Summary ISO 26262 seminar 2009-12-02

Type of document

Approved by	Date	Reg No.	
	2011-11-21		
Issued by	File	Issue	Page
Mattias Gudasic			1(4)
To	For information		

Scope

This document will go through the background for why a standard as ISO 26262 is needed, some of the chapters and areas in the standard and also how the standard will be used in the future within the automotive business globally.

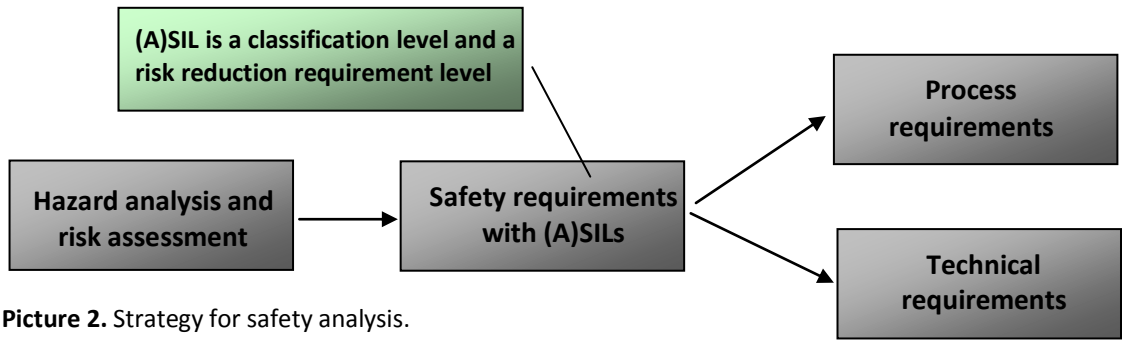
Background

An investigation made by WHO 1997 showed that traffic accidents caused as many as 4% of all deaths worldwide. Approximately 10% of these road accidents are caused by failure in technical systems, where E/E is a part of this.

Picture 1. Example of car accident with failure caused by failure in technical system.

Due to the fact that the technical complexity and integration complexity are increasing in today's vehicles, the need for a defined safety strategy for automotive business is growing. Also new annexes in **ECE legal requirements** has been added, where the OEMs are obligated and required to perform certification for braking and steering.

An overview of the strategy and working process to achieve a high functional safety for the automotive business can be seen in picture 2.



Picture 2. Strategy for safety analysis.

Summary ISO 26262 seminar 2009-12-02

KONGSBERG AUTOMOTIVE

Type of document

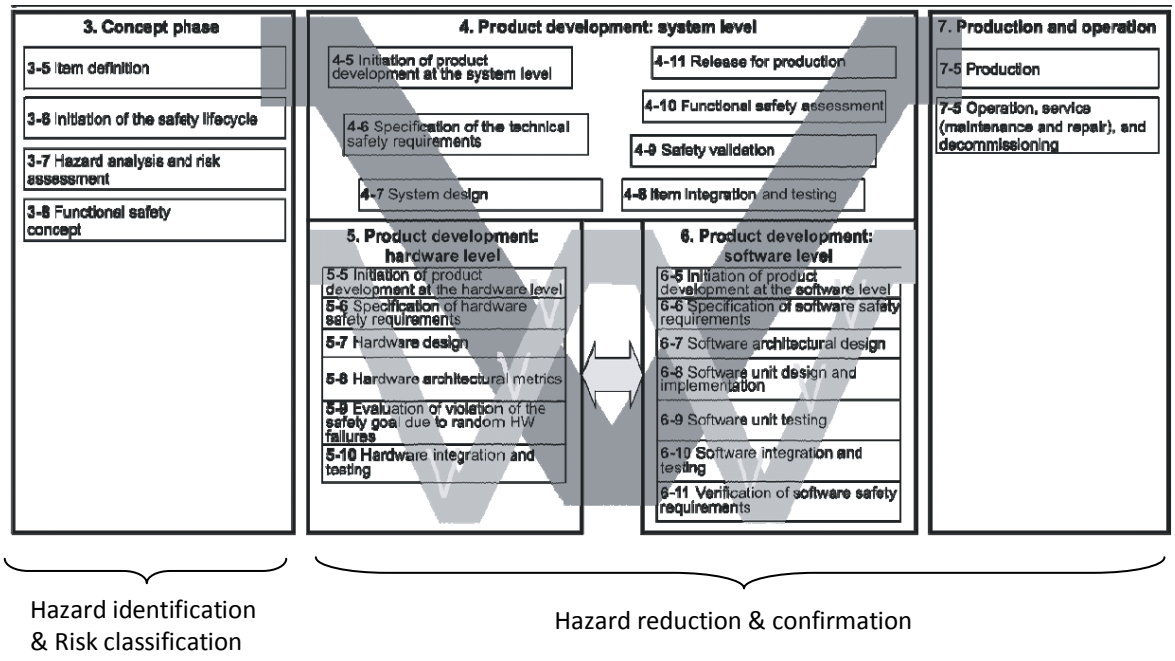
Approved by	Date	Reg No.	
	2011-11-21		
Issued by	**File**	**Issue**	**Page**
Mattias Gudasic			2(4)

ISO 26262

The ISO 26262 is the upcoming functional safety standard for the automotive industry, its release is planned to Q1 2011. It is applicable to all development of electrical and electronic systems that are related to safety. All major automotive OEMs and suppliers are active in this standardization effort. Main driver is German OEMs and suppliers. A majority of the automotive industry has already started working with the draft standard.

A safety lifecycle

Below, in picture 3, can be seen an abstract from ISO 26262 describing the working process for the safety procedure.



Output from the ISO 26262 safety lifecycle is a set of work products. A work product is a reference to the complete information concerning the results of associated requirements. It may be a document, a graph, a calculation sheet, a section in a document, a model or parts of a model.

For every hazard you identify, at least one safety goal should be defined. The safety goal is a top level product safety requirement that shall define how the actuator/function must **not** work. The ASIL and safe state are properties of a safety goal. From the safety goal you should be able to derive independent functional safety requirements and allocate them to logical components. This is called a functional safety concept and it includes allocation, partitioning, hardware and software interface descriptions etc.

Part 2 – Management of functional safety

The safety management during item development consists of the following areas

- Safety management

- Application of safety lifecycle
- Safety case
- Confirmation of functional safety

The safety management after release of production consists of the following areas

- A field monitoring process
- Someone responsible to maintain functional safety after SOP

Part 3 – Concept phase

The concept phase consists of

- Item definition
- Initiation of the safety lifecycle
- Hazard analysis and classification
- Safety goals
- Functional safety concept

The main purpose for this stage is to find the most critical hazards and to establish the required ASILs

Part 4 – Product development system level

The product development system level consists of

- Initiation of product development at system level
- Specification of technical safety requirements
- System design
- Item integration and testing
- Safety validation
- Functional safety assessment
- Release for production

The main purpose for this stage is to execute a design solution that complies with the required ASIL. This is done by using design guidelines (such as redundancy, monitoring system, checking functions, separate SW and so on) for safety critical products.

Part 5 – Product development hardware level

The product development hardware level consists of

- Initiation of hardware development
- Specification of hardware safety requirements
- Hardware design
- Hardware architectural metrics
- Evaluation of safety goal violation due to random HW failures
- Hardware integration and testing

At this stage the hardware design is established and tested. The hardware need to comply with the safety requirements regarding hardware. Methods that can be used are design walkthrough, safety analyses,

emulation by simulation and prototype hardware. An evaluation of safety goal violation should be performed, this done by investigating the failure rate for the component(s)/system.

Part 6 – Product development software level

The product development software level consists of

- Software development context and scope
- Software trends and safety
- Software development steps
    - Qualification of software components
    - Tools issues
    - Software safety analysis

Similar to part 5, the software design is established and tested. Design guidelines for software, safety analysis and methods for integration testing is performed.

Part 7 – Production and operation

Examples of required work products:

- Production control plan
- Documentation of performed control measures
- Assessment report for capability of the production process

Summary

The global automotive industry understands that there is a need of a standard that describes how to ensure a correct safety level for the electronics in a vehicle. The standard ISO 26262 is executed with all major car manufacturers globally involved, where BMW is one of the major driving force. So far only a draft version of the standard is released, but a non draft version is planned to be released during 2011.

The goal is also to introduce the ISO standard safety strategy as a requirement, for both car manufacturers and their suppliers, during 2011.