“What is Functional Safety?“
- Short Introduction of ISO 26262 -

25 June 2015

Yuji ITO
TÜV SÜD (Thailand) Ltd.
Introduction of a speaker

Yuji ITO

Automotive Homologation Manager (ASEAN)
TÜV SÜD (Thailand) Ltd. from Jan. 2014.

History
1981 – 1999
Worked for vehicle manufacturer in R&D Div., in
charge of Engine Development.

1999 – 2013
Worked for TÜV SÜD Japan. Ltd.
- Founded Automotive group in 1999.
- Appointed as recognized Homologation Expert.
- Led homologation business and FS business as
well as many engineering support to OEMs.

Contact address
E-mail: yuji.ito@tuv-sud.co.th
TEL: +66-2564-7847 (Ext. 527)
<table>
<thead>
<tr>
<th></th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What's Functional Safety??</td>
</tr>
<tr>
<td>2</td>
<td>Overview of ISO26262</td>
</tr>
<tr>
<td>3</td>
<td>Part 2: Functional Safety Management. (Who should do what?)</td>
</tr>
<tr>
<td>4</td>
<td>Part 3: Concept Phase (how to handle Risks?)</td>
</tr>
<tr>
<td>5</td>
<td>Part 7: Production Process</td>
</tr>
</tbody>
</table>

**AUTOMOTIVE SUMMIT 2015**

24-25 JUNE 2015

BITEC, Bangkok

**2015-6-25 TUV SUD (Thailand)**
Car and Electronics

Current Situation

Trends in Automotive Electric/Electronics (E/E)

- Increasing functionality and complexity of software-based car functions
- Increasing risks from systematic faults and random hardware faults
- Most of the new car functions are safety-related
Trend of Car Electronics

No. of ECU installed in a car

1980’s : average 10

2010’s : 50-60

Car Electronics component market in the world
(extract from JARI, 2011)
Trend of a CAR

In the conventional vehicle, driver’s action was transferred mechanically, and the basic function (drive, stop, turn) was executed.

Now a day, driver’s action is converted into a signal, and is processed. And then it's transferred to the devices through harness. The signal is again converted into a force and used to control the vehicle.

<table>
<thead>
<tr>
<th></th>
<th>Conventional</th>
<th>recent</th>
</tr>
</thead>
<tbody>
<tr>
<td>structure</td>
<td>simple</td>
<td>complicated</td>
</tr>
<tr>
<td>Safety function</td>
<td>normal</td>
<td>upgraded</td>
</tr>
<tr>
<td>Probability of normal failure</td>
<td>normal</td>
<td>less</td>
</tr>
<tr>
<td>Unpredictability of failure</td>
<td>less</td>
<td>high</td>
</tr>
</tbody>
</table>
How SAFETY is important?

Safety First

Of course Safety is the most important. But 100% safety seems not possible due to technology, cost etc. There remains a risk of Danger.

We have to think “Acceptable Risk”. (FS Point 1)
What is Functional Safety?

Example of railroad crossing. How much is the probability of collision?

**Intrinsic Safety**
Root causes of danger are completely removed.

**Functional Safety**
By adding functional measures, acceptable level of safety is ensured.

Assessment of the “**functional measures**” (safety functions) and its **numerical evaluation** is the basis of Functional Safety.
In this standard (ISO26262), Functional Safety means, in case “safety related system” is composed with “electric/electronic/programmable electronic systems”, a way of thinking concerning a reduction of risk to an acceptable level.

ISO26262 only concerns a risk of danger which is caused by e/e/pe system. Risk caused by mechanical system is out of the scope of ISO26262. (FS Point 3)
What is the standard “ISO 26262”?

ISO 26262 is a Automotive Functional Safety standard focused on **series-production passenger cars up to 3.5 t**.

Major contents are:

1. In order to reduce risks occurred from electronic control system to acceptable level, what should be considered in the each step of development stage?

2. Clear definition of the risks and measures to reduce it
   - Risk analysis and countable evaluation of the measures etc.

3. **Whole company organization and management system** to realize it
   - FS organization, V-V model development etc.  

2\textsuperscript{nd} edition of ISO26262 will most possibly be published in Jan. 2018, and motorcycle and commercial vehicle will be included in the scope.
Regulation & Standard

Topics to be investigated

1. Legal requirements for homologation (mandatory)
   - Legally binding
   - Application of, e.g., EU directives and UN ECE regulations (Europe)

2. Product Liability (voluntary)
   - Recommended
   - Application of IEC, ISO, EN or DIN standards ("State of the art")

ISO26262 belongs to here \((FS\ Point\ 5)\)
Required Obligations to be followed

Example case:

One driver stepped on the accel. pedal and brake pedal at the same time by mistake. As a result, vehicle didn’t stop and accident occurred. A driver was injured.

Legally there is no regulation. (*) (except for some countries)
But if most of the people thinks braking function must be prioritized in such case, what happens in law suit?

State of the Art.

The term "state of the art" refers to the highest level of general development, as of a device, technique, or scientific field achieved at a particular time. It also refers to the level of development (as of a device, procedure, process, technique, or science) reached at any particular time as a result of the common methodologies employed.

(Extract from Wikipedia)
Structure of ISO26262

Management

Concept phase

System development

Hardware

Software

Supporting process

Safety analysis

Production & operation

1. Vocabulary

2-5 Overall safety management

2-7 Safety management after release for production

3. Concept phase

3-5 Item definition

3-6 Initiation of the safety lifecycle

4. Product development: system level

4-5 Initiation of development

4-6 Specific safety requirements

4-7 System design

4-8 Item integration and testing

5. Product development: hardware level

5-5 Initiation of product

5-6 Hardware architecture metrics

5-7 Evaluation of violation of the safety goal due to random HW failures

5-8 Hardware integration and testing

6. Product development: software level

6-5 Initiation of product

6-6 Software unit design and implementation

6-9 Software unit testing

6-10 Software integration and testing

6-11 Verification of software safety requirements

8. Supporting processes

8-5 Interfaces within distributed developments

8-6 Specification and management of safety requirements

8-7 Configuration management

8-8 Change management

8-9 Verification

8-14 Proven in use argument

9-5 Requirements decomposition with respect to ASIL hazards and hazard dependent failures

9-6 Criteria for coexistence of elements

10. Guideline on ISO 26262 (informative)
Part 2. Functional safety management and processes
Functional Safety Management

1. Construct Functional Safety Management (FSM)
   - FS manual, FS Plan,
   - Work rule, Training etc.
   - Documentation
2. Construct FS Organization responsible for realization
   - appoint FS manager
   - appoint FS assessors
These should cover whole company as well as each Dept.

same like QMS but focusing on FS
Documents

Work Product:
All kinds of documents and evidences which are related with the decision taken.

Safety Case:
• is the compilation of all documents and data that explains the product is functionally safe.
• The safety case can be derived from the work products of the development phases.
• The safety plan forms the basis for the safety case.
• The safety case is the key requirement for the release for production.

ISO26262 requests to store all kinds of documents so that the history can be traced to prove the safety.
Part 3. Concept phase
How to handle risks

Analyze driving situation and investigate risks
  • (HAZOP etc.)

Classification of risks
  • Severity, exposure and controllability

Define **ASIL** level
  • From risk matrix

Define **safety goal**

Hazard analysis and risk assessment review
Risk Parameters: Severity, Probability & Controllability

- **Probability of damage**
  - always
  - sporadically
  - low
  - very low
  - extremely unlikely

- **Severity S**

- **Controllability C of a dangerous driving situation**

- **Exposure E to the dangerous driving situation**

- **Acceptable area**
  - low
  - high

- **Inacceptable area**

- **Not accepted risk**

- **Accepted residual risk**

- **Tolerable risk**
## Hazard and risk analysis: parameter S (severity)

<table>
<thead>
<tr>
<th>Class</th>
<th>S0</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>No injuries</td>
<td>light and moderate injuries</td>
<td>Severe injuries, possibly life-threatening, survival probable</td>
<td>Life-threatening injuries (survival uncertain) or fatal injuries</td>
</tr>
<tr>
<td><strong>Reference for single injuries (from AIS scale)</strong></td>
<td>AIS 0 Damage that cannot be classified safety-related, e.g. bumps with roadside infrastructure</td>
<td>more than 10% probability of AIS 1-6 (and not S2 or S3)</td>
<td>more than 10% probability of AIS 3-6 (and not S3)</td>
<td>more than 10% probability of AIS 5-6</td>
</tr>
</tbody>
</table>

AIS: Abbreviated Injury Scale
Hazard and risk analysis: parameter E (exposure)

Estimation of exposure probability

<table>
<thead>
<tr>
<th>Class</th>
<th>E1</th>
<th>E2</th>
<th>E3</th>
<th>E4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Very low probability</td>
<td>Low probability</td>
<td>Medium probability</td>
<td>High probability</td>
</tr>
<tr>
<td>Definition of frequency</td>
<td>Situations that occur less often than once a year for the great majority of drivers</td>
<td>Situations that occur a few times a year for the great majority of drivers</td>
<td>Situations that occur once a month or more often for an average driver</td>
<td>All situations that occur during almost every drive on average</td>
</tr>
</tbody>
</table>
Hazard and risk analysis: parameter C (controllability)

<table>
<thead>
<tr>
<th>Class</th>
<th>C0</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Controllable in general</td>
<td>Simply controllable</td>
<td>Normally controllable</td>
<td>Difficult to control or uncontrollable</td>
</tr>
<tr>
<td>Definition</td>
<td>Controllable in general</td>
<td>99% or more of all drivers or other traffic participants are usually able to avoid a specific harm.</td>
<td>90% or more of all drivers or other traffic participants are usually able to avoid a specific harm.</td>
<td>Less than 90% of all drivers or other traffic participants are usually able, or barely able, to avoid a specific harm.</td>
</tr>
</tbody>
</table>
Hazard and risk analysis: risk

Assign an **Automotive Safety Integrity Level (ASIL)** to each hazardous event.

In case of QM, ISO 26262 requirements do not apply.

ASIL D is the highest level.

<table>
<thead>
<tr>
<th>Severity S</th>
<th>Probability E</th>
<th>Controllability C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>C1</td>
</tr>
<tr>
<td><strong>S1</strong></td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>QM</td>
</tr>
<tr>
<td><strong>S2</strong></td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>ASIL A</td>
</tr>
<tr>
<td><strong>S3</strong></td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>ASIL A</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>ASIL B</td>
</tr>
</tbody>
</table>
ASIL level

Risk must be a risk of vehicle. So, ASIL level must be defined by vehicle manufacturer.

In case ASIL level becomes high, probability of risk (injury / death) becomes high.

Severe and thorough countermeasures are required.
One example: Influence of ASIL level

Hardware architecture metrics:
Probability of detecting the following failure which violates achieving safety goal
- Single Point Fault Metrics (SPFM)
- Latent Fault Metrics (LFM)
Below percentage of failure has to be detected.

<table>
<thead>
<tr>
<th>Hardware Architecture metrics</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPFM</td>
<td>≥ 90%</td>
<td>≥ 97%</td>
<td>≥ 99%</td>
</tr>
<tr>
<td>LFM</td>
<td>≥ 60%</td>
<td>≥ 80%</td>
<td>≥ 90%</td>
</tr>
</tbody>
</table>

SPFM: Probability of detecting failure which single occurrence violates achieving safety goal
LFM: Probability of detecting failure which violates achieving safety goal latently

ISO 26262-5, Table 4 & Table 5
Part 7. Production and operation
What should be done in Production?

- **Production planning**
  - Planning of the production process
  - Development of production control plan

- **Pre-production series production**
  - Production of items, systems or elements before release for production

- **Production**
  - Production of items, systems or elements after release for production
Requirements on production

- Specify the requirements of production from the FS point of view.
- Develop a production plan for safety-related products.
- Ensure that the required functional safety is achieved during the production process.
For production process planning evaluate item and consider:

- Requirements for production
- Conditions for storage, transport and handling
- Approved configurations
- Lessons learned
- Competence of personnel

Create production plan including:

- Production process flow and instructions
- Production tools
- Traceability measures
- Special measures
  - e.g. labelling of element
  - e.g. burn-in test

Examples:
- e.g. calibration and setup of sensor
- e.g. allowed storage time for element
Other important points
Interface of diverse development

- Choose supplier
  - Confirm the development capability of supplier acc. to ISO 26262
  - Clear request to comply the standard by RFQ
    Development scope, safety plan, ASIL etc.

- 「Development Interface Agreement」ISO 26262 Part 8 Annex B
  - Confirm safety manager of both parties
  - Share the safety life cycle
  - Actual activity, process and responsibility of each side
  - Shared information and work product
TÜV SÜD provides the following functional safety services for the automotive industry:

**Certification**
- Product certification
- Process certification
- Generic Tool Qualification

**Testing**
- Assessments
- Supplier audits

**Consulting**
- Workshops
- Project-related support

**Training**
- Standard Basic Trainings
- Advanced Trainings
- FSCP
TÜV SÜD
Thank you for your attention.
Please let me know if you have any question.