ACHIEVING FUNCTIONAL SAFETY OF AUDI DYNAMIC STEERING USING A STRUCTURED DEVELOPMENT PROCESS

Dr. Juergen Schuller*[1], Marnix Lannoije*[2], Dr. Michael Sagefka*[3], Wolfgang Dick*[4], Dr. Ralf Schwarz*[5]

**[1] Audi AG, I/EF-25, 85045 Ingolstadt, Germany, phone: +49-841-89-43759, email: juergen.schuller@audi.de*
**[2] Audi AG, I/EF-25, 85045 Ingolstadt, Germany, phone: +49-841-89-43780, email: marnix.lannoije@audi.de*
**[3] Audi AG, I/EF-25, 85045 Ingolstadt, Germany, phone: +49-841-89-42959, email: michael.sagefka@audi.de*
**[4] Audi AG, I/EF-25, 85045 Ingolstadt, Germany, phone: +49-841-89-40956, email: wolfgang.dick@audi.de*
**[5] Audi AG, I/EF-25, 85045 Ingolstadt, Germany, phone: +49-841-89-44519, email: ralf.schwarz@audi.de*

Abstract: Audi dynamic steering is a safety relevant electronic steering system. In order to achieve functional safety for this system a structured development process including all safety process aspects and several support processes have been defined and installed. Furthermore, the compliance of the implemented processes with the defined processes is strictly monitored by the internal quality assurance. Additionally, an external assessor is accompanying the product development in order to assure the functional safety of the product according to the requirements of international safety standards. Besides the enforcement of the processes, the challenge in this project is the coordination and monitoring of three suppliers together with the quality assurance and the external assessor. *Copyright © 2006 IFAC*

Keywords: safety, quality, processes, process models, requirements analysis, chassis control.

1. FUNCTIONAL SAFETY

Today the complexity and integration of electronic systems is continuously increasing in automotive applications, thus potentially increasing the risk for system failure or system malfunction. The goal of functional safety is to prevent hazards generated by an unintended behaviour of a system, thus decreasing the risk of system malfunction to an acceptable level[1]. For these safety relevant failures this acceptable risk level is called safety integrity level (SIL). In the only valid generic standard for functional safety (IEC 61508, 1998) four levels of safety integrity are defined, each being assigned a specific failure rate (failures per hour).

The safety integrity level of a system is determined with a risk analysis and is a function of the degree of damage caused by the failure, the probability of occurrence and the controllability of the system failure. The safety integrity measures which have to be implemented depend on the evaluated safety integrity level and are increasing with a higher SIL.

The safety integrity measures which are required in (IEC 61508, 1998) can be divided in 3 categories:

- functional safety management,
- development processes and
- product requirements for hardware and software architecture and safety integrity.

In this paper we will focus on the development processes.

In a letter to VdTÜV[2] (dated April 28, 2004), the VDA[3] stated that the generic standard for functional safety (IEC 61508, 1998) is not fully applicable for automotive industry, thus making it necessary to develop an application specific standard. Until the availability of the automotive standard, the generic standard (IEC 61508, 1998) can be only partially applied for the development of safety relevant automotive systems. This paper shows the adaptation of the normative process requirements to a safety relevant automotive system development.

[1] This level is not an absolute number but depends on the system and on social standards. The society usually accepts that technical systems fail at a certain (low) rate and cause damage without refusing to make use of the technique.

[2] German Association of Technical Inspection Agencies

[3] German Association of Automotive Industry

2. AUDI DYNAMIC STEERING

2.1 *System functionality.*

The principle of Audi dynamic steering is to superimpose an electronically controlled angle to the steering wheel angle in order to realise the following basic functionalities:

- increase steering comfort and vehicle handling at lower speeds by reducing the necessary steering wheel angle input of the driver and
- increase the driving safety at higher speeds by increasing the necessary steering wheel angle input of the driver, thus making the vehicle behaviour more tolerant to driver errors.

These basic functionalities can be realised with an algorithm called variable steering ratio, which is a characteristic diagram depending on steering wheel angle input and vehicle speed.

Additionally, the stabilisation of the vehicle is achieved with the same principle before the Electronic Stability Program (ESP) engages. This leads to a much more comfortable stabilisation (sometimes unnoticed by the driver) without deceleration, thus increasing the active safety of the vehicle.

2.2 *Safety integrity.*

A risk analysis has been performed using (Schwarz, 2005). The safety integrity level for all functionalities described in section 2.1 has been determined to ASIL D[4]. Unfortunately, the automotive specific standard for functional safety (Jung, 2005) is not published yet[5]; thus the requirements, which are associated with this safety integrity level, are not fully defined and not released. Thus, we have to refer to valid standard requirements of (IEC 61508, 1998) using a mapping of the automotive integrity levels to the standard safety integrity levels (ASIL D is similar to SIL 3).

Since it is sometimes difficult to apply the generic standard (IEC 61508, 1998) to automotive systems, Audi decided to make use of the know-how of TÜV[6] in order to interpret and adapt the normative requirements for this system development.

2.3 *System Architecture.*

Audi dynamic steering consists of the steering wheel angle sensor (LWS), the steering control unit (SCU), part of the ESP (ESP-DSA) and the actuator, see fig. 1; the electronically controlled orifice (ECO) adapts the hydraulic flow depending on the steering velocity generated by the driver and the dynamic steering system. The basic functionalities are deployed on the SCU, whereas the stabilisation functions are deployed on the ESP, called ESP-DSA. Audi is responsible for the whole system, whereas the suppliers are responsible for their delivered subsystem:

- SCU and actuator: ZF Lenksysteme GmbH;
- ESP-DSA: Robert Bosch GmbH;
- LWS: Leopold Kostal GmbH.

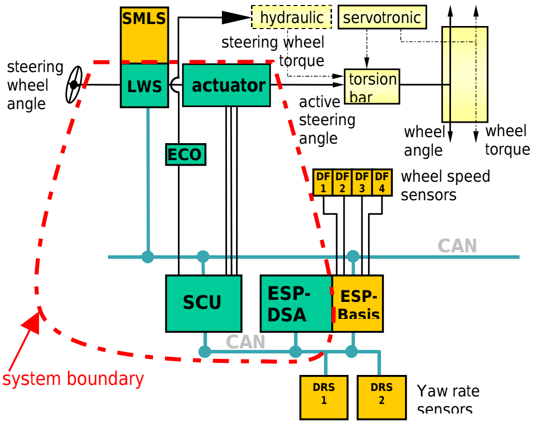

Fig. 1. System architecture of Audi dynamic steering.

3. STRUCTURED DEVELOPMENT PROCESS

The first step to a structured development process is the definition of a suitable process model. Several process models are known in literature (Eckrich, *et. al.*, 2002; Jung, and Woltereck, 2003; Reinelt, and Krautstrunk, 2005a) and used in practice. Also, (IEC 61508, 1998) proposes a process model for the safety life cycle of a product which consists of roughly four phases: concept, realisation, production and decommissioning. Here, we will focus on the realisation phase and discuss the defined process model.

3.1 *Process model.*

For the realisation phase the well-known V-model from software engineering (ISO/IEC 12207, 1995) has been adapted to this system development, see Fig. 2.

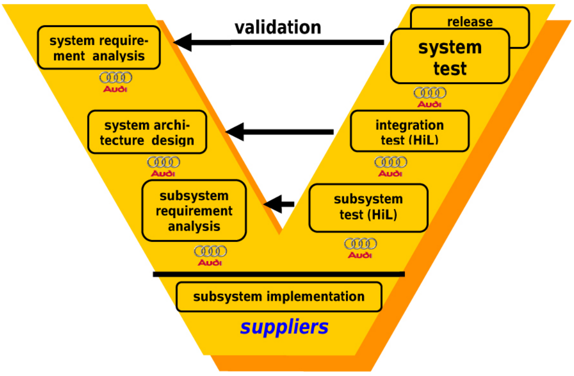

Fig. 2. Process model for the system development.

[4] FAKRA (Automotive Standard Committee in the German Institute for Standardisation) proposes 4 automotive safety integrity levels (ASIL), namely A, B, C and D, where D is the highest level.
[5] The final draft has been submitted to the ISO board but is not expected to become a standard before end of 2007.
[6] Technical Inspection Agency