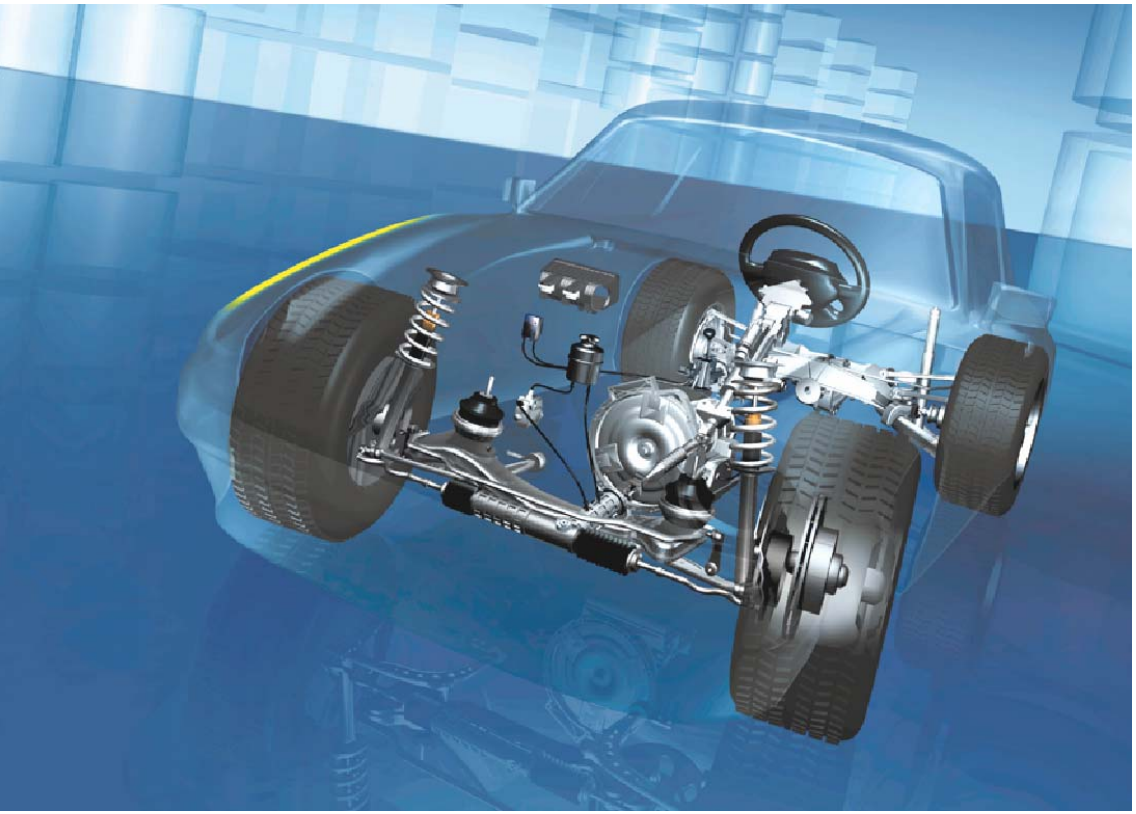


Safety related development process for automotive suppliers

Dr. Wolfgang Reinelt

ZF Lenksysteme GmbH,
Schwäbisch Gmünd, Germany

Email: Wolfgang.Reinelt@ZF-Lenksysteme.com

Fifth Bieleschweig Workshop "Systems Engineering„.

München, Germany, 5+6 April 2005

ZFLS Safety related development process

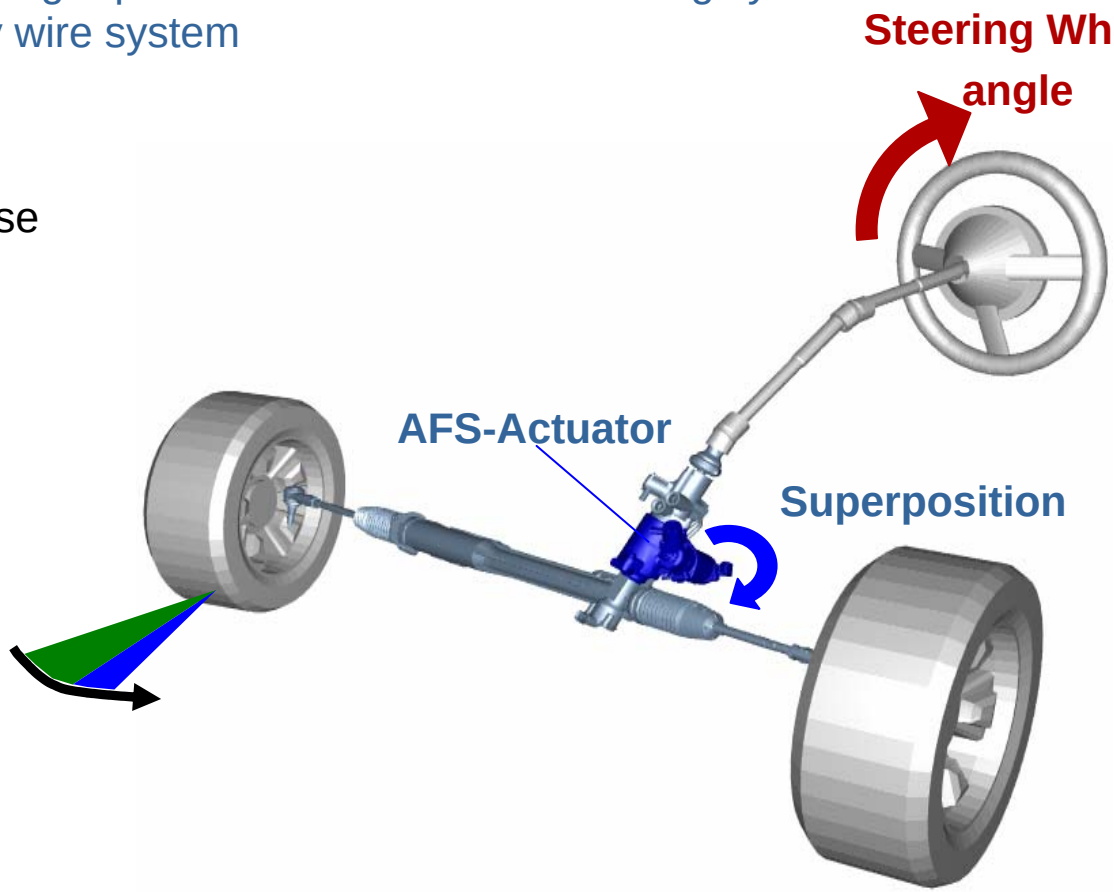
Outline

- Motivation: System overview active front steering
  Goals & constraints for setting up a safety related process
- Safety related development process: structure & work packages.
- New elements
- Exsting development processes that have been touched

Active Front Steering - System Overview

Electronically controlled superposition of an active angle to the steering wheel angle

- Permanent mechanical connection between steering wheel and road wheels
  - i.e. Active Front Steering represents an assistance steering system and does not match the definition of a steer by wire system
- Reduced steering effort
  - Comfort (driver)
- Enhanced lateral response
  - Agility
- Vehicle stabilisation
  - Active Safety



Active Front Steering – Variable Steering Ratio (1/2)

ZF Lenksysteme

Vary steering ratio between hand wheel and road wheel with respect to:

Vehicle Velocity

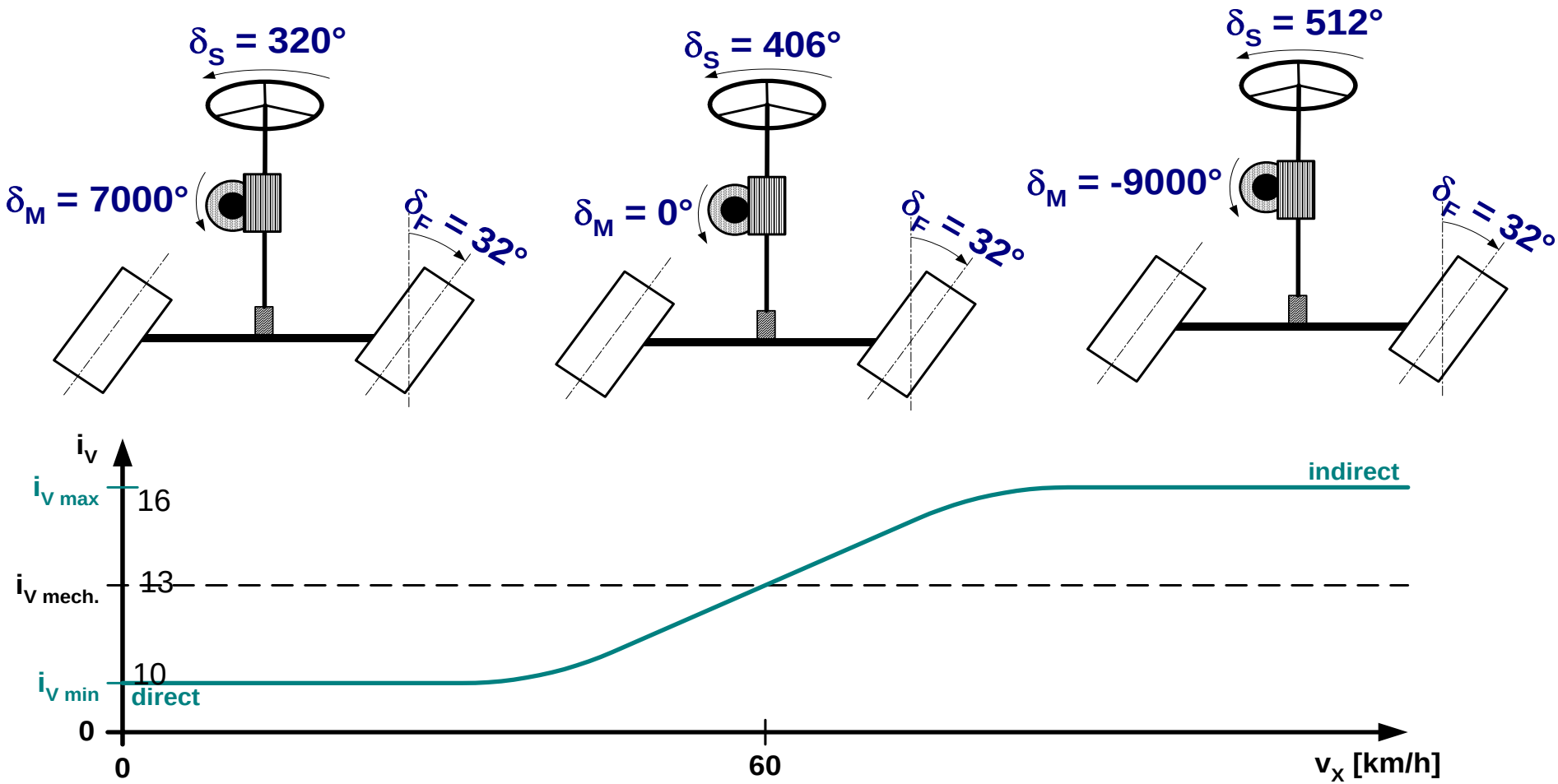
- Decrease steering effort in lower and middle velocity range.
- Indirect – safe - ratio at higher velocities.

Pinion & steering wheel angle

- High precision when driving straight
- Less steering effort for large steering angle (parking, ...)
- Modification of the steering behaviour (but same steering kinematics)

Active Front Steering - Variable Steering Ratio (2/2)

Example: steering ratio as a function of the vehicle velocity



ZF Lenksysteme

Different types of unintended behaviour

random:

hidden in
electrics, electronics, mechanics.

must be detected and **handeled** during runtime.

technical safety concept:

specifies approriate measures to detect and handle random faults/failures/errors.

explains, why these measures will lead to sufficient safety.

systematic:

hidden in
electrics, electronics, mechanics,
software, specifications
must be detected and **erased** before system gets into service.

safety development process:

supplies safety analysis of the system

derives **technical safety concept**

ends with proof of safety („safety case“)

Note: nature of unintended behaviour does not matter with respect to hazard/harm.

Drivers, goals & constraints

Drivers

- To acknowlegde the safety relevant nature of electronic steering systems (safety policy)
- Customer requirements within current projects
- ZFLS project Software development process
  Sub-goal: to derive safety requirements for the SW process

Goals

- To derive development process compliant to relevant safety standards that fits ZFLS‘s needs
- Based on experiences in former/current projects
- „Safety“ is a system level process with reqs to HW, SW, mechanics, sign-off‘s
- Create a company / group standard
- Valid for all products containing electrics, electronics, programmable electronics

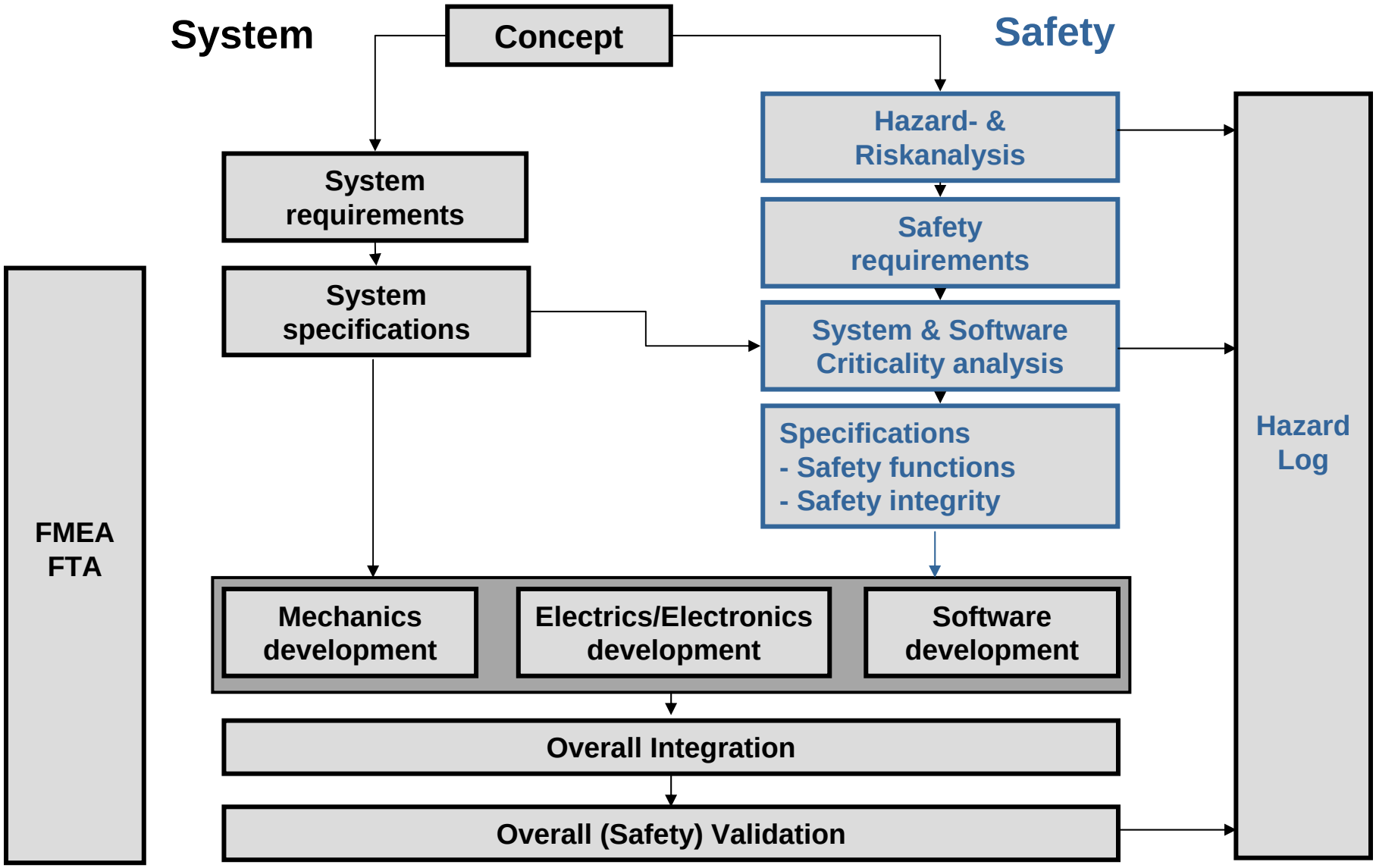
Constraints

- Aligns well with other processes, i.e. adds parts to existing processes rather than inventing a new one
- Flows down best practice form relevant standards.

Setting up the standard

- Collecting material from recent projects
- Lessons Learned
- Comparison to safety standards
- Alignment with existing ZFLS processes
- Internal/group review
- External review
- Sign off as preliminary company standard with two pilot projects

ZFLS - Safety related development process



ZFLS Safety related development process

Phases

- **Concept phase:**
  - System definition
  - Analysis of risks and hazards
  - Criticality analysis
  - Technical safety concept
  - Safety requirements specifications

- **Realisation phase:**
  - SW development process
  - HW development process
  - Verification & Validation
    - Vehicle testing programme
    - Rig test programme
    - Safety analysis: FMEAs, FTAs, Further measures

- **Production & Operation:**
  - Developement considers only the planning

Structure of the standard (1)

The standard talks about:

- Roles & Responsibilities
- Work packages of the life cycle
- Data Recording,Analysis and Corrective Action System (DRACAS)
- Interface to other processes
- Verification & Validation
- Milestones for projects
- Sign off‘s for prototypes
- Safety case
- Safety assessment
- suppliers

Structure of the standard (2)

Supporting documents to the standard

- Work packages safety programm plan SPP
- Hazard and risk analysis, criticality analysis, Hazard Log
- Safety Assessment
- Sign off‘s for prototypes
- Assessment of relevant standards
- Assessment of legislative documents
- Checklists, templates,...

- Relation to other company/group standards

New / revised elements (1)

Management activities

- Safety culture / safety policy
- Training & qualification

Safety programme plan

- Goal
  - Systematc planning of all safety related activities in a project
  - Basis for the safety case
- Contents
  - Resourcen, capacities, deadlines
  - Responsibilities
  - How to verify the result of a work package

Roles and Responsibilities

- Safety Manager (SaM)
  - Manager for sub-project „Safety“
  - Compiles ans tracks SPP
  - Interface to customer and suppliers
- Safety group (SaG)
  - Consists of: SaM (chair), project managers (system, SW,...), ISA
  - Approves work of SaM
- Independent Safety Assessor (ISA)
  - To be present for all projects
  - Must not have any other role in the projects
  - Level of independence prescribed by integrity level of the system

Key aspects of the talk

- Electronic steering systems are safety relevant systems.
- They can supply active safety (vehicle stabilisation) and definitely need functional safety.
- IEC61508 compliant develoment process in place at ZFLS, currently tested with pilot projects
- Good acceptance by customers so far.

Some references

ZFLS Active Front Steering Safety:

W. Reinelt, W. Klier & G. Reimann. System safety of Active Front Steering. at - Automatisierungstechnik (Oldenbourg Verlag). 53(1):36-43, January 2005

W. Reinelt et al. Active Front Steering (part 2): Safety and Functionality. SAE paper 2004-01-1101.

Safety related development process:

S. Amberkar et al. System safety process for by-wire systems. SAE paper 2000-01-1056.

W. Reinelt & A. Krautstrunk. Safety process for development of electronic steering systems. SAE paper 2005-01-0780.

Functional Safety Standards & automotive domain

M Woltereck et al. How to achieve functional safety and what safety standards and risk assessment can contribute. SAE paper 2004-01-1662.

BJ Czerny et al. Identifying and Understanding Relevant System Safety Standards for Automotive Systems. SAE paper 2003-01-1293.