

# Zertifizierung

## Echtzeitsysteme 2 - Vorlesung/Übung

**Peter Ulbrich**  
**Fabian Scheler**  
**Wolfgang Schröder-Preikschat**

Lehrstuhl für Informatik 4  
Verteilte Systeme und Betriebssysteme  
Friedrich-Alexander Universität Erlangen-Nürnberg

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



1

## Übersicht

- Allgemein
- Eine Zertifizierungsstelle: TÜV Nord
- Wichtige Normen
  - DO-178B & DO-248B, DO-254
  - IEC 61508

© {ulbrich, scheler, wosch}@cs.fau.de - EZL (SS 2010)

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>)**

## Arten der Zertifizierung

- **prozessorientierte** Zertifizierung
  - Beurteilung 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

© {ulbrich, scheler, wosch}@cs.fau.de - EZL (SS 2010)

4

© {ulbrich, scheler, wosch}@cs.fau.de - EZL (SS 2010)

3

## 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

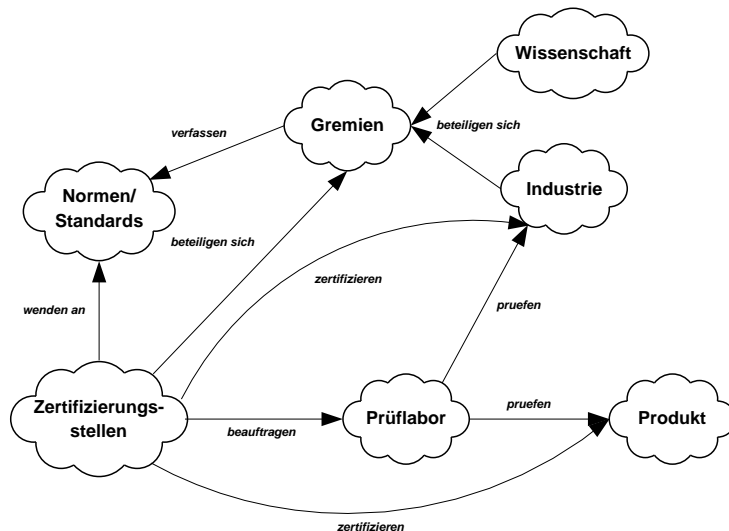


## Wer vergibt Zertifikate

- 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



- Überprüfung von Rechnern und Software
- Prüfung hinsichtlich diverser Normen
  - IEC 61508
  - IEC 61513
  - Wortschatzkriterien für Wörterbücher
  - ...
- Referenzen
  - Alstom – IEC 61508
  - BMW – IEC 61508
  - CATERPILLAR – IEC 61508
  - Conti Temic – IEC 61508
  - ...



- Luftfahrt
  - DO-178B & DO-248B (Software)
  - DO-254 (Hardware)
- Elektronische Systeme
  - IEC 61508



## DO-178B & DO-254

### DO-178B

*Software Considerations  
in Airborne Systems  
and Equipment Certification*

### DO-254

*Design Assurance Guidance  
for Airborne Electronic  
Hardware*

**Inkl. FPGAs und Firmware!**

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



## DO-178B & DO-254

- fünf mögliche Risikostufen

Risikostufe	Auswirkung
<b>Catastrophic</b>	Fehler führt zu Systemversagen und verhindert sicheren Flug und Landung, Todesopfer möglich.
<b>Hazardous</b>	Fehler ist schwerwiegend und schränkt die Flugsicherheit und Flugleistung signifikant ein, schwere Verletzungen und Sachschäden möglich.
<b>Major</b>	Fehler ist ernst und mindert die Flugsicherheit und schränkt die Flugleistung teilweise ein, leichte Verletzungen und Sachschäden möglich.
<b>Minor</b>	Fehler ist störend, mindert die Flugsicherheit aber nicht wesentlich und führt lediglich zu Unannehmlichkeiten für die Insassen.
<b>No Effect</b>	Fehler beeinträchtigt den Betrieb des Flugzeugs in keiner Weise.

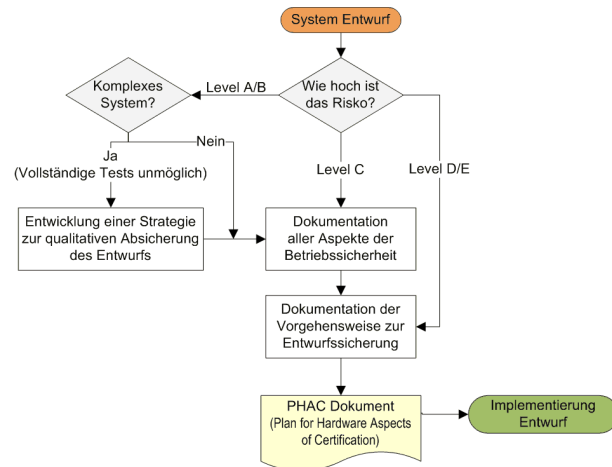
- Resultierende **Design Assurance Level** (DAL  $\hat{=}$  IEC65108 SIL)

DAL	Risikostufe	Fehlerwahrscheinlichkeit
<b>A</b>	Catastrophic	1x in 1 Milliarde Flüge
<b>B</b>	Hazardous	1x in 10 Millionen Flügen
<b>C</b>	Major	1x in 100.000 Flügen
<b>D</b>	Minor	1x in 100.000 Flügen
<b>E</b>	No Effect	Keine Auswirkungen



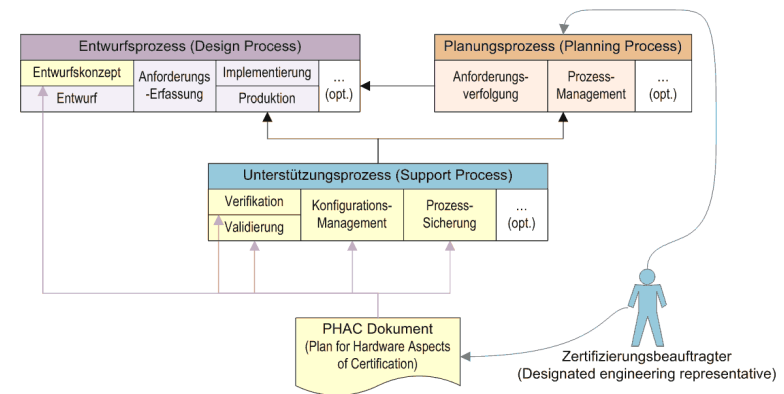
## Zertifizierungsstrategie (DO-254)

- Vorgehen am Beispiel der DO-254:



## Prozesse und Dokumente (DO-254)

- Implementierung des Entwurf mit Hilfe von Prozessen



- Dokumente für *Entwurf*, *Planung*, *Entwicklung*, *Konfiguration* und *Qualitätssicherung*

## DO-178B & DO-254 Spezifikation

### Umfang

- Spezifikation für die Zertifizierung (Konzeptionell)
- Keine Aussagen zur Umsetzung
- Überschaubar aber interpretierbar → Projektspezifisch
- Anforderungsanalyse und Verfolgung im Fokus

### Entwurf

- Konzeptioneller Entwurf vorgeschrieben (ermöglicht Abgleich)
- Detaillierter Entwurf in zertifizierbarer Sprache (UML, HDL)

### Test, Verifikation und Validierung

- Validierung hier: Anforderungen sind korrekt
- Vorgeschrieben → „Angemessene“ technische Umsetzung (Review, Test, Analyse)

## DO-178B & DO-254 Spezifikation

### Versions- und Konfigurationsmanagement

- Spezifikation verlangt lückenlose Aufzeichnung
- Anleitung für Anforderungen sonst beliebige Umsetzung

### Produkt Lebenszyklus

- Spezifikation berücksichtigt Produktlebenszyklus
- Verlangt aber keine Umsetzung → Projektspezifisch

### Produktion (DO-254) bzw. Integration (DO-178B)

- Außerhalb der Spezifikation → Weitere Standards

### Schnittstelle zur Zertifizierung

- Anleitung für die Kommunikation Entwickler ↔ Zertifizierungsstelle

## 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



## Wiederverwendung und DO-178B

- Bislang nur die Zertifizierung **kompletter Systeme**
- **Wunsch:** Wiederverwendung bestehender Software-Artefakte
  - Inklusive aller Teile des Zertifizierungsprozesses
  - Planungs-, Anforderungs-, Entwurfs- und Konfigurationsdaten, Quellcode

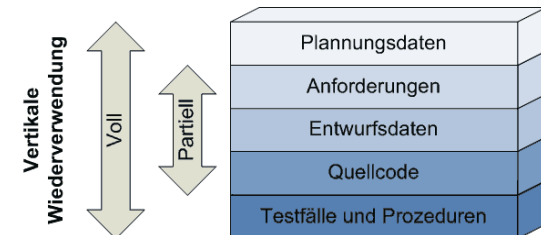


## Faktoren Wiederverwendbarkeit

- **Funktionale Anpassung**
  - Ungenutzte Funktionalität (entfernen / verbergen)
- **Unbeständige Anforderungen**
  - Sich ändernde Anforderungen benötigen Rezertifizierung
- **Bestehende Zertifizierungsebene**
  - Ziel-Zertifizierungsebene  $\leq$  Ausgangs-Zertifizierungsebene!
- **Ausgereiftheit**
  - Betriebsbewährtheit reduziert Zertifizierungsaufwand
- **Hardware Plattform**
  - Plattformabhängigkeiten schränken Wiederverwendung ein
  - Rezertifizierung bei Plattformwechsel



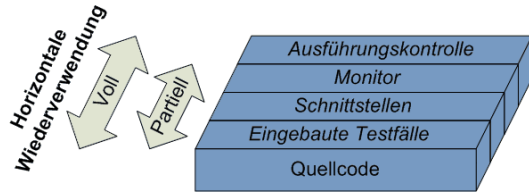
## Wiederverwendungsstrategien (1)



- **Vertikale Wiederverwendung**
  - Vererbung der Zertifizierungseigenschaften (Anwendbarkeit?)
  - Volle vs. Partielle Wiederverwendung
  - Fokus auf minimale Interaktion → *Schnittstellenzertifizierung*



## Wiederverwendungsstrategien (2)



- **Horizontale Wiederverwendung**
  - Bestehende Software Artefakte als Bibliothek
  - Vereinfachung/Funktionsreduktion → Partielle Wiederverwendung
  - *Schnittstellenzertifizierung*



## Wiederverwendungsstrategien (3)

- **Entwurf für Wiederverwendbarkeit**
  - Artefakte speziell für Wiederverwendung entworfen
  - Unbeständigkeit von Funktionen → Explosion/Fragmentierung Artefakte
  - Komplex und wiederverwendbar ↔ Einfach und projektspezifisch
- **Artefakt Anpassungen**
  - Wiederverwendung ohne Anpassungen erstrebenswert (selten)
  - Oft Regressionsanalyse und -tests notwendig (minimale Änderungen)
  - Tiefgreifende Änderungen ruinieren die Kostenersparnis
- **Anwendungspartitionierung**
  - Aufteilung in beständige und unbeständige Anforderungen
  - Trennung unterschiedlicher Zertifizierungsebenen
  - Erleichtert Wiederverwendung



## Wiederverwendungsszenarios (1)

- **Gemeinsame Funktionalität – Unterschiedliche Hardware**
  - Trennung in funktionale und hardwareabstraktions Ebene
  - Änderungen / Rezertifizierung beschränkt auf eine Ebene
- **Gemeinsame Funktionalität – Unterschiedliche Werkzeuge**
  - Durch Plattformwechsel (z.B. anderer Compiler)
  - Anderer Binärcode! → Rezertifizierung Werkzeugkette (Extrem teuer)
  - Wiederholung der Integrationstests
- **Gemeinsame Funktionalität – Unterschiedliche Standards**
  - Komplette Rezertifizierung nach neuem Standard
  - Ggf. Wiederverwendung einzelner Zertifizierungsdokumente möglich
- **Gemeinsame Funktionalität – Restrukturierung**
  - Aktualisierung des Softwareentwurfs und der Implementierung
  - Aufwendig und teuer → Nur in Ausnahmefällen (Strategisches Interesse)
  - „Never touch a running system!“



## Wiederverwendungsszenarios (2)

- **Unterschiedliche Funktionalität – Gemeinsame Plattform**
  - Wiederverwendung der „Umgebung“
  - Räumliche Isolation der funktionalen Änderungen → Regressionstest
- **Unterschiedliche Funktionalität – Unterschiedliche Plattform**
  - Neue Produktfamilie
  - Horizontale und vertikale Trennung erleichtert Wiederverwendung
- **Bestehende Funktionalität – Neues Flugzeug**
  - Erneute Dokumentation aller Aspekte der Betriebssicherheit
  - DO-178B unterstützt dieses Szenario bereits
  - Rezertifizierung der Anforderungen auf höheren Ebene ausreichend
  - Zertifizierungslevel darf nicht steigen



## Zusammenfassung

- Wiederverwendung kann Kosten senken und sogar die Sicherheit steigern
- Industriebeispiel:** Honeywell Primus Epic
  - Integrierte Bordelektronik neuester Generation
  - Produktlinienansatz → Modularisierung
  - FAA Abnahme des zentralen Modularisierungsentwurfs
  - Horizontale und vertikale Partitionierung eingesetzt
  - Betriebssystem (Digital Engine Operation System) erlaubt Trennung unterschiedlicher Zertifizierungsebenen
  - Fliegt im Dassault Falcon Jet (EASy Cockpit)



## 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 an bedacht werden



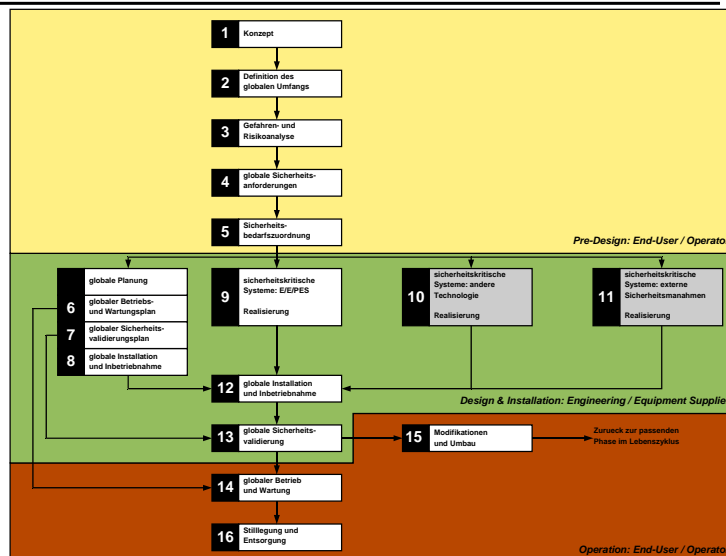
# IEC 651508: Struktur

- 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

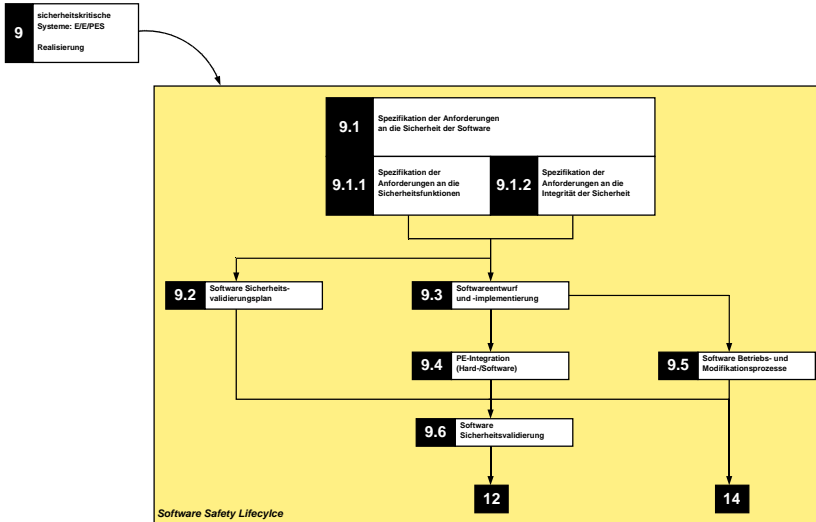


# IEC 61508: Part 1

- 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







### ■ 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

### ■ PE Integration & Sicherheitsvalidierung

- Kompatibilität von Hardware und Software
- Dokumentation der Umgebung, der Integration und der Validierung
  - Verfahren
  - Werkzeuge
- Validierung des Systems
  - Testen
  - Modellierung
  - Simulation
  - ...

### ■ Modifikationen

- entsprechende Schritte müssen wiederholt werden

- 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



## Zusammenfassung

### ■ Allgemein

- Arten der Zertifizierung
- Wer? Wo? Was? Warum?

### ■ TÜV Nord

- SEELAB und SEECERT

### ■ Normen

- DO-178B, DO-248B, DO-254, IEC 61508

