Current status: draft, more content and context has to be provided.

Management of Functional Safety

# ISO26262: fundamentals

* Quality management should be in place before starting with ISO26262.
* (Automotive)SPICE is a very good step towards ISO26262. (Disadvantage: only for SW, System level, supporting processes) From level 2 or 3 you are ready for the ISO26262.
* Define baseline before starting implementing the ISO
* The baseline becomes part of the Safety Policy
* The biggest risks should be accounted for in the system phase by defining the System Concept with a quality as high as possible. (and as early as possible). This will eventually save time and money.
* A forced, immediate introduction of the ISO doesn’t work and will raise resistance of employees.
* Full compliance to ISO26262 would be very expensive (e.g. 1 million Euro). So, to become as compliant as reasonably possible a planned strategy over multiple years can be a realistic approach.

- Take special situations into account:

\* SME’s developing generically applicable systems, initially without specific OEM as customer

\* How to introduce functional safety in existing designs/architectures

* Try to integrate the ISO into the currently existing working process. Maintain the proven in use concepts of the company.
* An AFSE can help the Safety Manager to gain enough authority within the company.
* At least three people should sign important documents like the HARA.
* After TSC: First HW Safety Case, than SW Safety case. Define HW-SW system level requirements and HW-SW interfacing. Perform a pre-analysis.
* When defining a process step, also define the infrastructure and tooling.
* System level ready: check of work product by safety experts.

- Highlight two strategies: maintain speed and keep risks in mind (‘agile’) or define and freeze requirements in an early stage (‘waterfall’). In the ‘agile’ process, usage of explicit maturity levels of documents is good practice.

- Clearly define who is the targeted audience: SME orientation

# DIA

* It is possible to let the safety management be done by an external party. For example you can let your customer do it.
* Always use a DIA, Development Interface Agreement. Use the RASIC chart (Responsible Accountable, Support, Informed, Cooperation) to set up the DIA.
* SME’s usually don’t have a Safety Department, so use external parties (AFSE’s/AFSM’s) to advise/review. DIA is very important in this aspect!

# HARA

* Preliminary HW FM process (part 5, clause 8) covering large IC’s can be valuable for SME’s.
* At least three people should sign important documents like the HARA.

# Safety case

* Safety case contains all ISO26262 related documents, also i.e. e-mail and meeting minutes. All documents have to be signed.
* Have the safety case reviewed by external party so the review report can be handed to the customer. The advantage is that not all documents in the safety case (like FMEA or test procedures) have to be handed over to the customer: IP protection.
* All documents shall be signed and reviewed.
* All Safety Case document should be under configuration/Change management.

Hints and tips:

- RP should advise which maturity level WP's should have reached in different stages

- RP should help defining priorities. (due to limited amount of resources/hours)