Funktionale Sicherheit – Testing unter den Bedingungen der Safety Integrity Levels

Präsentation auf dem Neu-Ulmer Test-Engineering Day

Sebastian Stiemke, MissingLinkElectronics, Neu-Ulm

Inhalt

- Idee hinter der Funktionalen Sicherheit
- Wirkkette Funktionale Sicherheit
- Safety Integrity Level
- Abriss spezielle Situation von programmierbaren Bausteinen
- Techniken und Meßmethoden für programmierbare Bausteine
- Proven in use - betriebsbewährt
- Tipps

mle
missing link electronics

… ja – es geht und es ist nur ein bisschen anders …

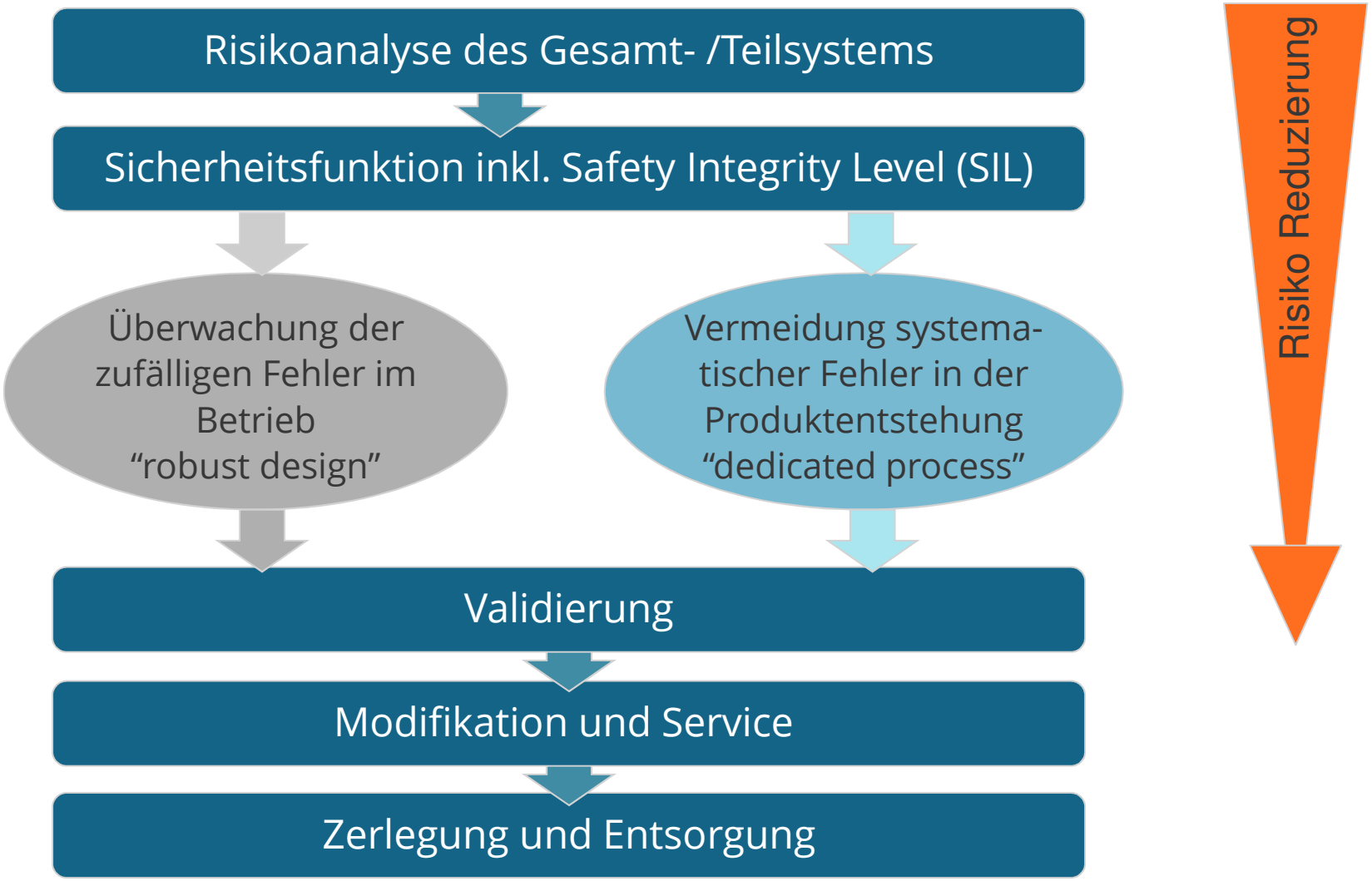
Idee hinter der Funktionalen Sicherheit (gem. EN 61508)

Funktionale Sicherheit ist die Fähigkeit von elektrischen/ elektronischen und programmierbaren elektronischen Systemen (E/E/PE) in einem sicheren Modus zu bleiben oder einen geplanten sicheren Modus einzunehmen im Falle des Auftretens von

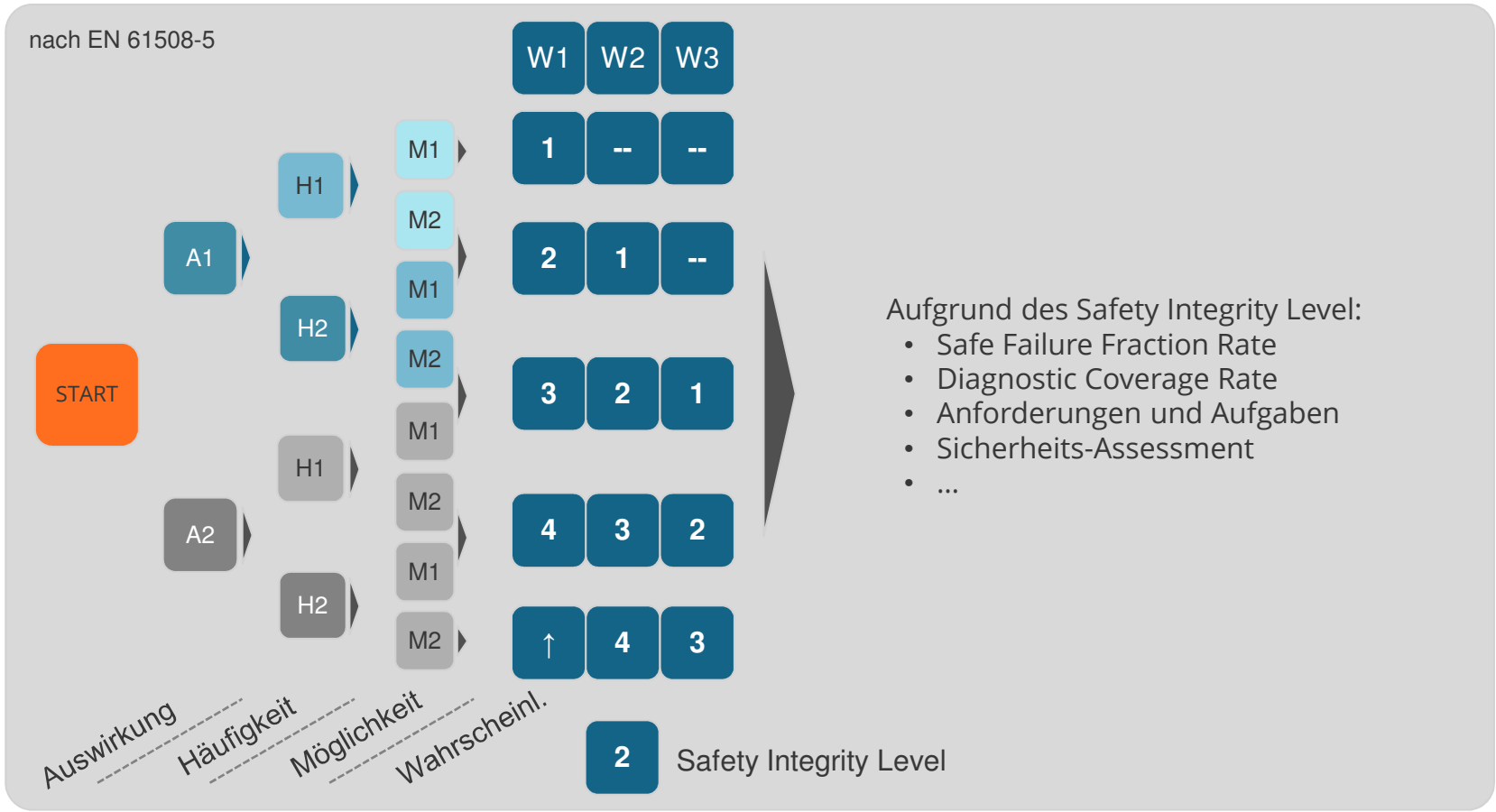
- zufälligen und/oder systematischen Fehlern mit gefährdenden Auswirkungen auf Mensch, Umwelt oder Produktionseinrichtungen
- Sicherheit bedeutet hierbei, die Gefahr, die vom System ausgeht

© Rabbarien

Sicherheitslebenszyklus (vereinfacht)

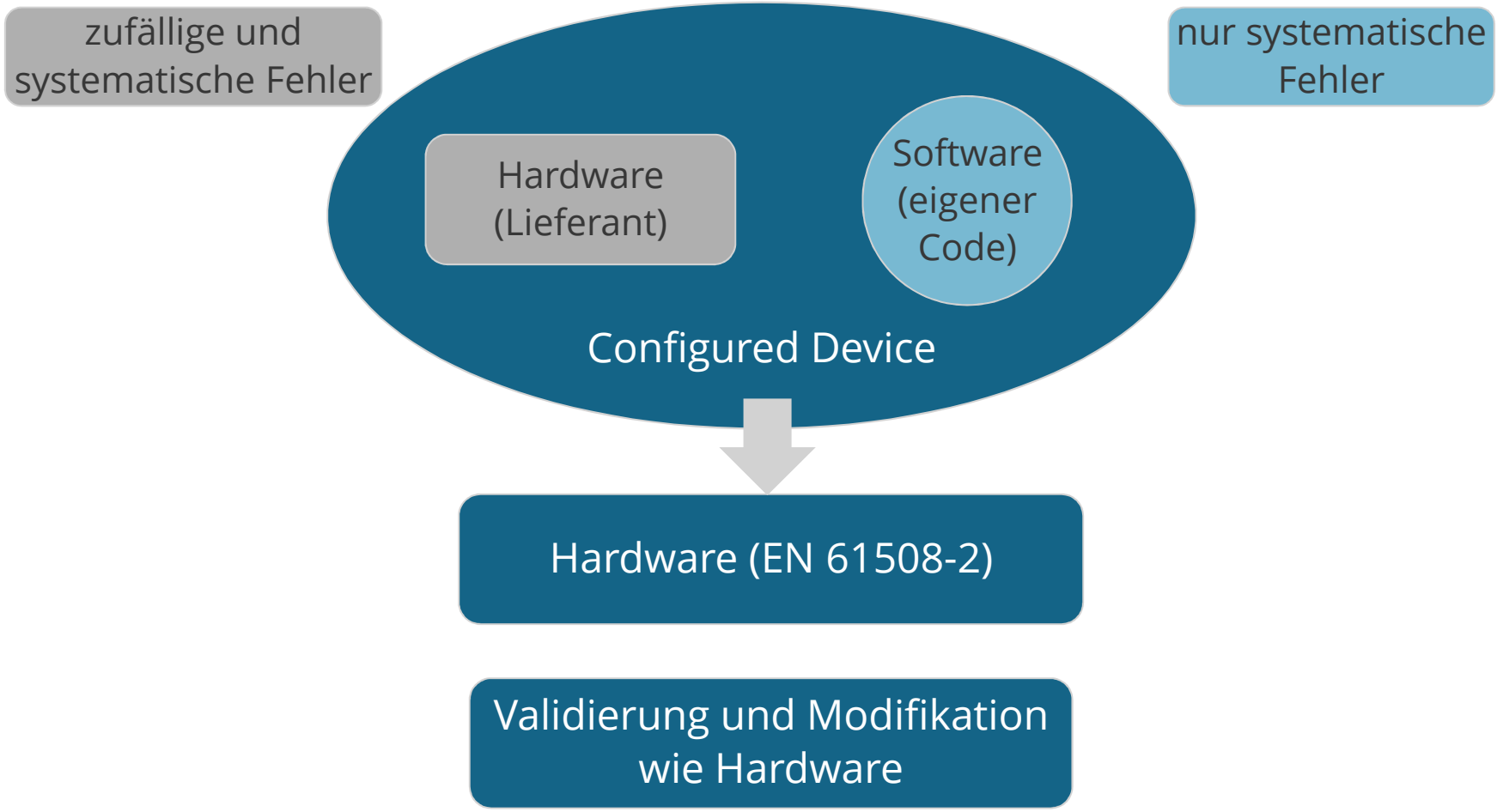


Risiko-Graph und Safety Integrity Levels

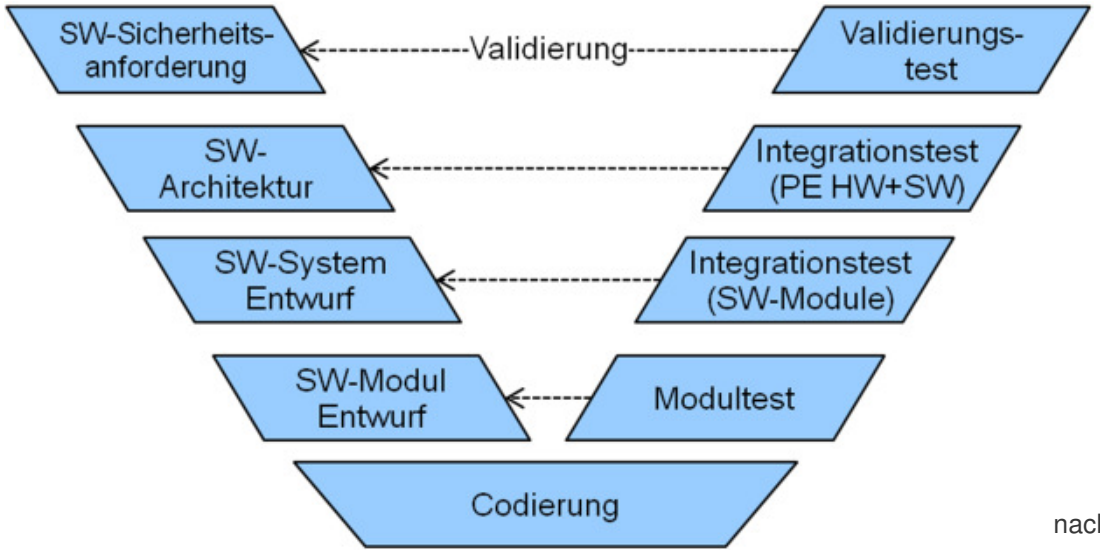


Der Risikograph ist nur eine Möglichkeit das Safety Integrity Level festzulegen (es besteht keine Normvorgabe)

Abriss spezielle Situation von programmierbaren Bausteinen



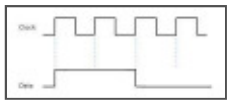
Entwicklungslebenszyklus für Software



nach DIN EN 61508-3

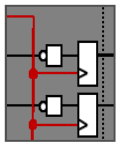
EN 61508-3 Anhänge bieten Informationen zu für die Auswahl von Verfahren und Maßnahmen für Spezifikation, Entwicklung, Validierung oder Modifikation, sowie Verfahren zur Feststellung der Sicherheitsintegrität
Der Anhang ist zur Information aber mit detaillierten Beschreibungen und Links zu den weiteren Erläuterungen der EN 61508-7

Verfahren und Maßnahmen (DIN EN 61508-2 Anhang F)

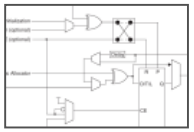


Specification,
Reference Signals

VHDL/ RTL
Description



Synthesis



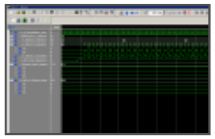
Routing

Configured Device

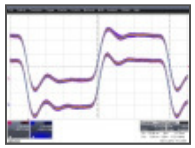
Moduls,
Timing Simulation

Stat. Timing
Analysis

Code inspection,
Funct. Simulation



HW Testing



Herstellung

Beispiele für Verfahren und Maßnahmen

Tabelle F.2 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während des Entwurfs und der Entwicklung von ASICs – Anwenderprogrammierbare ICs (FPGA/PLD/CPLD) (siehe 7.4.6.7)

Entwurfsphase	Ref.	Verfahren/Maßnahme	Siehe IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Schaltungs-beschreibung (Design entry)	1	Strukturierte Beschreibungsmethodik	E.3	++ hoch	++ hoch	++* hoch	++* hoch
	2	Entwurfsbeschreibung in (V)HDL (siehe Anmerkung)	E.1	++ hoch	++ hoch	++* hoch	++* hoch

EN 61508-2, Annex F

Beispiele:

- Design: Verwendung von Codierungsrichtlinien
- Synthesis: Consistency checks der Tools, IC Vendor Spezifikation
- Routing: Timing Analysis
- Produktion: Qualitäts-Management-System

Die “Proven in Use” Forderungen

25% der Verfahren und Maßnahmen des Anhang F fordern “betriebsbewährt”

- Entwicklung
  - Verwendung einer betriebsbewährten Entwicklungsumgebung
  - Verwendung betriebsbewährter (V)HDL-Simulatoren
  - Verwendung validierter Soft-Cores
- Synthesis
  - Interne Konsistenzprüfungen (mit Hinweis auf Beispiel)
  - Verwendung von betriebsbewährten Synthese Tools
  - Verwendung von betriebsbewährten Bibliotheken/CPLD Technologien
- Routing
  - Nachweis für der Betriebsbewährung für verwendete Hard Cores
- Fertigung
  - Verwendung von betriebsbewährten Prozesstechnologien
  - Verwendung von betriebsbewährter Schaltkreisfamilien
  - Betriebsbewährter Fertigungsprozess

Anforderungen an die Dokumentation zum Testing

- Zwei Zielrichtungen: Es muss zum einen die E/E Integration validiert werden, aber auch die Sicherheitsanforderungen des Ssystems
- Bei der Planung ist dabei sinnvollerweise folgendes zu dokumentieren
  - Welche Spezifikation liefert die Basis
  - Welches Testverfahren für z. B. die Sicherheitsfunktion bzw. –integrität
  - Kriterien zum Bestehen
  - Beschreibung Tests und Werkzeuge
  - Umgang mit Fehlern
- Bei der Umsetzung dann folgendes
  - Welche Spezifikation liefert die Basis
  - Welche Version wurde getestet
  - Welche Testwerkzeuge und in welchem Zustand
  - Ergebnisse, inkl. der gescheiterten Tests und Maßnahmen dazu

Tipps

Erfahrungen im Programmable IC design sind unabdingbar:

- Keine asynchronen Konstrukte erlaubt bzw. zu vermeiden (coding guideline)
- Module mit limitierten Funktionen und nicht bis an die Grenzen technisch ausgereizt
- Hohes Niveau von automatisiertem Testing (test benches) erforderlich mit entsprechender Testabdeckung
- Verschiedene Verantwortlichkeiten für Entwicklung, Testing, Reviews und Zertifizierung
- Deutliche detailliertere Dokumentation bei Entwicklung und Testing, nicht nur die Ergebnisse sind wichtig, sondern auch die Randbedingungen der Tests und die Gründe, warum man sich so entschieden hat

Zusammenfassung

Funktionale Sicherheit wird in allen Industriebereichen an Bedeutung zunehmen. Somit werden auch programmierbare Bausteine zunehmend Sicherheitsfunktionen übernehmen

- aber es ist machbar und möglich
- “Betriebsbewährt” ist das Hauptargument für Hardware, Werkzeuge und Mitarbeiter
- Umfassendes Testing und Validierung gem. Vorschlägen
- Weitreichende Dokumentation mit zusätzlichen Kommentaren
- Vermeidung von Änderungen, da aufwändig

Letztendlich entscheidet aber auch immer der Anwender, was er aus dem Thema Sicherheit macht

ese_Press_Automation

Missing Link Electronics
Industriestraße 4
89231 Neu-Ulm

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