IEC 61508 konforme Testfallerstellung nach SIL 3

Eugen Sawin

Problemstellung

- Voranschreitende Automatisierung der Sicherheitstechnik
- Sicherheitsfunktionen immer mehr in Software realisiert
- Zertifizierung nach Sicherheit und Verlässlichkeit wird notwendig

Fehlerquellen

- Ungenügende oder falsche Spezifikation
- Hohe Komplexität durch geringe Modularität
- Fehler im Design

  ⟶ Gefahren bei *fehlerfreiem* Betrieb

- Mangelndes Verständnis für Einsatzumgebung und Zweck der Software

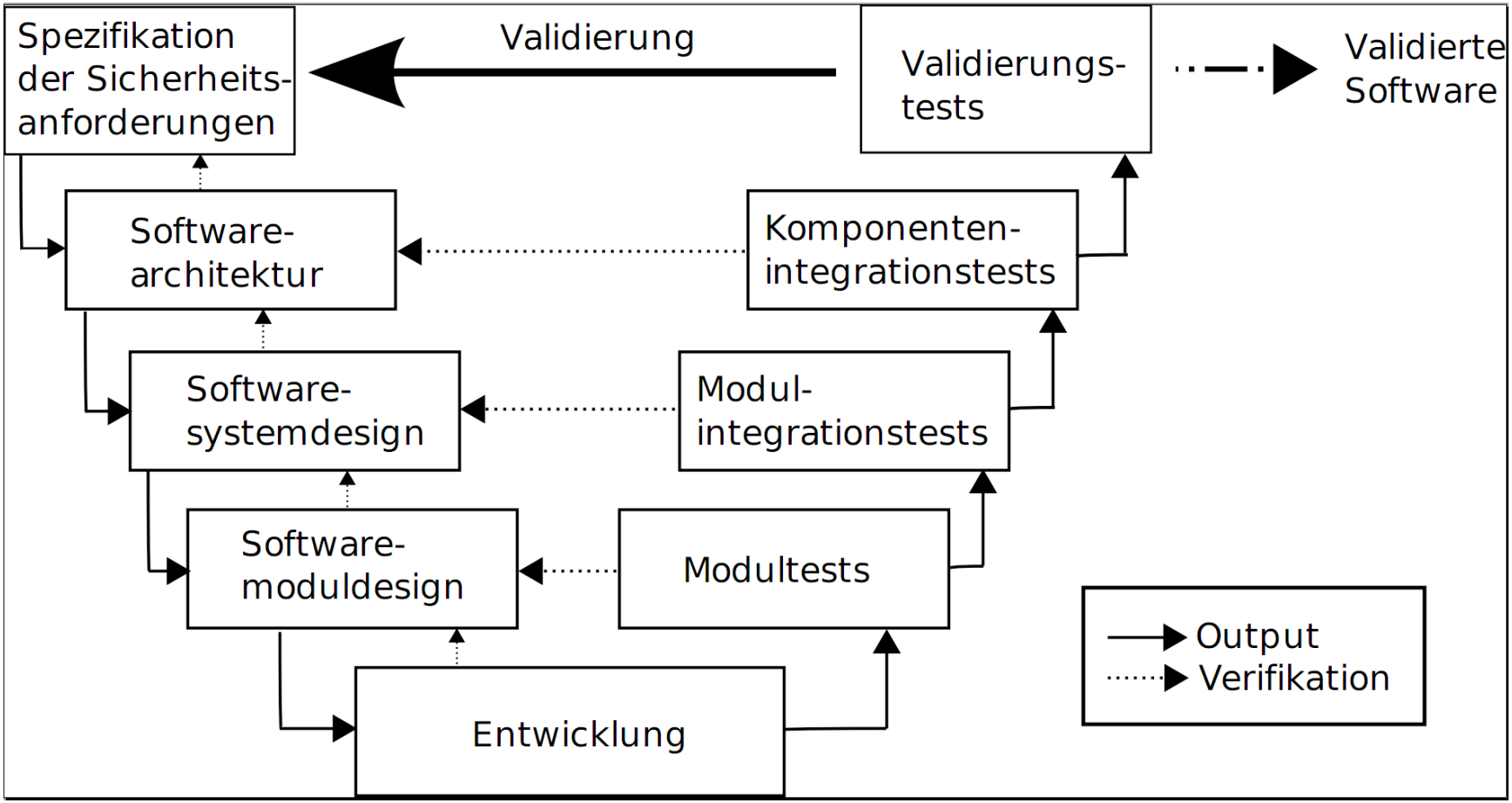
Fehlerentwicklungen Vermeiden

- Projektmanagement
- Dokumentation
- Isolation der Sicherheitsfunktionen
- Semi-formale Abnahme der Spezifikation
- Weitere Methoden
  - Checklisten
  - Werkzeugunterstützung
  - Formale Beweise

Dokumentation

- Projektphasendokumentation
- Versionierung
- Unterteilung in Zielgruppen
- Verfügbarkeit
- Unterstützung durch das Prozessmodell (V-Modell)

Entwicklungsprozessmodell



Personalkompetenz

- Erfahrung
  - Softwareentwicklung
  - Safety Engineering
  - Eingesetzte Werkzeuge
  - Organisatorisches Framework

IEC 61508

- **Allgemeine Norm für funktionale Sicherheit** von elektrischen, elektronischen und programmierbar elektronischen Systemen **mit Sicherheitsfunktion**

IEC 61508

- Eigenständige Norm
- Basis für Sektornormen
  - IEC 61511 für Prozessindustrie
  - IEC 61513 für Kernkraftwerke
  - DIN EN 50129 für Bahnanwendungen

Funktionale Sicherheit

- **Eine Funktion** zur Verminderung oder Beseitigung einer Gefahr

- **Nicht**: Beseitigung der Gefahrenquelle

Hazard Analysis

- Gefahren
  - Identifikation
  - Analyse

    ⟶ Risikomatrix

- Sicherheitsfunktionen
  - Spezifikation

Risikomatrix

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	III	III	III
Remote	III	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Risikoklassen

Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerabel only if risk reduction is impracticable or if the costs are grossly disproporionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

Risk Assessment

- Sicherheitsfunktion
  - Performance
  - Ausfallwahrscheinlichkeit
  - Qualitative und quantitative Methoden

    ⟶ Zielvorgabe für Safety Integrity Level

SIL für Low demand mode of operation

Safety Integrity Level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

SIL für High demand mode of operation

Safety Integrity Level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Risikoreduktion

- Verfahrens- und Designänderung
  - Beseitigung der Gefahr
  - Verminderung der Gefahr auf tolerierbares Niveau
- Sicherheitsfunktion
  - Abfangen/Verhindern eines gefährlichen Ereignisses
- Externe Faktoren

Spezifikation der Validierung

- Testplan
- Testdesigns
- Testfallspezifikation
- Testprozedur

Testplan

- Testplan
  - Zeitlicher Verlauf
  - Verantwortlichen
  - Testumgebung
  - Testaktivitäten

Spezifikation des Testdesigns

- Testdesign
  - Spezifikation der Sicherheitsfunktionen
  - Validierungsstrategie
  - Anforderungen an Testumgebung
  - Erfolgskriterien
  - Bewertung der Testergebnisse
  - Strategien zur Bewältigung von fehlgeschlagenen Tests

Testfallspezifikation

- Testfallspezifikation
  - Prozeduren der individuellen Testdurchläufe
  - Einstellungen des Systems
  - Ein- und Ausgabeparameter der Sicherheitsfunktion

Spezifikation der Testprozedur

- Testprozedur
  - Testverlauf
  - Prozeduren der eingesetzten Werkzeuge

Validierungsstrategien

- Probalistisches Testen
- Dynamische Analyse
  - Randwertanalyse
  - Error Seeding
  - Äquivalenzklassenanalyse
- Black-Box Testen

Functional Safety Assessment

- Nach Abschluss jeder Phase
- Personal mit der notwendigen Qualifikation
  - Aus einer unabhängigen Abteilung
  - Aus einem externen Unternehmen
- Stellt die erreichte SIL fest
- Basiert auf vorheriger Dokumentation und statistischen Tests

Ausblick

- IEC 61508 als Basis für weitere Standards
- Verbesserte Werkzeugunterstützung in allen Entwicklungsphasen
- Ausgereifte formale Beweisverfahren
- Modellbasiertes Testen
- Mögliche Vereinheitlichung der SIL-Bestimmung

Ende

Eugen Sawin
esawin@stud.fh-offenburg.de