What functional safety module designers need from IC developers

Embedded Platforms Conference – Microcontrollers and Peripherals
Nov 9th 2016 – 14:50 – 15:30

TOM MEANY
This presentation gives a
- short introduction to functional safety
- What the IEC 61508 standard states as regards IC level requirements
- What IC suppliers and especially analog IC suppliers can do to make the job of module designers easier

It is assumed the audience
- Has a general interest in functional safety
- Wonders what an IC manufacturer could do to make their life easier
What is functional safety?

► Safety is freedom from **unacceptable** risk
  - Cars are dangerous but people choose to accept the risk because of the benefits of car travel
  - Similarly hot coffee, electricity, getting out of bed

► Different from intrinsic safety and electrical safety
  - Functional safety is to do with the confidence that a piece of equipment will carry out its task when required to do so
Sector specific standards

IEC 61508

IEC 61513
Nuclear Sector

IEC 61511
Process Industry

IEC 62061
Machinery

EN 50128
Railway applications

ISO 10218
Robots

IEC 61131-6
Programmable Controllers

IEC 61800-5-2
Variable speed drives

IEC 61513
Nuclear Sector

IEC 61511
Process Industry

ISO 26262
Automotive

EN 50128
Railway applications

IEC 62061
Machinery

ISO 10218
Robots

IEC 61131-6
Programmable Controllers

IEC 61800-5-2
Variable speed drives

Avionics
D0178,D0254

Machinery
ISO 13849

Medical
IEC 60601

Home
IEC 60730

Analog Devices for Embedded Platforms Conference Nov 9th 2016
According to IEC 61508 the “goodness” of a safety function is expressed as a SIL level
- Four levels each at an order of magnitude apart
- Other standards and other application areas use different measures which are approximately the same

Standards such as IEC 61131-6(PLC), IEC 62061(machinery), IEC 61800-5-2(variable speed drives), IEC 61511(process control), EN 50402(toxic gas sensors) all use the SIL terminology directly
The key 3 requirements for functional safety

- Hazard analysis tells us what safety functions are required
- The risk assessment says how “good” they must be – expressed as a SIL
- There are 3 key requirements
  1) Implement design measures to prevent introduction of systematic failures
  2) Have good reliability
  3) Be hardware fault tolerant
An enhanced development process is required for functional safety

- It incorporates the requirements of IEC 61508 which are relevant for an integrated circuit
FS Requirement 2 – have good reliability

- Expressed in terms of FIT – unit is failure per billion hours of operation
- ADI numbers based on accelerated life test available at www.analog.com/ReliabilityData
  - Many customers need numbers according to IEC 62380 or SN29500
    - To calculate the numbers requires information such as transistor count not typically available to module designers
- Calculated values can be given in a safety manual to accompany the datasheet
  - Need to also consider soft errors
Key ideas - Safe Failure fraction and Redundancy

IEC61508 has the metric SFF (safe failure fraction)
- What fraction or percentage of faults will cause a safety violation
- Either show the failure is safe, detected by a diagnostic or is mitigated using redundancy, SFF must be higher than 90% for SIL 2 and 99% for SIL 3

Redundancy is typically applied at the system level but under limited circumstances can be usefully applied on-chip.
Not all integrated circuits need to be certified

Options include

1) Develop to the standard existing non-safety process and leave functional safety to module designers
2) Develop to the standard existing non-safety process but supply a safety manual
3) Develop to the functional safety process ADI61508 and self certify
4) Develop to the functional safety process ADI61508 and get external certification
So how can IC designers help module designers
Help reduce the time to market and ease certification

► Provide safety and non-safety versions of the same product
  ▪ Allows the safety version of a module to be developed easily from the non-safety version
    ▪ Perhaps with additional components populated

► Supply of pre-certified components which can be treated as a black box during module assessment
  ▪ Avoid the “what will TUV say?” dilemma

► Supply of a safety manual with the important functional safety information

► Analysis of system architectures to provide complementary products at the system level

► Analysis of system architectures to make sure products have the right features and performance to be integrated in a system
A safety manual and its contents

► For a part following either the internal or external process a safety manual will “automatically” be produced
  ▪ But for other parts IC suppliers can still decide to produce a safety manual

► The contents of that safety manual will include
  ▪ The development process used to develop your part even if not IEC 61508 compliant
  ▪ The reliability predictions
    ▪ Die size, number of die, number of RAM cells, number of FF, transistor count
  ▪ The available diagnostics
  ▪ A completed Annex F checklist
  ▪ Evidence to support any claims of on-chip separation
  ▪ Details of any assumed system level diagnostics
  ▪ Summary results from an FME(D)A
  ▪ Any fault exclusions which can be claimed
Annex F of IEC 61508-2:2010

F.1 General

For the design of Application Specific Integrated Circuits (ASICs) the following techniques and measures for the avoidance of failures during the ASIC-development should be applied.

Table F.1 – Techniques and measures to avoid introducing faults during ASIC’s design and development – full and semi-custom digital ASICs (see 7.4.6.7)

<table>
<thead>
<tr>
<th>Design entry</th>
<th>Technique/Measure</th>
<th>Ref</th>
<th>See IEC 61508-7</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Structured description</td>
<td>E.3</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Design description in (V)HDL (see Note)</td>
<td>E.1</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Schematic entry</td>
<td>E.2</td>
<td>NR</td>
<td>NR</td>
<td>NR</td>
<td>NR</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(V)HDL simulation (see Note)</td>
<td>E.5</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Application of proven in use (V)HDL simulators (see Note)</td>
<td>E.4</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Functional test on module level (using for example (V)HDL test benches) (see Note)</td>
<td>E.6</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Functional test on top level</td>
<td>E.7</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Functional test embedded in system environment</td>
<td>E.8</td>
<td>R medium</td>
<td>R medium</td>
<td>HR high</td>
<td>HR high</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Restricted use of asynchronous constructs</td>
<td>E.9</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Synchronisation of primary inputs and control of metastability</td>
<td>E.10</td>
<td>HR high</td>
<td>HR high</td>
<td>HR* high</td>
<td>HR* high</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Design for testability (depending on the test coverage in percent)</td>
<td>E.11</td>
<td>R &gt; 95 %</td>
<td>R &gt; 98 %</td>
<td>R &gt; 99 %</td>
<td>R &gt; 99 %</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Modularisation</td>
<td>E.12</td>
<td>R medium</td>
<td>R medium</td>
<td>HR high</td>
<td>HR high</td>
<td></td>
</tr>
</tbody>
</table>

► Even if a part not developed to a functional safety process can complete the Annex F checklist
Provide IC FME(D)A with the information needed for the module level FME(D)A

### IC level FME(D)A

<table>
<thead>
<tr>
<th>Block</th>
<th>Area</th>
<th>FIT</th>
<th>DC %</th>
<th>Diagnostics</th>
<th>$\lambda_S$</th>
<th>$\lambda_{DU}$</th>
<th>$\lambda_{DD}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>10</td>
<td>5</td>
<td>99</td>
<td>CRC</td>
<td>2.5</td>
<td>0.02</td>
<td>2.48</td>
</tr>
<tr>
<td>Converter</td>
<td>50</td>
<td>25</td>
<td>90</td>
<td>Reference inputs</td>
<td>12.5</td>
<td>1.2</td>
<td>11.3</td>
</tr>
<tr>
<td>Reference</td>
<td>20</td>
<td>10</td>
<td>99</td>
<td>Comparison</td>
<td>5</td>
<td>0.05</td>
<td>4.95</td>
</tr>
<tr>
<td>Regulator</td>
<td>20</td>
<td>10</td>
<td>60</td>
<td>Power on reset</td>
<td>5</td>
<td>2.0</td>
<td>3.0</td>
</tr>
</tbody>
</table>

### System level FME(D)A

<table>
<thead>
<tr>
<th>Component</th>
<th>FIT</th>
<th>DC %</th>
<th>Diagnostics</th>
<th>$\lambda_S$</th>
<th>$\lambda_{DU}$</th>
<th>$\lambda_{DD}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>U₁</td>
<td>50</td>
<td>86.8</td>
<td>See safety manual</td>
<td>25</td>
<td>3.3</td>
<td>21.7</td>
</tr>
<tr>
<td>T₂</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R₁</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C₁</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L₁</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Safety function summary

- $\lambda_{DU}$: 3.3
- $\lambda_{DD}$: 21.7
- $\lambda_S$: 25
- $\lambda$: 50
- DC: 86.8

### IC summary

1. **$\lambda_{DU}$**: 3.3
2. **$\lambda_{DD}$**: 21.7
3. **$\lambda_S$**: 25
4. **$\lambda$**: 50
5. **DC**: 86.8
Give module designer options on diagnostics

- A module designer could use comparison
  - Doubles the cost, doubles the PCB area, halves the reliability and still subject to CCF (common cause failure) which limits its effectiveness

- OR could use an ADC with built in diagnostics for the IC itself and at the system level
  - CRC on the SPI, CRC on the fuses, CRC on the internal references, Ability to generate internal 0, +/-FS and +/-20mV inputs, ability to check its clock and its reference, transducer burnout current sources
Features to assist in implementing redundant architectures

- If using comparison as a diagnostic synchronization issues can look like an error
  - If the two ADC are not synchronized a step input can look like a difference and trip the system
    - A SYNC pin can keep the ADC synchronized

- Per device diagnostics are still important to localize the fault
Other options for diagnostics

► What if comparison is not possible due to area constraints?

► What if cannot stop conversions to do reference conversions?

► A part like the AD7770 solves the issue by providing a SAR ADC which is fast enough to convert all 8 channels albeit with lower accuracy
  ▪ The SAR ADC has a different architecture and its own interface to limit CCF
Assist in meeting reliability goals

► High level of integration to reduce component count
  ▪ Integrated diagnostics
  ▪ Integrated redundancy
  ▪ Combination of features into a single piece of silicon

► Transistors on a piece of silicon are very reliable
  ▪ Take two ICs with 50k to 500k transistors – FIT rate according to SN29500 is 67 FIT each => total is 134 FIT
  ▪ Take one IC with 500k to 5M transistors and the FIT rate becomes 78 FIT => a reduction in total FIT of up to 100%
Pretending to be a module designers highlights to the IC designer the information their customers need to design in integrated circuits

- Goal – make it easier to use ICs in a safety design

- It also helps answer the questions related to features on individual integrated circuits
  - e.g. should there be diagnostics on an isolated current sensor such as the AD7403
Features to support redundant architectures

► Often three options
  ▪ Standard safety - perhaps 1oo1
  ▪ High safety – perhaps 1oo2
  ▪ High safety and availability – perhaps 2oo3

► Issues include
  ▪ How two DAC can share the load
  ▪ How to achieve a safe state
  ▪ How to disconnect a failing unit
  ▪ How to recognize which is the failing unit
  ▪ How to synchronize if using comparison as a diagnostic
IC designers can help clarify the standards

Annex E of IEC 61508-2:2010 only covers “duplication” and only digital ICs

- What about divergent redundancy?
  - Such as a part with an ARM M4F and an ARM M0 core?
  - What about a DAC with an on-chip ADC as a diagnostic?
IC designers need to know enough to talk to module designers

The standard is large and complex, and its contents are not easily absorbed. ……
Moreover, it is generic in nature, meaning that it is not targeted at any particular applications, although the thrust of it is more appropriate for complex safety-related control systems in the process, nuclear, railway and similar industries than for non complex machinery control.

- IEC 61508 and similar standards are often described as “large and complex”
- In the past discussions related to functional safety began with a description of what was meant by SIL
  - IC designers need to understand PL, MooN, HFT, DC, SFF, PFH……
Summary
Meeting functional safety requirements is difficult for module designers

Silicon suppliers can partner to

- provide the necessary interpretation of the standards
- supply the data needed by module designers
- give features needed by module designers

Module designers need to talk to their IC supplier early to plan the architecture
The END
Extra slides