TÜV Rheinland Industrie Service

Business Area:
**Automation / Functional Safety**

Contact

**Minsung Lee**

Sales Account Manager for Functional Safety

Phone: +82-2-860-9969
Mailto: minsung.lee@kor.tuv.com

Fax: +82-2-860-9862

www.tuv.com
As an international service group, we document the safety and quality of new and existing products, systems and services.

- founded in 1872
- 360 sites in 62 countries
- more than 14,500 employees
- 6 business sectors
  - 38 business areas and more than 2,500 different services
Applications Areas:
Automotive, Machinery, Process Industry, Oil & Gas, Power Plants, Nuclear Power Plants etc.
Services in Functional Safety

- **ISO 26262 Training**
  ISO 26262 demands that only experts may assess or manage Functional Safety. This training addresses System, Software and hardware engineers, managers responsible for the development and implementation of systems, software and hardware in a motor vehicle.

- **FSM Certification**
  It is a marketing argument to show the customer the quality of the development process.
  A certificated FSM System makes it unnecessary to do an assessment of the FSM at every single product assessment.

- **Consultancy**
  We can offer consulting support for all parts of ISO 26262 including HW / SW design as well as for the implementation of a FSM System in co-operation with qualified consulting companies.
Services in Functional Safety

- **Product assessment and certification**
  To prove the compliance of the product with the standard. It helps to show the freedom from negligence in case of product liability

- **Functional Safety Manager**
  We are supporting your Functional Safety Manager or taking over this role for specific projects, additional training and qualification is also available

- **Tool qualification**
  We support you throughout the whole process of tool qualification

TÜV Rheinland supports you with our services for Automotive to be in compliance with ISO 26262
More than 500 TÜV Rheinland „Functional Safety“ certificates have been issued worldwide.

More than 180 TÜV Rheinland certificates for safety-related products in power plants have been issued worldwide.
Automotive Clients
Example Projects

Projects before ISO 26262 was published

- Assessment of the fault control measures for a "trunk emergency de-lock" System
- Analysis of the safety concept of the EUCD Steering Column Lock System
- Validation of the MathWorks Real-Time Workshop Embedded Coder TM product with the Automotive Code Validation Suite (AVS) v4.0
- Several compiler validation
- Development tool Qualification (FPGA Design and development), also for ISO 26262
- …….
Example Projects

Projects after ISO 26262 was published

• Assessment of the power control for hybrid vehicles

• “Gap assessment report on a microcontroller unit for IEC 61508 Ed.2 and ISO 26262 compliance“, mainly for the development process

• Gap assessment of a R&D functional safety management process

• ………..
Current Situation in Europe

- Several European OEMs and Tier1 suppliers were involved in the creation of the ISO 26262 and are setting up their systems according the standard
  - BMW
  - Bosch
  - Volkswagen
  - ZF
  - ContiTeves
  - ...

- Tier1 suppliers are forced by the specifications of their customer (OEMs) to apply the ISO 26262 standard
- In the meantime most of these companies have set up their internal processes according the ISO 26262 for safety relevant designs
Current Situation in Europe

Which companies are also effected by the standard?

- There is a need on the market for ISO 26262 compliant tools, due to the requirement of tool qualification. Therefore tool vendor started activities to provide standard compliant tools.

- Safety mechanisms inside of MCU’s can support to fulfill the requirements of the ISO 26262. MCU manufacturers started to develop MCU’s for the use in ISO 26262 applications providing diagnostic like ECC for Flash / RAM, MMU, etc.

- Manufacturers of trucks, construction vehicles and motor bikes see the ISO 26262 as a chance to have a standard that is applicable for their areas (even if these areas are not in the scope of the standard)
What’s to do to implement ISO 26262 requirements

Our experiences with OEMs and Tier1 suppliers are;
Most companies developed also quite good systems in the pre ISO 26262 era.

- Well defined development model, usually according the V-model
- Well structured development processes
- Effective requirements tracking
- Collecting and evaluating of field data
- Extensive Verification / Validation activities
- Applying quality assurance measures ISO 9001
- Software development ASPICE compliant
- (Follow other Functional Safety standards)
What’s to do to implement ISO 26262 requirements

What are the biggest efforts for most companies?

- Showing that the internal Functional Safety Management is according to ISO 26262 standard
- Gaps in the design related to fault detection / fault control
- The calculation of safety related parameters (metrics)
- Setting up the SW architecture to fulfill interference freeness (how to fulfill ISO 26262 in an AUTOSAR architecture)
- Tool qualification
- Showing the competence of the team members
- Setting up the Safety Case
- Performing an audit and assessment that is recognized by the OEMs
What’s to do to implement ISO 26262 requirements

What does this mean in view of the implementation?

- It must not be changed everything
- Analyze the gaps in view of the standard requirements
- Define the safety life cycle phases
- Integrate the necessary additional measures into the existing system
- Develop the required documentation (safety case, work products, …)
Functional Safety Management

ISO 26262-2

Overall safety management:

- Defines a safety lifecycle model
- Is required to create and foster safety culture
- Defines responsibilities for safety for all relevant organizations
- Ensures necessary competence of personnel
- Ensures sufficient quality management activities
What is necessary concerning functional safety management?
Creating a safety culture

ISO 26262-2, 5.4.2

**Safety culture creating must start from the top management**
- Statement regarding safety policy
- Sufficient allocation of resources to maintain and support safety

**Examples**
- Nomination of dedicated safety manager with sufficient authority
- Policy which emphasizes safety over other aspects (deadlines, cost, ...)
- Escalation mechanisms for identified safety issues
- Necessary tools, templates, databases, human resources to maintain safety

Safety culture can be enhanced by periodic safety trainings
Functional Safety Management

For new developments of safety-related devices and systems as well as for system application, organisational and failure-avoidance measures have to be verified or validated repeatedly. It is advisable to integrate these measures fundamentally in the framework of a **Functional Safety Management System** within a company.

Auditors of TÜV Rheinland check acc. to the following certification procedure if a Functional Safety Management System has been integrated and applied accordingly.
FS Products

Services:
- Support in Hazard Analysis, Risk Assessment
- Gap analysis for products and FSM systems
- Assessment of Safety Concepts
- Safety analyses (FMEDA, FTA, …)
- Assessment of Applications, Safety Elements and SEooC
- Qualification of development tools
Safety Element out of Context (SEooC)

- **Safety Element out of Context** (SEooC)
  - A safety element for which an item (specific system, application, safety goal) does not exist at the time of the development.
  - A SEooC can either be a subsystem, a software component, or a hardware component.

Usually a microcontroller is considered as a SEooC.

- No defined safety goal
- Microcontroller alone (usually) **cannot perform a safety function**
- Still need support for functional safety

- A SEooC, which was developed in accordance to ISO 26262 is intended to be **reusable under given assumptions**.
Safety Element out of Context (SEooC)

- SEooC development can be seen as re-usable component development
- No knowledge of
  - System level hazards
  - Safety goals
  - Required ASIL
  - Functional safety concept
- These must be brainstormed based on expected use cases
- For an SEooC
  - Assume required ASIL
  - Assume possible functional safety requirements

Validation of SEooC occurs during safety validation of the final item, in which the SEooC is used.
The **TÜV Functional Safety Program** is a vocational qualification program for engineers, who work in the area of Functional Safety. **Trainings** are offered in cooperation with more than 12 international course providers. The following topics are offered:

- Safety Instrumented Systems (IEC 61511)
- Hardware/Software-Design acc. to IEC 61508
- Functional Safety of Machinery
- Automotive – System Design acc. to ISO 26262

Participants can obtain the following 2 qualifications acc. to their knowledge and Experience. By today more than **5,000 TÜV FS Engineers** have successfully participated in this program.
Course Provider of the TÜV Rheinland FS Program

Safety Instrumented Systems

- ABB
- ACM Automation
- TÜV Rheinland
- Honeywell
- Procept
- HIMA
- Invensys Operations Management
- Yokogawa
- RASC

ID: 3080/11 SIS FS Engineer

HW / SW

ID: 2798/10 HW / SW FS Engineer

Functional Safety of Machinery

ID: 2727/10 Machinery FS Engineer

Automotive

ID: 3000/10 Automotive FS Engineer

Qualification

TÜV Rheinland®
Preisely Right.
Automotive Training

- **Qualification Program for Functional Safety Engineer**

<table>
<thead>
<tr>
<th>Three years job experience in Safety</th>
<th>ISO 26262 Training</th>
<th>Exam</th>
<th>TÜV FS Engineer Automotive</th>
</tr>
</thead>
</table>

ID: 3812/11

TÜV Rheinland®

FS Engineer

We facilitate the safety competence for your engineers
Automotive Training

- **Functional Safety Manager** Responsibilities:
  - Driving the safety related processes
  - Creating the safety plan
  - Management of all functional safety work products
  - Steering the safety related activities in the projects
  - Moderating analysis sessions or performing safety analyses
  - Organizing reviews, audits and safety assessments
  - Interfacing with the customers and the suppliers for functional safety
  - Maintaining the safety case
  - Reporting to the project manager

We support your Functional Safety Manager in all his responsibilities or take over this role for specific projects
## Automotive Training

### Qualification Program for Functional Safety Manager

<table>
<thead>
<tr>
<th>Three years job experience in Safety</th>
<th>ISO 26262 Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ 1 day Functional Safety Management Workshop</td>
<td>ISO 26262 Exam including additional FSM questions</td>
</tr>
</tbody>
</table>

- **Execution of Safety Project in accordance with ISO 26262**
- Accompanied by TÜV Rheinland Safety Manager/Training on the job/Consultancy

We train your Functional Safety Manager to his responsibilities

---

TÜV Rheinland Qualified
Safety Manager in Automotive Projects

TÜV Rheinland
Precisely Right.
www.tuvasi.com

Find more information about our services at our website www.tuvasi.com and further details regarding:

- Time schedule for all Trainings
- Lists of all TÜV FS Engineers
- Lists of certified FS-products
- Overview of FS products and their safety-related parameters
- Information about FS events
- … etc.