2005-01-0780

Safety process for development of electronic steering systems

Wolfgang Reinelt, Alexander Krautstrunk
ZF Lenksysteme GmbH, Schwäbisch Gmünd, Germany

ABSTRACT

The safety related development process, currently in place at ZF Lenksysteme is outlined. The process model and its incorporation into the other development processes is described as well as roles and responsibilities. Particular focus is put on the derivation of the safety specifications. The latter procedure is highlighted with an example taken from the active front steering system, developed by ZF Lenksysteme.

INTRODUCTION

Electronically controlled steering systems for passenger cars such as electronic power steering [3], active front steering [1] or steer by wire [2] have significant impact on safety due to a possible unintended behaviour of the system. This has to be acknowledged during the entire lifecycle of the product. For steering system suppliers the particular focus is the development phase until start of production of the system. This contribution describes the safety related development process employed at ZF Lenksysteme in order to develop such a steering system in accordance to the relevant safety guidelines as well as other internal development processes such as software and electrics/electronics.

An overview of the workpackages, contained in the safety process will be given. Of particular interest are two itmes: Two main analyses have be carried out in the beginning: the first is the mapping of the system hazards onto risks of the vehicle level and the second is the mapping of faults, failures and errors onto the component level. These analyses are the hazard and risk analysis and the criticality analysis respectively. They are discussed and highlighted with an example taken from the respective analyses of the active front steering system.

Based on that, overall safety requirements can be derived, and on a more detailed level, also the specifications for safety functions of the components and their integrity. Another important source of requirements are those from safety standards such as [11,12,13] etc. Incorporating these requirements, the technical safety concept is developed. The example started in the above section will be continued here in order to derive specifications for a component of the active front steering system, in particular for a sensor.

Literature review: A system safety process for by-wire automotive systems has already been outlined in [6]: the key work packages and management tasks of a system safety process are discussed. Then some particular comments are made on system level risk analysis and the more detailed hazard analysis techniques. A safety programme is outlined for a steer by wire example on a quite generic level. Reference is made to [12]. This system level process is accompanied by a specific software process, outlined in [8].

[9] proposes a safety process with particular focus on distributed development (manufacturer-supplier). Using the development of an active front steeting system as an example, the hazard and risk analysis is discussed in some detail, trailed by derivation of safety requirements on a system level. Safety related management tasks are mentioned as well as interfacing development processes.

[7,9,10] give a good overview of relevant safety standards. Management standards discussed are [11,12,13] as system and management standards. Risk analysis standards such as [14] for a system level type of hazard and risk analysis are discussed, as well as standards for more detailed analysis methods such as FMEA and FTA.

DEVELOPMENT PROCESS

The ZF Lenksysteme safety lifecycle consists of three major phases: Concept, realisation and production & manufacturing. The first two phases are typically carried out by the Research and Development Engineering, the third by Production Engineering and Customer Service. The contents of the phases is:

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

Figure 1 aligns the safety specific measures with the other development activities. It is worthwile noting that at ZF Lenksysteme the safety activities are incorporated in the other development activities rather than they are separated out as an extra process.
Development processes in realisation phase are the same for both safety related and not safety related components. These processes are adopted to cope with the safety aspects.
Production & Operation Phase is only considered by planning actions to avoid hazards during assembly, operation and maintenance. Furthermore assembly tests are specified with the aim to eliminate the faulty units.
This paper discusses the concept phase in detail.

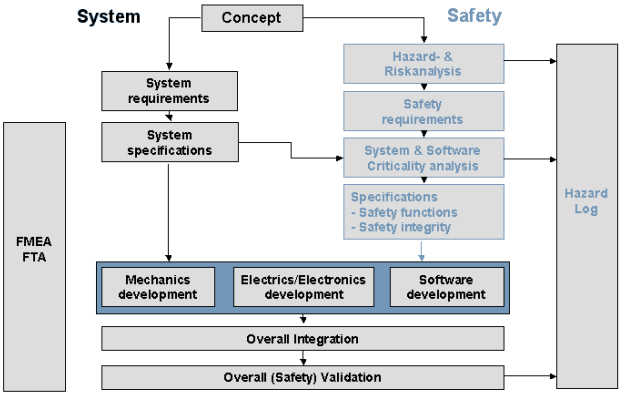

Figure 1 Development lifecycle including safety related activities.

SAFETY PROGRAMME PLAN

The work packages of the safety lifecycle have to be planned in detail in a safety programme plan (SPP). The deadlines, the required capacities and especially the responsibilities of the individual work packages have to be defined. The SPP is a management task the project manager has to agree upon.

The successful execution of the tasks of the safety programme plan is the basis for the safety case.

ROLES AND RESPONSIBILITIES

For the safety development process the following roles are introduced: safety manager, safety group and independent safety assessor.

The Safety Manager
- represents the subject “safety” towards the customers (automobile manufacturer), writes the safety statement of work with the customer as part of the contract,
- is sub-project manager for the sub-project „safety“
- makes the safety programme plan and supervises the execution of all analyses and actions, that are listed in the plan,
- carries out a risk assessment with respect to the safety of the product,
- collects and assesses all safety relevant information and supervises the realisation of corrective measures
- compiles a technical saftety concept,
- assesses changes to the draft concerning functional safety, before they are implemented,
- assesses the test programme (test rig, vehicle) concerning the requirements for the safety functions and the safety integrity

The Safety Group consists of:
- the safety manager (as chair),
- the sub-project managers for system, software and hardware (electronics) and if required, those sub-project managers, whose work influences the safety programme plan,
- the independent safety assessor.

The Safety Group moreover:
- appoints the independent safety assessor,
- authorises the technical safety concept,
- authorises changes to the draft concerning the functional safety, before they are implemented,
- authorises the test programme (test rig, vehicle) concerning the requirements for the safety functions and the safety integrity,
- releases the results of the safety assessment.

The independent safety assessor has to be appointed for each project. The degree of independency is regulated by the safety integrity requirements of the safety-related system. For pilot projects with higher requirements an external organisation is necessary, whereas for application projects an independent ZF Lenksysteme internal department is sufficient. The independent safety assessor:
- plans the activities for the assessment of functional safety and discusses this plan with the Safety Group,

- assesses the adequacy of the project´s safety programme plan,
- supervises the execution of the safety programme plan,
- assesses if the safety characteristics specifications are reached,
- assesses if the persons entrusted with safety subjects are sufficiently qualified,
- checks the admissibility of the safety releases,
- carries out a safety assessment and writes a report about it,
- reports directly to the project manager.
- is not allowed to take over any other roles in this project (in order to ensure the independency)

DERIVATION OF SAFETY SPECIFICATIONS

The route to the safety specifications consists of 5 stages, described in order of their appearance, possibly including some iterations.

SYSTEM DEFINITION

In this document, the functionallity as well as the safety functions on system basis are described and structured in logical blocks. Input and output of the single blocks are determined. Necessary components (ECU, sensors) are described functionally, references to certain details are made. The interfaces of the system are described on a logical and physical basis. The scope of the system as well as the interaction with other systems are described. Information about present safety regulations and legal regulations are obtained. Safety aims are described. The extent and the system boundaries for risk and hazard analysis are fixed.

Definition: safety function

The safety function is a „f*unction, being carried out by a safety related system in order to reach or to maintain a safe state for the EUC (Equipment und control), taking a fixed hazardous event into consideration*.“ [11] Referring to this definition, steering assistance functions are “safety functions” because they serve to maintain the safe state. All functions that help to reach the safe state form the second group of the safety functions. These functions are also called safety reactions.

HAZARD AND RISK ANALYSIS

The hazards of the system on highest level are identified and assessed. A connection to accidents on vehicle basis is made. The proceeding and the assessment criterions for the hazard and risk analysis have been agreed upon with the customer.

The result of the hazard and risk analysis, the risk classification with the help of Safety Integrity Levels (SIL), has a direct influence on the product and the processes that lead to the product and therefore on the product and development costs. For this reason the agreement with the customer about the risk classification is a must.

No particular methods are prescribed, but [14, 15] are recommended guidelines. The following requirements are posed:

- Determination of hazards and hazardous events under all reasonably foreseeable conditions
- Determination of sequences of events that can lead to hazardous events (accidents)
- Determination of the probabilities of hazardous events
- Determination of effects that are connected to the hazardous events
- Assessment of the risk of the hazardous events
- Determination of the necessary risk reduction for each hazardous event
- Documentation of the results

CRITICALITY ANALYSIS

Here, hazards on a system basis are connected with faults and failures of components (SW, HW etc) and a SIL is assigned to each component. The worst hazard on a system level will be sought for all possible component failures and therefore the integrity of the system`s safety function is mapped on the components. It directly serves as a plan for the technical safety concept, for the specification of safety requirements and for tailoring the development processes.

The procedure of the system / software criticality analysis is as follows:

- Determination of all safety functions of the Programmable Electronic System and the required safety integrity level (contents of the hazard and risk analysis)
- Structuring of the system in subsystems and units, description of the functions and interfaces
- Determination of malfunctions with their causes and implications
- Assignment of a SIL to each system component / SW-module, according to their contribution to the safety functions (The SIL of the safety functions is “inherited” by the contributing system components / SW-modules)
- Description of all diagnostic tests
- Determination of the diagnostic coverage for each component
- Determination of the critcality of the component (Does a malfunction of the component lead to an unsafe situation or are there any redundant safety functions to prevent such a situation?)

- If a redundant and independent safety function exists the SIL of the component can be reduced by one (according to [11])

It is quite effective to proceed backwards in the feedback control loop i.e. first the examination of the actuators, then the examination of the electronic control unit (ECU) and finally the examination of the inputs/sensors.

TECHNICAL SAFETY CONCEPT

The Technical Safety Concept serves to reach an understanding which measures or which combination of measures fulfil the functional safety.
The safety specifications in general allow a certain choice concerning the realisation. The technical safety concept makes this selection and gives a reason for the decision. In this argumentation it must be stated why this realisation fulfills the safety requirements on a system level. References to the criticality analysis and Hazard Log shall be made. The requirements for the components can be derived from here.

SAFETY REQUIREMENTS SPECIFICATION

The first aim of the Safety Requirements Specification is to specify the safety functions requirements and the safety integrity requirements, the second is to relate the safety requirements to the components.

AN EXAMPLE: SAFETY REQUIREMENTS FOR THE MOTOR ANGLE SENSOR OF AN ACTIVE FRONT STEERING SYSTEM

SYSTEM DEFINITION

Active Front Steering provides an electronically controlled superposition of an active angle to the steering wheel angle for passenger cars. Moreover control of electronically controlled orifice (ECO) valve and Servotronic unit are incorporated. Hence, this system combines the advantages of an electronically controlled superposition of an additional angle to the steering wheel angle with the reliability of a permanent mechanical connection between the steering wheel and the road wheels, cf. also [1] and Figure 2.

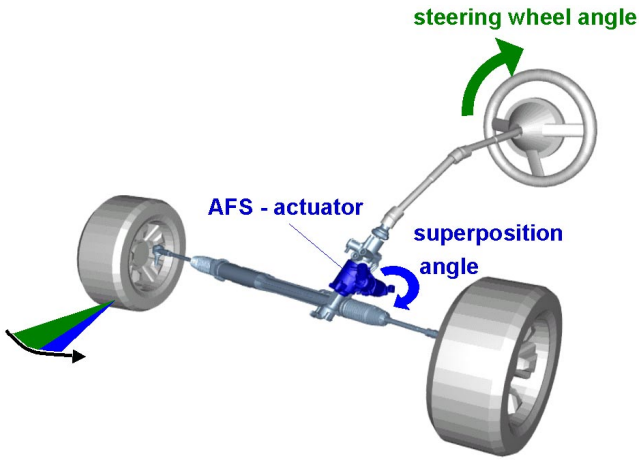

Figure 2: Principle of the angle superposition

The system contains the following electric and mechanic components (see [1]):

- Rack and pinion power steering system including the main gear, a Servotronic valve, a steering pump, and an oil reservoir with filter,
- Active Front Steering actuator including the synchronous motor with its respective electrical connections, the superposition gear system and the electromagnetic locking unit,
- electronic control system with the ECU, the pinion angle sensor, the motor angle sensor, the respective electrical connections of the ECU and the required software modules.

A system description also containing the safety specific parts has been used to carry out the safety analysis that is decribed in the following.

SAFETY FUNCTIONS, SAFE STATE, SAFETY REACTION AND HAZARDS

Obvious from the top-level description as given above, the system's safety function is:

- Angle superposition

- Transition towards "no angle superposition" state (safety reaction)

The safe state of the angle superposition is "no superposition", provided that the mechanical ratio of the steering system is safe in any vehicle state (in particular, speed). Consequently, the safety reaction is the transient behaviour from the "angle superposition 'on'" state to the "no superposition" state. Note, that is has to be confirmed that the safety reaction really is safe – in particular, this depends in the mechanical ratio, the variable ratio implemented and the vehicle itself. Based on this, the harzards arising from the angle superposition are:

- Angle superposition does not match to current driving situation; short: unintended actuator functionality

- System startup, i.e. transition from safe state back to “angle superposition ‘on’” state.
- Road wheel blocking.
- Hand wheel blocking.

CRITICALITY ANALYSIS: UNINTENDED ACTUATOR FUNCTIONALITY CAUSED BY FAILURE OF MOTOR ANGLE SENSOR

Give a hazard and risk analysis of the system’s safety function “angle superposition” (i.e. assessing the hazards listed in the previous sub-section), the task of the criticality analysis is to trace the SIL, assigned at system level, down to components. In this context, components are electric/electronic ones such als sensors or microcontrollers, as well as functions such as “vehicle speed calculation” which would then be mapped on e.g. a microcontroller and realised by software modules. As explained above, this will be done by tracing back the system level functionality backwards in the feedback control system.

This example aimes at assigning an SIL to the motor angle sensor as well as deriving the safety requirements based on this. The sensor used within the system is based on a magneto resistive principle and includes signal amplification and temperature compensation. It generates two analogue signals. For further details of the sensor, we refer to [4].

Fig.3 shows the position of the sensor inside the feedback control structure of the angle superposition safety function. The sensor is used for the feedback control of the motor, that moves the motor to the position desired by the variable ratio. Failures of the sensor could result in unwanted actuator functionalities, which is why the SIL of the safety function “angle superposition” is directly inherited by the motor angle sensor, cf. Fig.3.

Since the sensor generates two analogue signals, these can be monitored directly with respect to their amplitude, offset and radius. According to [11], these on-line monitoring measures can be claimed to have a “medium” diagnostic coverage. Hence the measures applied so far are not sufficient for the SIL assigned to the sensor, but only for the intended SIL less one.

According to the discussion above, the motor angle sensor including the analogue signal monitoring can be combined with a redundant and independent safety measure of the intended SIL less one to qualify for the SIL assigned to the sensor. Independence and sufficient diagnostic coverage of the safety measure in question has to be verified. Such a safety measure is described in [5]: based on signals independent of the motor angle, namely the motor’s currents and voltages, the actual motor position is estimated using filter techniques. Several methods can be used, for instance Lunenberger observers, based on a linear framework or extended Kalman filters, resorting to a non-linear system description. Accuracy and validated operating points have to be aligned with the safety concept. Independence of the above named measures, namely the sensor itself and on-line monitoring of the analogue signals, is reached by calculating the observer or filter on a different microcontroller.

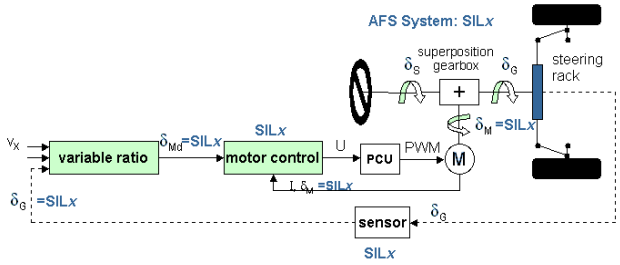

Figure 3 Example of a criticality analysis of an active front steering system.

Table A.14 – Sensors

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Idle current principle	A.1.5	Low	Only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC
Analogue signal monitoring	A.2.7	Low	
Test pattern	A.6.1	High	
Input comparison/voting (1oo2, 2oo3 or better redundancy)	A.6.5	High	Only if dataflow changes within diagnostic test interval
Reference sensor	A.12.1	High	Depends on diagnostic coverage of failure detection
Positive-activated switch	A.12.2	High	
NOTE 1 This table does not replace any of the requirements of annex C. NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding table A.1.			

Figure 4 Diagnistic coverage for safety measures for sensors according to [11, part 2, table A.14].

CONCLUSIONS

The ZF Lenksysteme safety-related development process has been described. Key elements of the process, that goes along with recognised safety standards are the proper roles and responsibilities as well as a consequent derivation of safety requirements top down from system analyses and requirements. The most important concepts for specifications of safety measures for components (hardware or software ones) – diagnostic coverage and independence – have also been highlighted by a practical example.

REFERENCES

1. W Reinelt, W Klier, G Reimann, W Schuster, R Großheim: Active Front Steering for passenger cars (part 2): Safety and Functionality. SAE Technical Paper 2004-01-1101. SAE World Congress. Detroit, MI, USA, Mar 2004.
2. W Harter, W Pfeiffer, P Dominke, G Ruck, P Blessing Future Electrical Steering Systems: Realizations with Safety Requirements. SAE Technical Paper 2000-01-0822. SAE World Congress, Detroit, MI, USA, Mar 2000.
3. H Köhnle: The Electromechanical Power Steering Systems of ZF Lenksysteme - Components, Function and Application. Paper F2004F293. FISITA World Automotive Congress, Barcelona, Spain. May 2004.
4. W Klier, W Reinelt: Active Front Steering for passenger cars (part 1):Mathematical modeling and parameter estimation. SAE Technical Paper 2004-01-1102. SAE World Congress. Detroit, MI, USA, Mar 2004.
5. W Reinelt, C Lundquist, H Johansson: On-line sensor monitoring in an active front steering system using extended Kalman filtering. SAE Technical Paper 2005-01-1271. SAE World Congress. Detroit, MI, USA, Mar 2005.
6. S Amberkar, JG D'Ambrosio, BT Murray, J Wysocki, BJ Czerny: A System-Safety Process For By-Wire Automotive Systems. SAE technical paper 2000-01-1056. SAE World Congress, Detroit, MI, USA. Mar 2000.
7. BJ Czerny, JG D'Ambrosio, PO Jacob, BT Murray: Identifying and Understanding Relevant System Safety Standards for Automotive Systems. SAE technical paper 2003-01-1293. SAE World Congress, Detroit, MI, USA. Mar 2003.
8. BJ Czerny, JG D'Ambrosio, PO Jacob, BT Murray, P Sundaram. An Adaptable Software Safety Process for Automotive Safety-Critical Systems. SAE technical paper 2004-01-1666. SAE World Congress, Detroit, MI, USA. Mar 2004.
9. C Jung, M Woltereck. Funktionssicherheits-konzept für die verteilte Entwicklung sicherheits-relevanter Systeme. VDI Conference Elektronik im Kraftfahrzeug, Baden-Baden, Germany. VDI Bericht 1789. Sep 2003
10. M Woltereck, C Jung, G Reichart: How to achieve functional safety and what safety standards and risk assessment can contribute. SAE technical paper 2004-01-1662. SAE World Congress, Detroit, MI, USA. Mar 2004.
11. IEC 61508: Functional Safety of E/E/PES Systems. International Electrotechnical Commission IEC, Geneve, Switzerland. Dec 1998.
12. MIL STD 882 D: System Safety Program Requirements. US Dept of Defense, Washington DC, USA. Feb 2000.
13. DS 00-56: Safety Management Requirements for Defence Systems. DEFSTAN. UK Ministry of Defence. Defence Procurement Agency, Glasgow, UK.
14. DIN V 19250 Vornorm: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. DIN Deutsches Institut für Normung e.V., May 1994.
15. MISRA - Motor Industry Software Reliability Association: Development Guidelines for Vehicle Based Software. MIRA, UK. November 1994

CONTACT

Dr. Wolfgang Reinelt, ZF Lenksysteme GmbH, EEMF Active Front Steering - Safety, 73527 Schwäbisch Gmünd, Germany, Phone: +49-7171-313110, Wolfgang.Reinelt@ZF-Lenksysteme.com

Alexander Krautstrunk, ZF Lenksysteme GmbH, EVE Advanced Engineering - Safety, 73527 Schwäbisch Gmünd, Germany, Phone: +49-7171-313674, Alexander.Krautstrunk@ZF-Lenksysteme.com