

# ***IEC 61508 2nd Edition: Get Educated. Get Compliant***

Welcome to the Webinar!

Thursday June 9, 2011

11 am - noon Pacific

noon - 1 pm Mountain

1 pm - 2 pm Central

2 pm - 3 pm Eastern

Moderator: Lori Dearman, Webattract



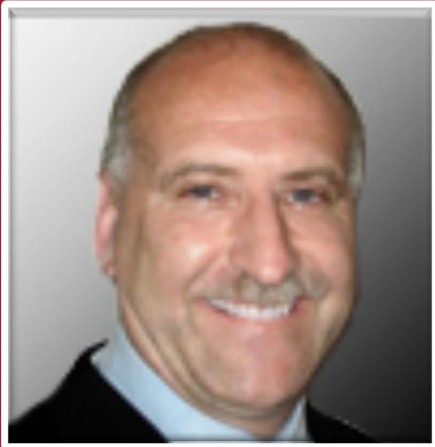
**Kevin Connelly**  
**UL Industry Manager**  
**Power & Controls**  
**Functional Safety**



**Thomas Maier**  
**UL Principal Engineer**  
**Functional Safety**



# Featured Speaker



**Kevin Connelly**  
UL Industry Manager Power &  
Controls, Functional Safety



# Why are these changes important?

*Changes provide benefits throughout the supply chain*



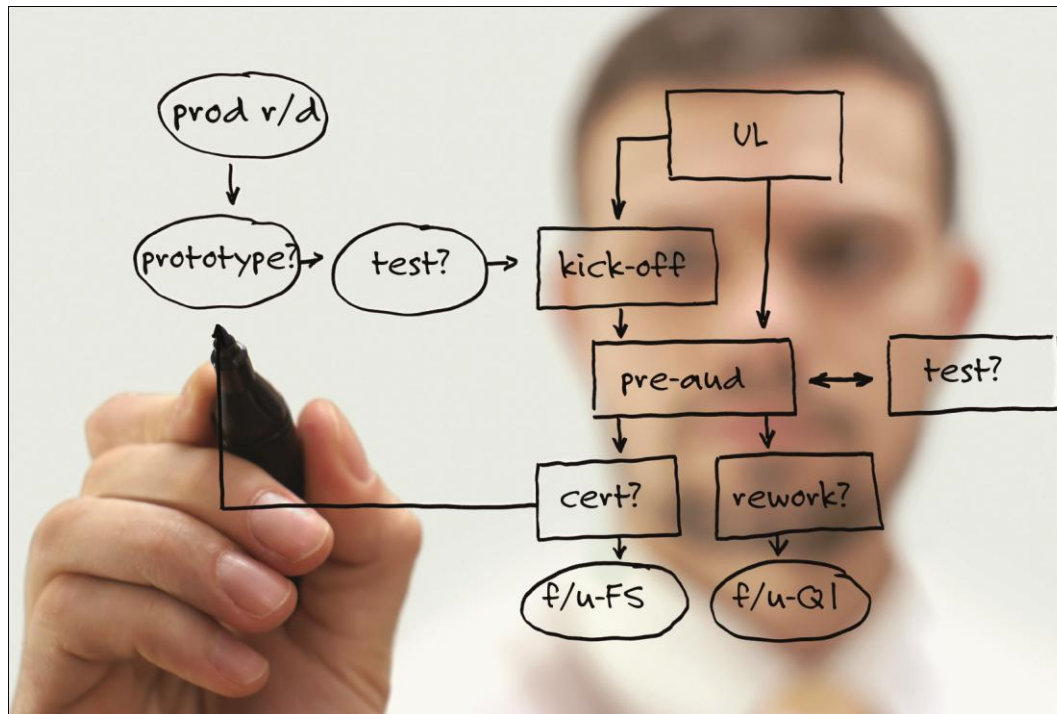
# Why are these changes important?

*Component Manufacturer now have formal requirements for sensors, ICs or Software.*



# Why are these changes important?

*Subsystem level will have more internal transparency and therefore better management of the product lifecycle.*



# Why are these changes important?

Now going to have a formal methodology for ASICs and FPGA



# Why are these changes important?

*End Users are going to have higher level of confidence.*

confidence



# Featured Speaker



**Thomas Maier**  
**UL Principal Engineer**  
**Functional Safety**

- Changes in summary
- Increased focus on traceability
- The concepts of elements and compliant items
- Redundant channels in a single integrated circuit
- Field Programmable Gate Arrays (FPGAs)
- Increased focus on EMC



# In Summary

To better reflect and formalize  
how the standard mostly has been used

To strengthen and clarify weakly or implicitly  
formulated requirements and loose ends



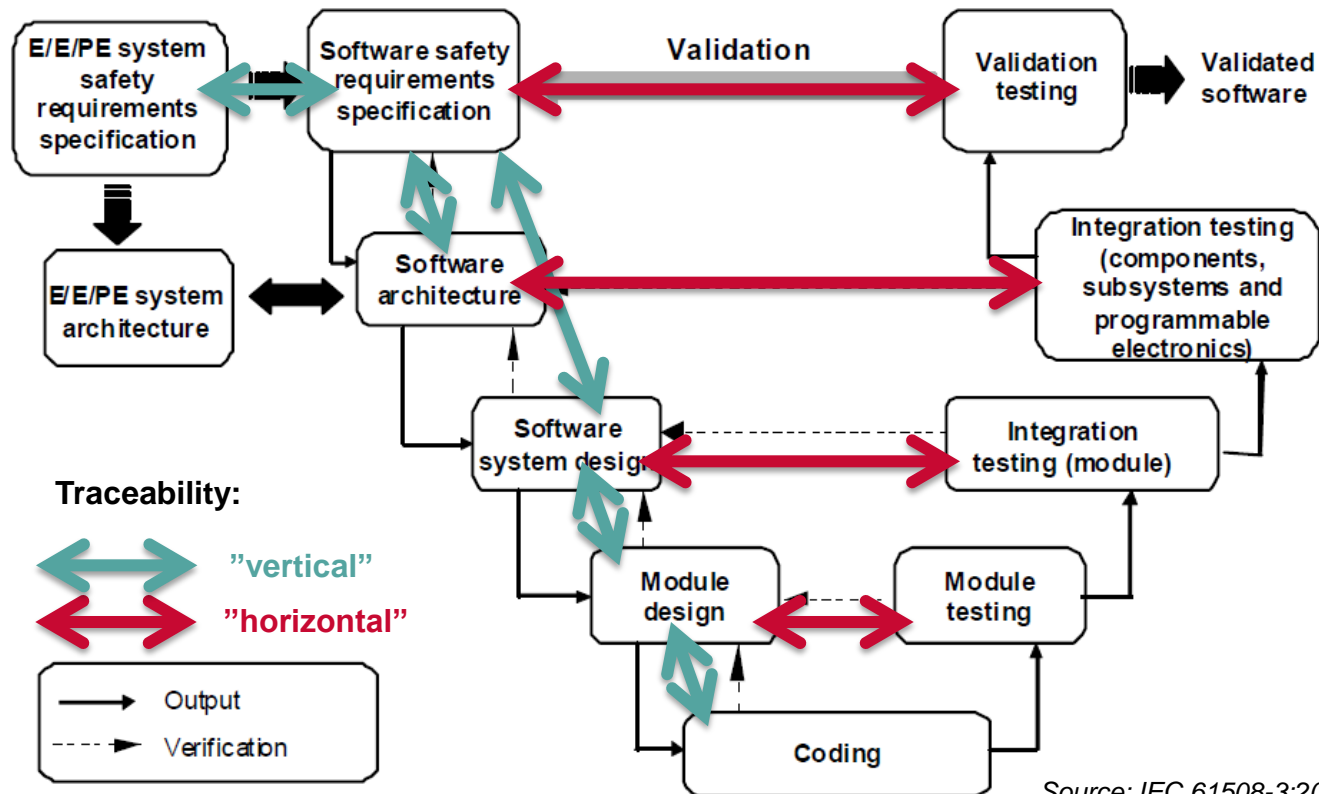
**increased focus on traceability**

# Increased focus on traceability

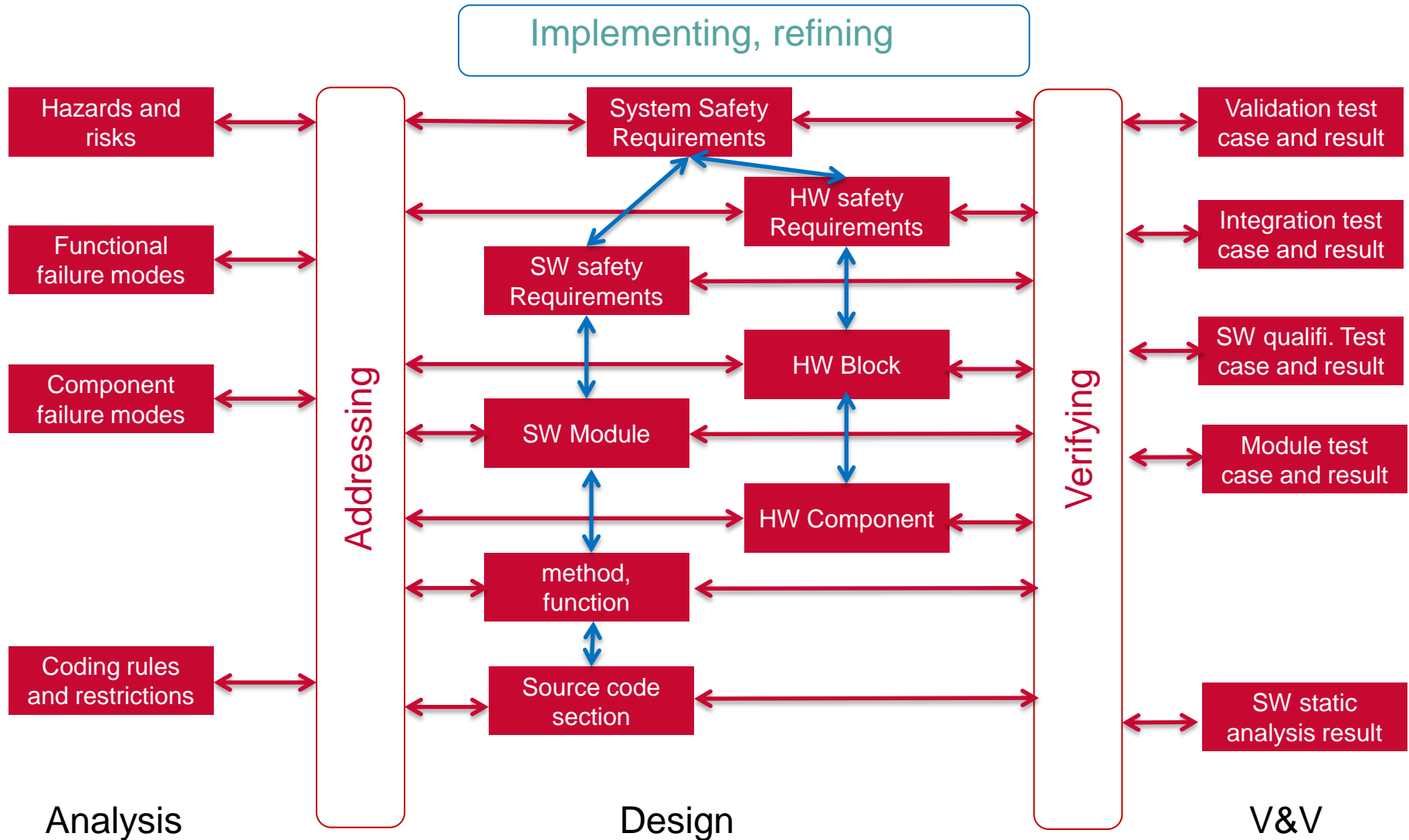
1st edition: From a formal perspective, the requirement for full traceability already existed in the 1st edition:

- As of tables B.2 and B.6, traceability can be considered "highly recommended" for SIL3.
- Part 3 of 1st edition explicitly required traceability between system and software safety requirements

2nd edition: explicitly required (at least for SIL 3) in all phases

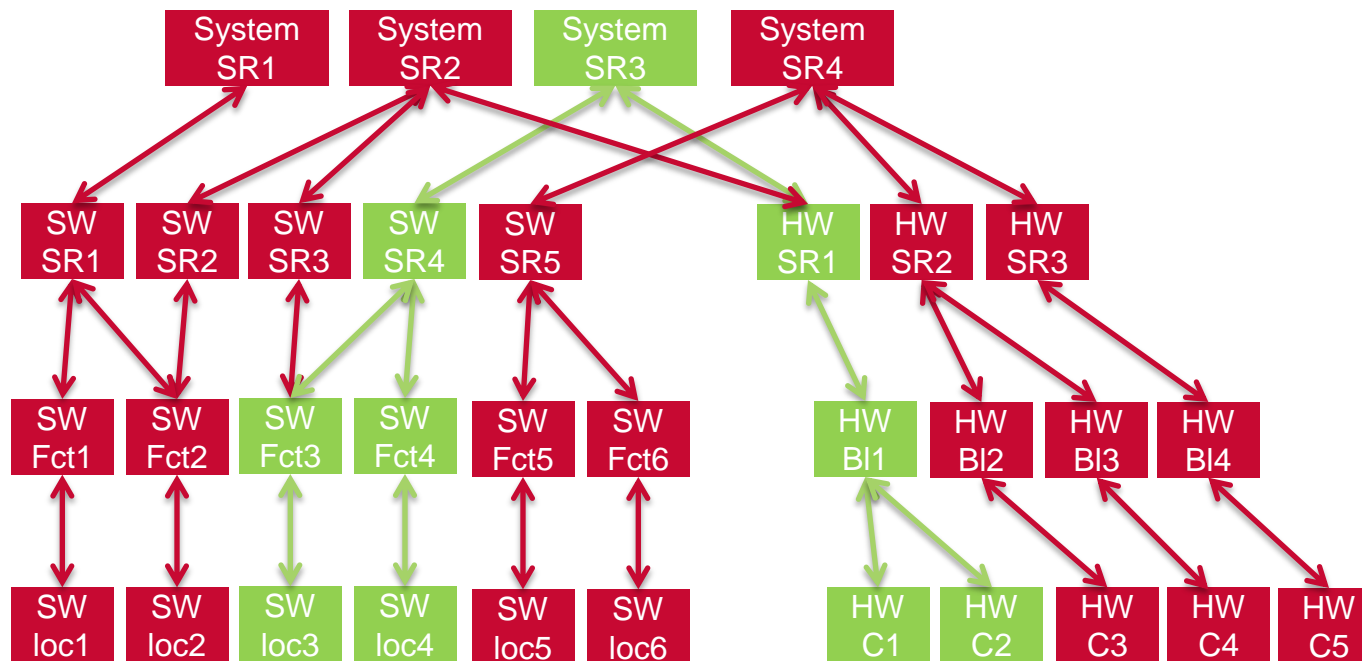


# Traceability and Construction of Safety Case



# Traceability and Change Management

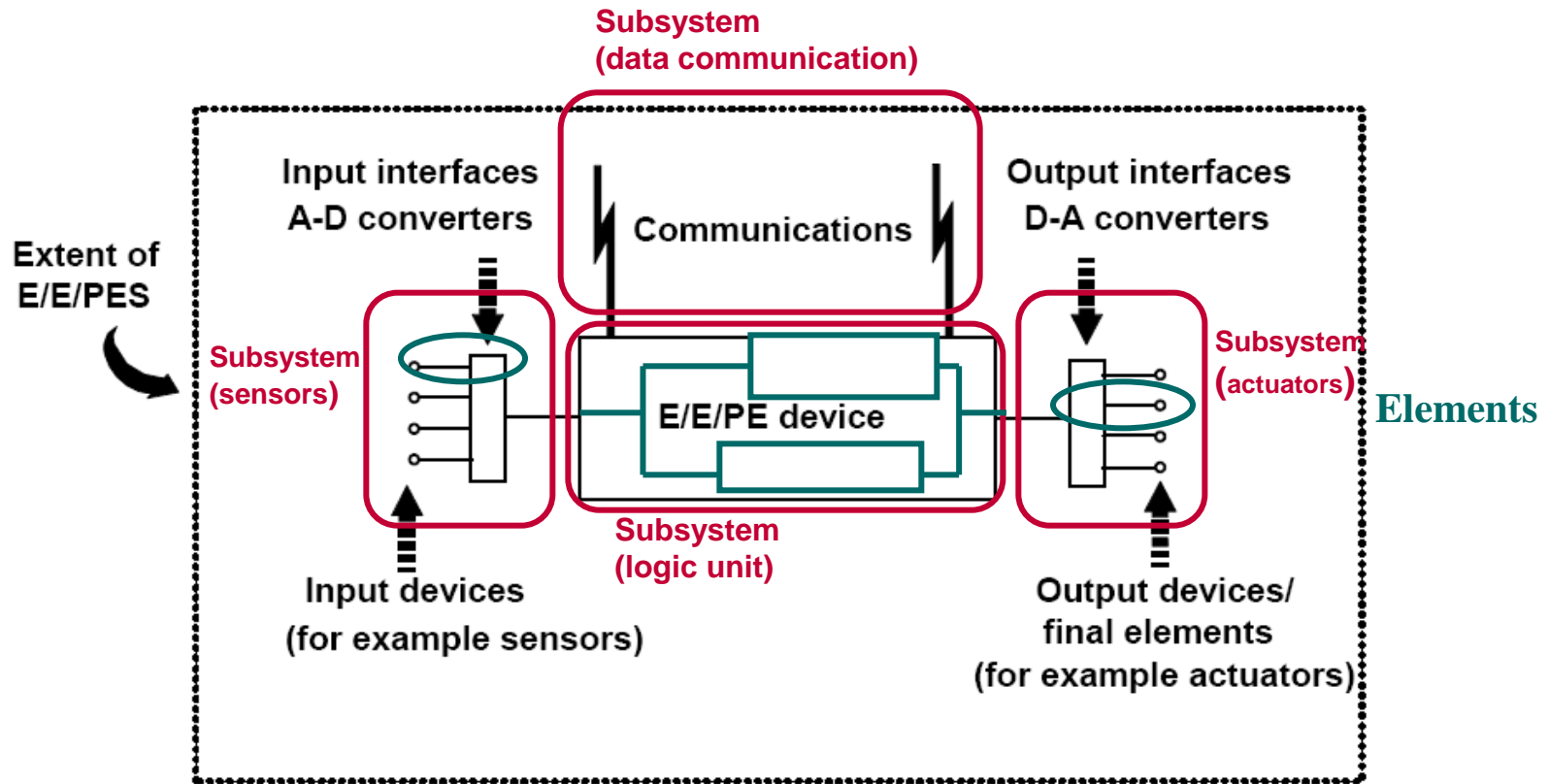
## Support of Impact Analysis for Complex Systems:



**the concepts of elements and compliant items**

# Elements and Compliant Items

E/E/PES consist of subsystems, subsystems consist of elements:



"Subsystem" and "element" are defined now in the 2nd edition of IEC 61508.



# Elements and Compliant Items

Design requirements in the 2nd Ed. are very much built around the element concept.

- Safe Failure Fraction, Systematic capability, are element properties
- The subsystem is built by combining elements

Elements can comprise hardware only, hardware and software combined, software only.

- Elements can consist / be built of elements
- Elements can be compliant items



# Safety manual for compliant items

Any item within the system hierarchy defined by IEC 61508:2010 can be a compliant item

- Software components (e.g. RTOS, communication protocol stack)
- Integrated circuits (microcontrollers, ASICs, FPGAs)

A compliant item must be accompanied by a safety manual

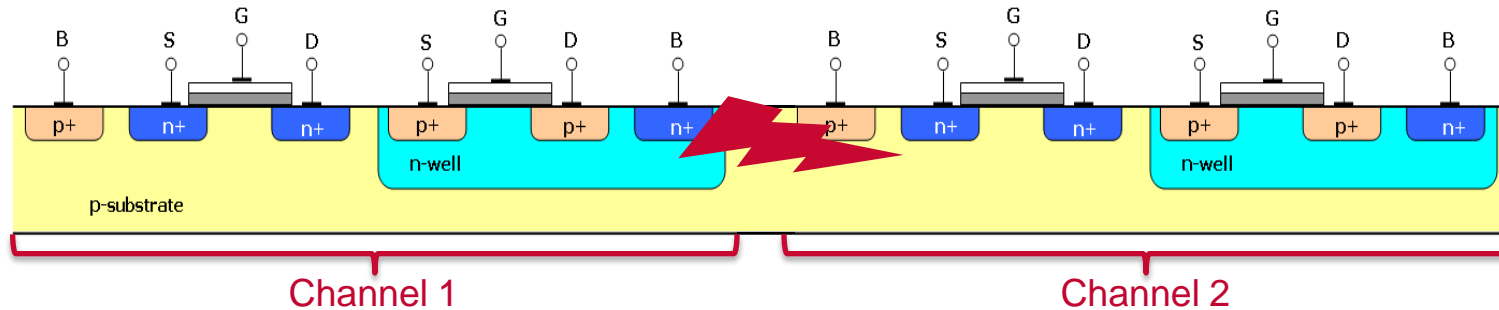
The requirements for these safety manuals are provided by Annexes D of Part 2 and Part 3.

- Part 2: compliant item in general
- Part 3: adds those aspects relevant for software



**redundant channels in a single integrated circuit**

# On-chip redundancy



**Trends: Multi-core processors and FPGA increasingly used**

**Natural questions:**

- Why wouldn't one multi-core SoC not implement multiple safety-related channels?

**This was up to now not allowed, had to be considered as one physical channel:**

- Electrical coupling, for example: Short circuits, cross talk between redundant signals
- Over-temperature will affect channels equally



# IEC 61508-2 2nd Ed, Annex E:

## How to realize physical redundancy on one single IC substrate

### Architectural requirements

Separate physical blocks on substratum for each channel and each monitoring element such as a watchdog.

- DC requirements for diagnostic elements, if only implemented once: 60%!

Each channel shall have its own separated inputs and outputs

- Separate clocks and clock signals
- Separate power supply

Minimum DC per channel: 60%

Over-temperature detection

- May be waived if other diagnostics has DC > 99% for each channel



# IEC 61508-2 2nd Ed, Annex E:

## How to realise physical redundancy on one single IC substrate

### Safety integrity limitations

- Highest SIL that can be claimed is SIL 3
- Systematic capability cannot be increased by combination of elements

### Layout requirements

- Separation of channels is achieved by
  - Increased distance: Factor 10 to 50 applied to normally required design rules
  - Isolation through potential rings (then increased distance not necessary)
- Separated inputs and outputs must not be routed through another channel/block.

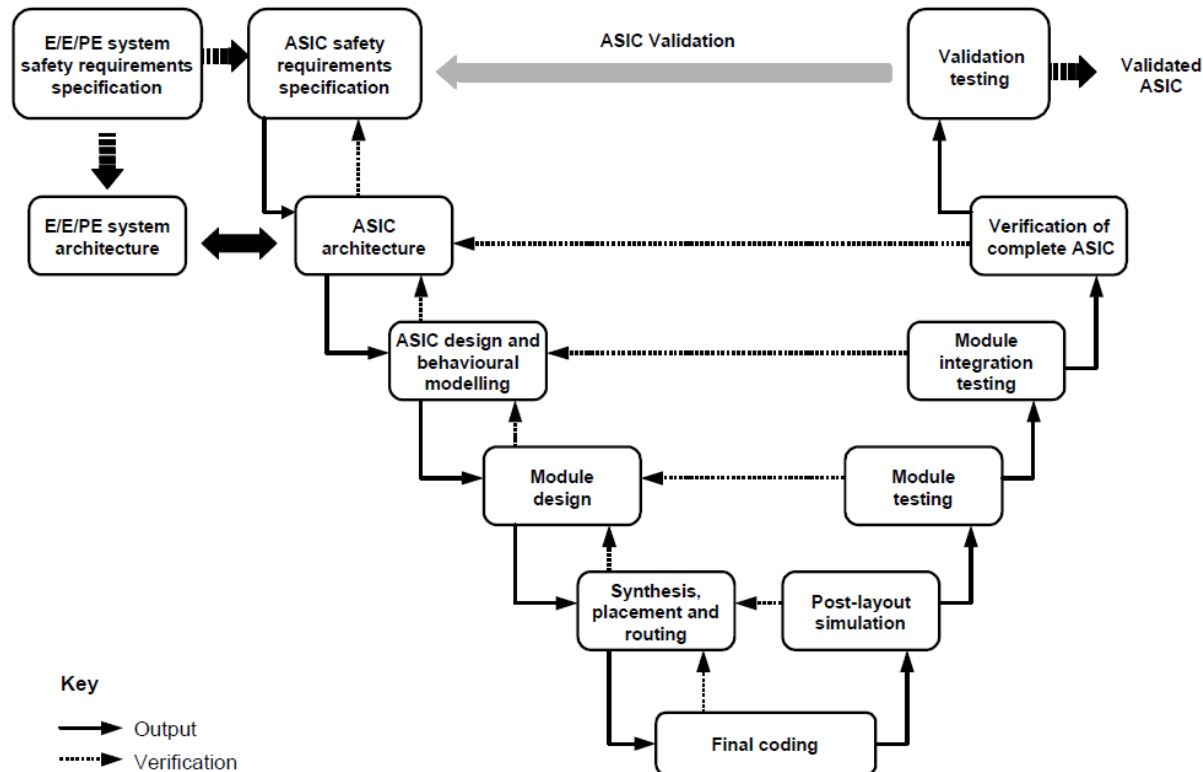


**field programmable gate arrays**  
**(FPGAs)**

# Development of ASIC's and FPGA's

IEC 61508:2010 recognizes the similarity between complex IC development and software development.

As a fundamental measure for fault avoidance, a more detailed lifecycle model is provided, in addition to the "conventional" E/E/PES lifecycle:



# Development of ASIC's and FPGA's

- Furthermore, IEC 61508-2:2010 refers to (informative) Annex F which provides techniques and measures to avoid the introduction faults in development of ASIC's (and FPGA's)

**Table F.2 – Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD) (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	– high	– high	NR	NR
	4	Design description using boolean equations		R high	R high	NR	NR
	5a	For circuit descriptions that use boolean equations: manual inspection in designs with limited (low) complexity		HR high	HR high	HR* high	HR* high
	5b	For circuit descriptions that use boolean equations: simulation of state transitions in designs with higher complexity		HR high	HR high	HR* high	HR* high



**increased focus on EMC**

# Electromagnetic immunity:

## Change from 1st to 2nd edition of IEC 61508

### 1st Edition IEC 61508-2 (in notes of clause 7.2.3.2)

- Recognizes that SIL is a factor when determining immunity levels
- Recognizes that it is difficult to determine the probability of immunity levels being exceeded
- Recognizes that increased levels don't provide a guarantee, but an increased confidence in safety integrity

### 2nd Edition of IEC 61508 refers to IEC/TS 61000-1-2 and IEC 61326-3-1

- Electromagnetic levels to be specified on the basis of IEC/TS 61000-1-2.
  - higher immunity levels than those specified in product standards may be necessary.
- In IEC 61508-2 Table A.16 (control of systematic failures) increased immunity is mandatory for all SIL, reference to IEC 61326-3-1



# IEC/TS 61000-1-2

This standard is not only about EMC test – it is primarily about appropriate design

- It is not feasible to demonstrate immunity by test only
- Provides techniques and measures in Annex B

The standard does recommend test against higher levels.

- Even against low-probability very high levels



# IEC 61326-3-1: EMC Test Plan

## Configuration of EUT

- Selection of most susceptible configurations and installations
- Selection of I/O ports

## Operation conditions during test

- representative "worst-case" operation modes
- EUT Software during test enables simulation of selected operation modes

## Performance criterion FS

- Safety function not affected; or
- disturbed temporarily or permanently, with a "safe" reaction.
- destruction of components is allowed.



# IEC 61326-3-1: Immunity Requirements

**Table 1a – Immunity test requirements for equipment intended for use in industrial locations – Enclosure port**

	Phenomenon	Basic standard	Tests for functions intended for safety applications	
			Test value – Performance criterion	
1.1	Electrostatic discharge (ESD)	IEC 61000-4-2	6 kV/8 kV contact/air <sup>a, b</sup>	FS
1.2	Electromagnetic field	IEC 61000-4-3	20 V/m (80 MHz to 1 GHz) <sup>c</sup> 10 V/m (1,4 GHz to 2 GHz) <sup>c</sup> 3 V/m (2,0 GHz to 2,7 GHz) <sup>c</sup>	FS
1.3	Rated power frequency magnetic field	IEC 61000-4-8	30 A/m <sup>d</sup>  No increased test level applies; see row 6 of Table A.1	FS
<p><sup>a</sup> Levels shall be applied in accordance with the environmental conditions described in IEC 61000-4-2 on parts which may be accessible by persons other than staff working in accordance with defined procedures for the control of ESD but not to equipment where access is limited to appropriately trained personnel only.</p> <p><sup>b</sup> For equipment intended to be used in SIL 3 applications, the number of discharges at the highest level shall be increased by a factor of 3 compared to the number as given in the basic standard.</p> <p><sup>c</sup> These increased values shall be applied in frequency ranges as given in Table 2 used for mobile transmitters in general, except when reliable measures are realised to avoid the use of such equipment nearby. ISM frequencies shall be taken into account on an individual basis.</p> <p><sup>d</sup> Applicable only to equipment containing devices susceptible to magnetic fields.</p>				

Source: IEC 61326-3-1



# Further Appreciated Changes

- New phase: System Requirements Specification, and new deliverables: system Safety requirements and System Design Requirements
- Clearer definition of safe and dangerous failures (as related to SFF calculation)
- Requirements for "proven-in-use" and "pre-existing software"
- Requirements for tool evaluation
- Modernisation of software development techniques and measures



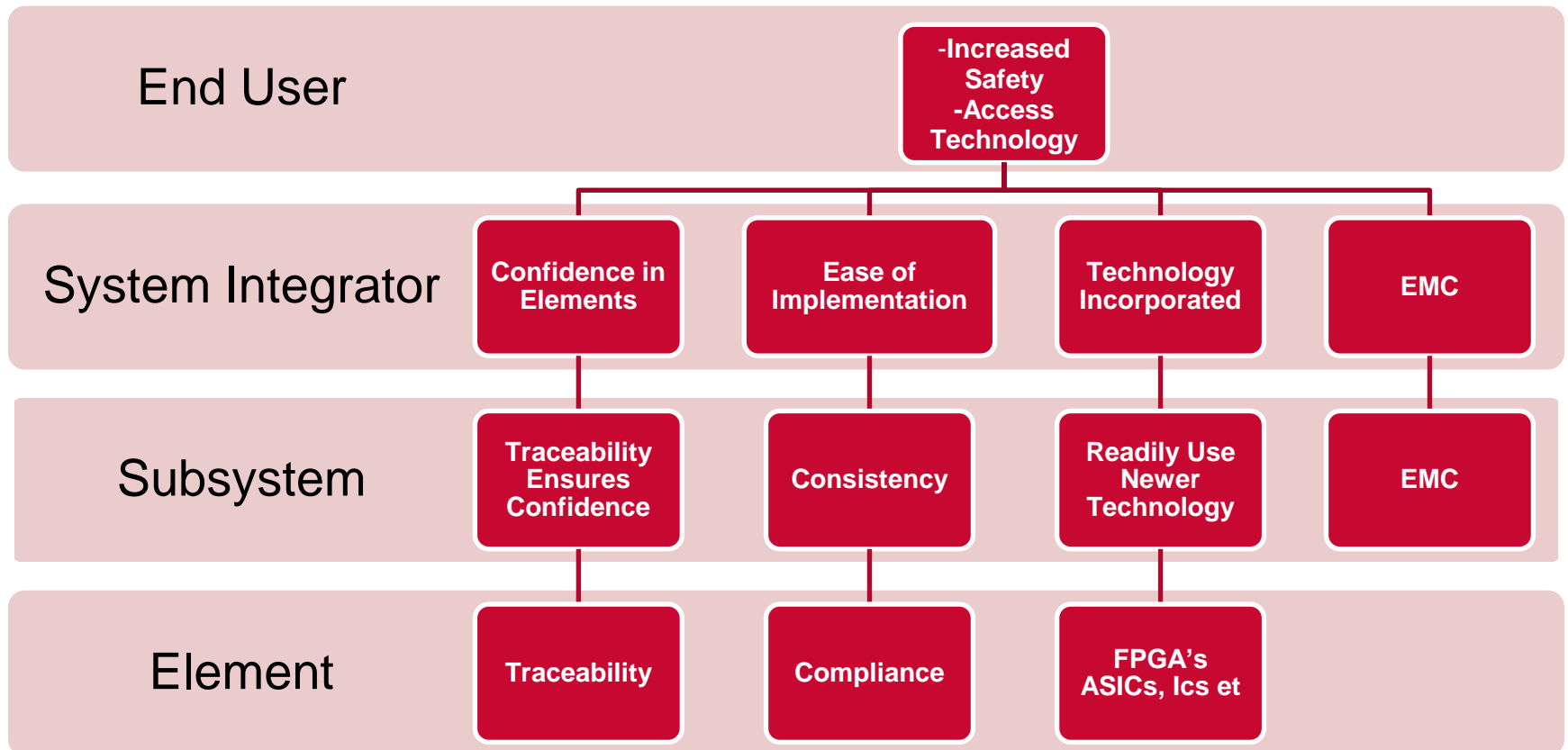
# Featured Speaker



**Kevin Connelly**  
UL Industry Manager Power & Controls  
Functional Safety



# Value add throughout the supply chain



# Certification adds value through the supply chain

End User/System Integrator /Subsystem

- Look for the UL Certification or Recognition Mark
- UL mark will include the edition / date of publication



# Getting Started



For more information:  
Download UL's white paper on [www.ul.com/functionalsafety](http://www.ul.com/functionalsafety)

**To request a quote for the UL Functional Safety Mark:**

**Contact:**

**Kevin Connelly**

**1-631-546-2691**

**[kevin.connelly@us.ul.com](mailto:kevin.connelly@us.ul.com)**



# **IEC 61508 2nd Edition: Get Educated. Get Compliant**

## **Ask The Experts Panel**

**Moderator: Lori Dearman, Webinar Producer with Webattract**



**Kevin Connelly**  
**UL Industry Manager**  
**Power & Controls**  
**Functional Safety**



**Thomas Maier**  
**UL Principal Engineer**  
**Functional Safety**

**For More Information:**

**[www.ul.com/functionalsafety](http://www.ul.com/functionalsafety)**

**Kevin Connelly at 1-631-546-2691**

**[kevin.connelly@us.ul.com](mailto:kevin.connelly@us.ul.com)**

