COMPONENT INTEGRATOR’S CHALLENGES FOR ISO26262 COMPLIANCE
RICCARDO VINCELLI

- Joined Renesas in 2000 (at that time still Hitachi)
- Manager of the **Functional Safety Competence Centre** in Renesas
  - Cross-European team with locations in Germany and UK
- Responsible for safety analysis and technical safety assessments
- Covering HW (MCUs, SoC and MSIG) and SW products
- Acting as corporate advisor
  - Including corporate education (e.g. e-learning)
- Active in ISO-TC22-SC23-WG08 since 2005
  - Contributed to ISO26262 1st edition and now 2nd edition as well as ISO PAS 19451
RENESAS CONTRIBUTION TO SAFETY STANDARDISATION

- Very active within Standardisation Bodies being Member of: ISO, SAE, JSAE
- Strong Participation and contribution to Key Standards (ISO26262, ISO PAS 19451, SAEJ2980)
- Active in all following Groups related to Semiconductor aspects:

- **Basic Failure Rate**
  - Suitable FIT sources
  - Distribution of FIT

- **HW qualification**
  - “Complexity” issue
  - Applicability of ISO26262-8,13

- **Analog**
  - How to perform safety analysis on analog elements

- **Multicore**
  - How to cope with multiple cores including ASIL decomposition

- **Fail Operational**
  - Limitations in ISO26262 to cope with fail operational requirements?

- **Dependant Failure Analysis**
  - Applicability to digital elements
  - Applicability to analog elements

- **IPs**
  - Issues related to Intellectual Properties and Programmable Logic Devices

- **Fault injection**
  - Applicability to digital elements
  - Applicability to analog elements
ISO26262 OPTIONS FOR HW COMPONENTS SELECTION

- Can I use a COTS not necessarily developed for Automotive Applications?
  - Is the Component Functionality simple enough?
  - If so I can use through a “Safety Qualification”

- Can I re-use a Component from one of my previous Projects?
  - Do I have a Component meeting same Functional Requirements?
    - If so I can use it if I have enough Field Data to claim PIU

- Can I use a Component developed for Generic Automotive Applications?
  - This is related to development out of Context (i.e. SEooC)
  - Supplier is responsible for Capabilities of Component. Integrator is responsible for Suitability*

- Can I develop or request from my Component Supplier a Component based on my exact Spec?
  - This is a development “in-context”. Integrator has the main responsibility in terms of Safety Requirements*

* DIA shall be referred to in term of Responsibility

COTS: Commercial Off The Shelf
SEooC: Safety Element out of Context
PIU: Proven In Use
KEY OPTIONS OF IN AND OUT OF CONTEXT DEVELOPMENTS

OEM

Tier 1

Supplier x

In-Context

Requirements

System

Assumptions

Component x

Other suppliers

Supplier x

Partially in-Context

Requirements

Component x

Other suppliers

Requirements

Component x

Other suppliers

Partially in-Context

Other suppliers

Requirements

Component x

Other suppliers

Fully out-of-Context

Requirements

Component x

Other suppliers

Requirements

Component x

Other suppliers

Requirements

Component x

Other suppliers
**FOCUS ON SEoOC – COMPONENT SUPPLIER’S TASKS**

**Lifecycle**
- Selection of ISO26262 Process Requirements adopted for the Development of the HW Component

**Safety Concepts**
- Definition (Assumption) of Safety Requirements for the Development of the HW Component (including co-existence aspects, etc)

**Safety Analysis**
- Analysis of Component Safety Capabilities vs Safety Concept
  - Including Dependency Failure Analysis

**Metrics Computation**
- Compute Hardware Architecture Metrics (SPFM, LFM), PMHF/cut-set based on the defined Safety Concept

**Verification Reviews and Confirmation Measures**
- Perform applicable Verification Reviews, Confirmation Reviews, Safety Audit and Assessment (out of Context)

FOCUS ON SE00C – COMPONENT INTEGRATOR’S TASKS

Lifecycle

- Address Gaps in ISO26262 Process Requirements

Safety Concepts

- Understand Gaps in Safety Requirements and take required Actions

Safety Analysis

- Judge Impact of difference in Safety Concept on the Safety Analysis

Metrics Computation

- Compute Hardware Architecture Metrics (SPFM, LFM), PMHF/cut-set based on the actual Safety Concept

Verification Reviews and Confirmation Measures

- Take required Actions to bring Work Products received “in context”

CHALLENGES IN TERM OF METRICS COMPUTATION 1/5

- Just looking at the Architectural Metrics Computation several Challenges exist
- Integrator has to “Customize” several Parameters based on the required “Context”
  - Raw FIT rate
  - Elements related to the Safety Concept
  - Impact of Fault/Failures
  - Safety Mechanisms
Raw FIT rate (Independent from Safety Goal)

- Raw FIT used by the Component Supplier must be adjusted based on
  - Specific strategy adopted for the overall System/Item
    - Several options allowed by ISO26262
    - FIT provided by Component Supplier may reflect a different Strategy
  - Expected Mission profile
    - Parameters such as Temperature Cycles, on/off Period, etc influence FIT Value
    - FIT provided by Component Supplier will most likely not consider a Real Profile
Selection of SR Elements (required for each Safety Goal)

- A Component includes several Elements
  - Application Independent
    - Expected to be used in all Applications (representing the Core of the Component)
    - For these Elements Results could be re-used straight (but not always)
  - Application Dependent
    - Elements whose usage depends on the Particular Application
    - Integrator ought to compute Metrics based on the correct Elements used
    - This includes also the definitions of pins used
    ⇒ Mandatory as part of the Verification Reviews in ISO26262-5, 8 and 9
Adapt Impact of each Fault/Failures (required for each Safety Goal)

- Each Fault can be classified into 3 categories:
  - Directly Violating the specified Safety Goal
  - Violating the specified Safety Goal only in combination with one or other Faults/Failures
  - Never violating the specified Safety Goal
- Analysis provided by the Component Supplier is based on the Assumed Safety Concept
  - Depending on the Strategy a Conservative Approach may be adopted to ensure Wide Usage
- When considering the same Fault/Failures in the Context of the Final System Impact may differ
- Correct Classification is required as affecting Metrics and Safety Mechanism Strategy
Refine Safety Mechanisms (required for each Safety Goal)

- Safety Analysis must reflect the Actual Configurations adopted for the Safety Mechanisms
- Safety Mechanisms included in the Component Safety Concept can be
  - On-chip Safety Mechanisms (HW)
    - Configurability by Integrator possible in some cases
  - SW Safety Mechanisms
    - SW provided by the Component Supplier: Configurability by Integrator possible
    - SW not in responsibility scope of Component Supplier: Analysis provided may require significant Adaptations to reflect Reality
  - System Safety Mechanisms
    - Analysis provided may require significant Adaptations to reflect Reality

- Refinement may also be related to timing as well as coverage
RELIANCE ON FAULT INJECTION RESULTS

- Fault Injection allows to perform several Checks required to support Safety Claims
  - Systematic Faults
    - Verify Correct Implementation of Safety Requirements (e.g. Safety Mechanisms)
  - Random HW Faults
    - Check Impact of Faults
    - Check Fault Coverage
    - ...
- Fault Injection should not be considered as “the Solution” to all Problems
  - An Educated Strategy is required
  - When Fault Injection is used Implications/Risks must be clearly Understood
  - In many cases Fault Injection is not possible with the Current Status of EDA Tools due to lacking of suitable Fault Models
Most suitable Approach to verify Coverage depends on a number of Steps

Approach used should be justified and documented

Risks must be considered Independently of the Approach used

Especially when running simulations “out of Context” there is a risk that Results are not always Representative of an “in Context” Situation

Component Suppliers should clarify in their Work Products if Coverages provided represent

- A Reference Value – to be adjusted based on Final Application Details
- A Precise Value – to be used as is
CONCLUSION

- Functional Safety Compliance is a relatively new Challenge that the Automotive Community has to face
- Strategy to select Components and re-usability of Work Products is not trivial and must be carefully considered
  - Building up an Item Safety Case is not just a simple matter of adding up together all Evidences received
  - Proper “Customization” of results is required
- When using Simulation Results to quantify Architectural Metrics special considerations are required to judge dependency on the particular “Context” of Interest
Thank you for your attention!