

# Metodik systemutveckling, PIP, säkerhet

*Peter Öhman*  
*Chalmers*

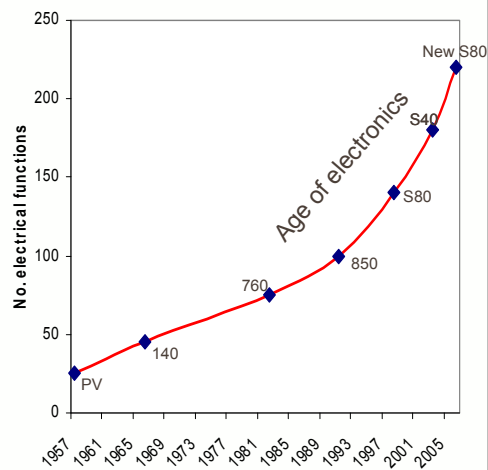
**CEDES**  
Cost Efficient Dependable Electronic Systems



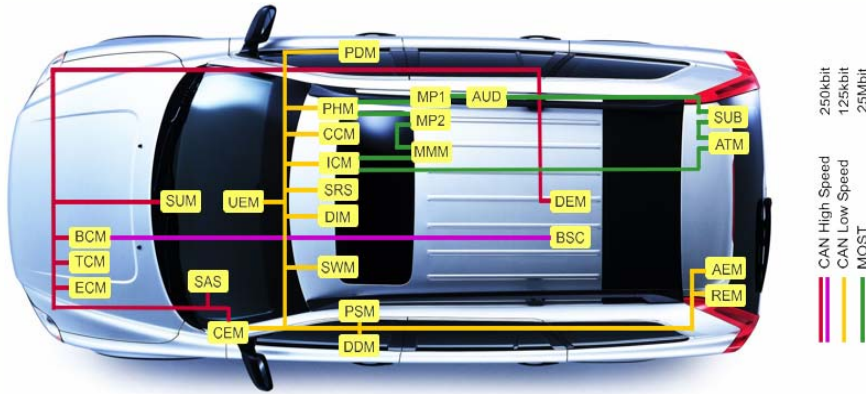
**IVSS**  
Intelligent Vehicle Safety Systems

## Trends in the automotive industry

- Functional growth
  - Environment
  - Safety
  - Infotainment
  - Safety
- Safety related examples:
  - Active safety functions
  - Convenience features
  - Exchanging mechanical solutions with electronics



## The Electrical System of a Car



Licentiate Thesis, Volvo Car Corporation, Fredrik Törner, ftörner  
 Issue date: 2006-09-25, Security Class: Public  
 Page 3



## Automotive Industry Characteristics

### The global market

- Large companies with many brands: FMC, GM, VW...
- Internal platforms supporting several vehicles
- Large supplier base, with hierarchy: Tier 1 – Tier 2 - ...

### Industry characteristics

- Vehicle engineering – Truly multidisciplinary
- Vehicle world production: 45'000'000 vehicles/year
- Embedded ECUs: 60-100 in premium, 20 in mass-market
- 100 fuses, 50 switches, 70 electrical machines
- 20%-30% of the vehicle component cost is electronics
- Cost sensitive, each cent counts

Licentiate Thesis, Volvo Car Corporation, Fredrik Törner, ftörner  
 Issue date: 2006-09-25, Security Class: Public  
 Page 4



# Automotive evolution

- The value of electronics and software is expected to grow from 15-25 percent today to 25-40 percent of the vehicle value by 2010
- Analysts show 90 percent of innovation by 2010 will be electronics-related, and 80 percent of that is in the Software area
- Electronics systems are getting more and more complex with infrastructure reaching its limits



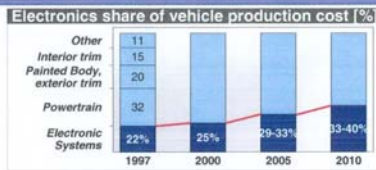
KTC-Electronics  
 Volvo 3P, Martin Ulander  
 5 2008-03-11

**VOLVO**

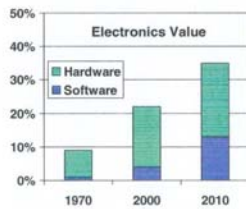
## Industry Trends



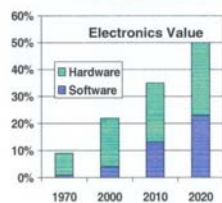
- Electronics leads all other categories of growth
- Software is the largest portion of this electronics vehicle growth



Electronics is expected to grow to 33-40% of vehicle value.



Software will continue to grow to nearly half of the overall electronic value of content as well - nearly 30% annual growth.



As the shift to hybrid engines and fuel cell engines occurs, the value of electronic vehicle content is expected to reach closer to 50%, with software again a crucial component.

Source: Reuse of Software in Distributed Embedded Automotive Systems, Audi 2004, Embedded Automotive Electronics Symposium, Peugeot, June 23, 2004, Roland Berger, Automotive Engineering 2010, Mercedes 2003

06/26/2006

EESE - Copyright © Ford Motor Company, 2006 - Ford Proprietary

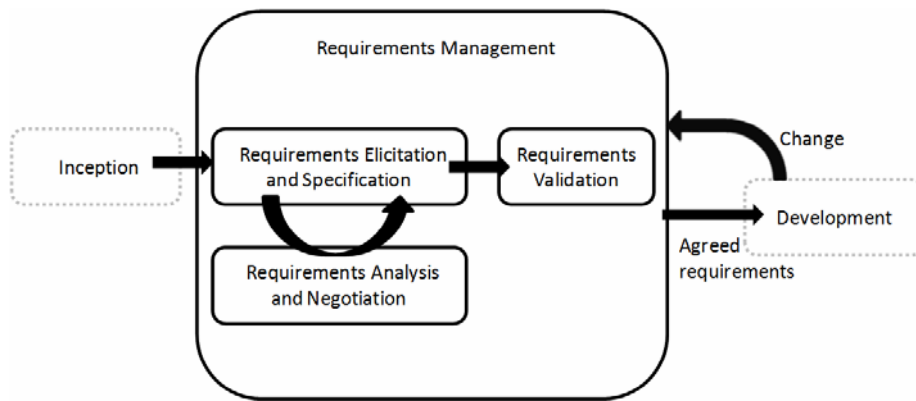
3

**Delprojekt 2: Det funktionella Campus Lindholmen**

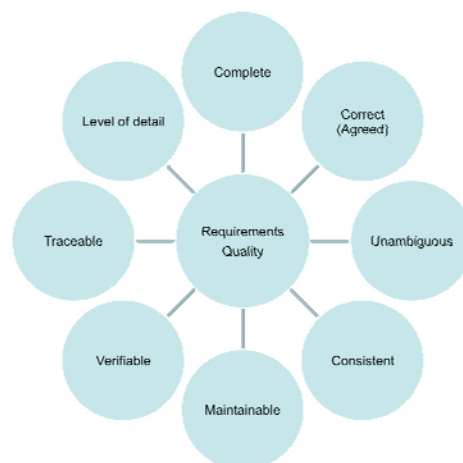


**Delprojekt 1: Ett öppet Campus Lindholmen**

## An overview of the RE life-cycle



## The Quality of Requirements



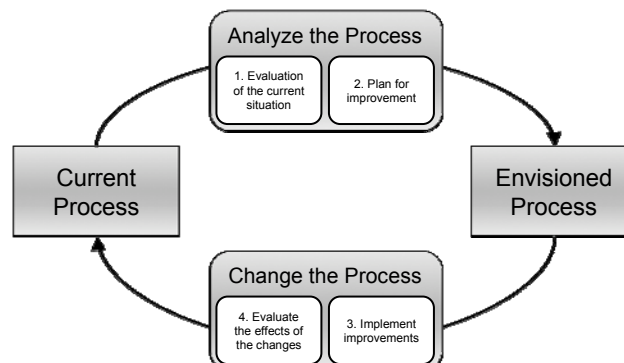
## Automotive Software RE Challenges

- The number of user requirements increases with every generation.
  - ▶ Increasing number of vehicle **functions**.
  - ▶ Increased customer **expectations**.
  - ▶ Increasing number of vehicle **variants**.
- Characteristics affecting Automotive RE:
  - ▶ Many **non-functional requirements**.
  - ▶ Integration of **control-logic** and discrete event systems.
  - ▶ **Distributed** development.
  - ▶ Needs appropriate **product line** approaches (variants, customization, brands).
  - ▶ High amount of **reuse** possible.
  - ▶ **Multi-disciplinary** system development.



## Software Process Assessment and Improvement

“the changes implemented to a software process that bring about improvements”  
[Olson et al 89]



## Existing SPI frameworks and methods

- Prescriptive (Model based)
  - ▶ Best practices that have proven successful in other companies.
  - ▶ Frequently used for supplier assessment
    - Benchmarking, Maturity levels.
  - ▶ CMM, CMMI, SPICE (ISO/IEC15504), ISO9001 etc.
  - ▶ Light-weight adaptations (generally targeted at SMEs)
    - Modular Mini-assessment Method (MMA), IDEAL, Dynamic CMM, MESOPYME, RAPID, SPIRE, SPINI, MARES etc.
  
- Inductive (Bottom-up)
  - ▶ Starting point in a thorough understanding of the current situation.
  - ▶ Improvements based on each company's specific needs.
  - ▶ Quality Improvement Paradigm (QIP) etc.



## Research Questions

- How can communication between different stakeholders in early phases of software development be improved?  
enable the design and implementation of
- How can current requirements engineering practices be improved in order to achieve high quality specifications?  
of quality modeling software.”
- How is software process improvement aimed at specific process areas best carried out to be cost effective and to minimize the associated risks?



## Conclusions

- Communication between OEM's and suppliers can be aided by employing use cases.
- A use case standard for embedded systems is needed to enable communication.
- Use cases are only suitable when describing functionality-driven components.



## Conclusions

- Defect types with highest intensity:
  - ▶ Missing element and/or Incorrect Linguistics
  - ▶ Misuse of preconditions.
  - ▶ Misuse of alternative flows.
- Should not be invalidated by remaining defects.
- None of the existing guidelines studied had complete coverage of the high intensity defect types.
- Suggested improvements:
  - ▶ Domain specific taxonomy.
  - ▶ Better and more guidelines.
  - ▶ Improved reviews.



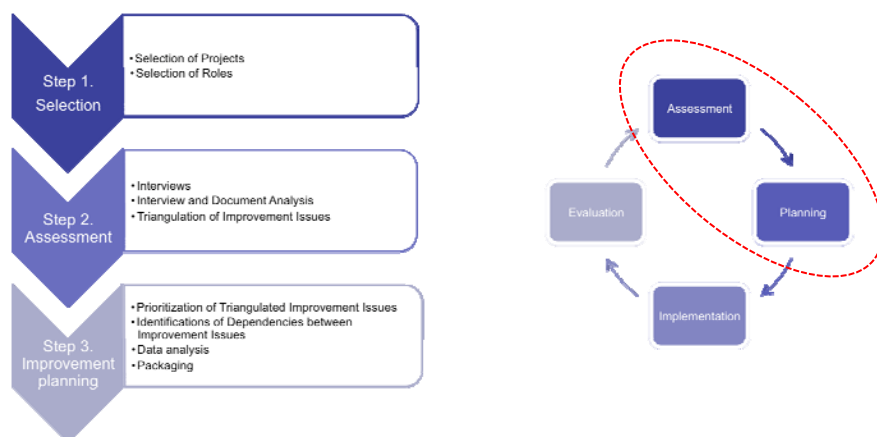
# iFLAP

- iFLAP – improvement Framework utilizing Light weight Assessment and improvement Planning.
  - ▶ Builds on earlier work by Tony Gorschek and Claes Wohlin<sup>1</sup>.
  - ▶ Inductive approach, involving practitioners in improvement issue identification and planning.
  - ▶ Triangulation of sources to confirm issues.
  - ▶ The method and a multiple case study performed at VTEC is presented.
    - Improvement effort targeting RE practices.

1. Gorschek and Wohlin, "Identification of Improvement Issues Using a Lightweight Triangulation Approach", 2003  
Gorschek and Wohlin, "Packaging Software Process improvement Issues – A method and a case study", 2004.



## iFLAP – An overview



## Conclusions iFLAP

### ■ Light-weight

- ▶ Scalable.
- ▶ Low initiation threshold.

### ■ Inductive

- ▶ Interviews with practitioners are the leading data source in elicitation of improvement issues.
- ▶ Prioritization and identifications of dependencies between improvement issues are performed by practitioners.
- ▶ Commitment and Involvement.

### ■ Validity

- ▶ Assures the reliability of findings by triangulation of multiple data sources.

**CEDES**  
Cost Efficient Dependable Electronic Systems



## Safety related automotive functionality - Examples

**City Safety**



**Adaptive Cruise Control**



**Passive Safety Systems**



**Blind spot information system**



**Electrical Stability Control**



**Electrical Parking Brake**

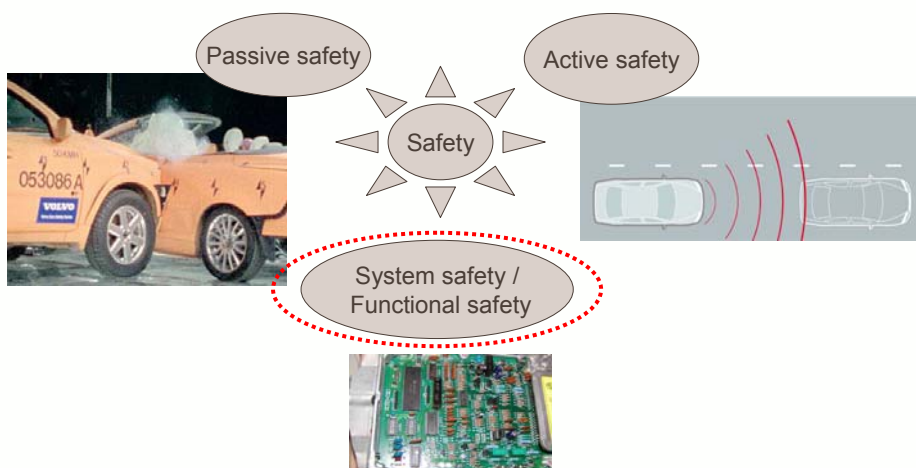


## Concept of Safety

*“freedom of unacceptable risk” where risk is defined as “combination of the probability of occurrence of harm and the severity of that harm”. [IEC-61508 1998]*



## Safety – Automotive perspective



## System Safety - how do we handle it today?

Additions to the normal development process:

- Hazard analysis => Safety requirements
- Safety analysis (FTA,...)
- Safety verification (FMEA,...)

Three standards:

- IEC-61508 1998
- MISRA SAG (1995, 2007)
- ISO 26262 – Under development, 2011?

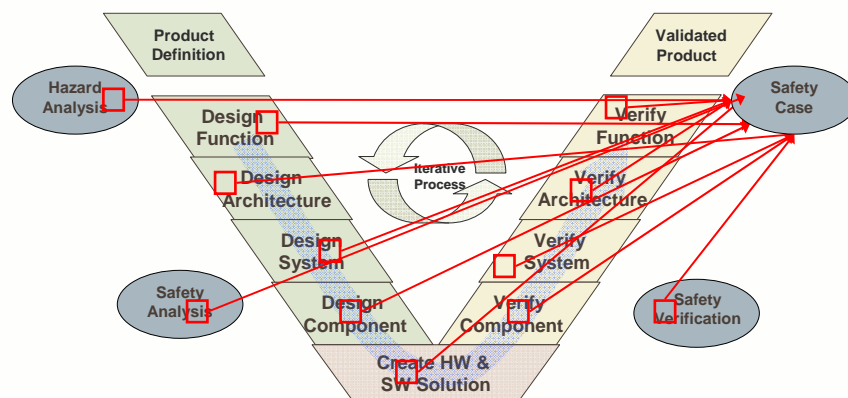
However, no widely accepted scientific measurement method for safety exists. (yet!)

Safety cases

- ISO-26262 requires a safety case, but is not clear on what is intended.
- Possible interpretation of legal requirements for steer & brake systems.
- In use for some systems, initiated by engineers.

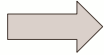


## Safety cases explained...



## Research questions

- Need of efficient methods
- More safety related electronics
- New complex safety systems
- Safety cases as promising approach for addressing safety.



*How can a safety case, which is appropriate for electronic control systems in the automotive industry, be developed?*

*RQ1: What methods are suitable and efficient for determining the evidence of safety?*

*RQ2: What is the automotive industry's view of safety cases?*

*RQ3: How can the safety case approach be adapted to fulfill the needs identified in RQ2?*



## Conclusions

RQ – How can a safety case, which is appropriate for electronic control systems in the automotive industry, be developed?

RQ1 – Evidences

Evaluated efficiency of hazard identification and proposed improvement of quality.

RQ2 – Automotive view

Identified drivers, usage areas, issues and requirements for a safety case.

RQ3 – Design of automotive safety case

Proposed a framework on automotive safety cases (risks, structure, content)

Meta model for safety argumentation notation

