Mastering Functional Safety and ISO-26262

Riccardo Vincelli, Functional Safety Manager
Takashi Yasumasu, Chassis and safety Manager

Class ID: 0C17I
Renesas Electronics America Inc.

© 2012 Renesas Electronics America Inc. All rights reserved.
Riccardo Vincelli

- Manager, Functional Safety Competence Centre
  - Renesas Electronics Europe

- **Current position**
  - Working since 2000 at Renesas Electronics Europe
    - Involved in safety activities since 2005 for development of Renesas components based on IEC61508 and ISO26262
    - Active in the standardisation process of both IEC61508 2nd edition and ISO26262. In particular contributed to ISO26262 both at national level in UK than at International level
    - Member of SAE J2980 safety group

- **Previous position**
  - Responsible for Development of Communication IP for Renesas Automotive MCUs
  - Member of ISO Standardization Groups for Data Communication
Renesas Technology & Solution Portfolio
Microcontroller and Microprocessor Line-up

### 2010

- **1200 DMIPS, Superscalar**
  - Industrial & Automotive, 65nm
  - 600µA/MHz, 1µA standby

- **500 DMIPS, High Performance**
  - Industrial & Automotive, 90nm
  - 250µA/MHz, 0.2µA standby

- **165 DMIPS, FPU, DSC**
  - Automotive, 40nm
  - 190µA/MHz, 0.3µA standby

- **1200 DMIPS, True Low Power**
  - Industrial & Automotive, 130nm
  - 144µA/MHz, 0.2µA standby

### 2013

- **1200 DMIPS, Performance**
  - Automotive, 40nm
  - 600µA/MHz, 35µA deep standby

- **350µA/MHz, 1µA standby**

- **500 DMIPS, Low Power**
  - Industrial & Automotive, 150nm
  - 190µA/MHz, 0.2µA standby

- **242µA/MHz, 0.2µA standby**
  - Industrial, 90nm

- **600µA/MHz, 1.5µA standby**
  - Automotive & Industrial, 65nm
  - 600µA/MHz, 1.5µA standby

- **165 DMIPS, FPU, DSC**
  - 165µA/MHz, 35µA deep standby

- **25 DMIPS, Low Power**
  - Industrial, 90nm

- **25 DMIPS, Capacitive Touch**
  - Industrial & Automotive, 130nm
  - 350µA/MHz, 1µA standby

### Key Features

- **32-Bit High Performance, High Scalability & High Reliability**

- **Engine, Meters, Chassis, Air Bags**
- **Preventive Safety, Car Audio, Body, HEV/EV**

© 2012 Renesas Electronics America Inc. All rights reserved.
‘Enabling The Smart Society’

- Cars and trucks clearly one of the biggest elements of the smart society – many dramatic innovations.

**Challenge:**
- How to develop these innovations safely and in full compliance with ISO 26262

**Solution:**
- *Renesas have extensive expertise in ISO 26262, a set of microcontrollers developed in compliance with the standard, and the expertise to assist customers in applying these microcontrollers*
Renesas experience in complying to ISO26262

- Our first experiences
- Gaining internal expertise
- Key challenges and the “IEC 61508 effect”
- Renesas approach toward functional safety
- How we planned Automotive MCU for ISO26262
- Conclusion
Our First Experiences
The first projects

- Renesas efforts to address faults has been always a priority
  - Zero defects our key policy for systematic faults
  - Minimal FIT our key policy for random faults
  - Involvement and promotion of solutions to address remaining risks our key strength
    - Renesas is always on the driver seat

- Renesas has always been a key supplier of solutions for safety applications

- With the emerging requirements for safety compliance Renesas invested since 2005 to have proven products
  - First priority: DCLS MCUs targeting IEC61508 SIL3 requirements

DCLS: Dual Core Lock Step
Px4 and SH7226

- Dual Core Lock Step MCUs for Chassis applications

SIL3 and ASIL D capabilities confirmed by TUV-SUD

Example of results achieved

- SFF > 99.84% (SIL3: >99%)
- PFH = 2.553 * 10^{-10} (SIL3: < 10^{-7})
Renesas contribution on standardisation

- 2005 → German national group for IEC61508
- 2005 → UK and Japanese national groups for ISO26262
- 2009 → International group for ISO26262
- 2011 → SAE safety working group
Key challenges and the “IEC 61508 effect”
Need for internal expertise

- Functional safety is a complex topic
- Functional safety standards are difficult to master

Further challenges

- ISO26262 can lead to multiple interpretations
- Many companies/consultants were (and still are) very much IEC61508 focused
  - But automotive has different constraints to consider
- Often concept of safety, availability and reliability are mixed up
  - “It must always work. Then needs to comply to ISO26262!”
- ISO26262 terminology is still often read with IEC61508 “eyes” leading to many misunderstanding. E.g.
  - IEC61508: Item is an element of the final Control System
  - ISO26262: Item is the final system at vehicle level

- In-house expertise is required to take right judgements
Understand own responsibilities

- ISO26262 addresses the complete product safety lifecycle
  - Each part is dedicated to a certain aspect of the lifecycle

• How to prepare a tailored program for Renesas?

Which part is relevant to Renesas?
Address the key challenges

Specifications misunderstanding
How to make sure specifications are clearly understood?

Safety Concepts
How to address gaps in applications knowledge to define right assumptions?

“The safety analyses shall be performed in accordance with appropriate standards or guidelines”
Which guidelines should be used?

Computation of HW metrics
ISO26262-9 8.4.1

Dependent failures
How to perform dependency analysis and overcome “Beta IC contamination”?

Interface to our customers
How to simplify selection of components for our customers?
How to flexibly adjust results to proprietary application profiles
Renesas approach toward functional safety
Creation of internal expertise

From learning …

- First exposure
  - Acquired initial background on safety requirements
  - Worked with market leaders in the area

- Gain of confidence
  - Exposure to system aspects
  - Selected a group of experts in Renesas to join ISO26262 and IEC61508 WGs

- Strategy definition
  - Definition of internal safety approach
  - Received acceptance from the market

- Biz as usual
  - Compliance as part of normal daily work
  - Continuing cooperation in ISO (and IEC) WGs to improve safety

… to mastering

- Single DCLS MCU for EPS
- MCU + ASIC solution for Airbag
- General
- All new products

Focus on IEC61508

Focus on ISO26262
First required enhancements

Functional safety requires to enhance
- Organisation
- Development flow

- Confirmation reviews &
- Technical Functional Safety Assessments
- Functional Safety Audits &
- Process Functional Safety Assessments
ISO26262 approaches for elements development and their relevance

An element can be

1. Already existing in the market (COTS)
   - Mainly standard components as sensor, etc
   - A (safety) qualification is required prior to use it

2. Already existing and PIU
   - E.g. used already in a very similar application for several years
   - Precise and accurate field data required to claim this class!

3. Developed specifically for the target item (“in context”)
   - Clear specification defined by the customer
   - ISO26262 shall be adopted as state of the art flow
   - Development also known as Distributed Development (DD)

4. Developed for more than one usage (“out of context” or SEooC)
   - The component developer try to address requirements from major target customers
   - ISO26262 shall be adopted as state of the art flow even if some deviations with respect to 3 applies

COTS: Commercial Off The Shelf  PIU: Prove In Use  SEooC: Safety Element out of Context
## ISO26262 tailoring for MCU and ASIC projects

<table>
<thead>
<tr>
<th>ISO26262 part</th>
<th>Applicability to MCUs</th>
<th>Applicability to ASICs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 – Management of functional safety</td>
<td>Applicable to both developments activities</td>
<td></td>
</tr>
<tr>
<td>3 – Concept phase</td>
<td>To be considered only to make reasonable assumptions at MCU level</td>
<td>Driven by our customers</td>
</tr>
<tr>
<td>4 – Product development at the system level</td>
<td>Mostly applicable</td>
<td>Different options possible</td>
</tr>
<tr>
<td>5 – Product development at the hardware level</td>
<td>Mostly applicable</td>
<td></td>
</tr>
<tr>
<td>7 – Production and operation</td>
<td>Mostly applicable</td>
<td></td>
</tr>
<tr>
<td>8 – Supporting processes</td>
<td>Mostly applicable</td>
<td></td>
</tr>
<tr>
<td>9 – ASIL oriented and safety oriented analysis</td>
<td>Mostly applicable but …</td>
<td>Mostly applicable but …</td>
</tr>
<tr>
<td></td>
<td>ASIL decomposition used to define assumptions</td>
<td>ASIL decomposition driven by our customers</td>
</tr>
</tbody>
</table>

Part 1 and 10 only containing informative requirements. Part 6 (SW) excluded in this presentation.
Renesas solutions for the key challenges

Specifications misunderstanding

- Simulation models of our MCUs available for early analysis

Safety Concepts

- Renesas is market leader in automotive for MCU, ASIC, ASSPs
- Thanks to WW marketing teams information are shared to define safety concepts

Computation of HW metrics

- Internal methodology created
- Full compliance to ISO26262 confirmed

Dependent failures

- Internal methodology available based on checklist approach
- New ISO26262 sub-group set-up to synchronise on approach

Interface to our customers

- Proprietary GUI created to estimate capabilities of our MCUs in customer profiles
Flexibility of Renesas GUI

Customer

Safety system analysis

Safety MCU analysis

MCU safety database

λAS, λAPP, λDCF, λLF

Flexibility of Renesas GUI

MCU development

Safety MCU development

MCU

ID | Fault Coverage settings | Ext WDT | EPS Loop | CAN Layer | SW Test (including MISG) | SPFM | LFM | SFF | PMHF
---|------------------------|---------|-----------|-----------|---------------------------|------|-----|-----|------
0  | yes, but any SM requiring SW action(ADC test, channel ID, ADC reg check) disabled | no | no | ro | no | 84.9227 | 94.5362 | 80.3328 |
1  | yes | no | no | no | yes | 84.9942 | 98.3186 | 83.5652 | 1.5988E-09 |
2  | yes | no | no | no | yes | 87.0116 | 98.7457 | 85.9201 |
3  | yes (Internal WDT not needed with Ext. WDT) | yes | no | no | yes | 94.2928 | 99.0551 | 93.4058 |
4  | yes | yes | no | yes | yes | 96.6426 | 99.0789 | 95.7515 |
5  | yes | yes | yes | yes | yes | 99.3593 | 99.9647 | 97.3248 | 8.3586E-11 |
6  | yes | yes | yes | yes | no | 99.117 | 99.8049 | 98.9237 |
Safety culture spread

- How to spread the safety culture within the company?
- Decision taken to create an internal e-learning program

A virtual guide takes each involved employee into the basics of safety with a description of their job role

A set of questions must be answered to complete the course
How we planned Automotive MCU for ISO26262
Takashi Yasumasu

- Manager for Chassis & Safety technical marketing
  - Renesas Electronics Corp. Automotive system div.
- Working since 1993 at Renesas Electronics
  - ex. Hitachi semi-conductor division and Renesas technology
  - Involved on safety activities since 2007 for Automotive
    IEC61508 SIL3 system solution by MCU plus ASIC
  - Active in the standardisation process of ISO26262. In particular contributed to ISO26262 part10 in Japan SAE
  - Member of Japan SAE Functional Safety WG group and JASPAR Functional Safety WG since 2009
  - Member ISO26262 WG16 semi-conductor WG from Japan
  - Technical Marketing leader for global Chassis & Safety application, Mainly responsible for the following MCUs
    - RH850/P1x series for Chassis
    - RH850/R1x series for Safety
Challenge for applying ISO26262 on MCU

- SEooC based development with assumed safety requirement for wide variety of automotive application

- Standard is changed from previous IEC61508 to ISO26262.
  - Similar, but there are differences for MCU
    - SFF for MCU vs. SPF/LF for item development
    - Beta IC table vs. Dependent failure analysis

- Necessity to implement the “State of the art” architecture with wide acceptance in the market
  - ISO26262 description is not concrete for the implementation of the safety mechanism

SEooC: Safety Element out of Context
SFF: Safe Failure Fraction
SIL: Safety Integrity Level

SPF: Single Point Fault
LF: Latent Fault
ASIL: Automotive Safety Integrity Level
Product Line ups for Automotive MCU
Wide variety of products for many application by 40nm MCU

*including SOC devices
Source: Strategy Analytics Jun/2012 & Renesas Estimate
Fundamental strength of RH850 series

Leading 40nm Flash MCU Process technology
Smallest Die size & Lowest Power consumption

Smallest Size

World smallest Flash MCU@40nm
40nm MCU is 25% die area of 90nm

40nm MCU

Lowest Power

<table>
<thead>
<tr>
<th>90nm Process</th>
<th>40nm Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>mA/MHz</td>
<td>mA/MHz</td>
</tr>
<tr>
<td>Competitor</td>
<td>RENESAS</td>
</tr>
<tr>
<td>(90nm)</td>
<td>(90nm)</td>
</tr>
<tr>
<td>2.81</td>
<td>1.08</td>
</tr>
<tr>
<td>(38%)</td>
<td></td>
</tr>
<tr>
<td>RENESAS</td>
<td>RENESAS</td>
</tr>
<tr>
<td>(40nm)</td>
<td>(40nm)</td>
</tr>
<tr>
<td>0.51</td>
<td>0.51</td>
</tr>
</tbody>
</table>

Our 40nm technology has enough capability to avoid power and size overhead for having H/W Safety Mechanism!
ISO26262 SEooC MCU Safety Life Cycle in Renesas

**Safety goal**

**Functional safety concept,**
(FSR, preliminary architectural assumption)

**Technical safety concept,**
(TSR, System design)

**Safety requirement**
Coming from each Application’s safety Concept is the key

**Gap analysis is necessary at integration in case of using MCU SEooC**

**MCU safety concept**

**MCU safety plan**

**MCU safety assessment**

**MCU testing and validation**

**HW safety Requirement**

**HW safety verification**

The accuracy of assumed safety requirement is the key
In case of SEooC

© 2011 Renesas Electronics Corporation. All rights reserved.
Safety requirement led by Safety concept

- To have more accuracy when defining safety requirement, we start with the safety concept with external measures
  - Assumed Hardware Software Interface
    - H/W, S/W requirement
  - Assumed External measures
    - Hardware: ASSP, ASIC
  - Assumed “system” Safety Goal and FTTI
    - FTTI for MCU

Example of the Safety Concept (EPS)

Example of the Safety Requirement

FTTI: Fault Tolerant Time Interval
## Assumed hazardous Event and ASIL

MCU FTTI: MCU fault tolerant time Interval

Notes: The information above is an example based on market survey by Renesas.

<table>
<thead>
<tr>
<th>Application</th>
<th>Hazardous Event Example</th>
<th>ASIL</th>
<th>MCU FTTI(1%)</th>
<th>RH850 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chassis</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPS</td>
<td>1. Self steer during driving</td>
<td>D</td>
<td>200us 1ms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Steering Wheal lock</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABS</td>
<td>One wheel lock during hard braking</td>
<td>C</td>
<td>1ms</td>
<td></td>
</tr>
<tr>
<td>Stability Control System</td>
<td>one wheel lock during driving</td>
<td>D</td>
<td>1ms</td>
<td></td>
</tr>
<tr>
<td>Booster (electrical Motor supporter)</td>
<td>one wheel lock during driving</td>
<td>D</td>
<td>1ms</td>
<td></td>
</tr>
<tr>
<td><strong>Passive Safety</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Airbag</td>
<td>Inadverted deployment during driving</td>
<td>D</td>
<td>10ms</td>
<td></td>
</tr>
<tr>
<td><strong>Active Safety</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mid Range &amp; Long Range Radar Systems (MRR/LRR)</td>
<td>Inadverted hard braking during driving</td>
<td>D</td>
<td>10ms</td>
<td></td>
</tr>
<tr>
<td><strong>Power train</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Powertrain</td>
<td>decreasing of engine torque</td>
<td>B</td>
<td>10ms</td>
<td></td>
</tr>
<tr>
<td>Transmission</td>
<td>speed down on express way</td>
<td>C</td>
<td>10ms</td>
<td></td>
</tr>
<tr>
<td><strong>Body</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Front beam</td>
<td>Both of front lamps turn off during night driving</td>
<td>B</td>
<td>10ms</td>
<td></td>
</tr>
<tr>
<td>Brake lamp</td>
<td>no brake lighting during braking</td>
<td>C</td>
<td>10ms</td>
<td></td>
</tr>
<tr>
<td>Meter</td>
<td>Wrong gear position</td>
<td>B</td>
<td>10ms</td>
<td></td>
</tr>
<tr>
<td>HEV/EV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motor control</td>
<td>Sudden torque Up/Down</td>
<td>C</td>
<td>TBC</td>
<td></td>
</tr>
</tbody>
</table>
Multi core strategy for performance and Safety

- High performance
- Real time operation
- Dual lock step architecture
- Cost and performance
- 1oo1D Architecture
- Fast time to detect the faults
- No latency for error detection
- Dual core lock step

Hybrid (DCLS plus single core)
- Engine Control, ADAS

Single Core
- Airbag/Body Central gateway

DCLS
- (Dual Core Lock Step)
- Braking/Steering Motor Control

Dual DCLS
- ADAS, Server
RH850/P1x Safety Mechanism outline

**CPU**
- Dual Core Lock Step
- Comparator
- Memory Protection Unit
- Logic-BIST
- Redundant DMAC/INTC

**Memory**
- ROM: ECC (SECDED), CRC Address Parity
- RAM: ECC (SECDED)
- M-BIST
- Address Parity
- EEPROM: ECC (SECDED)

**Others**
- Bus: End to End S.M.
- ECM: Control behavior at Error
- Clock Monitor
- Voltage Monitor

**Peripheral**
- 12 bit ADC:2 Self Test
- Timer: Output Monitor
- Input Monitor
- CAN: Parity on data
- Loop back

---

© 2011 Renesas Electronics Corporation. All rights reserved.
Safety mechanism for Application independent parts

Trying to have rich safety mechanism by hardware to achieve fast FTTI

- Standard MCU
- Error Correction
- Systematic Faults
- Built In Self Test
- Redundancy
- Clock Monitors

ECM

Common Cause

- Inverted signals
- 2-clock delay
- Layout Separation
- Power separation
- Cross talk analysis

- In-/Outputs
- Inputs
- Outputs
- Error
- Clock

Safety Block

Functional Block
Application dependent safety mechanism

*Application Dependent Part is to be analyzed by each Safety Goal*

**Input** → **Judge** → **Output**

**Braking**
- Wheel Speed Pulse
- Input Capture Timer
- PWM Timer
- Solenoid Control (PWM)

**EPS**
- Torque Sensor Motor current
- 12bit SAR ADC
- PWM Timer
- 3 Phase PWM output (U/V/W)

**ADAS**
- Vision Radar (LRR/MRR)
- High speed Serial ADC
- CAN
- Command via CAN

Application Dependent Part → Application Independent Part → Application Dependent Part

Application Dependent Part

© 2012 Renesas Electronics Corporation. All rights reserved.
## Safety Mechanism for Input and Output

<table>
<thead>
<tr>
<th>Assumed FTTI</th>
<th>Input</th>
<th>Output</th>
<th>Test Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brake</td>
<td>Timer (IC)</td>
<td>Timer (PWM)</td>
<td>(Input) TIMER INPUT MONITOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Output) PWM OUTPUT MONITOR</td>
</tr>
<tr>
<td>EPS</td>
<td>ADC Or Serial</td>
<td>Timer (PWM)</td>
<td>(Input) ADC Diagnosis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Output) PWM OUTPUT MONITOR</td>
</tr>
<tr>
<td>ADAS</td>
<td>CAN</td>
<td>CAN</td>
<td>(Input) CAN software protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Output) CAN software protocol</td>
</tr>
</tbody>
</table>

End to end protection by the combination of H/W and S/W
Test Pattern of on chip communication : Input

- Assumed Technical Safety Requirement
  - Timer (Input Capture) works correctly
  - Correct transfer to L-RAM

- Mission Logic
  - Timer (Input Capture)
  - Bus interconnect (Address/Data)
  - L-RAM

- Safety Mechanism (On chip comms.)
  - Hardware: TIMER INPUT MONITOR
  - Software: Read from Timer0 and 1

- Merit
  - E2E from Input to L-RAM (read after write)
  - Easy implementation into application program
  - Effective for Transient fault

L-RAM: Local RAM, tightly coupled RAM with Dual Core Lock Step
Test Pattern of on chip communication: Output

- Assumed Technical Safety Requirement
  - Timer (PWM Output) works correctly
  - Correct transfer to L-RAM

- Mission Logic
  - Timer (PWM output)
  - Bus interconnect (Address/Data)
  - L-RAM
  - CPU

- Safety Mechanism
  - Hardware: TIMER OUTPUT MONITOR
  - Software: Read from Timer input

- Merit
  - E2E from L-RAM to Timer Output
  - Easy implementation into application program
  - Effective for Transient fault

L-RAM: Local RAM, tightly coupled RAM with Dual Core Lock Step
Functional Safety Support for Renesas customer

- Concept FMEDA
  - Qualitative FMEDA
  - Metrics analysis
  - Sub part size information for FIT calculation

- Safety Manual
  - How to use safety mechanism
  - Recommendation of timing for application usage
  - Qualitative DC

- Work Products
  - SEooC based work products

To achieve easy verification
In system, work products is Prepared
- Assumed Safety Requirement
- Safety Analysis
- Safety Design … etc
Conclusion
Renesas support for your ISO26262 development

- Safety Hardware and Work Products
  - e.g. H/W Safety Mechanism by each product family

- Safety Software and Work Products
  - e.g. Core Self Test Software

- Independent Checks
  - i.e. Confirmation Measures done by our internal independent organization

- Safety Consultancy
  - e.g. Workshops, GUI tool
Questions?
Please Provide Your Feedback...

- Please utilize the ‘Guidebook’ application to leave feedback

or

- Ask me for the paper feedback form for you to use...