ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

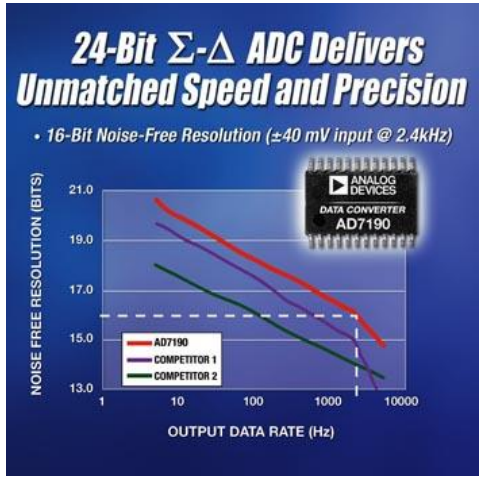
What functional safety module designers need from IC developers

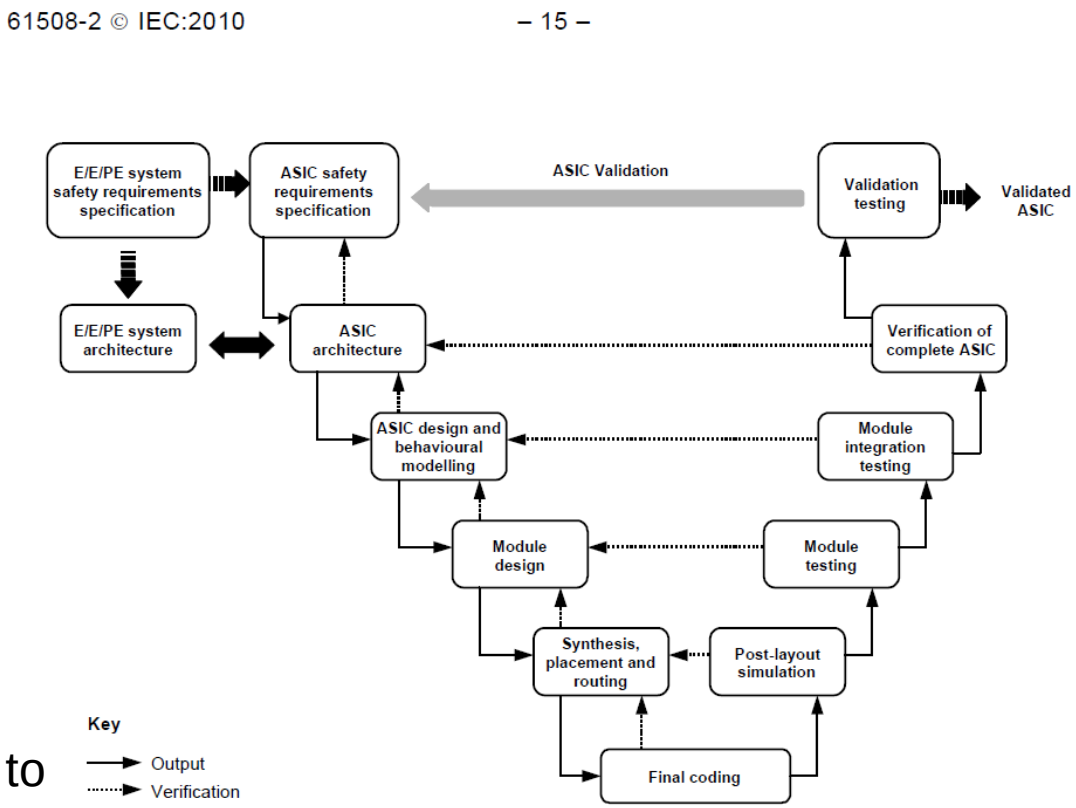
Embedded Platforms Conference – Microcontrollers and Peripherals
Nov 9th 2016 – 14:50 – 15:30

TOM MEANY

50 ADI 1965 2015

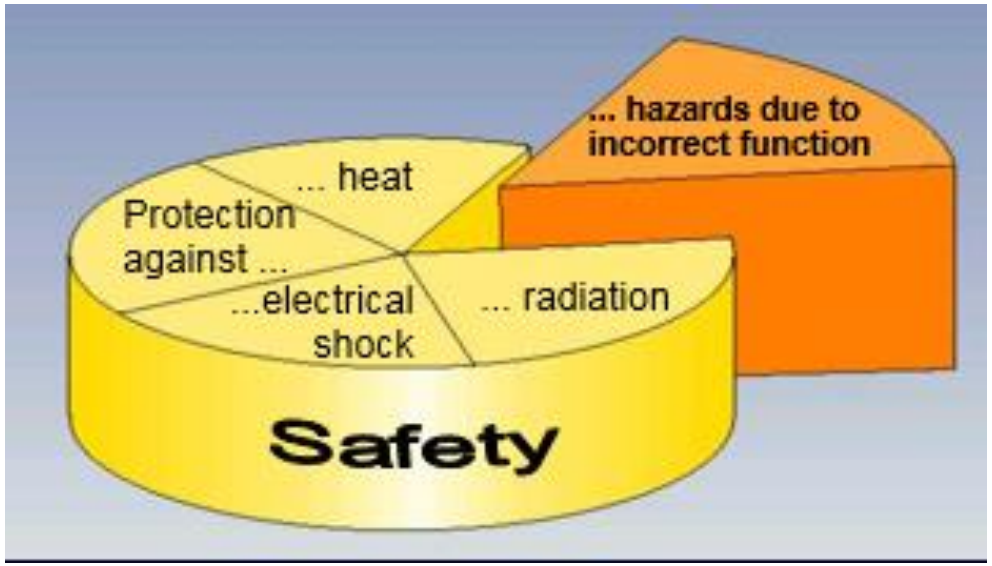
Introduction





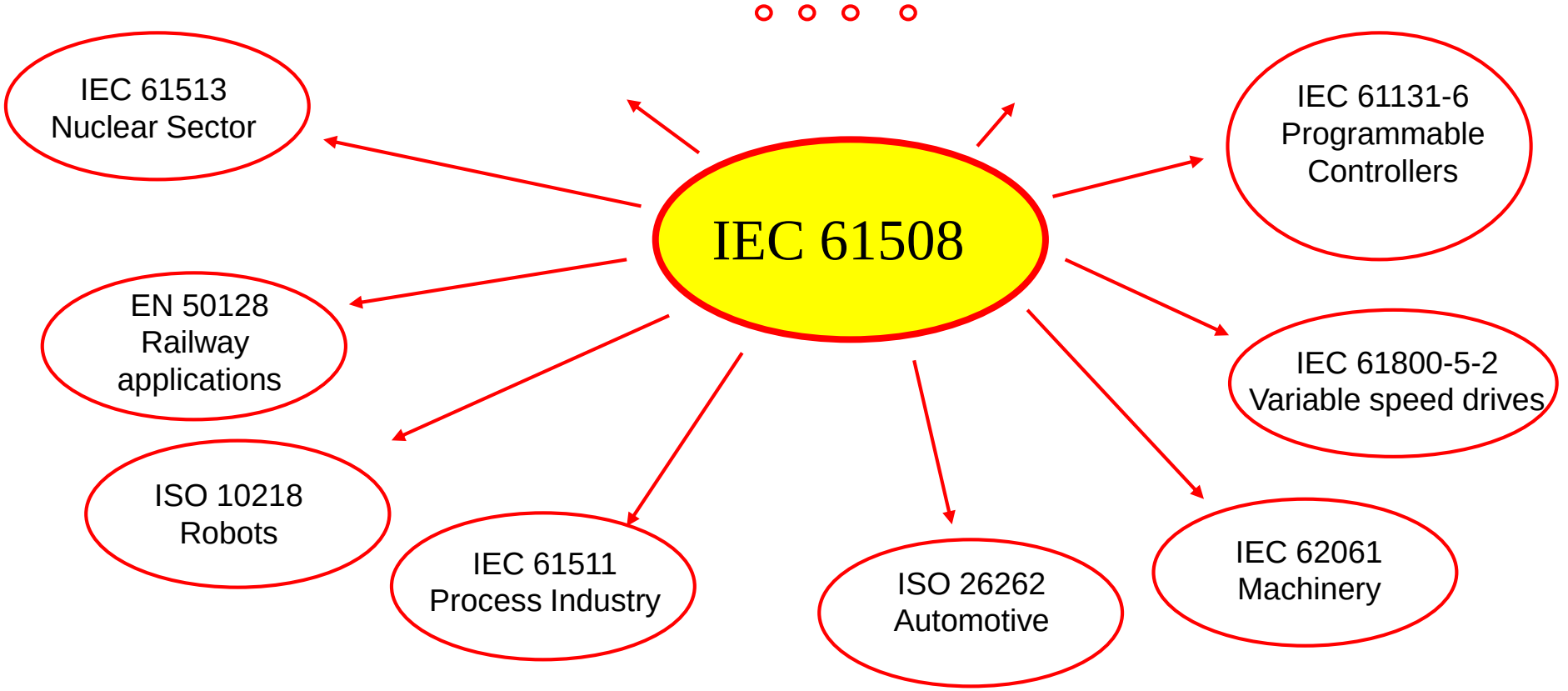
- This presentation gives a
  - short introduction to functional safety
  - What the IEC 61508 standard states as regards IC level requirements
  - What IC suppliers and especially analog IC suppliers can do to make the job of module designers easier
- It is assumed the audience
  - Has a general interest in functional safety
  - Wonders what an IC manufacturer could do to the 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

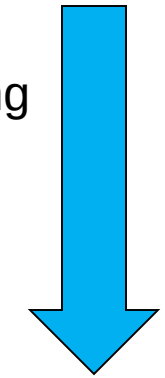
Sector specific standards



Avionics	Machinery	Medical	Home
D0178,D0254	ISO 13849	IEC 60601	IEC 60730

A Measure of safety

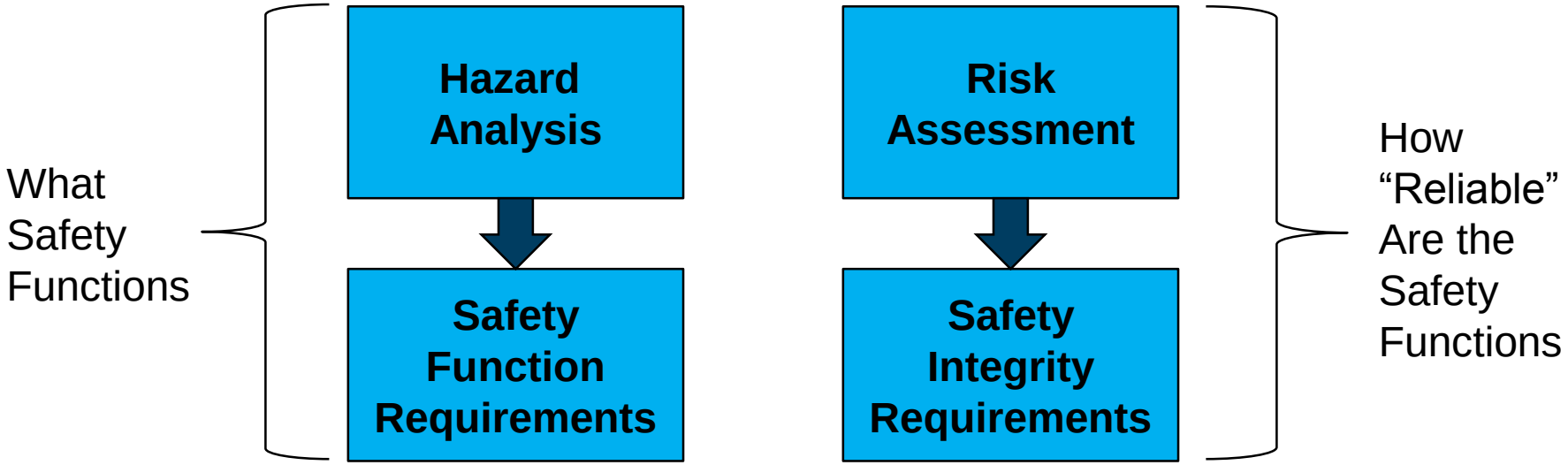
Increasing safety



IEC 61508 SIL	ISO 26262 ASIL	Avionics LEVEL	ISO 13849 PL	Nuclear Categories
1	A	D	b	A
2	B	C	|	|
3	C/D	B	|	|
4	-	A	e	C
			-	

- 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

FS Requirement 1 – an enhanced development process

Specification No: ADI61508 Rev. A
TITLE: Development Process for Functional Safety according to IEC 61508

REVISION HISTORY

Revision history for this document is located in adlib. Hard copy of this document, if not marked "CONTROLLED DOCUMENT" in red, is by definition uncontrolled and may be out of date. Downloaded copies of this document are also considered out of date.

TABLE OF CONTENTS

- An enhanced development process is required for functional safety
  - It incorporates the requirements of IEC 61508 which are relevant for an integrated circuit

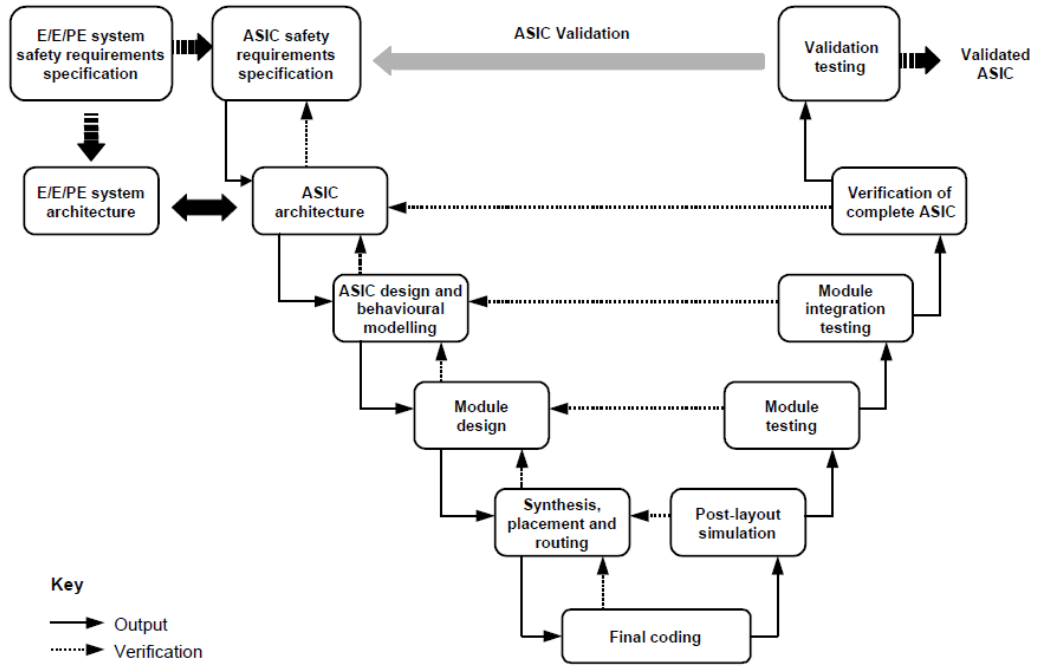
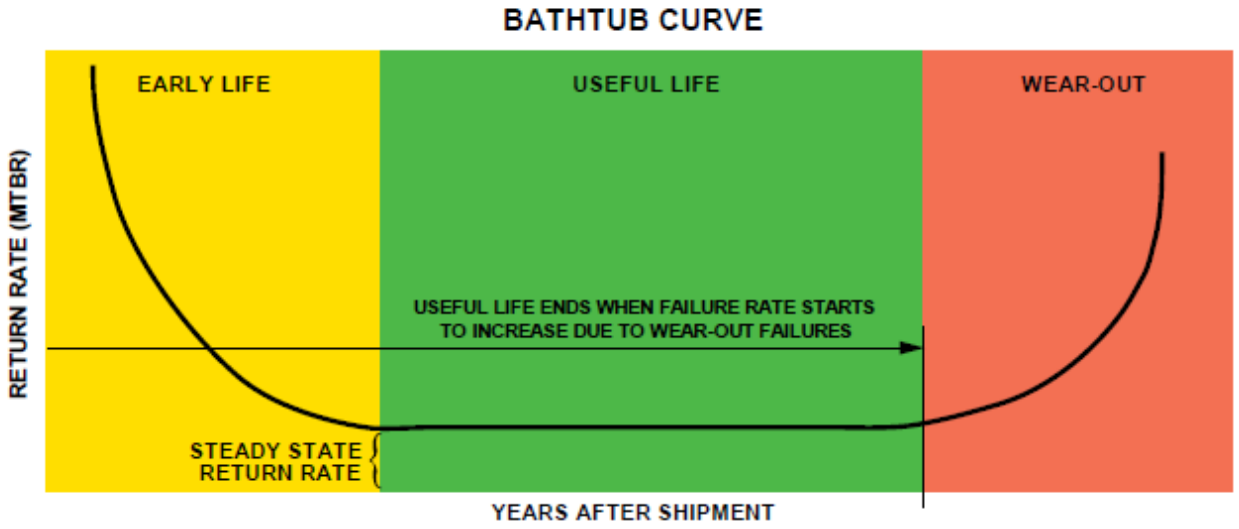


Figure 3 – ASIC development lifecycle (the V-Model)

FS Requirement 2 – have good reliability



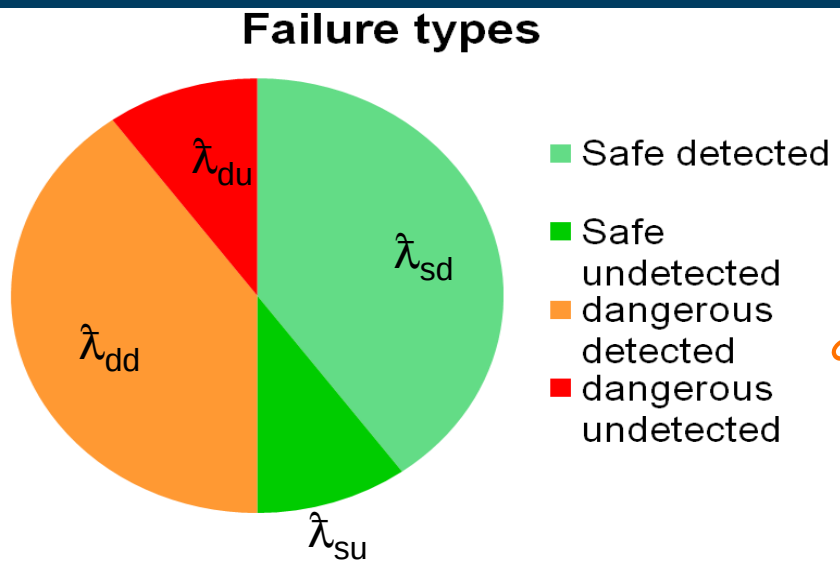
TR 62380 - 31 -

MATHEMATICAL MODEL :

$$\lambda = \left\{ \underbrace{\left(\lambda_1 \times N \times e^{-0.35\times a} + \lambda_2\right)}_{\lambda_{die}} \times \left\{ \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}} \right\} + \left\{ \underbrace{2.75\times10^{-3} \times \pi_\alpha \times \left(\sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0.68} \right) \times \lambda_3}_{\lambda_{package}} \right\} + \left\{ \underbrace{\pi_I \times \lambda_{EOS}}_{\lambda_{overstress}} \right\} \right\} \times 10^{-9} / h$$

- 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

FS requirement 3 -Metrics for fault tolerance



SFF estimates what percentage of faults are safe or detected HFT means it can operate despite faults

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

- 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

Specification No: ADI61508 Rev. C
TITLE: Development Process for Functional Safety according to IEC 61508

REVISION HISTORY

Revision history for this document is located in adlib. Hard copy of this document, if not marked "CONTROLLED DOCUMENT" in red, is by definition uncontrolled and may be out of date. Downloaded copies of this document are also considered out of date.

TABLE OF CONTENTS

- 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

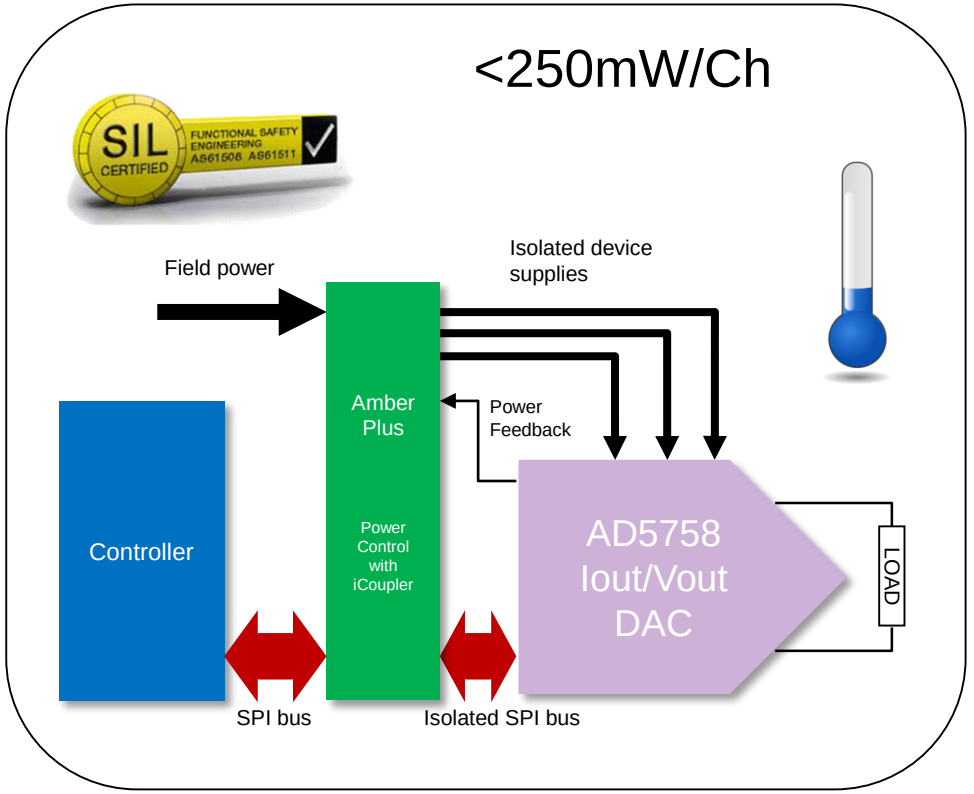
ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

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

ANALOG DEVICES

ADuCM360
Safety Manual
ADI Confidential

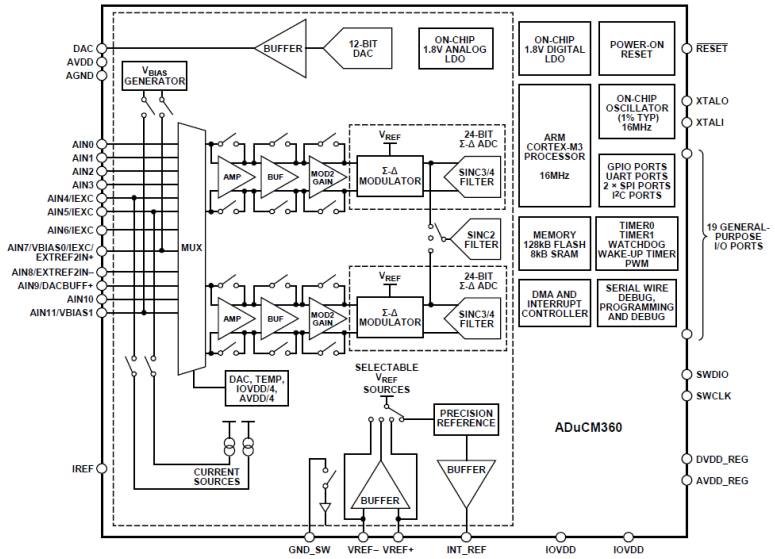
One Technology Way • P.O. Box 9106 • Norwood, MA 02062-9106, U.S.A. • Tel: 781.329.4700 • Fax: 781.461.3113 • www.analog.com

SCOPE

This Safety Manual provides information to facilitate integration of the ADuCM360 into a system with functional safety requirements according to IEC 61508 or ISO 13849.

AUTHOR/APPROVERS

Document Author	Role



Annex F of IEC 61508-2:2010

Annex F
(informative)

Techniques and measures for ASICs – avoidance of systematic failures

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.

NOTE 1 This informative annex is referenced by 7.4.6.7.

NOTE 2 The following techniques and measures are related to digital ASICs and user programmable ICs only. For mixed-mode and analogue ASICs no general techniques and measures can be given at the moment.

- Even if a part not developed to a functional safety process can complete the Annex F checklist

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)

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

Provide IC FME(D)A with the information needed for the module level FME(D)A

IC level FME(D)A

Block	Area	FIT	DC %	Diagnostics	λ_S	λ_{DU}	λ_{DD}
Interface	10	5	99	CRC	2.5	0.02	2.48
Converter	50	25	90	Reference inputs	12.5	1.2	11.3
Reference	20	10	99	Comparison	5	0.05	4.95
Regulator	20	10	60	Power on reset	5	2.0	3.0

IC summary

λ_{DU}	3.3
λ_{DD}	21.7
λ_S	25
λ	50
DC	86.8

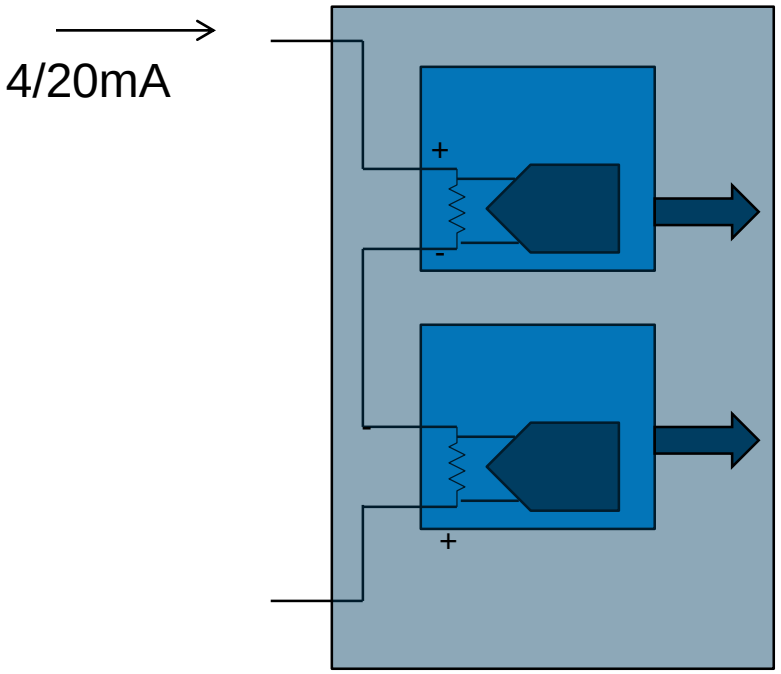
System level FME(D)A

Component	FIT	DC %	Diagnostics	λ_S	λ_{DU}	λ_{DD}
U_1	50	86.8	See safety manual	25	3.3	21.7
T_2						
R_1						
C_1						
L_1						

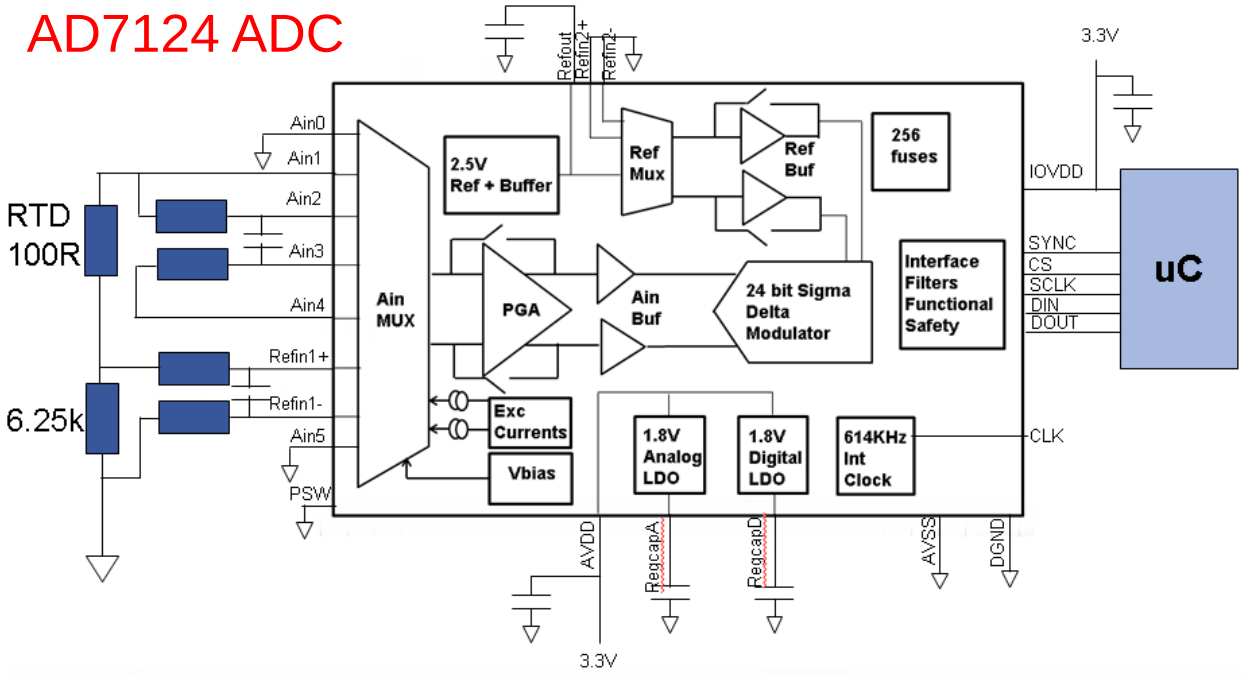
Safety function summary

λ_{DU}	
λ_{DD}	
λ_S	
λ	
SFF	

Give module designer options on diagnostics

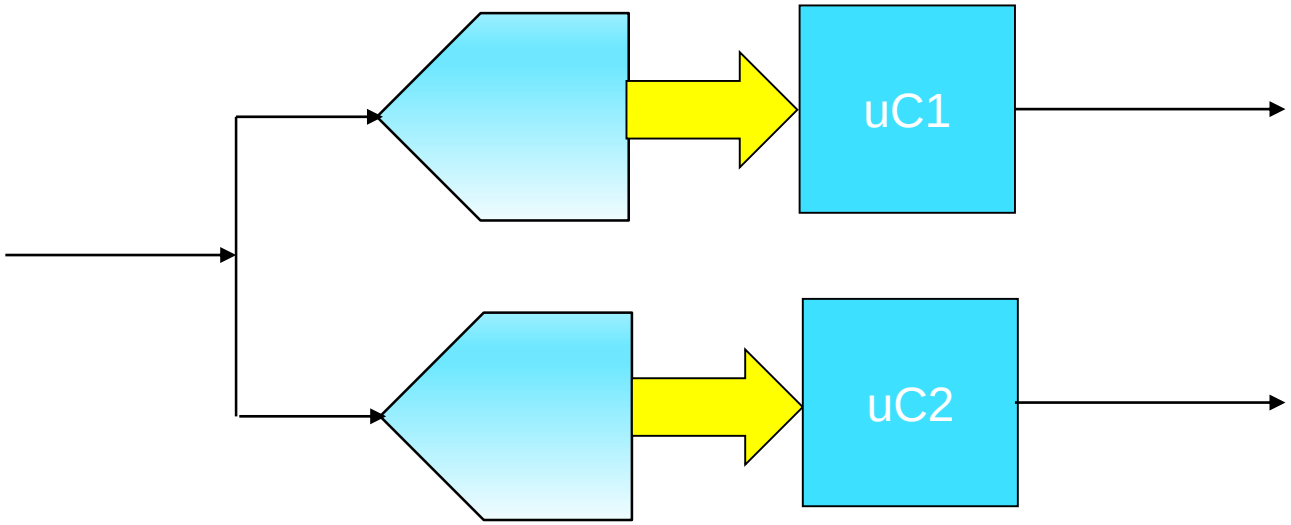


AD7124 ADC



- 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



61508-2 © IEC:2010 – 51 –

Table A.2 – Electrical components

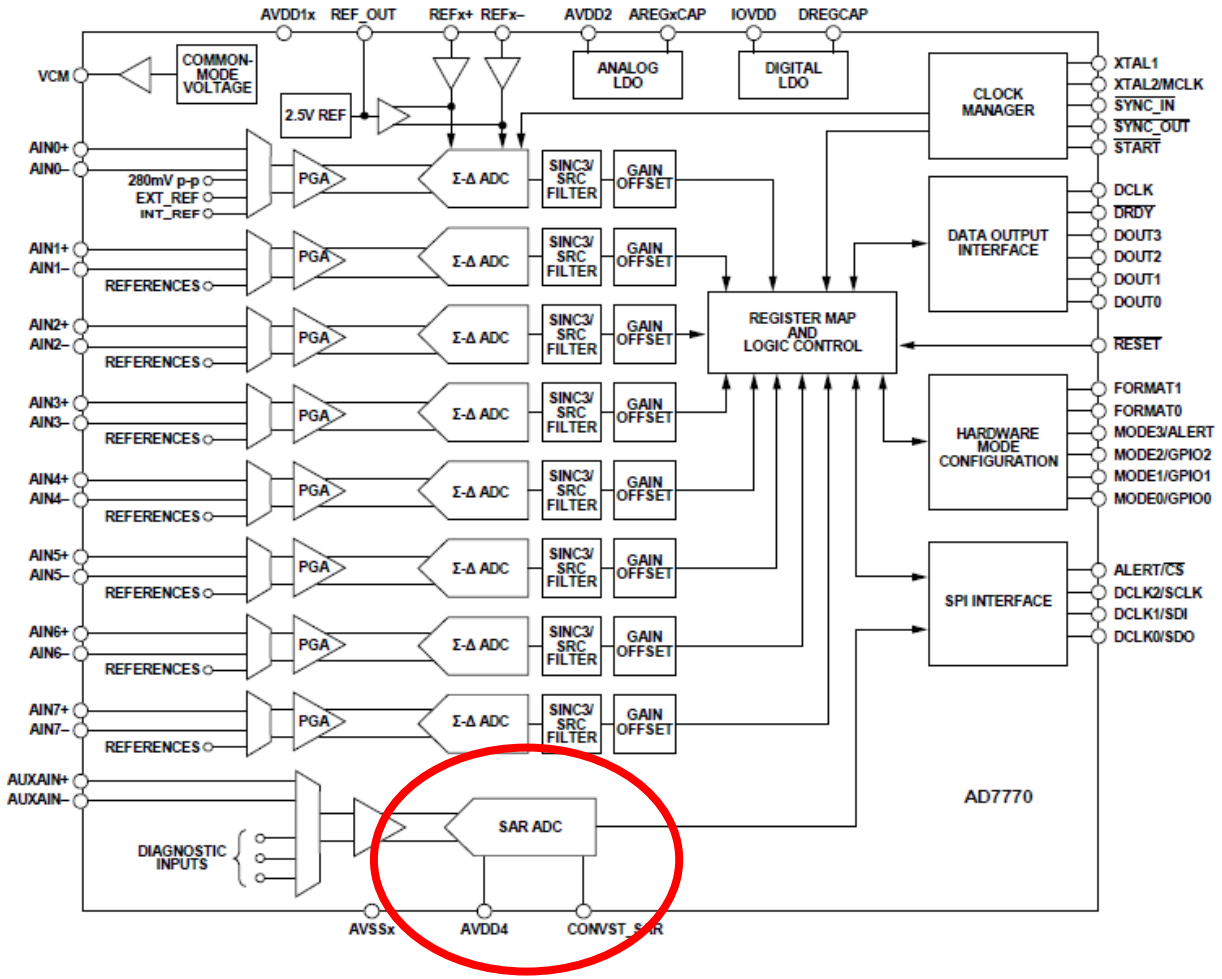
Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection
Monitoring of relay contacts	A.1.2	High	Relay switching rate should be taken into account when quantifying the effect of random failures
Comparator	A.1.3	High	High if failure modes are predominantly in a safe direction
Majority voter		High	Depends on the quality of the voting

NOTE 1 This table does not replace any of the requirements of Annex C.
NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage.
NOTE 3 For general notes concerning this table, see the text preceding Table A.1.

- 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

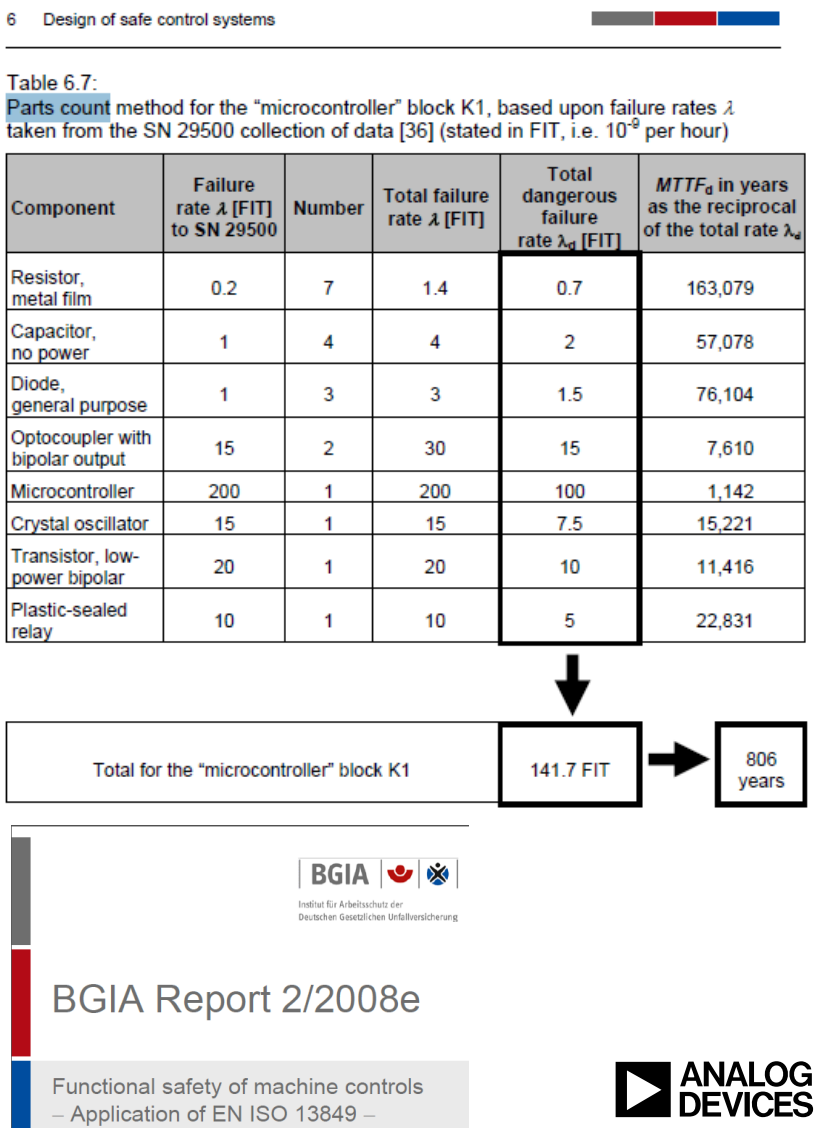
- What if comparison is not possible due to area constraints?
- What if cannot stop conversions to do reference conversions?
- A part like the AD7770 solves the issue by providing a SAR ADC which is fast enough to convert all 8 channels albeit with lower accuracy
  - The SAR ADC has a different architecture 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%



6 Design of safe control systems

Table 6.7:
Parts count method for the "microcontroller" block K1, based upon failure rates λ taken from the SN 29500 collection of data [36] (stated in FIT, i.e. 10^{-9} per hour)

Component	Failure rate λ [FIT] to SN 29500	Number	Total failure rate λ [FIT]	Total dangerous failure rate λ_d [FIT]	$MTTF_d$ in years as the reciprocal of the total rate λ_d
Resistor, metal film	0.2	7	1.4	0.7	163,079
Capacitor, no power	1	4	4	2	57,078
Diode, general purpose	1	3	3	1.5	76,104
Optocoupler with bipolar output	15	2	30	15	7,610
Microcontroller	200	1	200	100	1,142
Crystal oscillator	15	1	15	7.5	15,221
Transistor, low-power bipolar	20	1	20	10	11,416
Plastic-sealed relay	10	1	10	5	22,831
Total for the "microcontroller" block K1				141.7 FIT	806 years

BGIA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

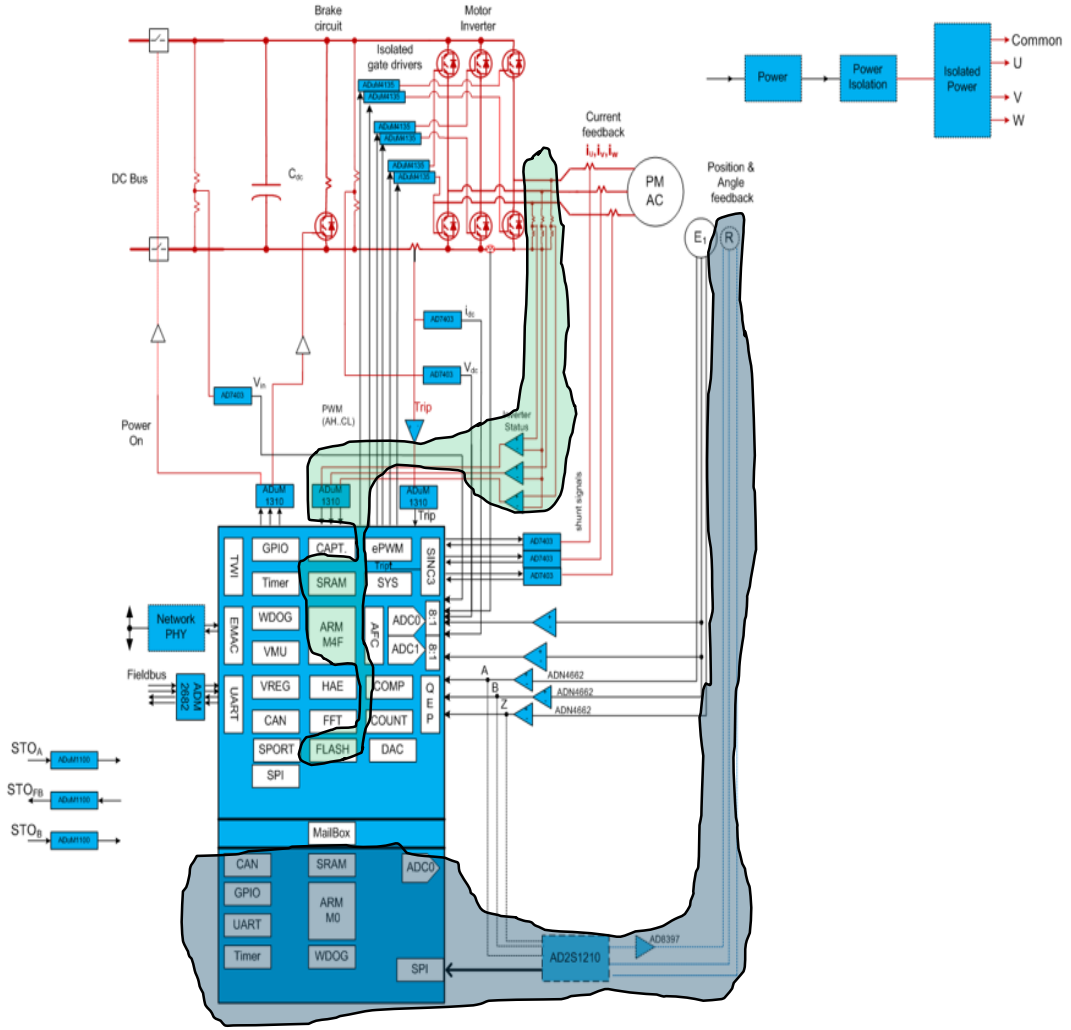
BGIA Report 2/2008e

Functional safety of machine controls
– Application of EN ISO 13849 –

System level thinking – a motor control example

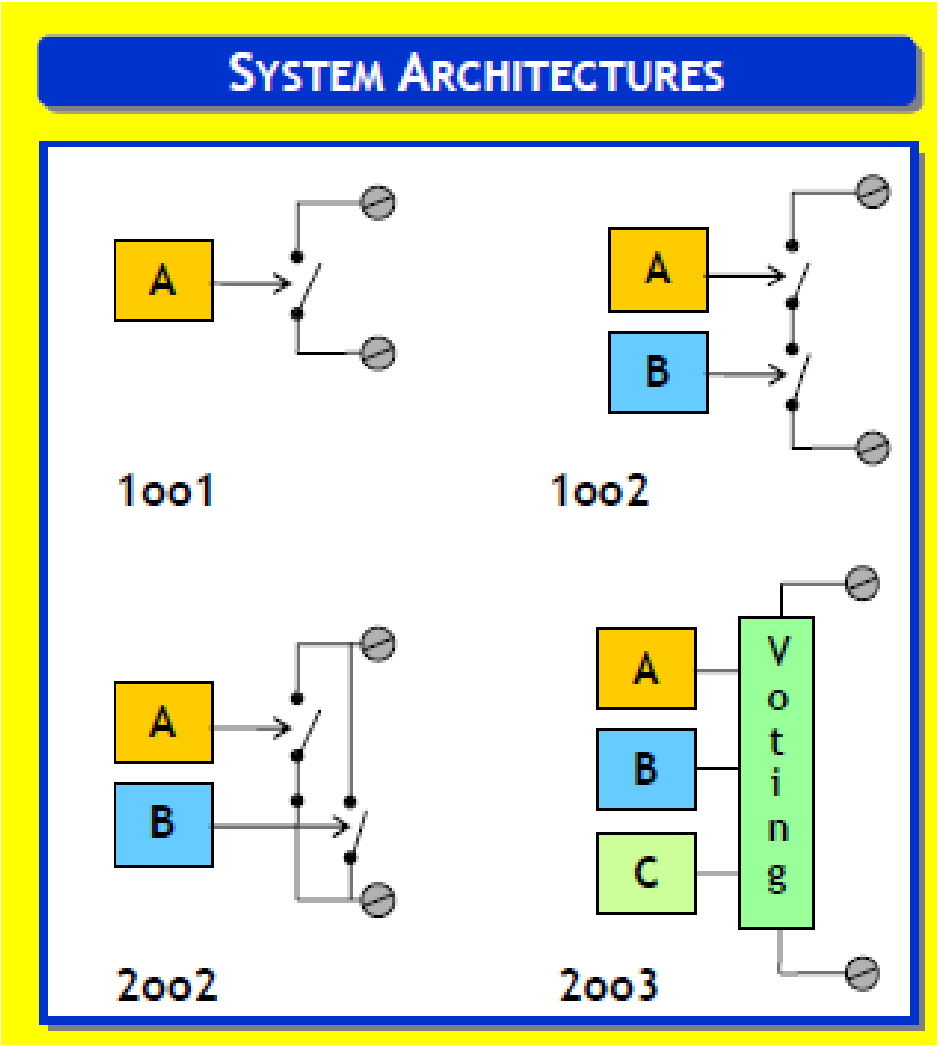
- Pretending to be a module designers highlights to the IC designer the information their customers need to design in integrated circuits
  - Goal – make it easier to use ICs in a safety design

- 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

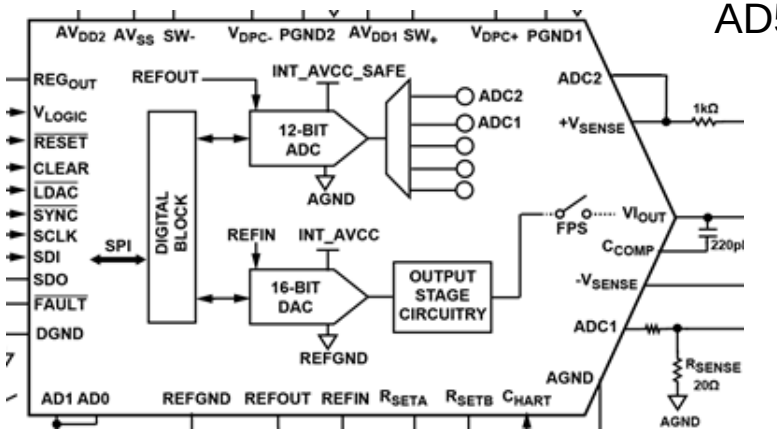
Annex E
(normative)

Special architecture requirements for integrated circuits (ICs) with on-chip redundancy

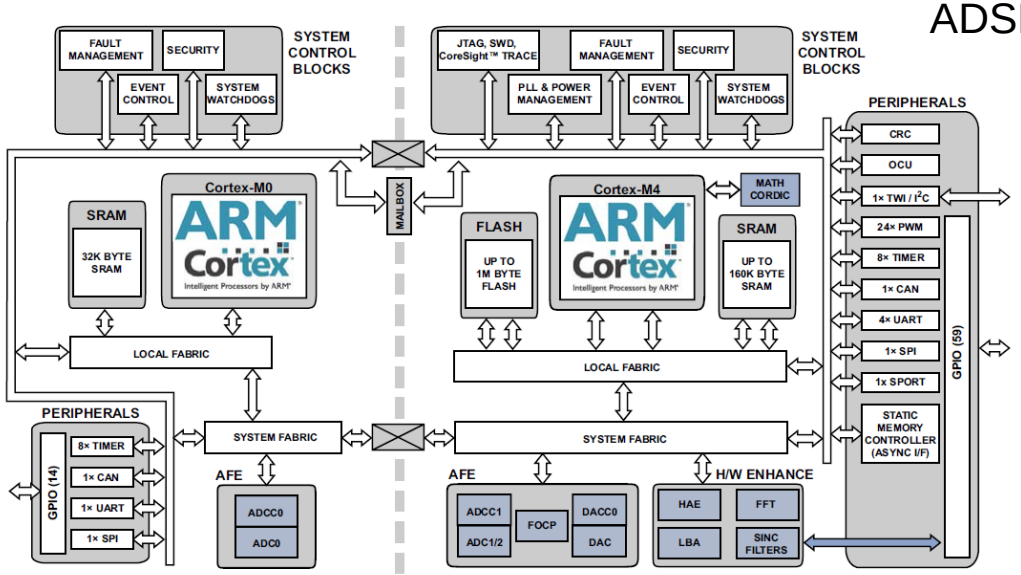
application. On-chip redundancy as used in this standard means a duplication (or triplication etc.) of functional units to establish a hardware fault tolerance greater than zero. According to

nature, for example it is limited up to SIL 3 and a set of restrictive requirements have been specified. The following requirements are related to digital ICs only. For mixed-mode and analogue ICs no general requirements can be given at the moment. Common cause analysis

AD5758

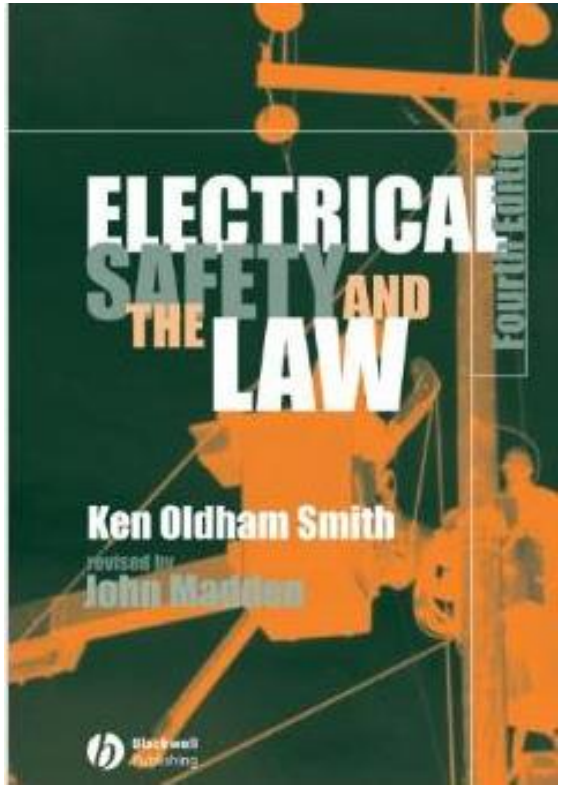


ADSP-CM41X



- 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.

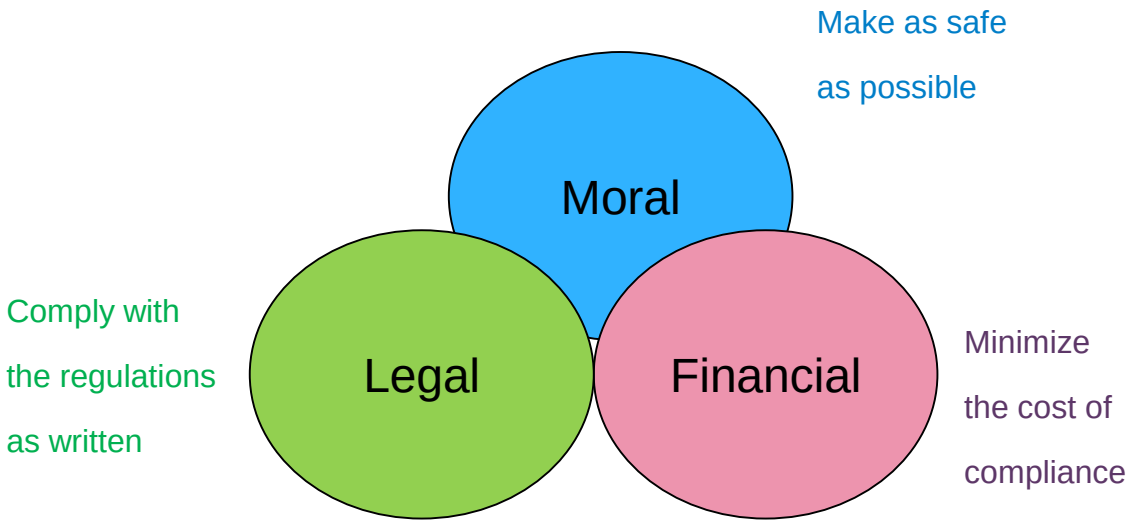
- IEC 61508 and similar standards are often described as “large and complex”
- In the past discussions related to functional safety began with a description of what was meant by SIL
  - IC designers need to understand PL, MooN, HFT, DC, SFF, PFH……

ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

Summary

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

ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

The END

ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

Extra slides