Introduction to ISO 26262
Functional Safety for Road Vehicles
Why should we discuss about functional safety?

- Safety is one of the key issues of future automobile development
  - in the area of driver assistance
  - in vehicle dynamics control and
  - active and passive safety systems

- Development and integration of these functionalities
  - needs a safe system development processes and
demonstration that all reasonable safety objectives are satisfied.
Why should we discuss about functional safety?

- **Society, customers, clients, government**
  - Have high expectations regarding the prevention of accidents and damage to the health of persons
  - Expect reduction of risk to a tolerable level

- **Manufacturers and distributors**
  - Want to satisfy the desires of their customers and of the society
  - Try to avoid loss of reputation caused by accidents
  - Would prefer to avoid claims for damages
Example safety functions in a modern car

- Adaptive front lights
- Anti-locking braking system
- Vehicle stability control
- Traction control
- Electronic brake force distribution
- Emergency brake assist
- Collision prevention
- Lane departure warning system
- Adaptive power steering
- Parking assistant
- Adaptive suspension control
- Electronic brake system
- Seat-belt pre-tensioning
- Airbags
- Driver drowsiness detection
- Driver monitoring system
- Adaptive high beam (lights) assistant
- Adaptive cruise control
- Autonomous cruise control
- Tire pressure monitoring system
- Automatic front light height adjustment
- …
Trends in safety systems in cars

- ABS
- Air bag
- Electronic stability control
- Adaptive cruise control
- Lane departure warning

Increasing complexity

Amount of software in cars

Lines of software source code


100.000.000
10.000.000
1.000.000
100.000
10.000
1.000
100
10
Functional safety standards for cars

- IEC 61508 – Functional safety of E/E/PE safety-related systems
  - Development started late 1980’s to address increasing complexity in safety-related systems
  - Initial demand from process industry
  - First version published in 1998
  - 2nd Edition published in 2010

- Why ISO 26262?
  - Automotive needs are rather different than those of machinery or process sector
  - Increasing complexity in automotive safety-related systems
    - Electronic stability control
    - Electronic brake assist
    - …
Why is a new standard for cars required?

- Common uncertainty about the interpretation of IEC 61508 for development, production and maintenance
- Safety lifecycles are different
- Restrictive requirements in IEC 61508
- Supply chains in the automotive industry are complex
- Differences in development technologies and methods
ISO 26262 is intended to be applied to safety-related systems which include one or more electrical/electronic (E/E) systems; and are installed in series production passenger cars with a maximum gross weight up to 3,500 kg.

ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

ISO 26262 does not address the nominal performance of E/E systems.
<table>
<thead>
<tr>
<th>Part 1 – Vocabulary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 2 – Management of functional safety</td>
</tr>
<tr>
<td>Part 3 – Concept phase</td>
</tr>
<tr>
<td>Part 4 – Product development at the system level</td>
</tr>
<tr>
<td>Part 5 – Product development at the hardware level</td>
</tr>
<tr>
<td>Part 5 – Product development at the software level</td>
</tr>
<tr>
<td>Part 7 – Production and operation</td>
</tr>
<tr>
<td>Part 8 – Supporting processes</td>
</tr>
<tr>
<td>Part 9 – ASIL oriented and safety oriented analyses</td>
</tr>
<tr>
<td>Part 10 – Guideline on the application of ISO 26262</td>
</tr>
</tbody>
</table>
ISO 26262 –
From idea to final product in five (large) steps

- Everything starts with an idea:
  - Your company wants to develop a better braking system
  - An existing design for lane departure warning needs modification
  - Existing product is too costly / difficult to manufacture / unreliable / ...
  - ...

- For complex systems, functional safety can be a factor if
  - Functional failure can lead to hazardous event
  - Loss of function can lead to hazardous event
  - Hazard analysis and risk assessment shows that **ASIL** is required

Functional safety required?
ISO 26262 –
From idea to final product in five (large) steps

- Next thing to do is to establish **functional safety management** for the development project

- This provides a framework to **coordinate and monitor all safety activities**
ISO 26262 –
From idea to final product in five (large) steps

- In order to know, what possible hazardous events need to be considered, it is necessary to perform hazard analysis and risk assessment.

- For each identified hazardous event, it will be necessary to define an associated safety goal:
  - How safe state is achieved or mainainted
  - What is the required ASIL

**Step 3**

**Hazardous event:**
Hans gets out of the cage

**Safety goal:**
Ensure that the cage door is not opened while Hans is awake

**Hans the Hungry Lion**
cute, but very dangerous
**Sidestep:**
ASIL? Never heard that one before…

- ISO 26262 introduces the Automotive Safety Integrity Level, **ASIL**

- Two key differences to Safety Integrity Level (SIL) as defined in IEC 61508:
  1. ASIL **does** implicitly determine the level of acceptable risk
  2. ASIL **does not** implicitly specify the requirements for probability of dangerous failure, $\lambda_{du}$

- ASIL is specified in one of four discrete levels:

  ![ASIL Levels](image)
  
  - **ASIL A**: Lowest safety integrity level
  - **ASIL B**: ASIL A
  - **ASIL C**: ASIL B
  - **ASIL D**: Highest safety integrity level
ISO 26262 – From idea to final product in five (large) steps

- Considering the identified safety goals, a safety concept is developed, which describes
  - Basic system architecture
  - Technical means to achieve and maintain safety

- The detailed system level, hardware and software design and development will follow the safety concept

- During design and development, necessary safety measures and verification activities are used

- Item is integrated, tested according to plan
ISO 26262 – From idea to final product in five (large) steps

- Safety validation is used to ensure that the developed item is suitable to fulfill the safety goals allocated to it.

- Functional safety assessment provides an additional level of confidence in the safety of the item, by considering both product and process aspects.

- Safety case provides the argument for the sufficient safety of the developed item, with suitable supporting evidence.

- Production and operation phase can start

- Monitoring of field data is required
Basic building blocks for functional safety

- Functional safety management
  - Who, when, what?
  - Competency management

- Safety lifecycle
  - System level, ISO 26262-4
  - Hardware level, ISO 26262-5
  - Software level, ISO 26262-6

- Verification and validation
  - At each lifecycle phase
  - For final product
  - Functional safety assessment

- Safety case
Functional safety management

- Overall functional safety management
  - Development and maintenance of safety culture
  - Definition of competency management
  - Definition of general safety lifecycle and processes

- Safety management during concept phase and product development
  - Allocation of resources, including safety manager
  - Planning and coordination of safety activities
  - Development of the safety case
  - Performing sufficient confirmation measures

- Safety management after release for production
  - Production monitoring
  - Maintaining field monitoring processes
Safety lifecycle model for development

**Concept phase**
- Item definition
- Initiation of the safety lifecycle
- Hazard analysis and risk assessment
- Functional safety concept

**Product development phase**
- Product development
  - System level
- Production planning
- Operation planning

**After start of production**
- Production
- Operation, service and decommissioning

- Hazard analysis and risk assessment
- Functional safety concept
- Production planning
- Operation planning

**Product development**
- Hardware
- Software

**Item definition**

**Initiation of the safety lifecycle**

**Functional safety concept**

**Production**

**Operation, service and decommissioning**
ISO 26262 – summary

- ISO 26262 will be published in late 2011
  - Describes **state-of-the-art** of functional safety design for automotive systems

- ISO 26262 is not currently references from directives, or other regulations
  - Non-compliance can still result in **product liability** issues

- Early preparation for the adoption of ISO 26262 is essential
  - Large number of **requirements for all aspects of product design, development and productions**
ISO 26262 – summary

- Functional safety management
  - Management of safety organization
  - Competency requirements
  - Safety culture is essential

- Technical requirements
  - Random hardware failures, architectural metrics
  - Systematic failures
  - Software development requirements

- Production and operation requirements
  - Production control, quality assurance
  - Field feedback monitoring, continuous improvement