Functional Safety in Electrical Power Steering Systems - Experiences

Dr.-Ing. Frank Schöttler, Volkswagen AG
Agenda

1. Design of the Electrical Power Steering from Braunschweig
2. Development tasks and interfaces
3. Safety Goals and Validation Criteria
4. Basic Safety Architecture
5. Implementation and Verification
6. Assessment
Design of an Electrical Power Steering system
Technical Highlights

- Steering system for MQB Platform with
  - 9 kN rack force,
  - Delivering an ASIL-D compliant steering angle signal.
- Compliant and safe implementation of functions programmed by the customer.
- Actor for requests from
  - ESP (Driver Steering Recommendation),
  - Lane assist,
  - Parking assist.
- Degraded modes to avoid sudden loss of steering support.
### Development Tasks and Interfaces

- **Customer**
  - Volkswagen Braunschweig
  - System Requirements
    - System responsibility
    - Safety Concept
  - Steering functions development
  - Mechanical development
  - System approval
  - System integration
  - Process responsibility

- **Development Partner**
  - Hardware development
    - Operating System
  - Motor development
  - Sensor development
System requirement structure

- Mitgeltende Unterlagen
- Kunden-Lastenhefte

Lastenheftanalyse

- Projektmanagement-Anforderungen
- Mitgeltende Regeln

- Technische Systemanforderungen
- Funktionales Sicherheitskonzept

- System-Architektur
- Sicherheits-Architektur

Komponentenzerlegung

- Lenkfunctionen
- Kugelgewindetrieb
- Elektronik-Leistungsteil
- Lenkgetriebe-Gehäuse
- Motor

Anforderungen an den Kunden
Validation criteria

The actual hazards are fixed by intensive proband tests.

Decision criteria is the subjective value derived from probands’ feel.

Target:
Control of failure modes which lead to a driving situation rated as „critical“ by the probands.
Definition of safety goals

The HARA is derived in conjunction with our customer.

Availability is part of the safety goals.
Basic safety architecture

- Modified 3-layer architecture
- Redundant torque sensors with digital data transmission
- Internal creation of steering angle signal with TruePowerOn functionality
- Digital motor position sensor
- Two independent switch off paths
- Multiple degraded modes for a maximum of availability
Software implementation

Layer 3

Sensor Check
Comfort function check
Steering angle check
Steering function check
Motor check
Platform Check

Sensor input
Steering angle calculation
Main Steering function
Motor

CAN Bus Input

Comfort functions
Customer software functions
Interface for external requests

CAN Bus Output
Degraded modes and availability

Hardware:

- Driving possible after loss of one steering torque sensor.
  - A test signal is applied to the steering system to ensure the diagnostic coverage, about 60h of driving possible.
- Support force with two motor phases possible.
- Most Peripheral elements use replacement values.

Software:

- Most software modules can be switched off independently.
- Development of Layer-1 functions according to methods and measures from ISO26262.
Structure of analytic verification

Verification of a consistent system level is based on a complete function and failure net.

Vehicle system level \rightarrow System FMEA \rightarrow P-FMEA

ECU-System-FMEA

Steering functions SW-FTA

Mechanical Component FMEA

Hardware FMEDA

Software FMEA
Remarks concerning the analytic verification

The structure of the analytic verification is directly connected to the requirement structure.

Design and production FMEA are integral part of the verification.

The overall analytic structure integrates every requirement to the system including

− Mechanical integrity,
− Functional safety,
− EMV compliance, environmental compliance etc.

The Software FTA is part of this structure.
Contents of the „Sicherheitsbewertung“

– Validation of safety goals and their successful implementation in the steering system and in das Auto,

– Evaluation of the development process to reach the goal of the functional safety (Functional Safety Audit),

– Completeness and correctness of every work product connected to functional safety (Safety Case),

– Evaluation of outputs to reach the safety goals (part of a functional safety assessment),

– Project status taking all aspects of a safety relevant development into account including status of the mechanical implementation.
Assessment structure

The assessment takes the project as a whole, not differing between customer requirements and project realizations.
Remarks to the standard

Positive:
– Communication has become easier.

Negative:
– Too much interpretation possible in the standard.
– A single letter between A and D is not sufficient. Limits and timing have to be defined also.
– Connections between mechanical parts and the overall system analysis are still specific to project or supplier.
Vielen Dank!