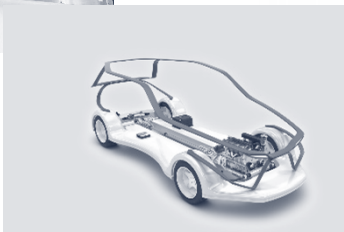
Institut für Qualitäts- und Zuverlässigkeitsmanagement GmbH
(Institute for Quality and Reliability Management)
Dr.–Ing. Marco Schlummer & Dr.-Ing. Jan Hauschild



# LESSONS LEARNED & CURRENT TRENDS REGARDING FUNCTIONAL SAFETY AUTOMOTIVE





IQZ Your Quality Supplier

spid

# INTRODUCTION IQZ

Consulting and research partner at the state of the scientific and technical knowledge

Office Hamburg

Head Office Wuppertal

Quality Management


Risk Management

Safety Management


Reliability Management



Co-operation partners in Korea, China, and the USA


**Aug 2015**

**Automotive Industry**

…

…well established processes…

…highly skilled engineers…

…profound methodological knowledge…

**„Everything is fine and everybody knows what to do!“**

# AGENDA

**"Lessons Learned" in the past**

- Role of the Safety Manager
- Reliability versus Safety
- Difficulties with Failure Rates

**Upcoming trends in Functional Safety or aspects to keep an eye on**

- Connection of Safety & Security
- Outlook on 2nd Edition of ISO 26262
- Functional Safety & Autonomous Driving

# Lessons Learned

- ISO 26262 deals with many issues


- **Line Organization** (ISO 26262-2, cl. 5.4.2.2)
  - „The organization shall institute, execute and maintain organization-specific **rules and processes** to comply with the requirements of ISO 26262.“
- **Project Organization** (ISO 26262-2, cl. 6.4.3.1)
  - „The safety manager shall be responsible for the **planning and coordination** of the functional safety activities in the development phases of the safety lifecycle.“

*Role of the FSM is PLANNING & COORDINATION – NOT EXECUTING the activities!*

# Role of the FS-Management within line organization and project organization

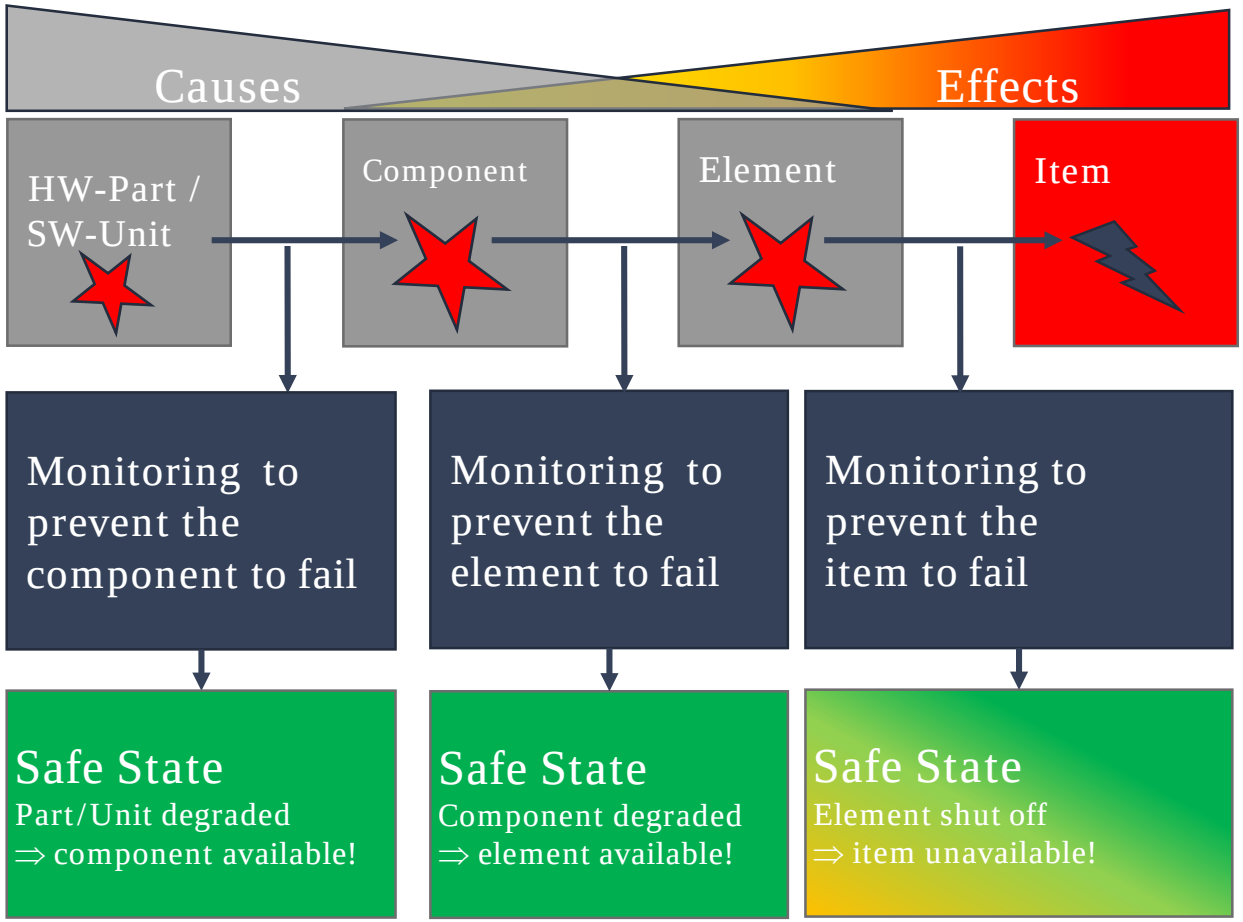
Safety Plan

| Activities | Executor |
| --- | --- |
| • Identification and Definition of Safety Requirements | • Requirements Engineer |
| • Technical Safety Concept | • Architects and Developers |
| • System Safety Testing | • System Tester |
| • Coding Software | • Programmers |

**Function of FS-Management within project is the compilation of the complete and correct safety case:**

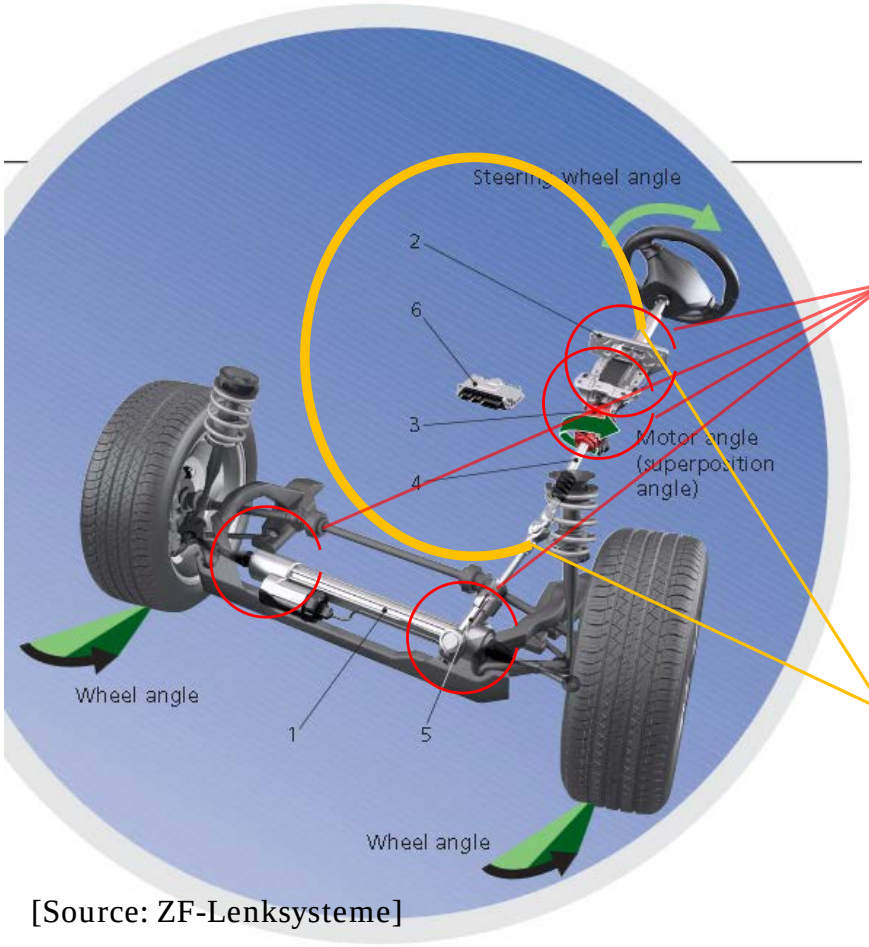
- Prepare safety plan
- Delegate activities to executors
- Advise development of activities
- Review work products
- Ensure safety case

# Monitoring of Causes vs. Monitoring of Effects - Reliability vs. Safety




*Safety could be influenced by monitoring causes and effects – Reliability could be influenced by monitoring causes!*

# Monitoring of Causes vs. Monitoring of Effects - Reliability vs. Safety




[Source: ZF-Lenksysteme]

Monitoring on part/unit or component level
- High effort for monitoring
- Increase of element reliability

Monitoring on element level
- Less effort for monitoring
- Decrease of element reliability

*The monitoring concept has an impact on safety, reliability , complexity and costs!*

# Difficulties With Failure Rates

- Projects sometimes suffer under high pressure on reaching very strict target values for random hardware failures (PMHF)
- ISO 26262-5, clause 9.4.2.1, Note 1
  *„These quantitative target values [...] do not have any absolute significance and are only useful to compare a new design with existing ones“*

**Some experiences regarding related difficulties from past projects**

- If a normative target value (given by the well known table 6 in ISO 26262-5) is not met for a sub-system, DO NOT PANIC! Boundaries of the entire item together with the system design must be taken into account (-> task of the OEM) and the values do not have an absolute significance.
- If you use one of the mentioned „commonly recognized industry sources“ be aware of their weaknesses; e.g.
  - MIL-HDBK: very conservative and not recognized in automotive industry
  - SN 29500: easy to handle but not feasible for detailed ASIC-considerations
- 3 sources are provided in ISO 26262 for deriving possible target values
  -> why always pick the table with the FIT-values?
  -> why not estimate your own target values from your own field data?

# Some remarks on difficulties within distributed developments (OEM – TIER 1 – TIER 2 – ...)

- OEM must clearly communicate the FIT-portions to his suppliers (-> „FIT-budgeting“)
  - OEM requires: „Ensure that your sensor reaches the ASIL C target value for PMHF“
  - Supplier states: „PMHF value of my sensor is below 95 FIT“
  - Result is that OEM only has 5 FIT left for the rest of the function which may include several ECU and other components

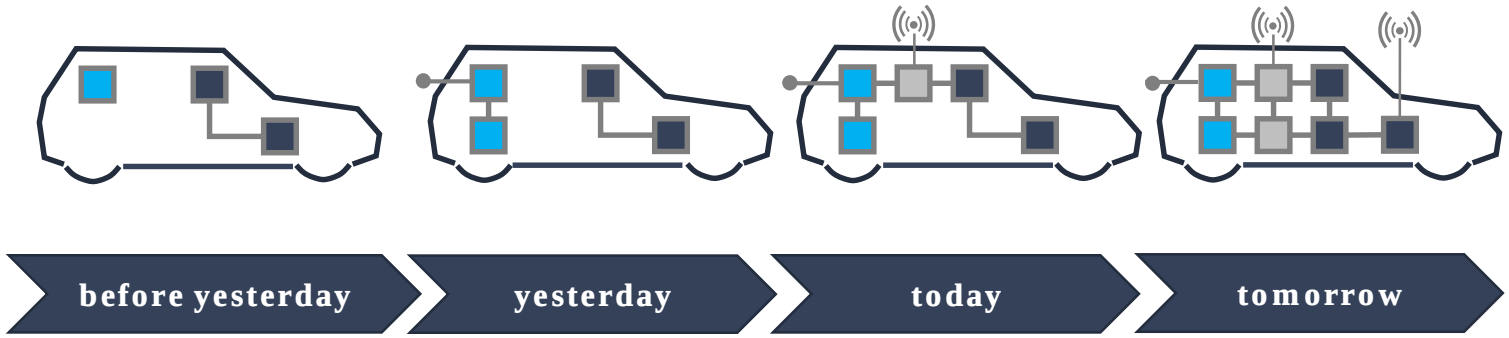
- If an industry standard shall be used within a project, ensure that all involved parties use the same one
  - Otherwise you‘ll get a mixture of partial results that are very hard to compare and to combine to the final result regarding the violation of a safety goal

*Communication is one of the most important things – not only in private life!*

# FuSa Trends

# V2V-Communication – the automotive digital revolution

- The development evolves from a self-sufficient system to an interactive and networking system: safety warnings, traffic information, infotainment, …
- Safety - Accident prevention: standards available
- Security - Attack prevention: non-standardized




*The interfaces between safety and security shall be specified and assessed!*

# Safety and Security – Borders are Blurring

**Jeep –Uconnect System**

- Uconnect serves as an interface to smartphones and tablets and manages navigation and multimedia
- Hacker gained access to the vehicle and controlled the radio, wipers, ventilation as well as the motor and steering from more than 1,000 kilometres distance

**BMW – ConnectedDrive**

- ConnectedDrive includes internet functions, the transmission of service data as well as the operation of functions such as heating, door lock or air conditioning via smartphone app
- Hacker opened the door via smartphone

**Chevrolet Corvette – Insurance Black Box**

- Black Box for storage driving inputs for insurance purposes was used as gateway into the car
- Hackers controlled the brakes and windscreen wipers using SMS text messages
- Method is not manufacturer-specific

*With respect to FuSa security becomes more and more important!*

# 2ND EDITION ISO 26262: PAS SUB GROUPS – PUBLIC AVAILABLE SPECIFICATION

Passenger Cars

ISO 26262 1st Edition

1st Edition November 2011

revision

ISO 26262 2nd Edition

2nd Edition 201?

Road Vehicles

## ISO PAS from three sub-groups

- Commercial vehicles , i.e. Trucks, Buses (and trailers).
  - *PAS 19284* Nominal and informative guidance to be integrated into 2nd Edition
    - Separate PAS not needed at this time
    - Sub group considering challenges specific to T&Bs such as vehicle supply chain, variants, use cases, interface with machinery etc.
- Motorcycles
  - *PAS 19695* submitted to the ISO DIS ballot
    - to be integrated into 2nd edition
  - Proposal for motorcycle specific risk classification schema
- Semiconductors
  - *PAS 19451* in development providing guidance covering:
    - Dependent Failure Analysis; Base Failure Rate; Analogue; PLD; IP; Multicore

## Agreed 36 month ISO project for 2nd Edition - started 15th Jan 2015

| 1st Edition development | 1st Edition experience | 2nd Edition development |
|---|---|---|
| 2005-2011 | 2012..... | 2015-2018 |

- Safety of the Intended Functionality (SotIF)
- SW sub group
  - safety analysis for software
- Confirmation Measures
  - Delineation between process and technical requirements
  - Aim to clarify scope of audit and assessment
- Fail Operational
- Role of ISO 26262 with cybersecurity
- And many more discussions to be continued
  - Scope definition
  - Item definition
  - Hardware metrics
  - Role of ISO 26262 with autonomous vehicles
  - etc.

# Three Dimensions of Autonomy

## How much autonomy?

| Driver only | Assisted Driver | Semi-automated | Highly automated | Fully automated |
|---|---|---|---|---|

## Autonomy in how much?

## Autonomy of how much?

City Safety

ACC

CMbB

Autopilot

One function

Set of related functions

All functions (no driver)

Source: Johansson, 2015

# ISO 26262 and Automated Driving / Autonomous Vehicles

- 2 fundamental aspects why ISO 26262 can become problematic:

| Things are much more complicated | Things are fundamentally different |
|---|---|
| • Item Definition for extremely complex functionalities<br>  • "Networked functions"<br>• Specification of safe maneuvers<br>• Safety concepts much more complex<br>  • Possible need for explicit AD blocks<br>  • Fail-operational states will be necessary | • Manual driver is not focused on traffic<br>  • Studies: ~5 sec. to take back control<br>• No manual driver in the loop<br>  • How to deal with the parameter for controllability? |

*The future in the automotive industry will be challeging for all involved persons and functional safety will play a major role*

# THANK YOU FOR YOUR ATTENTION


Dr.-Ing. Marco Schlummer

Managing Director

_____

Mobile + 49 (0)1522 / 955 774 7
Phone + 49 (0)202 / 515 616 93
Fax + 49 (0)202 / 515 616 89

schlummer@iqz-wuppertal.de

www.iqz-wuppertal.de