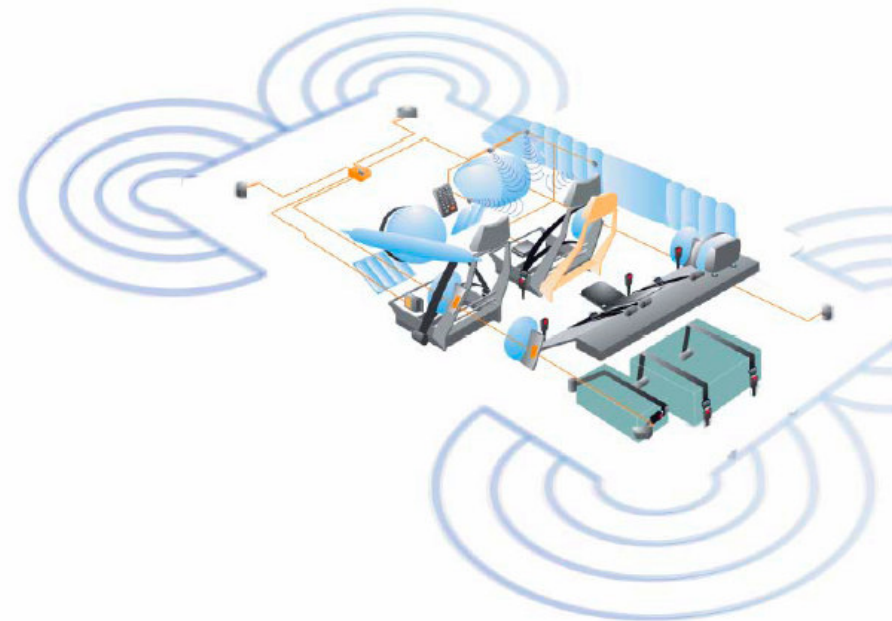
A premium car today has more than 50 computers onboard

They co-operate via one or more local area networks



Why use computers in cars?

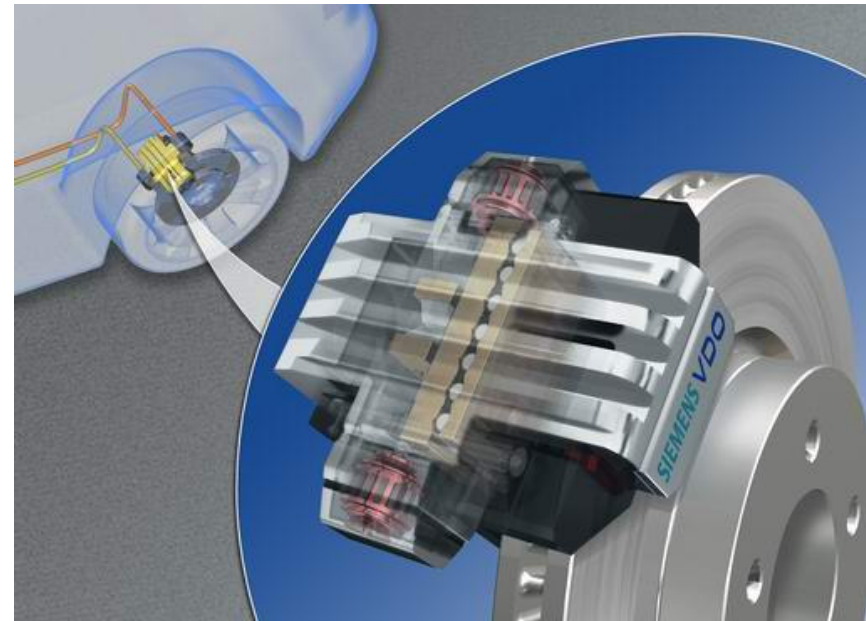
- Functions implemented in software are:
 - Cheap to reproduce
 - Easy to upgrade
- Functions implemented in software will give:
 - Great flexibility
 - Advanced functions
 - Complex system
 - for good and bad



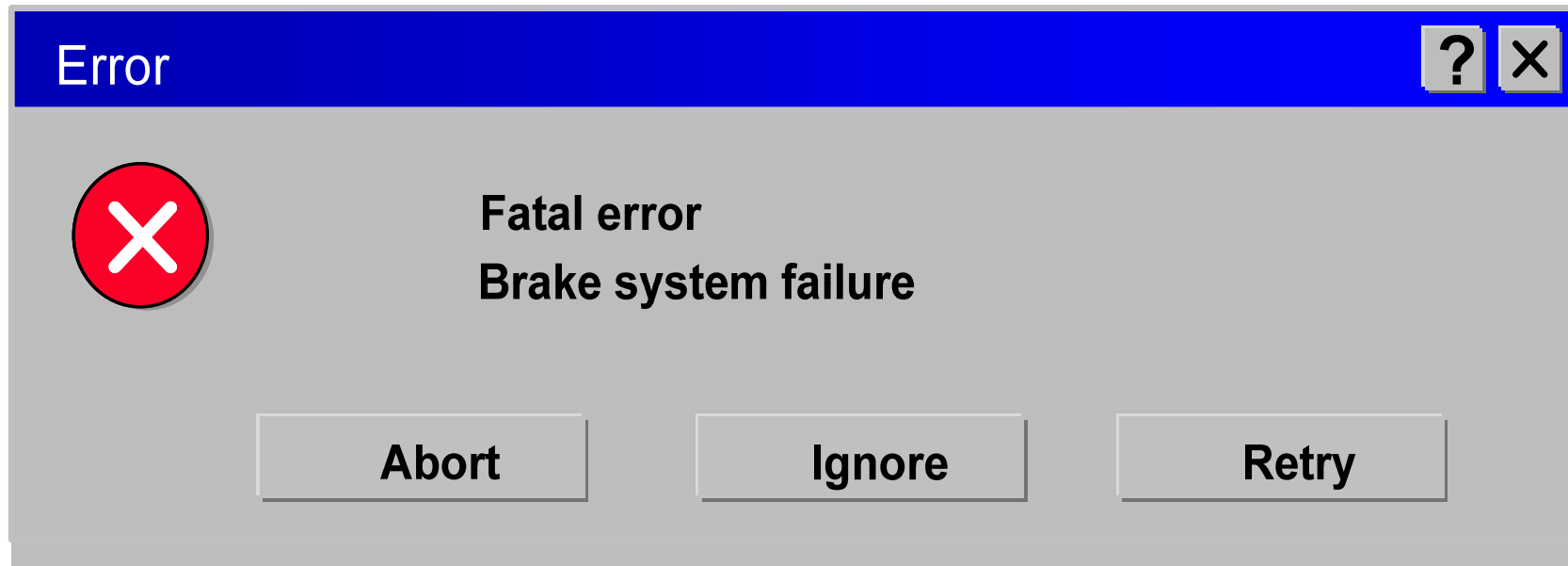
A few examples

Anti-lock Braking System
Electronic Stability Program
Adaptive Cruise Control
Collision Mitigation System
Brake-by-Wire

All these are
active safety systems



And when the program fails?



Can we trust software?

- A new program has on average 50 faults / kLoC (thousand lines of code).
- Commercial software normally has 3 – 5 faults / kLoC.
- A majority of failures in new cars depend on faults in the electrical system.
- An investigation made in 1984 on failures of the IBM mainframe operating systems revealed that 1/3 of all failures had occurred only **once** at only **one** customer => MTTF 5000 years.
- Some software engineering journals regularly reports spectacular failures caused by software faults.

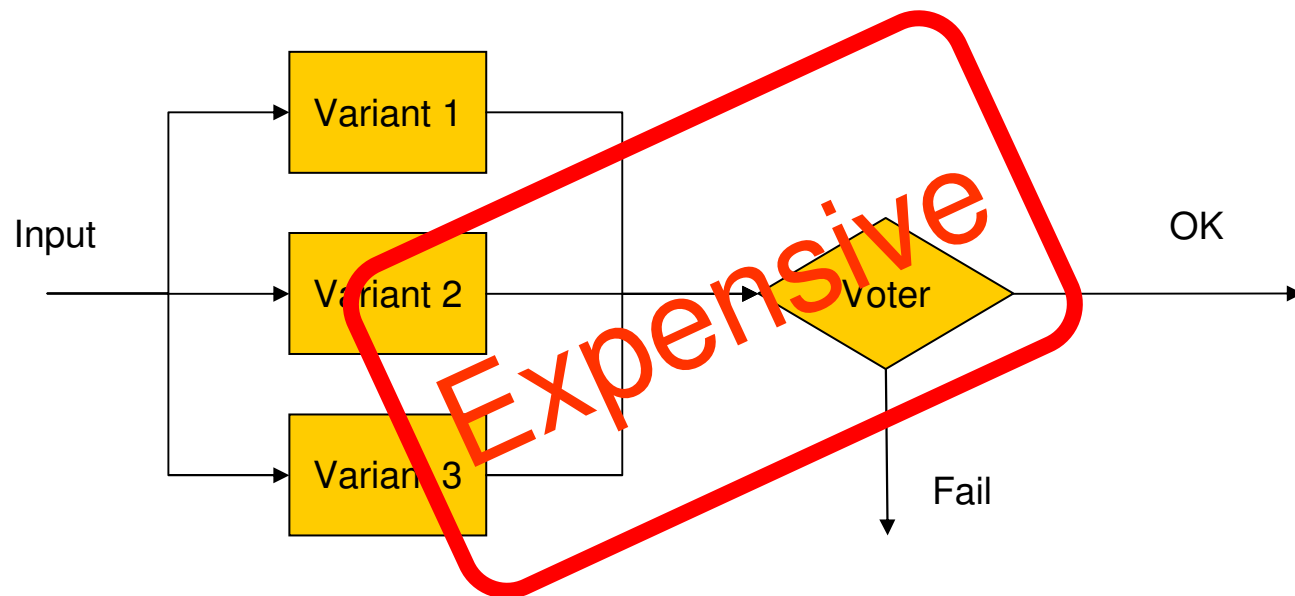
The problem

- The probability of failure in a component of a safety critical system must be $< 10^{-7} / \text{h}$ according to IEC 61508.
- Software testing can never show the absence of faults, it may show the presence of faults
- Software development is a complicated process with few metrics
- Software is an abstract product

The solution

- Build safety critical systems to be **fault tolerant**. They must tolerate
 - Faults in input, operation and design
 - Failures in hardware
- Hence the software system must automatically
 - Detect
 - Confine
 - Diagnose faults
 - Recover from erroneous state
- This requires
 - Redundancy – more than one unit for a certain function
 - Diversity – the function is implemented differently in each unit

Triple modular redundancy – the conventional way



The CEDES Solution

- Each electronic unit is associated with a manufacturing cost
- Instead of electronic units
 - use **software** for the necessary **redundancy** and **diversity**

Work in CEDES is **interdisciplinary**

- Methods to **analyse models** of software to early identify critical parts
- Techniques to **build fault tolerant** parts in software
- Techniques to analyse software with **mathematical formalism**
- Methods to **control work** in development of software
- Methods to **measure** progress and quality in suppliers' work
- **Experiments** on real system to verify research results
- Close **co-operation** with other research projects

Organisations i CEDES



Volvo Cars

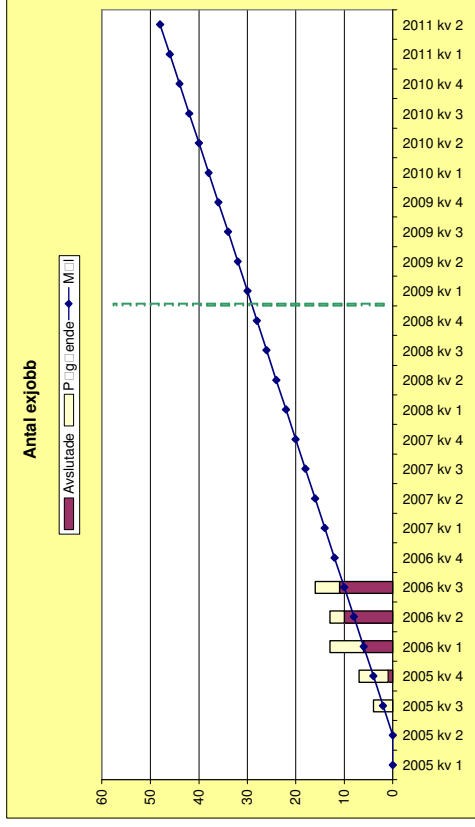
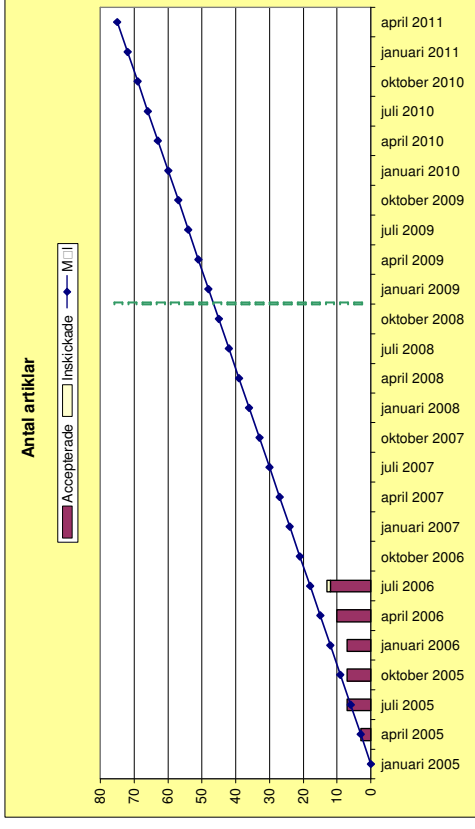
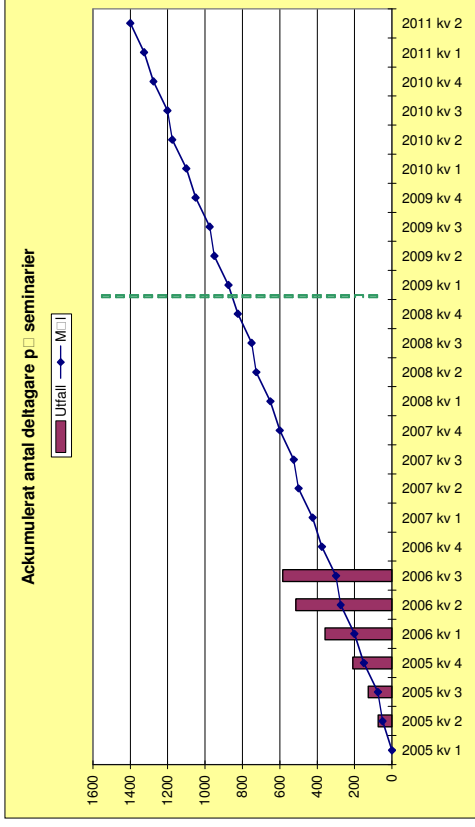
Cost Efficient
Dependable Electronic Systems



CEDES delivers



Intelligent Vehicle Safety Systems



Current work

- Defects in early design specifications
- Method for early hazard identification
- Usefulness of Aspect-orientation
- Robustness of base brake controller
- Static analysis of exception safety in C++
- Symbolic fault injection

Hall of Fame

IEEE Requirements
Engineering:

"An Empirical Quality Assessment
of Automotive Use Cases"

A technique for fault
tolerance assessment
of COTS

SAFECOMP 2005

Aspect oriented software
implemented node level fault
tolerance.

IASTED International Conference on Software
Engineering and Applications (SEA)

SAFECOMP 2006

Assessment of Hazard Identification Methods
for the Automotive Domain

"Defects in Automotive
Use Cases"

**ACM-IEEE
International
Symposium On
Empirical
Software
Engineering**

How will CEDES contribute to the goals of IVSS?

- Road safety, Vision Zero is the goal
 - Active safety systems require advanced control
 - Advanced control requires advanced electronics and software
 - Standard vehicles require low cost components
- Economic growth
 - Safety is a core value for Swedish road vehicle manufacturers
 - Active safety systems will enable continued international success
- Technical systems for a global market
 - Attractive products
 - High reliability
 - Low cost can be achieved with new technology and methodology

CEDES

Cost Efficient Dependable Electronic Systems

