Functional Safety and Automotive SW - Engineering
Introduction ISO 26262 @ Daimler

Dr. Juergen Schwarz
Senior Manager
Functional Safety & E/E - Processes

WOCS 2012
September 27, 2012, Tokyo, Japan
Overview

- Importance of Software in Automotive Engineering
- Automotive Safety
- Introduction of the functional safety standard ISO 26262
- Conclusion
Meaning of Software in Automotive Engineering

70 - 90% of all innovations in vehicle development is nowadays based on embedded systems.
20% of the price of a modern vehicle is caused by embedded electronics. Until 2015 it will rise up to 35 - 40%.
50 - 70% of the overall development cost of electronic control units is attributed to software development.
Meaning of Software in Automotive Engineering

Approximately **80%** of electronics functionality in modern vehicles is based on software.
Increasing Share of Software and E/E

- More than 65 ECUs
- More than 6000 signals
- More than 20 bus systems
- More than 30 million lines of code
Meaning of Software in Automotive Engineering

Conclusion:

Electric/Electronics and software are decisive core competence areas for vehicle development
Overview

- Importance of Software in Automotive Engineering
- Automotive Safety
- Introduction of the functional safety standard ISO 26262
- Conclusion
Exemplary Safety is an important brand value.

Safety is an essential part of the brand Mercedes-Benz.
Some Key Daimler Safety Innovations

2010 Active Lane Keeping Assist and Active Blind Spot Assist, Night View Assist PLUS, LED-High-Performance headlamps for passenger cars

2006 PRE-SAFE® Brake for passenger cars: autonomous partial braking; Active Brake Assist for Mercedes-Benz trucks

2000 First Lane Keeping Assist system for trucks

1995 First Electronic Stability Program (ESP®); all Mercedes passenger cars have been equipped with ESP® as standard since 1999

1981 Airbag and belt tensioner available for a standard production passenger car for the first time

1978 World premiere of anti-block braking system (ABS) for passenger cars; Daimler launched the first ABS for commercial vehicles in 1981

Dr. Jürgen Schwarz | RD/ESF | 27.09.2012
Innovation by means of E/E and Software

Daimler’s Vision of Accident-free Driving

- Further improvement of vehicle safety by means of connectivity of systems
- Enhancement of ‘senses’: from ‘feeling’ to ‘seeing’ vehicles which communicate with their environment
Innovation by means of E/E and Software

“Accidents caused when turning or crossing”

- Nearly every third severe accident happens when turning or crossing
- Future technologies support the driver in unclear traffic situations
- Combination of stereo-vision and anticipating movement analysis
- Risk of accidents through crossing vehicles, cyclists or pedestrians can be detected early
Safety Needs (Video with a 5 Tonne Truck unloaded)
Safety Innovation by means of E/E and Software
Active Brake Assist
Connection of Vehicle with External World
Car-to-Car Communication

Example: Slippery road surface or fog

- Vehicles send danger warnings automatically
- Nearby drivers can react immediately and thereby avoid accidents
Building Blocks for a Safety Culture

Exemplary Safety being an important brand value & the Vision for accident-free driving are the building blocks for establishing a safety culture within the Daimler company.
Overview

- Importance of Software in Automotive Engineering
- Automotive Safety
- Introduction of the functional safety standard ISO 26262
- Conclusion
Introduction of the functional safety standard ISO 26262

- The automotive industry introduced a new standard ISO 26262 on functional safety in November 2011
- Daimler having introduced already many safety innovations without such a standard, what is the benefit?
Increasing Requirements with respect to System Safety

Driven by:
- Complexity/Integration
- Competence of the systems

Obligation to prove System Safety within Type Approval General Inspection Product Liability

Dr. Jürgen Schwarz | RD/ESF | 27.09.2012
The new quality of automotive safety systems

• Former safety systems could focus mostly on a single signal, e.g. the Crash signal for Airbag systems or the yaw rate signal of the ESP.
  • For the organization that means, that the responsibility for the safety relevant development could also be very clearly addressed

• The next generation of safety systems will be based on the network of different systems that will have to collaborate for establishing new safety functionalities
  • For the organization that means, that there will be a distributed responsibility for the safety issues.
  • The organization shall create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety.

How to introduce this new way of development?
The standard ISO 26262 comprises a complete lifecycle.
System Development
Safety-oriented development modules

Legend:
- Development phase
- Functional safety-specific activity
- Standard development

System definition
- Hazard analysis and risk assessment
- Functional safety concept
- System FMEA
- Tech. safety concept for HW
- Tech. safety concept for SW
- Component-FMEA
- FTA/FMEDA

Implementation
- Integration and test module, component, system
- Quantitative safety analyses for ASIL C, D
- Safety case
- Initial sample inspection report
- Release for production
- Safety case

Verification
- Quantitative safety analyses for ASIL C, D

Validation
- Integration and test module, component, system
- Initial sample inspection report
- Release for production

Legend:
- Development phase
- Functional safety-specific activity
- Standard development

Dr. Jürgen Schwarz | RD/ESF | 27.09.2012
ASIL-classification determines requirements to the development

Examples

Example: Low beam
Hazard: Failure of low beam during driving at night
S-Goal: Provide low beam

Example: ESP
Hazard: Faulty activation of brakes
S-Goal: Avoid unintended braking

Example: Window lifter
Hazard: Pinching extremities
S-Goal: Avoid unintended closing

Example: Radio
Hazard: Unintended increase of loudness
S-Goal: -

Example: el. Steering column lock
Hazard: Faulty lock during driving
S-Goal: Avoid unintended locking

(ASIL = Automotive Safety Integrity Level)
### Additional Scopes for the Implementation of ISO 26262 (extract)

<table>
<thead>
<tr>
<th></th>
<th>QM</th>
<th>ASIL A</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification of safety concept</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handling of single point faults (metrics)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handling of latent faults (metrics)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carrying out of FMEA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carrying out of safety assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carrying out of safety audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation of FTA / FMEDA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation of common cause analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qualification of tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation of a safety case</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
General roll-out scenario

ISO Milestones

Legend:  
CD = Committee Draft;  
DIS = Draft International Standard;  
IS = International Standard


Pilot projects

Consideration of ISO 26262 requirements for new systems

Complete development process with respect to ISO 26262  
(applicable for all projects with release of requirements specification after April 2011)

Goal:
- Demonstrate changes due to the ISO 26262
- Feedback to ISO working group

Goal:
- Early implementation of the standard

Goal:   
Incremental implementation of the ISO 26262.
Functional Safety within Daimler AG
Responsibility and Tasks

Functional Safety Contacts
Responsible persons on department level are assigned to control the operative implementation of the functional safety requirements

- Representation of Daimler interests in the different committees
- Harmonization between the BUs
- Development of functional safety methods/processes
- Independent review entity
- Installation of organizational structures
- Expertise and organizational structure within BUs
- Review entity for BUs
- Coordination between the projects
- Process instructions
- Operational coaching of projects
- Further development of functional safety expertise
- Generation of feedback for the standard
- Adaptation of standard for specific projects
Functional Safety within Mercedes-Benz
Organization / Management

Functional safety contacts:
- Execution of hazard analysis and risk assessment → results in ASIL
- Creation of safety plan
- Development of functional safety concept
- Development of technical safety concept

Central Functional Safety Team
- Independent review in order to verify and confirm the safety cases

Steering committee ISO 26262:
- Level 2: Confirmation of determined ASILs A+B
- Level 1: Confirmation of determined ASILs C+D

Dr. Jürgen Schwarz | RD/ESF | 27.09.2012
What does the Organization have to provide?

- Clear distribution of the tasks addressing Functional safety management and functional safety engineering
- Realization of a 4-eyes-principle for safety tasks
- As safety has often massive influence to the product, the management has to be involved right from the beginning
- Involvement of the management on a regular basis
  - During the introduction phase even a higher frequency of management meetings have to be provided to get management decisions quickly

---

Dr. Jürgen Schwarz | RD/ESF | 27.09.2012
Four abstraction levels for the description of functional safety methods and processes

Functional safety in the product development process (MDS)

Quality Manual

Templates, Examples, ...

Checklist / Guideline
Qualification Concept

Overview

Goal
Competence for the development of safety-related Electronics and Software.

I. Classical Training
- Complete overview
- Module training

II. Private Study
- Training documents
- Supporting Documents

III. Training on the Job

Qualification | Functional Safety – Portal | Competence Centre

Dr. Jürgen Schwarz | RD/ESF | 27.09.2012

Usage within all business units with high numbers of access

FuSi-Portal (ISO26262)

Number of registered user

Dr. Jürgen Schwarz | RD/ESF | 27.09.2012
Overview

- Importance of Software in Automotive Engineering
- Automotive Safety
- Introduction of the functional safety standard ISO 26262
- Conclusion
Conclusions
Developing safety culture @ Daimler AG

■ **Exemplary Safety** being an important brand value & the **Vision for accident-free driving** are the building blocks for establishing a safety culture within the Daimler company

■ Introduction of new functional safety standard affords
  ■ Precise planning of the ramp-up scenario
  ■ Clear assignment of the responsibilities
  ■ Necessity of timely management decisions within introduction phase
  ■ Maximal standardization – central control of all requirements
  ■ Usage of new ways for training / qualification and process-control

The requirements of the functional safety standard ISO 26262 requires a safety culture but also helps to establish a safety culture