Safety Integrity Level Compliant Programmable System Design

Presentation Embedded World 29 Feb 2012

Sebastian Stiemke, MissingLinkElectronics, Neu-Ulm

Content

- Idea of Functional Safety
- Functional Safety Chain
- Safety Integrity Level
- Special Situation of Programmable Devices
- Techniques and Measures for Programmable Devices
- Proven in use

… yes – it is possible …

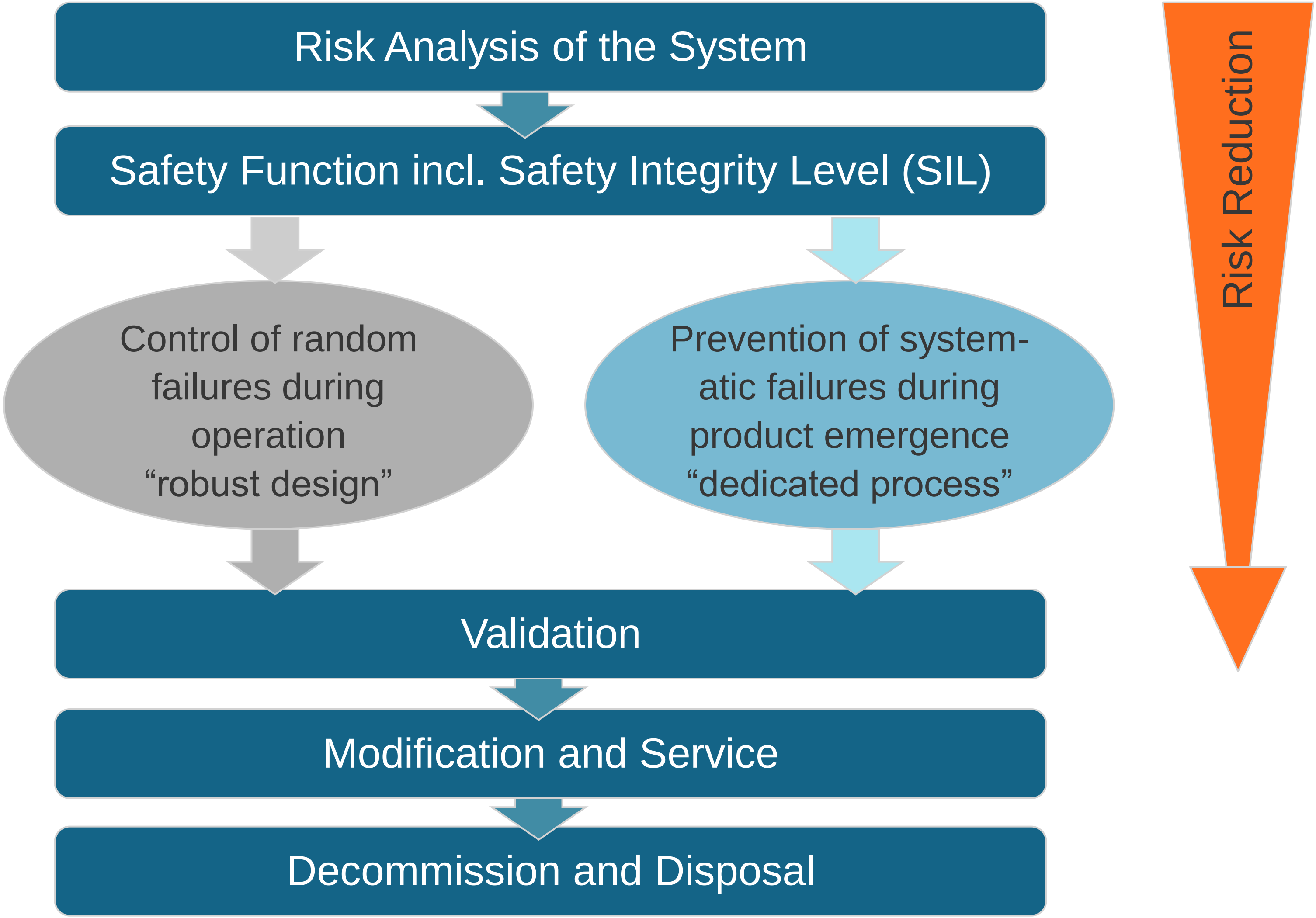
Idea of Functional Safety (acc. EN 61508)

Functional Safety is the ability of an electric/ electronic/programmable electronic system (E/E/PE) to stay in safe state or to initiate a coordinated safe state in case of an

- random and/ or systematic failures with dangerous impact to people, environment or serious machine damages

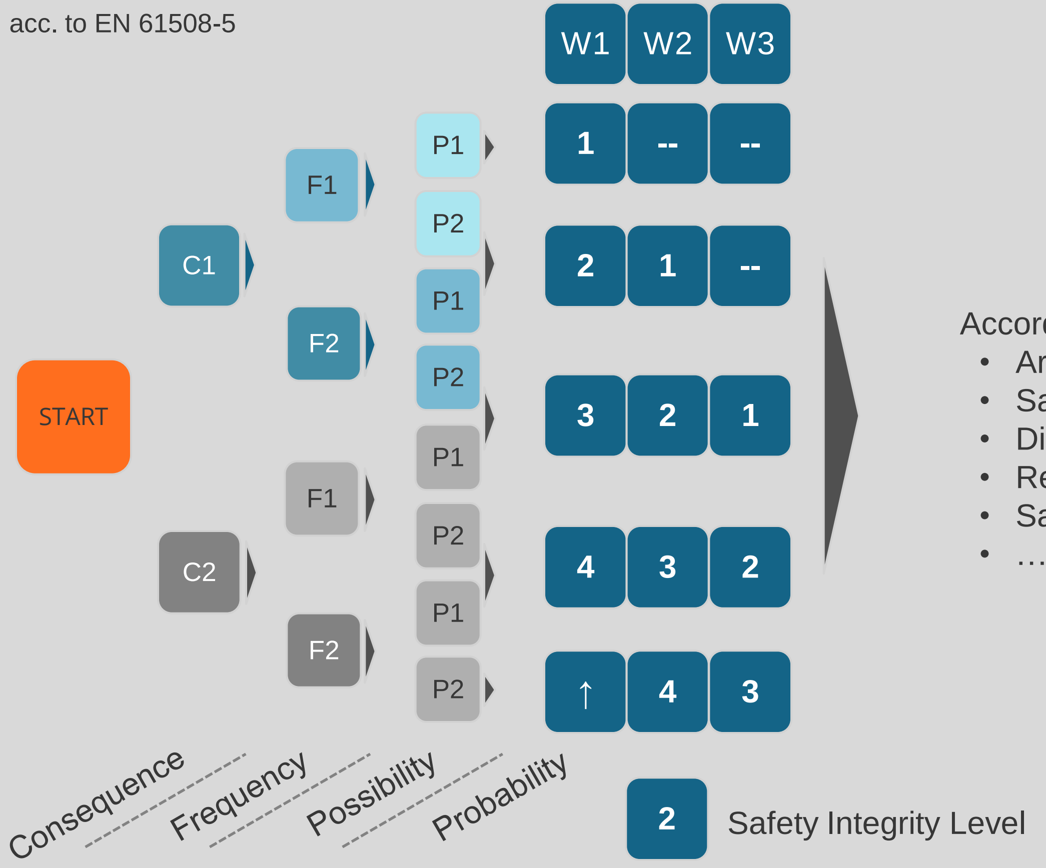
© Rabbarien

Functional Safety Chain (simplified)


Risk Analysis of the System
Safety Function incl. Safety Integrity Level (SIL)
Control of random failures during operation “robust design”
Prevention of system-atic failures during product emergence “dedicated process”
Validation
Modification and Service
Decommission and Disposal
Risk Reduction

Risk Graph and Safety Integrity Levels

acc. to EN 61508-5



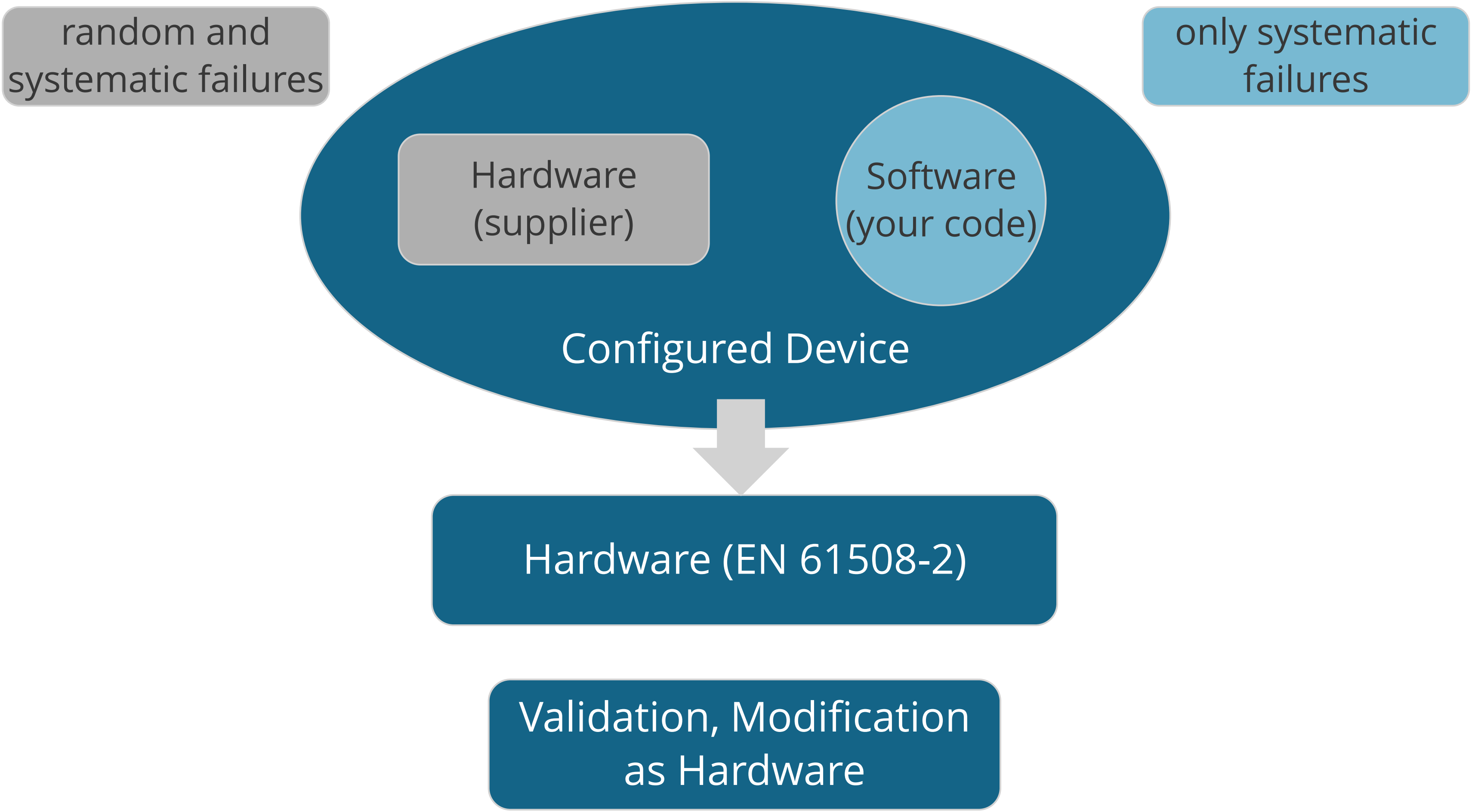
W1	W2	W3
1	--	--
2	1	--
3	2	1
4	3	2
↑	4	3

According to the Safety Integrity Level:

- Architecture
- Safe Failure Fraction Rate
- Diagnostic Coverage Rate
- Requirements and Tasks
- Safety Assessment
- …

Risk Graph is only one option to determine the Safety Integrity Level

Special Situation of Programmable Devices



random and systematic failures

only systematic failures

Hardware (supplier)

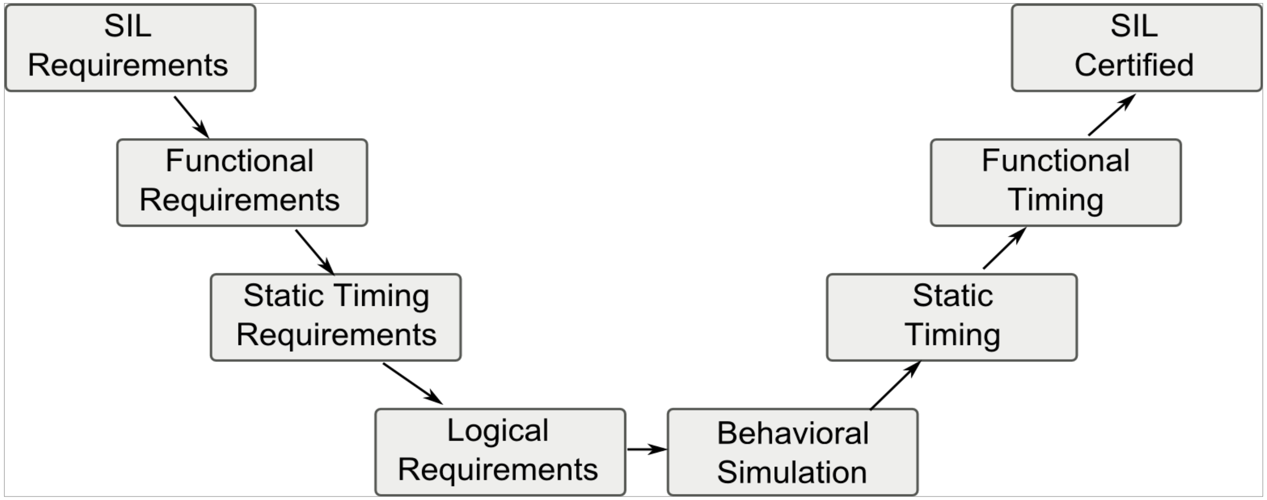
Software (your code)

Configured Device

Hardware (EN 61508-2)

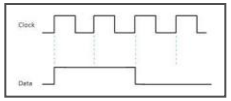
Validation, Modification as Hardware

Programmable Devices Process



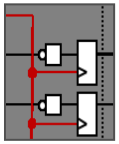
EN 61508-2 Annex F (Techniques and measures for ASICs –avoidance of systematic failures) and special for programmable devices Table F.2 (Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/ PLD/CPLD)).
The annex is informative but with detailed descriptions and links to the additional comments of EN 61508-7

Technique and Measures (Annex F)

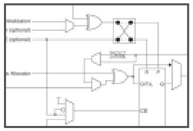


Specification,
Reference Signals

VHDL/ RTL
Description



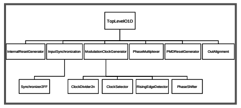
Synthesis



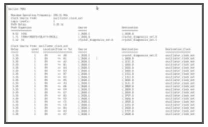
Routing

Configured Device

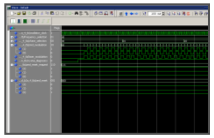
Moduls,
Timing Simulation



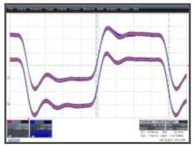
Stat. Timing
Analysis



Code inspection,
Funct. Simulation



HW Testing



Manufacturing

Examples for the Techniques/ Measures

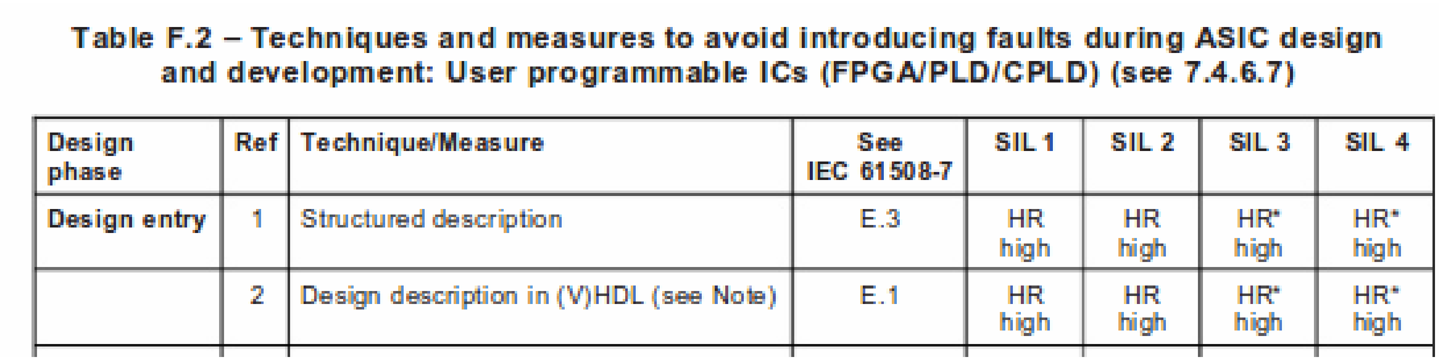


Table F.2 – Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD) (see 7.4.6.7)

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

EN 61508-2, Annex F

Examples:

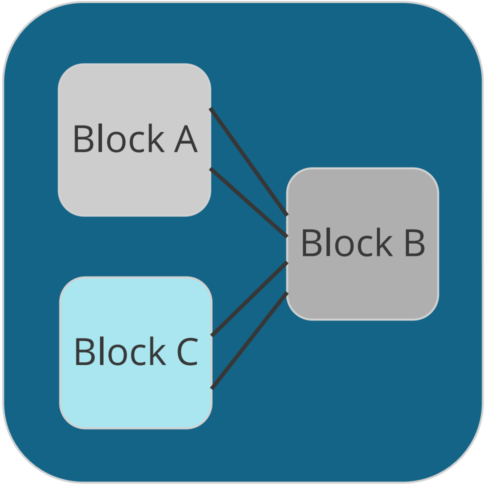
- Design: Use of coding guidelines
- Synthesis: Consistency checks of the tools, IC vendor requirements
- Routing: Timing Analysis
- Manufacturing: Quality Management

Proven in Use Problem

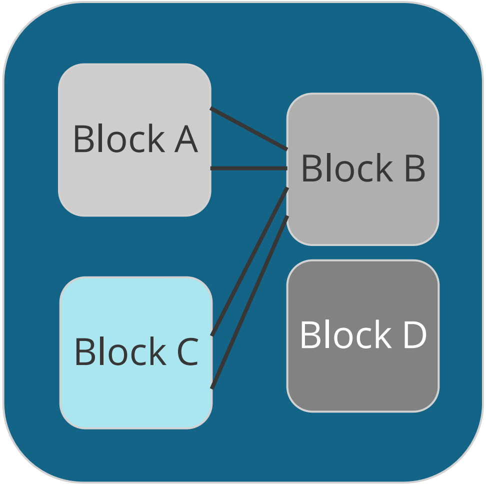
25% of the techniques and measures of Annex F require “proven in use”

- Design
  - Application of a proven in use design environment
  - Application of proven in use (V)HDL-simulators
  - Application of validated soft-cores
- Synthesis
  - Internal consistency checks
  - Application of proven in use synthesis tools
  - Application of proven in use libraries/CPLD technologies
- Routing
  - Justification of proven in use for applied hard cores
- Manufacturing
  - Application of a proven in use process technology
  - Application of proven in use device-series
  - Proven in use manufacturing process

Modification of HDL Code



primary placing



modified placing,
without any changes at A,B,C

Modifying of “soft hardware” often means that you have to restart the validation process

Solutions

Experience in programmable IC design is recommended for functional safety

- No asynchronous constructs (coding guideline)
- Modules with limited functions
- High level of automatic testing (test benches)
- Various responsibilities for design, testing and review, certification
- More detailed documentation not only results also reasons

Conclusion

Functional Safety will become more important in the future for all industries. The probability that programmable devices will get safety function get higher as well

- It is possible
- “Proven in use” is the major item for hardware, tools and people
- Comprehensive testing, validation
- Detailed documentation with additional comments
- Reduced modifications

Missing Link Electronics
Marlene-Dietrich-Straße 5
89231 Neu-Ulm

www.MLEcorp.com
Tel: +49 (731) 141-149-0