Qualitätssicherung von Software

Prof. Dr. Holger Schlingloff

Humboldt-Universität zu Berlin
und
Fraunhofer FIRST

Wo stehen wir?

1. Einleitung, Begriffe, Software-Qualitätskriterien
2. manuelle und automatisierte Testverfahren
3. Verifikation und Validierung, Modellprüfung
4. statische und dynamische Analysetechniken
5. Softwarebewertung, Softwaremetriken
6. Codereview- und andere Inspektionsverfahren
7. Zuverlässigkeitstheorie
   - FMEA, FMECA
   - Fehlerbaumanalyse
   - stochastische Softwareanalyse
8. Qualitätsstandards, Qualitätsmanagement, organisatorische Maßnahmen

Zuverlässigkeitstheorie

- Quantitative Ermittlung von Ausfallwahrscheinlichkeiten
- Ursprung: Bewertung von Hardware
  - Alterung, Umwelteinflüsse, Materialfehler, ...
- Auch für Software einsetzbar?
  - Zertifizierungsproblematik, z.B. Cenelec
  - vorausschauende Hinweise auf Schwachstellen
    - welche Teile sollen Review unterzogen werden
    - Testüberdeckungsgrad

FMEA

- **F**ailure **M**ode and **E**ffects **A**nalysis
  - Identifikation potentieller Fehler und Auswirkungen
  - Quantifikation der Risiken
  - Entscheidungshilfen, Verbesserungsmaßnahmen
- „Probably the most commonly used analysis technique in embedded system design“
- Produkt- und Prozess-Sicht
  - System- oder Produkt-FMEA
    - systematische Analyse der möglichen Funktionsfehler
    - Berechnung der funktionalen Zusammenhänge der Komponenten
  - Prozess-FMEA
    - Analyse möglicher Fehler im Herstellungsprozess
    - Berücksichtigung der beteiligten Akteure

Wie wird bewertet?

- Analyse jeder Komponente
  - mögliche Fehler
  - Ursachen für den Fehler
  - verbundenes Risiko
- Vorgehensweise
  1. Abgrenzen der Betrachtungseinheit
     (Systemstruktur)
  2. Funktionsanalyse
     - Zusammenhänge den einzelnen Elementen aufzeigen
     - Funktionskritische Merkmale erkennen
  3. Fehleranalyse
  4. Risikobewertung
  5. Verbesserungsmaßnahmen

Bewertung

- Risikoprioritätszahl = A * E * B
  - A = P(Auftreten): Eintrittswahrscheinlichkeit
  - E = P(Entdeckung): Wahrscheinlichkeit, dass Fehler sich auswirkt bevor er entdeckt und beseitigt werden kann
  - B = Bedeutung: Gewicht der Folgen
- Richtlinie
  - **RPZ > 0,01:** unbedingt Maßnahmen festlegen und umsetzen
  - **0,004 < RPZ < 0,01:** gegebenenfalls Maßnahmen festlegen und umsetzen
  - **RPZ < 0,004:** mit Restrisiko leben

Beispiel

Funktion / Komponente	Fehler	Folgen	Ursachen	Prüfung	A	E	B	RPZ
Netzkabel	Isolation beschädigt	Stromschlag	äußere Einwirkung	Sichtkontrolle	0,2	0,1	0,4	**0,008**
	Kind zieht am Kabel	Verletzung	Spieltrieb	Bedienungsanleitung	0,5	0,2	0,7	**0,07**
	Kabelbruch	Geräteausfall	mech. Belastung	Funktionstest	0,1	0,3	0,1	**0,003**

nach P. Vetsch, Rheintal Handelsgesellschaft, Mauren

- Beispiel Steer-by-wire System

Maßnahmenvorschläge

- Vermeidung von Fehlerursachen!

- Bei hohen Auftrittswahrscheinlichkeiten
  - Qualitätssicherung stärken
- Bei geringen Erkennungswahrscheinlichkeiten
  - Möglichkeit der Fehleroffenbarung einbauen
- Bei schwerwiegenden Folgen
  - Auswirkungen begrenzen

Durchführung

- Phase 1: Vorbereitungen durch den Projektleiter
  - Abgrenzung und Struktur des Untersuchungsobjektes
  - Team, Zeitpunkt, Unterlagen
- Phase 2: Durchführung der FMEA
  - Information des Teams über das Objekt
  - Funktions- / Prozessanalyse durchführen
  - Brainstorming über mögliche Fehler (Fehleranalyse)
  - Risikobewertung der identifizierten Fehler
  - Dokumentation im FMEA-Formular
- Phase 3: Verbesserungsmaßnahmen
  - Verbesserungsmaßnahmen erarbeiten
  - Neubeurteilung, Dokumentation

FMECA

- Erweiterte FMEA mit der Analyse der Fehlergefährlichkeit (**F**ailure **M**ode, **E**ffects and **C**riticality **A**nalysis)

- Die Schwere des Fehlers wird quantitativ bestimmt
  - Verlust in € bzw. Schadenshöhe

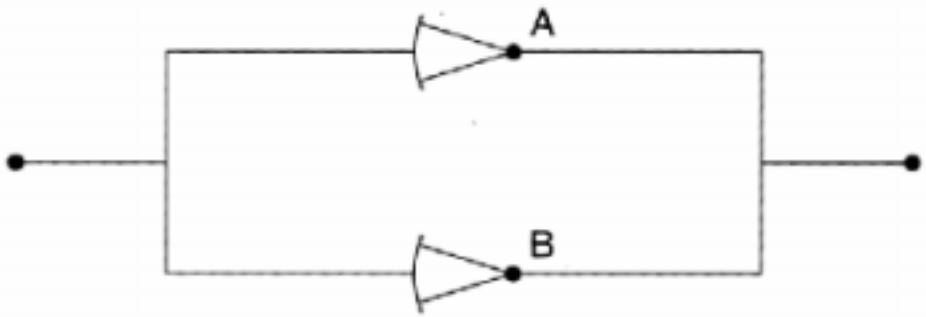
Gefährdungsanalyse (Hazard Analysis)

Gefährdungsklassen, z.B. in MIL-STD-882B:

- **Category 1:** *Catastrophic:* may cause death or system loss
- **Category 2:** *Critical:* may cause severe injury, severe occupational illness, or major system damage
- **Category 3:** *Marginal:* may cause minor injury, minor occupational illness, or minor system damage
- **Category 4:** *Negligible:* will not result in injury, occupational illness, or system damage

Gefärdungswahrscheinlichkeit

- **Frequent:** Likely to occur frequently to an individual item, continuously experienced throughout the fleet or inventory
- **Probable:** Will occur several times during the life of an individual item, frequently throughout the fleet or inventory
- **Occasional:** Likely to occur sometime during the life of an individual item, several times throughout the fleet or inventory
- **Remote:** Unlikely to occur but possible during the life of an individual item; unlikely but reasonably expected to occur in a fleet or inventory
- **Improbable:** Extremely unlikely to occur to an individual item; possible for a fleet or inventory
- **Impossible:** Cannot occur to an item or in fleet or inventory



Critical	Failure probability	Failure mode	% failures by mode	Effects	
				Critical	Noncritical
A	1×10^{-3}	Open	90		X
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	
B	1×10^{-3}	Open	90		X
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	

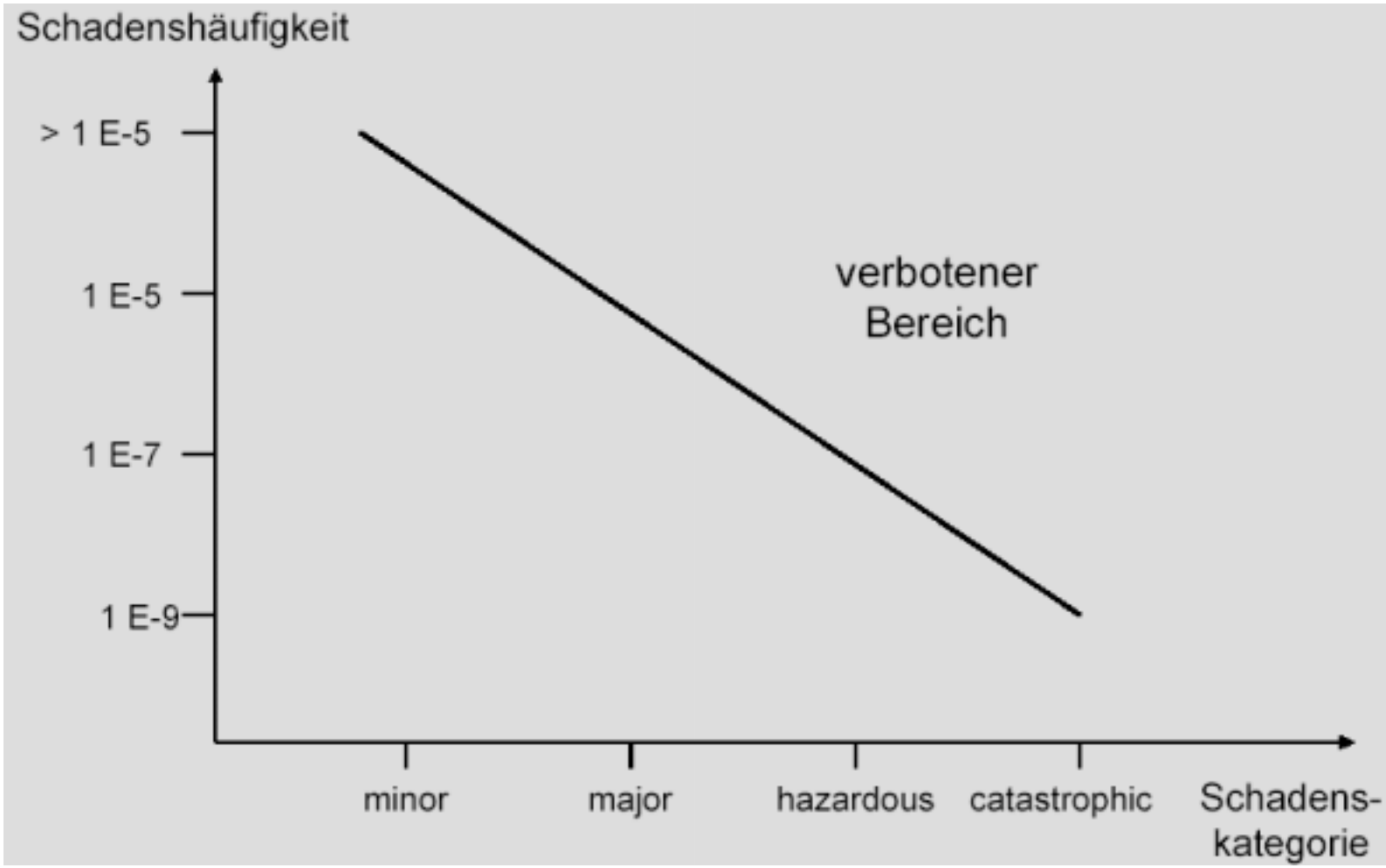
FIGURE 14.9
FMEA for a system of two amplifiers in parallel. (Source: W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D.C., 1981, page II-3) [Leveson]

Failure Modes and Effects Criticality Analysis

Subsystem _____ Prepared by _____ Date _____

Item	Failure Modes	Cause of Failure	Possible Effects	Prob.	Level	Possible Action to Reduce Failure Rate or Effects
Motor Case	Rupture	a. Poor workmanship b. Defective materials c. Damage during transportation d. Damage during handling e. Overpressurization	Destruction of missile	0.0006	Critical	Close control of manufacturing processes to ensure that workmanship meets prescribed standards. Rigid quality control of basic materials to eliminate defectives. Inspection and pressure testing of completed cases. Provision of suitable packaging to protect motor during transportation.

Schadensart und -Häufigkeit



Beispiel: Cenelec SIL

Table A.1 – SIL-table

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

- SIL = safety integrity level
- System-SIL wird bestimmt durch RAMS-Analyse gemäß EN50126
  (Reliability, Availability, Maintainability, Safety)

Bestimmung der Software-SIL

- Software-SIL richtet sich nach System-SIL

  „... werden auf Basis der Risikostufe für den Einsatz der Software im System entschieden...“

- Im Allgemeinen ist Software-SIL gleich der System-SIL

  „Without further precautions, the software safety integrity level shall be, as a minimum, identical to the system safety integrity level.“

- Ausnahmen möglich, falls zusätzliche Sicherungsmaßnahmen eingeführt werden

  „if mechanisms exist to prevent the failure of a software module from causing the system to go to an unsafe state, the software safety integrity level of the module may be reduced“

  Beispiel: HW-Watchdog, Voter o.ä.


QUALITY
CONTORL
A. BACALL