

# Zertifizierung

## Echtzeitsysteme 2 - Vorlesung/Übung

**Fabian Scheler**  
**Michael Stilkerich**  
**Wolfgang Schröder-Preikschat**

Lehrstuhl für Informatik IV  
Verteilte Systeme und Betriebssysteme  
Friedrich-Alexander Universität Erlangen-Nürnberg

<http://www4.cs.fau.de/~{scheler,mike,wosch}>  
{scheler,mike,wosch}@cs.fau.de



1

# Übersicht

- Allgemein
- eine Zertifizierungsstelle: TÜV Nord
- wichtige Normen
  - DO-178B & DO-248B
  - IEC 61508
- Forschung: Zertifizierung von Softwarekomponenten



© {scheler,mike,wosch}@cs.fau.de - EZS2 (SS 2007)

2

## Definition: Zertifizierung

*„Das Verfahren bzw. das Ergebnis des Verfahrens, bei dem einem Unternehmen bestätigt wird, dass es über ein Qualitätsmanagement-System verfügt, das den entsprechenden Normen entspricht. Als Zertifizierung bezeichnet man die Bestätigung der Abläufe auf Normenkonformität durch eine unabhängige akkreditierte Zertifizierungsgesellschaft.“*

**QM-Lexikon (<http://www.quality.de>)**



© {scheler,mike,wosch}@cs.fau.de - EZS2 (SS 2007)

3

## Arten der Zertifizierung

- **prozessorientierte** Zertifizierung
  - Beurteilung des des Softwareentwicklungsprozesses
  - keine Überprüfung von Produkten
  - Annahme: Einhaltung von Normen ↔ Software hoher Qualität
- **produktorientierte** Zertifizierung
  - überprüft gewisse Eigenschaften des Produkts
  - Rückschlüsse vom Softwareentwicklungsprozess möglich
- **projektbegleitende** Zertifizierung
  - Prüfung des Entwicklungsprozesses eines bestimmten Produkts



© {scheler,mike,wosch}@cs.fau.de - EZS2 (SS 2007)

4

## Arten der Zertifizierung: Beispiele

- ISO 9000-3
  - prozessorientiert
  - spezifiziert diverse Phasen des Softwareentwicklungsprozesses
    - Vertragsabschluss
    - Festlegung der Forderung des Auftraggebers
    - Planung von Entwicklung und Qualitätssicherung
    - Entwurf & Implementierung
    - Testen & Validierung
    - Abnahme & Vervielfältigung
    - Lieferung, Installation, Wartung
- RAL-GZ 901
  - Prospektprüfung
  - nur im Prospekt zugesicherten Eigenschaften werden geprüft

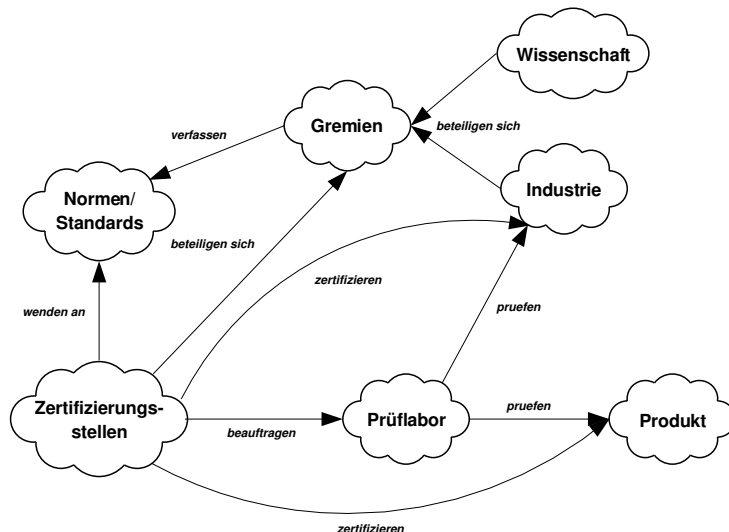


## Wer vergibt Zertifikate

- Auftraggeber
  - Bewertung der Lieferanten
- anerkannte Zertifizierungsstellen
  - im Auftrag von Unternehmen
  - Unteraufträge an Prüflabors
- Wer entscheidet über die Anerkennung eines Zertifikats?
  - der Auftraggeber / Kunde



## Überblick: Zertifizierung



## TÜV Nord: Prüfstelle SEELAB

- Prüfstelle nach DIN EN ISO/IEC 17025
- Inspektionsstelle nach DIN EN ISO/IEC 17020
- Dienstleistungen in den Bereichen
  - Leittechnik
  - Automatisierungssysteme
  - Soft- und Hardware
- Aufgaben: Nachweis von
  - Qualität
  - Zuverlässigkeit
  - Sicherheit (safety & security)im Auftrag von Industrie und Behörden



# TÜV Nord: Zertifizierungsstelle SEECERT

- Überprüfung von Rechnern und Software
- Prüfung hinsichtlich diverser Normen
  - IEC 61508
  - IEC 61513
  - Wortschatzkriterien für Wörterbücher
  - ...
- Referenzen
  - 3SOFT GmbH – IEC 61508 (in Vorbereitung)
  - Alstom – IEC 61508
  - BMW – IEC 61508
  - Conti Temic – IEC 61508
  - ...



# Wichtige Normen

- DO-178B
  - Allgemein
  - Konzept
  - Prozesse und Dokumente
- DO-248B
- IEC 61508
  - Allgemein
  - Ansatz und Konzept
  - Struktur
  - Lebenszyklus
  - Part 1 & Part 3



# DO-178B

## *Software Considerations in Airborne Systems and Equipment Certification*

- Komitee:
  - **RTCA** (*Radio Technical Commission for Aeronautics*)
  - **EUROCAE** (*European Organisation for Civil Aviation Equipment*)
- Anwendung durch:
  - **FAA** (*Federal Aviation Administration*)
  - ...
- erlaubt nur die Zertifizierung **kompletter Systeme**



# DO-178B

- fünf mögliche Risikostufen

<b>Catastrophic</b>	Fehler kann Systemversagen verursachen
<b>Hazardous</b>	Fehler kann die Sicherheit oder Leistung des Systems vermindern, ein weiterer Betrieb des Systems ist nur noch unter erschwerten Bedingungen möglich. Insassen können verletzt werden
<b>Major</b>	Fehler ist ernst, aber nicht schwerwiegend. verursacht z.B. bei Passagieren keine Verletzungen aber Unbehagen
<b>Minor</b>	Fehler ist störend, aber nicht schwerwiegend. Kann bei Passagieren beispielsweise zu Unannehmlichkeiten führen
<b>No Effect</b>	

- je nach Risikostufe wird der Level für DO-178B bestimmt

		zu erfüllende	unabhängig zu
Level	Risiko	Vorgaben	erfüllende
<b>A</b>	Catastrophic	66	25
<b>B</b>	Hazardous	65	14
<b>C</b>	Major	57	2
<b>D</b>	Minor	28	2
<b>E</b>	No Effect	0	0



## DO-178B: Prozesse und Dokumente

### ■ Planung

- Dokumente: alle möglichen Pläne (Software development, certification, quality assurance, ... plan)

### ■ Entwicklung

- Dokumente: Anforderungen, Entwurf, Quellcode, ausführbarer Binärcode
- Verfolgbarkeit von der Anforderung über den Quellcode zum Binärcode
- Entwicklungsmodelle: V-, Spiral-, Wasserfallmodell

### ■ Verifikation

- Dokumente: Verifikationsfälle und -prozeduren und Ergebnisse
  - Review von Requirements, Design und Quellcode
  - Testen von Binärcode
  - Code Coverage
- Testen: Modul-, Integrations- und Akzeptanztest



## DO-178B: Prozesse und Dokumente

### ■ Konfigurationsmanagement

- Umgebung
  - Softwareentwicklung
  - Testen
  - Analyse
  - Integration
- alle Dokumente, Software und Hardware

### ■ Qualitätssicherung

- Reviews, Audits
- Protokolle
- Schnittstelle zum Zertifizierungsprozess



## DO-248B

### ■ DO-178B Standard hat Schwächen in den Bereichen

- Anforderungsdefinition und -analyse
- Partitionierung (z.B. welche Techniken sind wann adäquat?)
- Verifikation
- COTS Software
- Einfluss von Software auf die Sicherheit des Gesamtsystems

### ■ DO-248B

- erläutert den DO-178B Standard (keine Erweiterung)
- korrigiert 12 Fehler
- enthält 76 FAQ
- enthält 15 Diskussionspapiere



## IEC 61508

*Functional safety of  
electrical/electronic/programmable electronic  
safety-related systems*

### ■ Komitee:

- **IEC** (*International Electrotechnical Commission*)
- **CEN** (*Comité Européen de Normalisation*)

### ■ Anwendung durch

- Industrie
- Behörden
- ...



## IEC 61508: Allgemein

- generischer Sicherheitsstandard
  - dient als Basis für branchenspezifische Standards
  - z.B. IEC 61511 - Prozessindustrie
  - z.B. IEC 61513 – Kernkraftwerke
  - Standard für Automobilindustrie in Vorbereitung
- hauptsächlich für E/E/PES
- Entwicklung
  - 1984: TÜV Richtlinien, Safety-Klassen 1-9
  - 1989: DIN 19250/VDE 0801 Safety-Klassen 1-9
  - 1997: IEC 61508, SIL 1-4
- erlaubt die Zertifizierung **einzelner Komponenten**



## IEC 61508: Ansatz

- Rangliste der Fehlerquellen
    - 1) Spezifikation
    - 2) Modifikationen nach Inbetriebnahme
    - 3) Betrieb & Wartung
    - 4) Entwurf & Implementierung
    - 5) Installation & Inbetriebnahme
  - spezifische Eigenschaften von E/E/PES
    - hohe Komplexität
    - elektronische Interferenz
    - nur Hardwarefehler können quantifiziert werden
    - Software kann nicht ausreichend quantitativ bewertet werden
    - Zuverlässigkeit von Software kann nur optimiert, kaum garantiert werden
    - hohe Kompetenz im gesamten Lebenszyklus notwendig
- Standard umfasst den **kompletten Lebenszyklus** eines Systems



## IEC 61508: Konzept

- **Safety Integrity Level (SIL)**
  - richtet sich nach der PFD (*Probability of Failure upon Demand*)

SIL	PFD
4	$10^{-5} - 10^{-4}$
3	$10^{-4} - 10^{-3}$
2	$10^{-3} - 10^{-2}$
1	$10^{-2} - 10^{-1}$

- **Risikofunktion**
  - Funktion aus Wahrscheinlichkeit und Schwere von Fehlern
  - es bleibt **immer** ein Restrisiko
  - notwendige Risikoreduktion = Risiko – tolerierbares Risiko
  - muss ALARP (*As Low As Reasonably Practicable*) reduziert werden
- **Sicherheitsfunktion**
  - Maßnahmen zur Reduktion des Risikos
  - müssen von Anfang bedacht werden

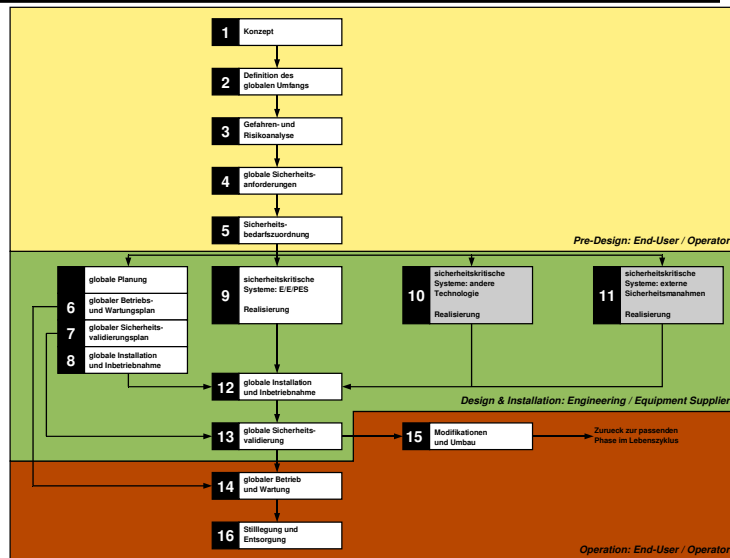


## IEC 61508: Struktur

- Teil 1: General Requirements
  - Teil 2: Requirements for electrical, electronic, programmable electronic systems
  - Teil 3: Software requirements
  - Teil 4: Definitions and abbreviations
  - Teil 5: Examples of methods for the determination of safety integrity levels
  - Teil 6: Guidelines on the application of Parts 2 & 3
  - Teil 7: Overview of techniques and measures
- Teil 1-3: normativ, Teil 4-7: informativ



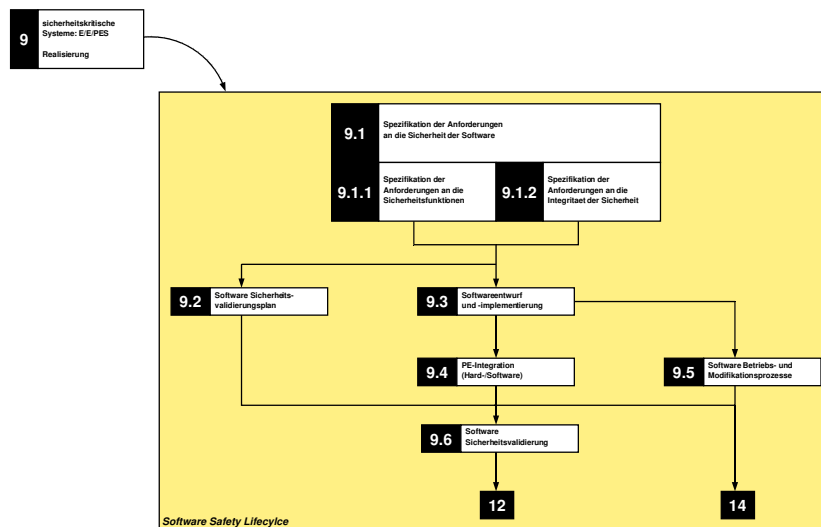
# IEC 61508: Lebenszyklus



# IEC 61508: Part 1

- definiert die **Aktivitäten des Lebenszyklus**
  - Entwicklung der Sicherheitsanforderungen
  - Zuordnung der Sicherheitsanforderungen zum System
  - Installation, Inbetriebnahme und Validierung des Systems
  - Betrieb, Wartung, Modifikation und Stilllegung des Systems
- Beschreibt die Anforderungen an die
  - Handhabung der funktionalen Sicherheit
  - Bewertung der funktionalen Sicherheit

# IEC 61508: Part 3



# IEC 61508: Part 3

- Software Qualitätssicherung**
  - Konfigurationsmanagement
    - beinhaltet alles, was zum Erstellen der Software verwendet wird
    - Sicherung/Dokumentation der kompletten Entwicklungsumgebung
  - Formale Dokumentation der Veröffentlichung relevanter SW
    - Sicherungskopien
    - lebenslange Betreuung
- Entwurf & Implementierung**
  - Architektur
  - Review und Evaluation
  - geeignete Entwicklungswerkzeuge (je nach SIL)
  - Verifikation der Anforderungen

## IEC 61508: Part 3

- **PE Integration & Sicherheitsvalidierung**
  - Kompatibilität von Hardware und Software
  - Dokumentation der Umgebung der Integration und Validierung
    - Verfahren
    - Werkzeuge
  - Validierung des Systems
    - Testen
    - Modellierung
    - Simulation
    - ...
- **Modifikationen**
  - entsprechende Schritte müssen wiederholt werden



## Zertifizierung von Softwarekomponenten

- Problemstellung und Lösungsansatz
- Usage-based Testing
- Zertifizierung
  - Prozess
  - Ergebnis
  - System
- Future Work

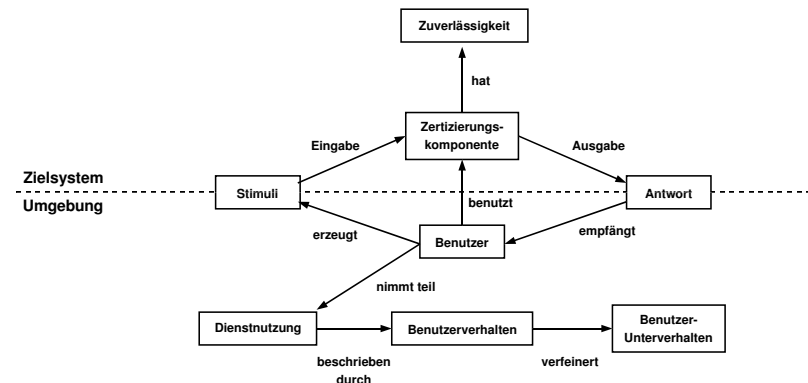


## Problem und Lösungsansatz

- **Problem**
  - Zertifizierung kompletter Systeme: teuer & aufwendig
  - Zertifizierung von Komponenten: genaue Verwendung der Komponenten oft nicht absehbar
- **Lösungsansatz:**
  - Zertifizierung auf Basis wiederverwendbarer Softwarekomponenten
  - Zertifizierung im Hinblick auf Verwendungsprofile
- Hier:
  - Zertifizierung der Zuverlässigkeit
  - Usage-based testing
  - Objekt-orientierte Software



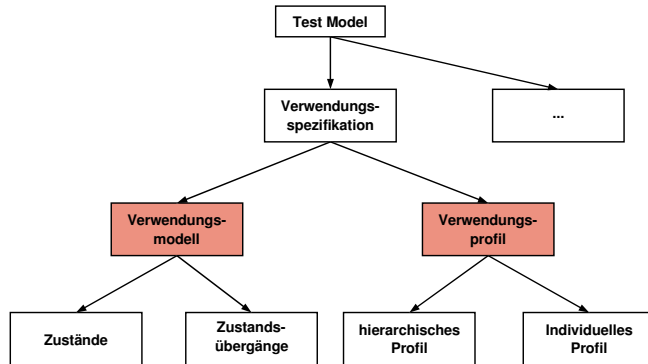
## Usage-based testing



- Beschreibung der Verwendung/Umgebung durch Modelle
- Generierung von Testfällen mit Hilfe dieser Modelle



# Modellierung der Umgebung



## Verwendungsmodell

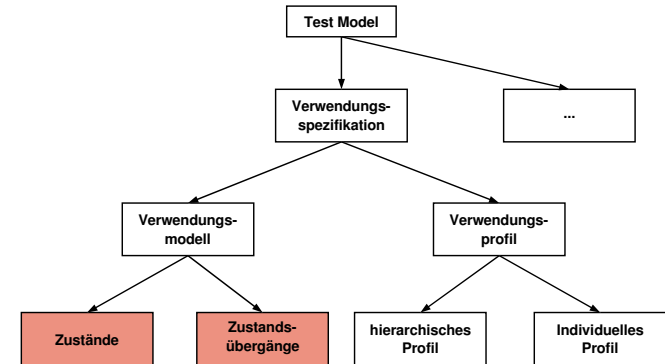
- modelliert die möglichen Verhaltensweisen der Benutzer

## Verwendungsprofil

- quantifiziert die verschiedenen Verhaltensweisen hinsichtlich der Wahrscheinlichkeit ihres Auftretens



# Modellierung der Umgebung

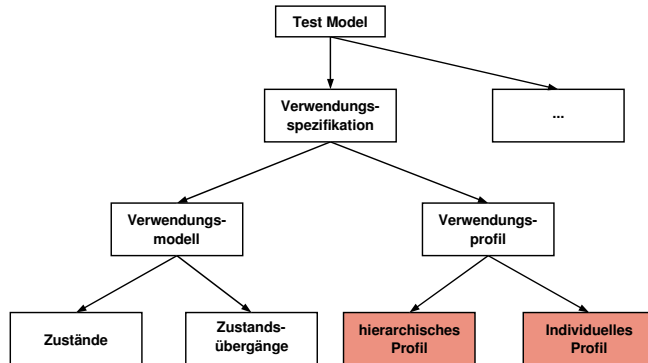


## Verwendungsmodell ist ein Zustandsautomat und besteht aus

- Zuständen
- Zustandsübergängen



# Modellierung der Umgebung



## hierarchisches Profil

- Wahrscheinlichkeit für das Auftreten eines spezifischen Benutzers

## individuelles Profil

- das Profil eines speziellen Benutzers, für die Benutzung eines Dienstes



# Modellierung der Umgebung

## Kombination

- Testumgebung
- Modell der Umgebung

## → Benutzertypen

- Benutzer mit demselben Verhalten (demselben Ziel, i.d.R. haben diese Benutzer identische Verwendungsmodelle)

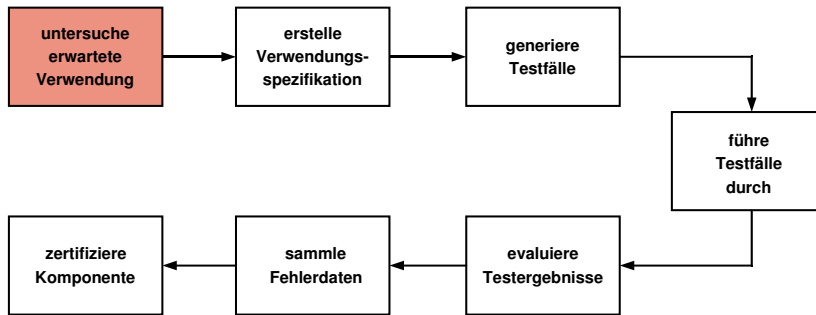
## → Benutzersubtypen

- Benutzertypen mit demselben Verwendungsprofil
- Benutzer haben dasselbe statistische Verhalten





## Zertifizierung: Prozess

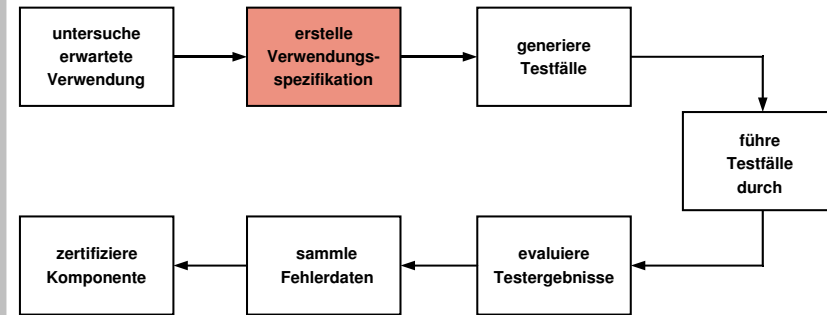


### ■ Untersuchung der **erwarteten Verwendung**

- Studien ähnlicher Systeme
- keine genauen Verwendungswahrscheinlichkeiten (VW), sondern relative Wahrscheinlichkeiten verschiedener Dienste



## Zertifizierung: Prozess

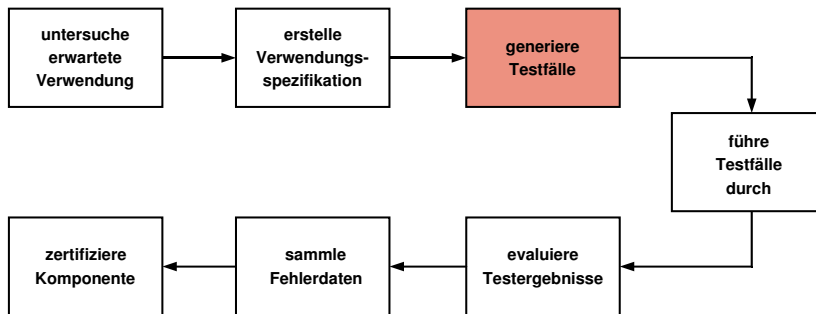


### ■ Erstellung der **Verwendungsspezifikation**

- identifiziere Dienste der Komponente
- finde Benutzertypen und -subtypen → **Verwendungsprofil**
- erwartete Verwendung → **Verwendungsmodell**
- Analyse der Spezifikation: wird die erwartete Verwendung beschrieben?



## Zertifizierung: Prozess

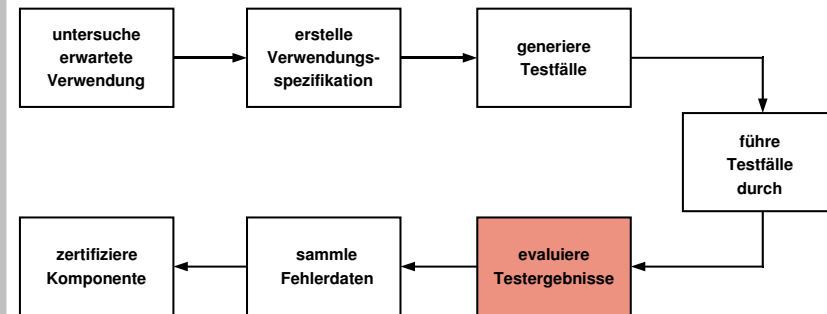


### ■ Generierung von **Testfällen**

- Stimuli werden aus der Verwendungsspezifikation erzeugt
- Tester agiert als System und erstellt die erwarteten Antworten
- Erstellung der Testfälle kann parallel zur Entwicklung erfolgen
- Zukunft
  - Verwendung von *Use-Cases* und *Szenarios*
  - automatische Prüfung gegen die Anforderungsspezifikation



## Zertifizierung: Prozess

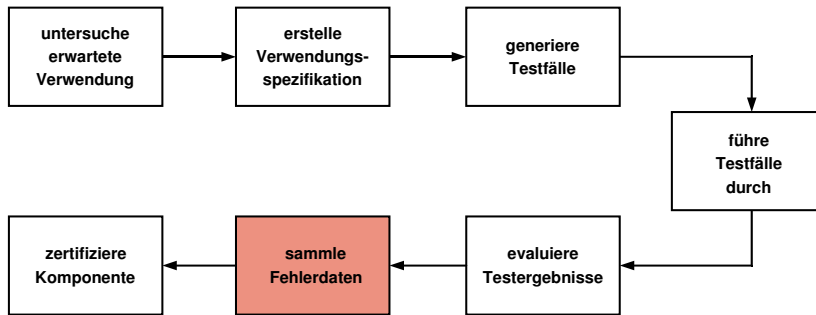


### ■ Evaluation der **Testergebnisse**

- Analyse der Log-Dateien



## Zertifizierung: Prozess

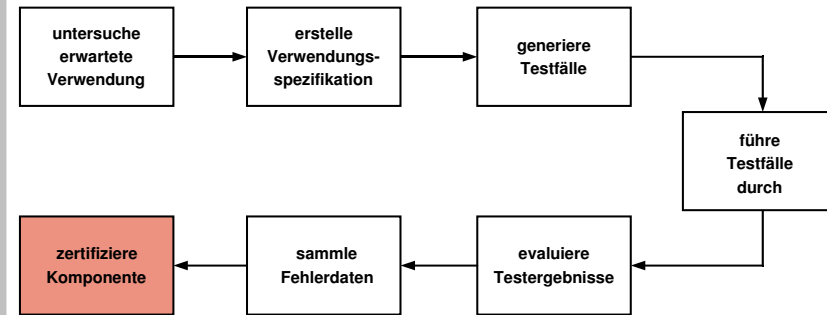


### Fehlerdaten

- Zeitspanne zwischen Fehlern



## Zertifizierung: Prozess



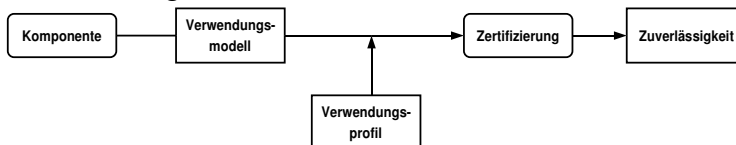
### Zertifizierung

- Anwendung der Modelle zur Bewertung von Zuverlässigkeit

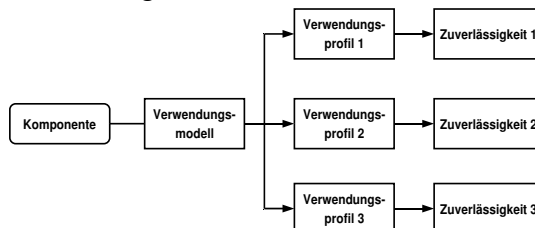


## Zertifizierung: Ergebnis

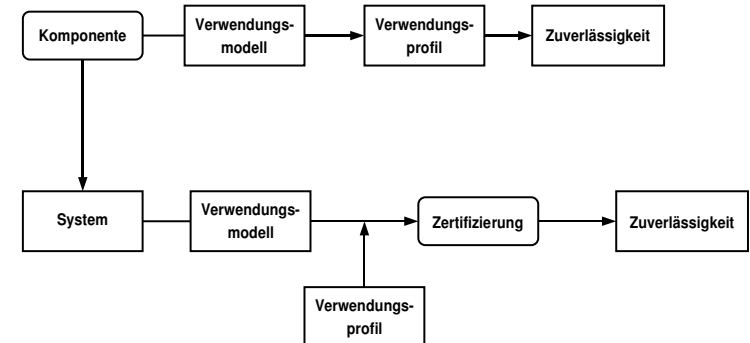
- ein Verwendungsmodell, ein Verwendungsprofil
- ein Zuverlässigkeitsmaß ...



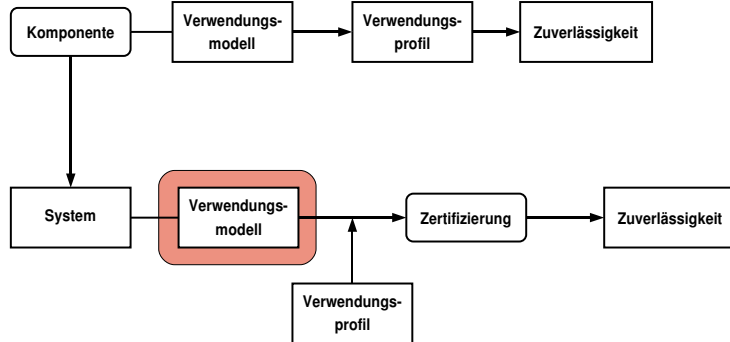
- ... mehrere Verwendungsprofile
- mehrere Zuverlässigkeitsmaße



## Zertifizierung: System



## Zertifizierung: System

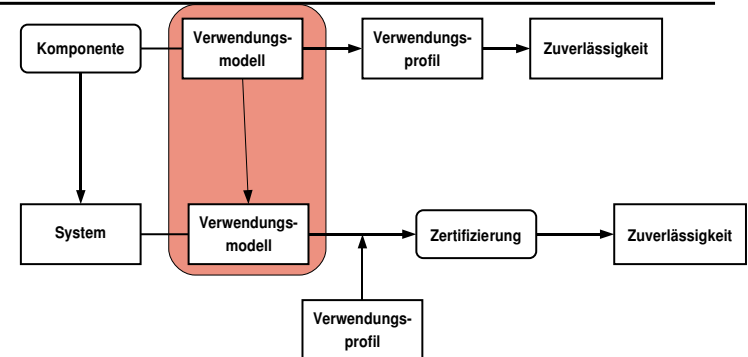


### ■ Ansatz 1

- Verwendungsmodell wird **neu erstellt**
- ✓ unabhängig von den verwendeten Komponenten
- ✗ Nachteil
  - aufwändig, teuer
  - Änderung einer Komponenten erfordert neue Zertifizierung des Systems



## Zertifizierung: System

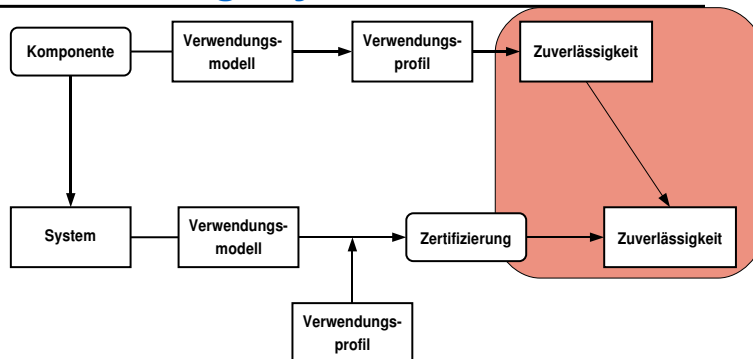


### ■ Ansatz 2

- **komponiere** Verwendungsmodelle des System und der Komponenten
- ✗ Nachteil
  - Relation: Komponenten ↔ Teile des Verwendungsmodells des Systems erforderlich
  - Änderung einer Komponenten erfordert neue Zertifizierung des Systems



## Zertifizierung: System



### ■ Ansatz 3

- Systemzuverlässigkeit leitet sich aus der Zuverlässigkeit der Komponenten ab
- ✗ Nachteil: geringere Genauigkeit der Zertifizierung



## Future Work

- erneute Zertifizierung falls sich Modelle ändern
  - wann ist eine erneute Zertifizierung notwendig?
  - Abstandsmaße für
    - Verwendungsprofile
    - Verwendungsmodelle
- OO: Oberklassen und Unterklassen
  - Lässt sich das Verwendungsmodellen übertragen?



- Allgemein
  - Arten der Zertifizierung
  - Wer? Wo? Was? Warum?
- TÜV Nord
  - SEELAB und SEECERT
- Normen
  - DO-178B, DO-248B, IEC 61508
- Zertifizierung von Komponenten
  - basierend auf Usage-based Testing
  - Future Work

