

---

# Todo list

do fehlt a stuck . . . . .	8
----------------------------	---



# 1 Einführung

Das Hochhalten von Softwarequalität ist eine sehr anspruchsvolle Aufgabe, welche eine gewisse Planung voraussetzt. Gerade bei Projekten mit hohen Budgets und materiellen Einsätzen werden hohe Anforderungen an das Qualitätsmanagement gesetzt.

Einige bekannte Fehlschläge in der Softwareentwicklung hätten wahrscheinlich mit besseren Qualitätssicherungsmaßnahmen verhindert werden können:

- Pioneer 4 verfehlte den Mond
- unnötige Mahnungen durch die französische Finanzverwaltung
- das Herausgeben von faulen Krediten, was schlussendlich zum Bankencrash geführt hat
- Verlust einer Segelyacht im Pazifik

## 1.1 Verifikation und Validierung

Die Begriffe sollten klar getrennt werden, da sie nicht synonym verwendet werden können, und bei Softwareprozessen und Softwarequalität eine gewichtige Rolle spielen.

Die Verifikation stellt fest ob die Software mit der vorhandenen Spezifikation übereinstimmt, wohingegen die Validierung bestimmt ob die Software für den Kunden auch wirklich nützlich ist.

## 1.2 Technical Debt

Technical Debts sind ein wichtiges Thema in der Qualitätssicherung. Der Begriff wurde aus dem Finanzwesen übernommen (Debt = Schulden). In der Softwareentwicklungen ist damit gemeint, dass ungeschickte Lösungen irgendwann gefixt werden müssen.

Diese technische Schulden kann man bewusst eingehen, um Termine zu halten. Allerdings muss man immer im Hinterkopf behalten, dass man diese Schulden zu einem späteren Zeitpunkt auch wieder bezahlen muss.

Einer der größten Unterschiede zwischen klassischen und agilen Projektmanagementmethoden ist der Umgang mit diesen technischen Schulden. Bei agilen Methoden werden diese Schulden bewusst eingegangen, um ein schnelleres iteratives Vorgehen zu gewährleisten. Bei diesen Methodiken ist allerdings auch die Gefahr einer Überschuldung ungleich höher als bei den klassischen.

Allerdings werden in der Regel auch bei klassischen Methoden technische Schulden verursacht, nämlich in Form von Änderungen in den Anforderungen, auf welche in agilen Methoden besser reagiert werden kann.

## 2 Hausaufgabe Besprechung

Es sollte klar definiert werden was in den Sonderfällen passiert bzw. was in diesen Fällen zurückgegeben wird (z.B. komplexe Zahlen da in Wurzel negative Zahl). Gleitkommzahlen sind "Teufelswerk"! Wenn man zwei gleiche Zahlen (die berechnet wurden aber unterschiedliche Rundungsfehler haben) voneinander voneinander subtrahiert bleibt nicht 0 übrig sondern der Rundungsfehler. Durch Rundungsfehler können somit 2 verschiedene Ergebnisse entstehen die eigentlich eines wären - darum könnte man anstatt der Mitternachtsformel eine andere Formel / einen anderen Ansatz verwenden (z.B. Newton-Näherungsverfahren).

Äls Softwareentwickler ist es durchaus erlaubt sein Hirn einzuschalten! - Gleitkommzahlen sind Teufelswerk!"



## 3 Wichtige Begriffe

- Softwareprozesse (Abfolge von Tätigkeiten, durch die ein Software-Produkt entsteht)
- Vorgehensmodell (Vereinfachte Beschreibung eines Softwareprozesses)
- Methode (Strukturierter Ansatz für die Software-Entwicklung)

### 3.1 Software-Engineering

Software-Engineering ist eine technische Disziplin welche eine Lösung für den Anwender bieten will unter Einsatz von Theorien, Methoden und Werkzeugen und Berücksichtigung von Organisation, Management und Entwicklung.

### 3.2 Informatik

Grundlage der Wissenschaft für Software-Ingenieure (Theorie, Konzepte, ...).

### 3.3 ESSENCE Kernel Overview

In diesem Model gibt es verschiedene Zustände für die Anforderungen und jeder dieser Zustände hat selbst wieder Kriterien welche einem dabei helfen in welchem Zustein ein Projekt ist.

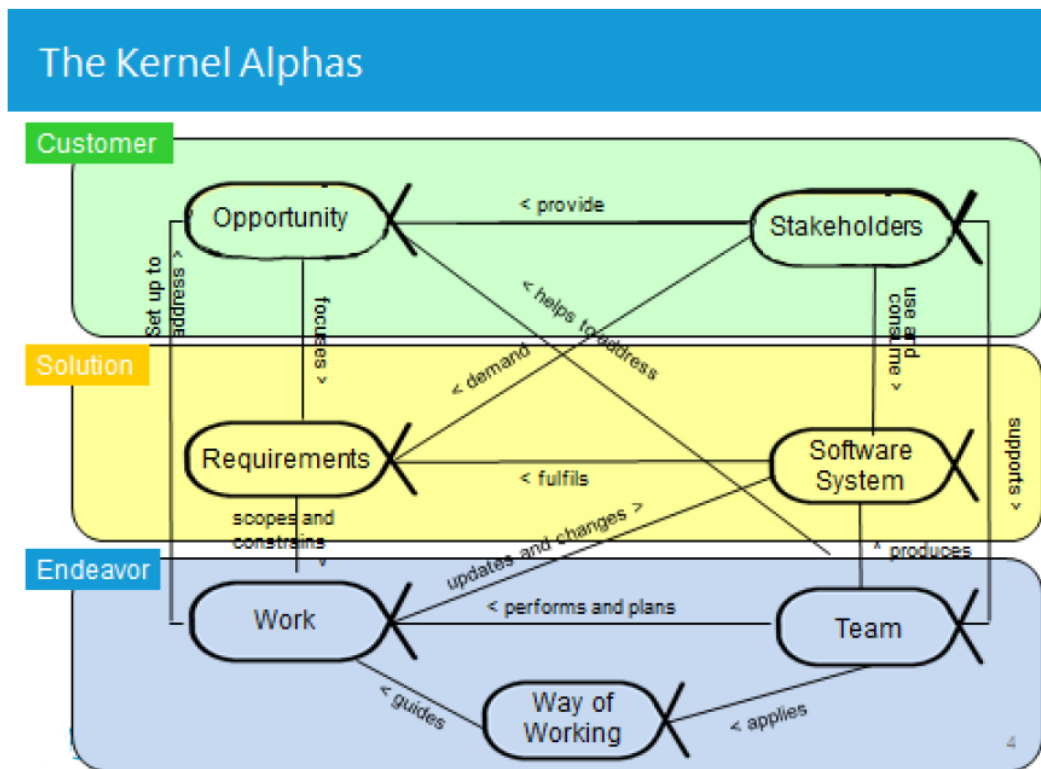


Abbildung 3.1: ESSENCE Kernel Overview

**Zustände:**

- Conceived
- Bounded
- Coherent
- Accepted
- Addressed
- Fulfilled

## 3.4 Qualität

Grad in dem die inhärenten Eigenschaften des Produkts Anforderungen erfüllen.



- **Explizite Anforderungen**
- **Implizite Anforderungen** - Anforderungen welche existieren aber den Stakeholdern nicht bewusst sind.
- **Nicht explizite Anforderungen** - Stakeholder wissen, dass sie diese Anforderungen gibt aber sie teilen diese nicht mit (sind quasis eh klar).
- **Objektiv** - Vollkommen klar, dass man etwas braucht.
- **Subjektiv** - Vermeintliche Anforderungen, welche nicht wirklich wichtig sind.
- alle betroffenen / interessierten Personen

### 3.4.1 Begriffsabgrenzung

**Technisches computer-basiertes System** System welches ausschließlich aus Soft- und Hardware-Komponenten besteht.

**Soziotechnisches System** System bestehend aus einem oder mehreren technischen Systemen, den Menschen die es bedienen, den notwendigen Arbeitsprozessen, organisatorischen Richtlinien, usw.

*Systeme:*

- haben systemspezifische Eigenschaften die nur dem System als Ganzem zugeordnet werden können
- sind häufig nicht deterministisch
- hängen von organisatorischen Zielen ab

## 3.5 Kritische Systeme

Relevante Systemeigenschaften für kritische Systeme sind:

- Reparierfähigkeit
- Wartbarkeit
- Überlebensfähigkeit
- Fehlertoleranz

**Kritisches System** Systeme, bei dessen Ausfall oder Fehlfunktion großen Schaden anrichten kann (wirtschaftliche Verluste, physische Schäden, Gefahr für Gesundheit und Leben von Menschen).

**Sicherheitskritisches System** Schäden an der Umwelt und/oder Gefahr für Gesundheit und Leben von Menschen (Bohrinsel im Golf von Mexiko).

**Aufgabenkritisches System** Aufgaben die ein System erledigen sollte werden nicht durchgeführt (z.B. Bank).

**Geschäftskritisches System** Extrem hohe Kosten bzw. signifikante Gewinnausfälle können die Folge eines Systemausfalls sein.

t a stuck

## 3.6 Sammlung von Anforderungen

### 3.6.1 Interviews

#### Technik

- Interviews mit Fragebogen
- Geschlossene Interviews vorgegebener Fragebogen abarbeiten
- Offene Interviews mit einer Diskussion zwischen Analyseteam und Beteiligten

#### Durchführungsempfehlung

- Mischung aller Methoden
- Vorbereitung aller Diskussionen als geschlossenes Interview
- gut und interessiert zuhören
- gezielt Fragen

#### Probleme

- Jargon des Anwendungsgebiets
- Implizites Wissen

### **Eignung**

- Verständnis der Benutzeranforderungen
- Ergänzung zu anderen Informationsquellen mit zum Beispiel Dokumentationen oder Beobachtungen

### **Szenarien**

- Grundbestandteile
  - Ausgangssituation
  - Ereignisablauf
  - Ausnahmen und ihre Behandlung
- Varianten
  - Ad-hoc
  - Formell

## **3.6.2 Ethnografische Methode (Völkerkunde)**

Grundidee: Beobachten ohne einzugreifen

- Beobachten der alltäglichen Arbeit im normalen Umfeld
- Notieren von Auffälligen
- Diskussion mit Experten
- Ableitung der Anforderungen

### **Stärken**

- Erkennen von impliziten Anforderungen
- Erkennen von nicht explizierten Anforderungen
- Erkennen von Abweichungen

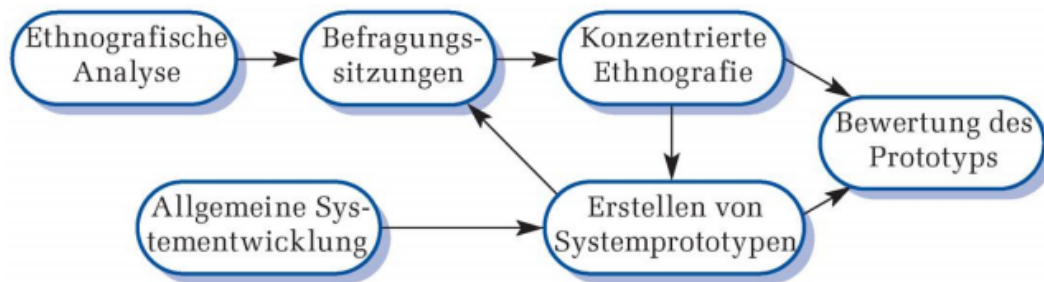


Abbildung 3.2: Verknüpfung von Ethnografie und Prototypen nach Sommerville (Copyright Pearson Studium 2007)

## 3.7 Klassifizierung von Anforderungen

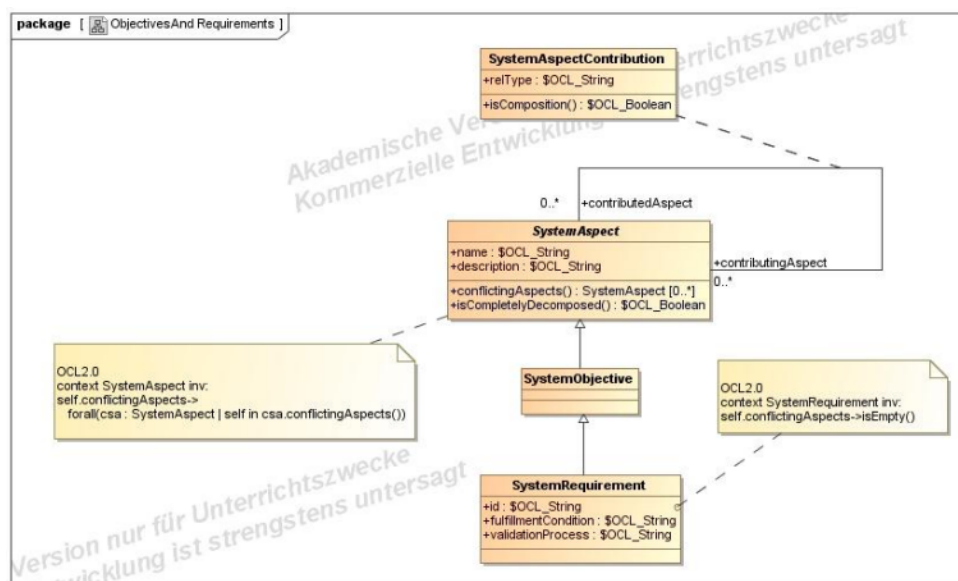


Abbildung 3.3: Metamodell

### Aufgaben

- Erkennen von Duplikaten / Synonymen
- Beziehungen zwischen Anforderungen
- Gruppierung der Anforderungen

## 3.8 Validierung von Anforderungen

Wichtige Prüfungen sind:

- Gültigkeitsprüfung
- Konsistenzprüfung
- Vollständigkeitsprüfung (schwierig, aber mit etwas Bauchgefühl machbar)
- Realisierbarkeitsprüfung
- Verifizierbarkeitsprüfung

### 3.8.1 Techniken

Prototypen erstellen und Testfälle entwickeln. Falls das nicht möglich sind die Anforderungen schlecht definiert.

### 3.8.2 Review

**Teamzusammensetzung** Es sollten Vertreter aller am Projekt beteiligten bzw. vom Projekt betroffenen Gruppen auf Anwenderseite, ausserdem Systemarchitekten und Vertreter der Softwareentwickler.

**Durchführung** Die Führung der Analyse liegt bei den jeweiligen Anwendervertretern. Diskutiert werden sollten alle Anforderungen. Dadurch können Fehler, Konflikte und Widersprüche aufgedeckt werden. Das Ergebnis ist ein Review Bericht.

**Prüfungen** Die Konsistenz der Anforderungen sollten am Ende geprüft werden. Ausserdem sollte eine Vollständigkeitsprüfung durchgeführt werden.

### 3.8.3 Priorisierung von Anforderungen

**Grundgedanke** Phasenweise Implementierung der Software.

#### **Prioritätsfestlegung**

Teams festlegen, die nicht miteinander kommunizieren sollten. Ausserdem wird eine Bewertungsformel festgelegt.

**Nutzwertanalyseteam** Bewertet den Nutzen für die Anwender.

**Kostenanalyseteam** Schätzt die Kosten jeder Anforderung

#### **Auswertung**

##### **Einflussgrößen**

- Nutzwert jeder Anforderung
- Kosten jeder Anforderung
- Obergrenze des Aufwands für Stufe 1
- Abhängigkeiten

**Ergebnis** Liste der Anforderungen für nächste (bzw. erste) Ausbaustufe

### 3.9 Systemmodelle

**Kontextmodelle** Definiert die Systemgrenzen des Gesamtsystems und des technischen Systems. Das Gesamtsystem umfasst das Technische System und die Menschliche Komponente und definiert den Kontext. Das Technische System definiert den Scope.

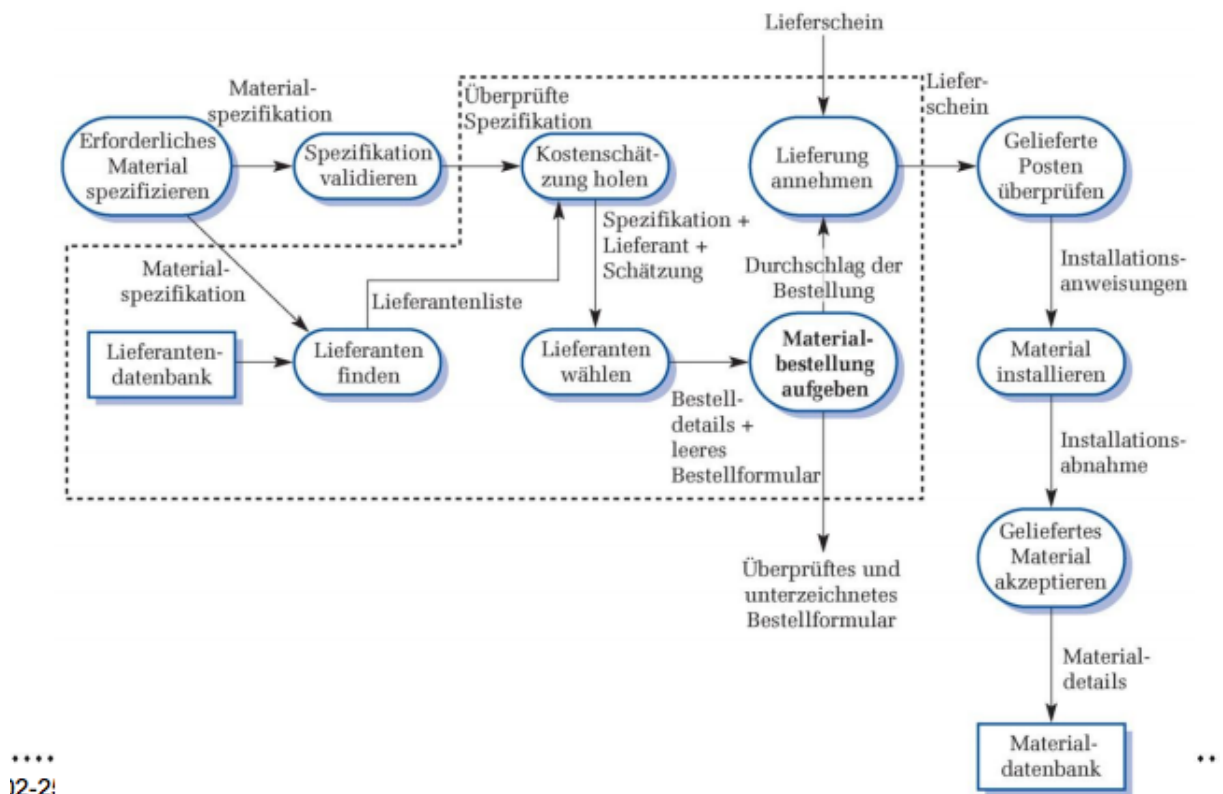


Abbildung 3.4: Kontextmodelle

**Verhaltensmodelle** Definiert die Abläufe in einem System. Sie können Datenfluss (Datenfokus) - oder Ereignis (Ereignisfokus) - Orientiert geschehen. Ausserdem gibt es Mischformen davon. Dafür können Datenflussdiagramme (Abbildung 3.5), Zustandstabelle (Abbildung 3.6) und ähnliches verwendet werden.

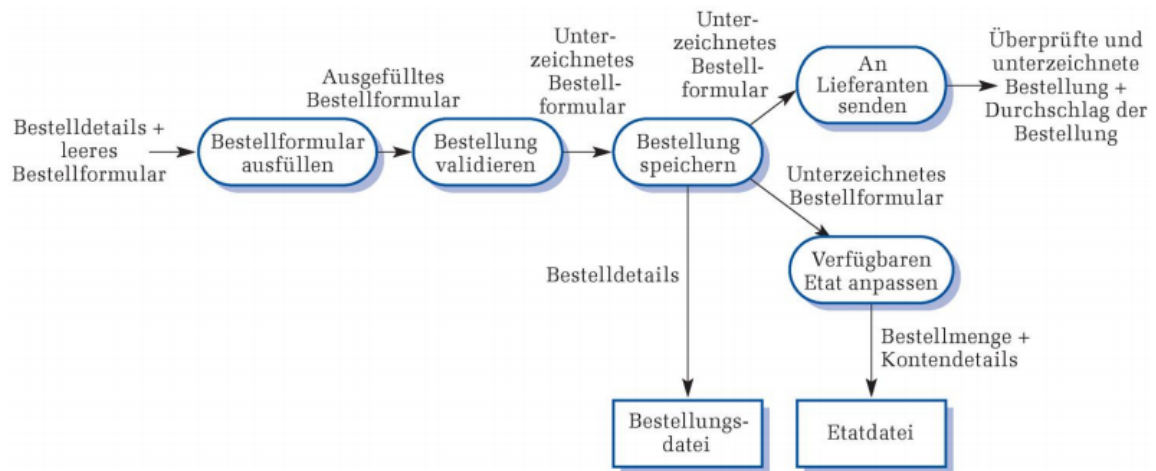


Abbildung 3.5: Datenflussdiagramm

**Datenmodelle** Definiert die logische und persistente (lokal, übergreifend mittels Datenbank und Datenaustausch) Datenstruktur. Dazu kann ER-, UML-Diagramme, OWL oder andere Ontologie-Darstellungen und andere.



Zustand	Beschreibung
Warten	Das Gerät wartet auf eine Eingabe. Die Anzeige zeigt die aktuelle Zeit an.
Halbe Leistung	Die Geräteleistung wird auf 300 Watt gesetzt. Die Anzeige zeigt „Halbe Leistung“ an.
Volle Leistung	Die Geräteleistung wird auf 600 Watt gesetzt. Die Anzeige zeigt „Volle Leistung“ an.
Zeiteinstellung	Die Garzeit wird auf die Eingabe des Benutzers gesetzt. Die Anzeige zeigt die gewählte Garzeit an und wird bei der Einstellung der Zeit aktualisiert.
Deaktiviert	Der Betrieb des Geräts ist aus Sicherheitsgründen deaktiviert. Das Licht im Gerät ist eingeschaltet. Die Anzeige zeigt „Nicht bereit“ an.
Aktiviert	Der Betrieb des Geräts ist aktiviert. Das Licht im Gerät ist ausgeschaltet. Die Anzeige zeigt „Bereit“ an.
Betrieb	Das Gerät ist in Betrieb. Das Licht im Gerät ist eingeschaltet. Die Anzeige zeigt den Countdown der Garzeit an. Nach dem Ende der Garzeit ertönt fünf Sekunden lang ein Signal. Das Licht im Gerät ist eingeschaltet. Die Anzeige zeigt „Kochvorgang beendet“ an, während das Signal ertönt.
Stimulus	Beschreibung
Halbe Leistung	Der Benutzer hat die Taste „Halbe Leistung“ betätigt.
Volle Leistung	Der Benutzer hat die Taste „Volle Leistung“ betätigt.
Timer	Der Benutzer hat eine der Tasten für die Zeitschaltuhr betätigt.
Zahl	Der Benutzer hat eine Zifferntaste betätigt.
Tür offen	Die Gerätetür ist nicht geschlossen.
Tür geschlossen	Die Gerätetür ist geschlossen.
Start	Der Benutzer hat die Starttaste betätigt.
Abbruch	Der Benutzer hat die Abbruchtaste betätigt.

Abbildung 3.6: Zustandtabelle

**Objektorientierte Modellierung** Vereinigt die Funktionalität von Daten- und Verhaltensmodelle und können Daten, Datenflüsse, Datenstrukturen und Ereignisse erfassen. Als Notation wird meist UML verwendet.

Sind die Klassen in dem Diagramm Abbildung 3.7 wirklich **Klassen** oder **Rollen**? Nein das sind eindeutig Rollen.

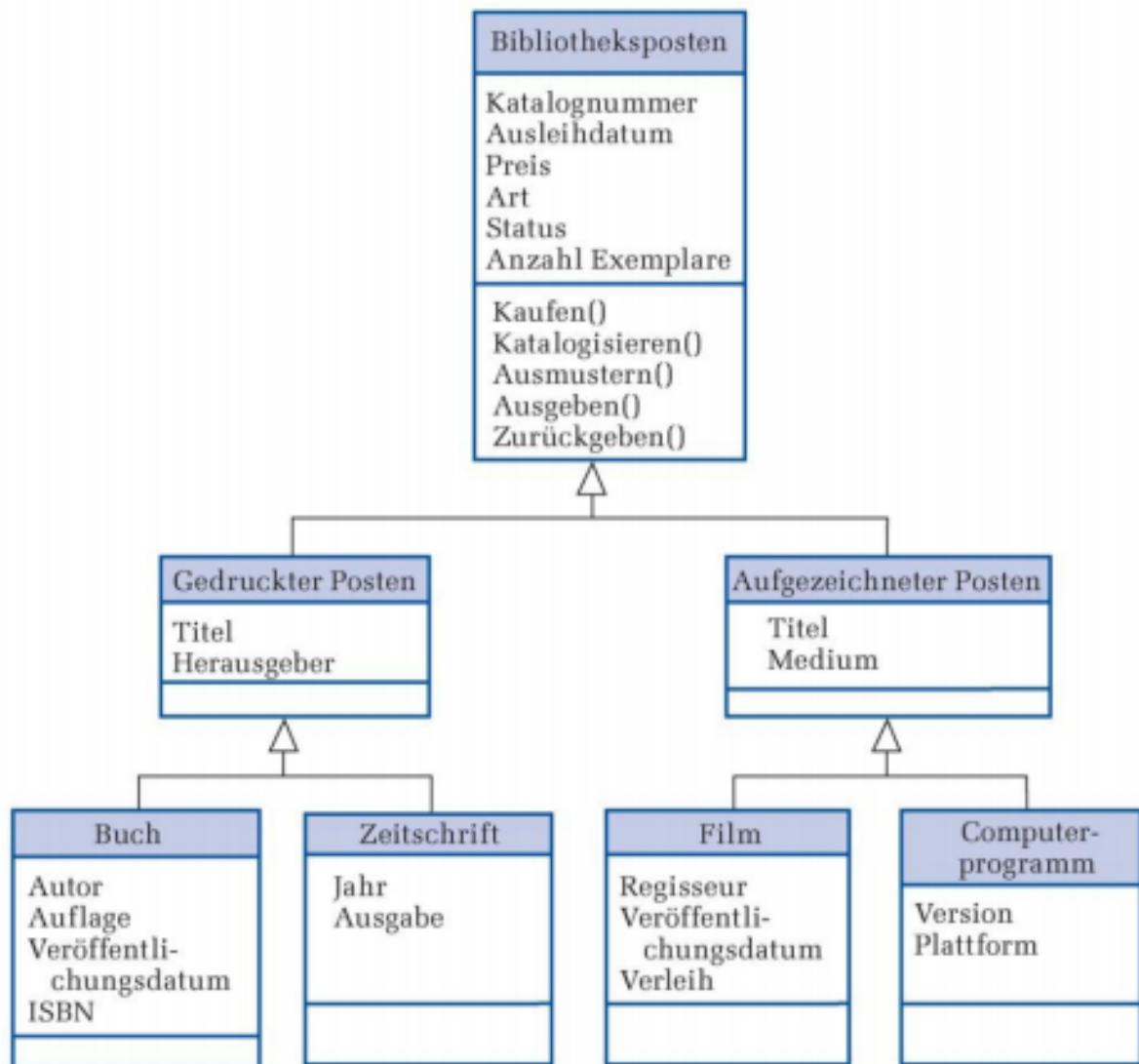


Abbildung 3.7: Objektorientierte Modellierung

**Strukturierte Methoden** Detailliert definierte Vorgehensweise bei der SW-Entwicklung. Normalerweise basierend auf einem Satz von Diagrammtypen. Definiert zusätzliche Regeln und Richtlinien. Beispiele dafür sind JSP, V-Modell oder RUP. Nachteile davon sind Mangelnde Unterstützung nicht-funktionaler Anforderungen und Anwendbarkeit für konkretes Problem oft schwer zu entscheiden.

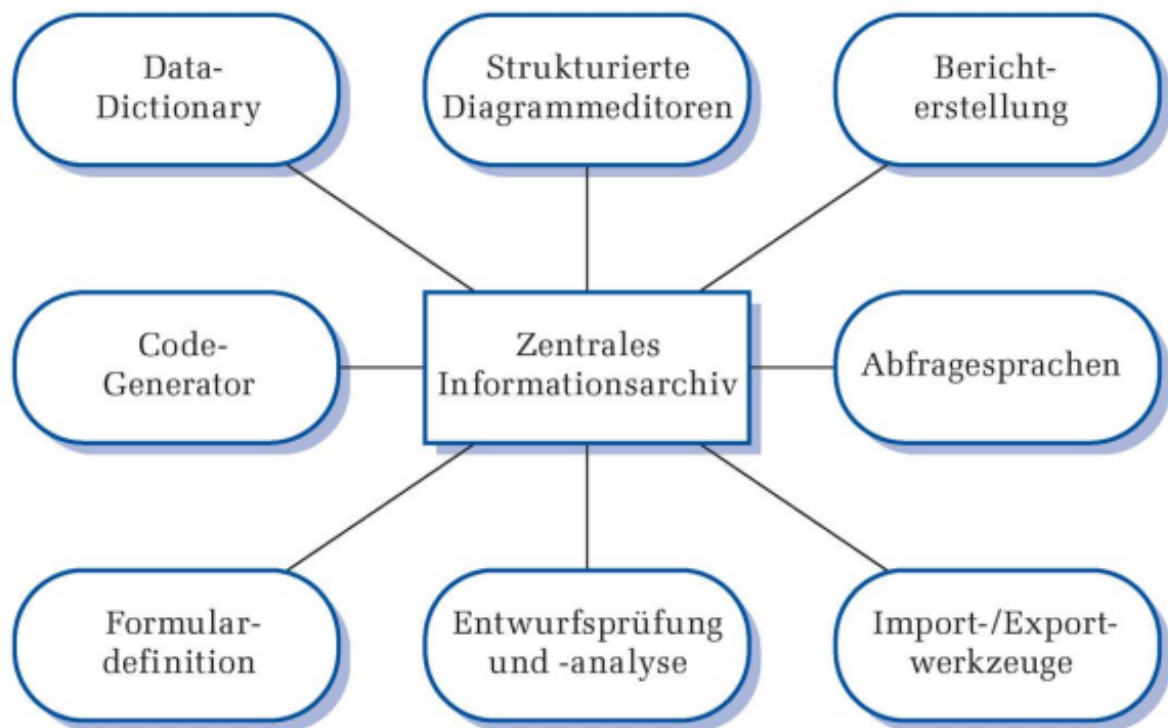


Abbildung 3.8: Strukturierte Methoden

## 3.10 Anforderungsmanagementsystem

Die Anforderungen an ein System ändern sich mit der Zeit, diese können ursprünglich unvollständig sein. Oder es verbessert sich das Verständnis des Problems / es entsteht eine bessere Sicht der Dinge. Aber auch das Umfeld kann sich verändern, z.B. wirtschaftlich, technisch, juristisch ...

Der Prozess umfasst:

- das
  - Sammeln
  - Verstehens
  - Klassifizierens
  - Validierens
  - Priorisierens

- von
  - Anforderungen
  - Änderungen der Anforderungen
- und ihren Auswirkungen auf
  - andere Anforderungen
  - Entwurfsentscheidungen
  - das System

**Dauerhafte Anforderungen** Sie sind relativ stabil und sind mit dem Kern der Anwendung verwoben. Oft aus Standardisierten Modellen entnommen.

**Veränderliche Anforderungen** Anforderungen mit hoher Änderungswahrscheinlichkeit. Können wirtschaftliche Randbedingungen, technische Randbedingungen und gesetzliche Randbedingungen.

## 3.11 Pflichtenheft

Zusammenstellung der vollständigen und detaillierten Benutzeranforderungen und Systemanforderungen (großes Problem ist die Vollständigkeit). Darf nach Fertigstellung nicht mehr geändert werden und muss so implementiert werden wie es festgehalten wurde (auch wenn es sich um kompletten Blödsinn handelt). Dies muss aus juristischen Gründen so sein da eine nachträgliche Änderung als eine Benachteiligung der Mitbewerber interpretiert werden kann.

**Synonyme** sind die Begriffe Produktdefinition, Produktspezifikation, Systemdefinition und Systemspezifikation.

**Adressaten des Pflichtenhefts** sind unter anderem Systemkunde, Manager, Systementwickler, Systemtester, Systemwarter und Juristen.

**Informationen im Pflichtenheft** sind qualitative und quantitative Anforderungen (mandatory requirement) sowie zusätzliche Wünsche (optional requirements) dessen Erfüllung als sehr positiv betrachtet werden und informative Bestandteile. Diese Bestandteile dienen dem Verständniss und sind streng genommen unverbindliche Informationen.

In vielen Ländern gelten Abbildungen, Tabelle und Anhänge als informative Bestandteile, wenn sie nicht anderst gekennzeichnet sind (engl. "normativ").

#### Aufbau des Pflichtenhefts

- Einleitung
  - Ziele des Pflichtenhefts
  - Anwendungsbereich des Produkts
  - Definitionen, Akronyme und Abkürzungen
  - Referenzen
  - Überblick über das Pflichtenheft
- Allgemeine Beschreibung
  - Produktperspektive
  - Produktfunktion
  - Produktcharakteristika aus Benutzersicht
  - Beschränkungen
  - Voraussetzungen und Abhängigkeiten
- Spezifische Anforderungen (funktionale u. nicht funktionale Anforderungen)
- Anhänge
- Index

## 3.12 Anforderungen an kritische Systeme

**Funktionale Anforderungen** unterstützen Definition von Funktionen zur Fehlerprüfung, zur Wiederherstellung im Fehlerfall und Aspekte zum Schutz gegen Systemausfälle.

**Als nichtfunktionale Anforderungen** werden u.a. die Systemzuverlässigkeit und Systemverfügbarkeit festgelegt.

**Negativanforderungen** Beschreibung von Verhalten oder Eigenschaften, die das System auf keinen Fall zeigen darf.

## 3.13 Risikomanagement

Risikomanagement besteht aus Gefahrenbestimmung, Risikoanalyse und Gefahrenklassifizierung, Gefahrenvereinzelung und Festlegung zur Risikominimierung.

**Murphys Law** Alles was schief gehen kann, wird irgendwann einmal schief gehen.

**Risikoerkennung** Ziel ist es zu Erkennen von Risiken und Gefahren. Probleme die dabei entstehen können sind die Wechselwirkung zwischen Systemkomponenten bzw. die Wechselwirkungen mit der Umwelt.

**Risikoanalyse und Risikoklassifizierung** Analyse von Unfallwahrscheinlichkeit, Schadenswahrscheinlichkeit und Schadenshöhe. Risiken sind klassifizierbar in:

- nicht tolerierbar
  - großer Schaden und / oder hohe Schadenswahrscheinlichkeit
  - Maßnahmen: unter allen Umständen Risiko ausschließen
- as low as reasonably possible (ALARP)
  - höchstens mittleres Schadenspotential und mittlere Schadenswahrscheinlichkeit
  - Maßnahmen: zumindestens Ausschluss des Schadens unter Beachtung von wirtschaftlichen, vertraglichen oder technischen Randbedingungen
- vernachlässigbar
  - geringes Schadenspotential und / oder geringe Schadenswahrscheinlichkeit
  - Maßnahmen: Reduzierung der Schadenswahrscheinlichkeit ohne negativen Einfluss auf wirtschaftliche, technisches, oder vertragliche Randbedingungen oder andere Systemanforderungen

**Risikozerlegung** Ziel es die Ursachen aufzudecken. Dazu können Reviews, Checklisten, Petri-Netze, formale Logik und Fehlerbäume verwendet werden.

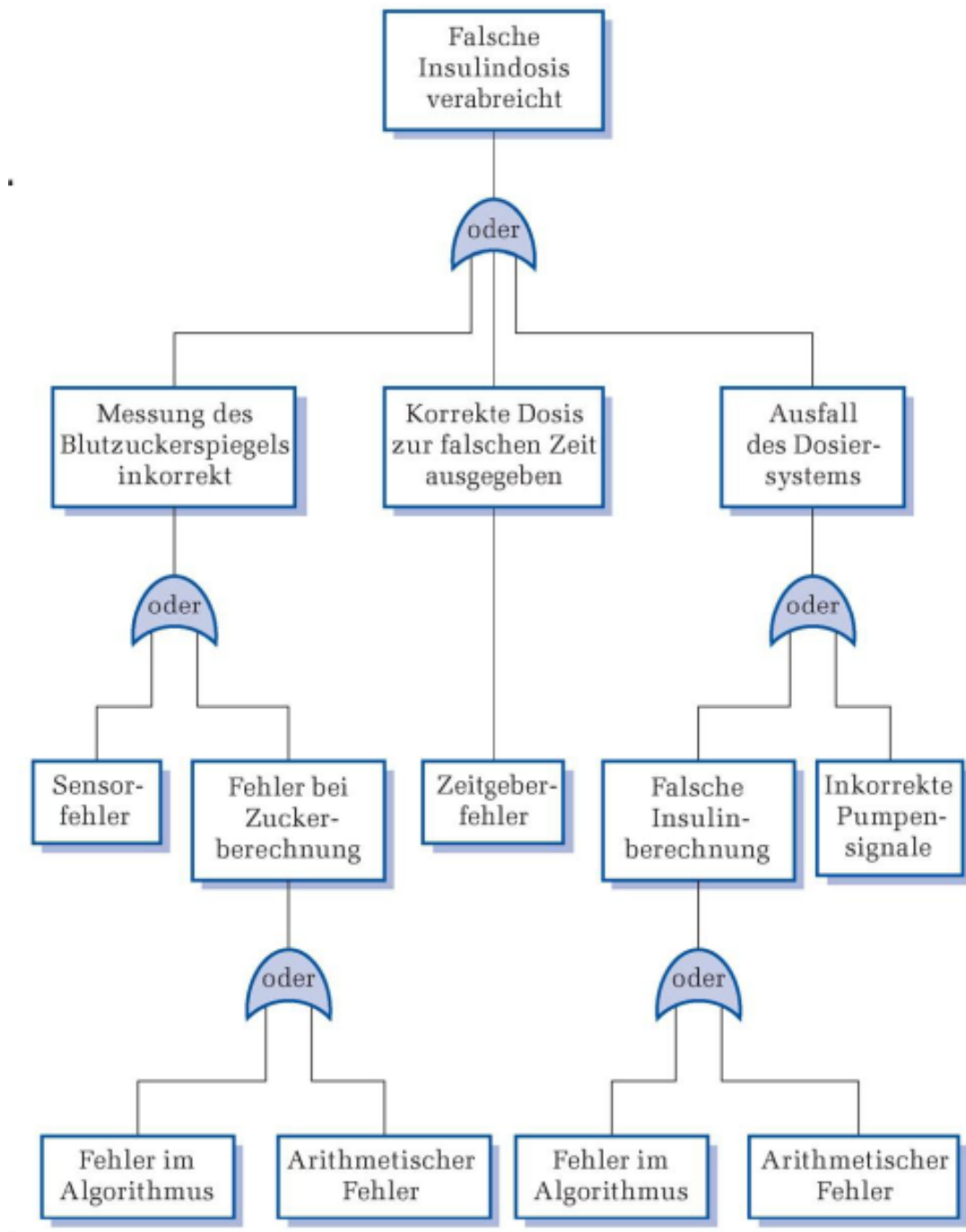


Abbildung 3.9: Fehlerbaum

**Risiko-Minimierung** Ziel ist das Vermeiden des Auftretens von Gefahren. In der Praxis bedeutet dies eine Kombination aller Strategien.

### 3.14 Betriebssicherheit

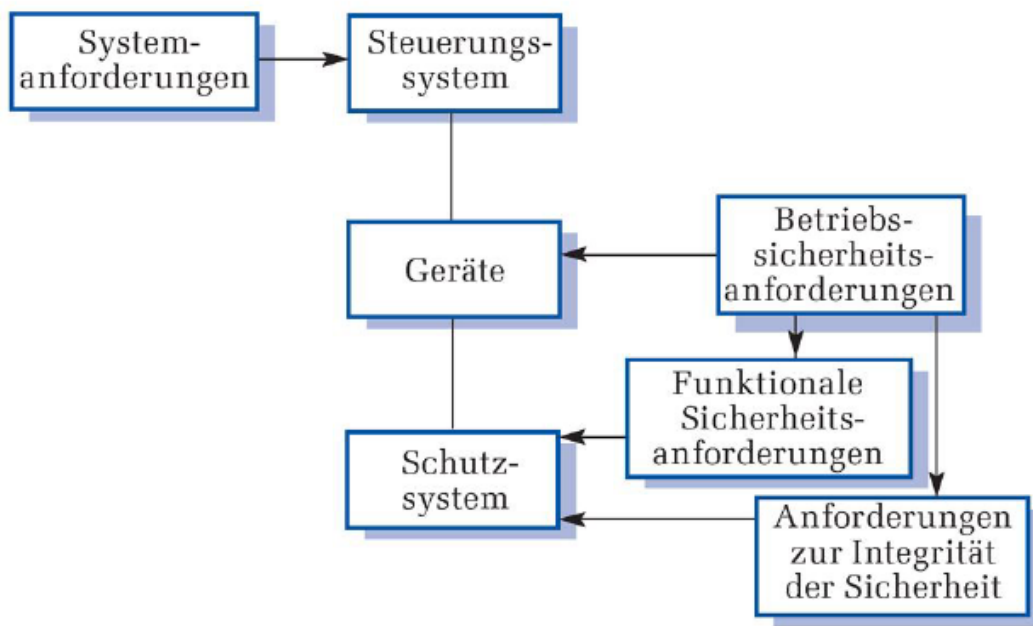


Abbildung 3.10: Betriebssicherheit nach IEC 61508

#### Klassifizierung

- Klasse 1 - Fehler die andere Anwendungen betreffen können
- Klasse 2 - Fehler die andere Benutzer der selben Anwendung betreffen können
- Klasse 3 - Wesentliche Funktion steht ohne Work-Around nicht zur Verfügung
- Klasse 4 - Wesentliche Funktion steht nur über Work-Around zur Verfügung bzw. Sekundärfunktion steht nicht zur Verfügung
- Klasse 5 - Verbesserungswunsch



## 3.15 Systemsicherheit

Hierbei geht es um direkte und indirekte Bedrohungen.

**Direkte Bedrohung** wie z.B. unbefugtes Eindringen und DOS.

**Indirekte Bedrohung** wie Aufwand um Sicherheitsmaßnahmen zu installieren, konfigurieren und aktuell zu halten. Auch inkludiert sind Fehler und Nachlässigkeiten der Systemverwalter und monopolartige Stellungen einiger Hard- und Softwareanbieter da eine weite Verbreitung von Sicherheitslücken sehr wahrscheinlich ist.

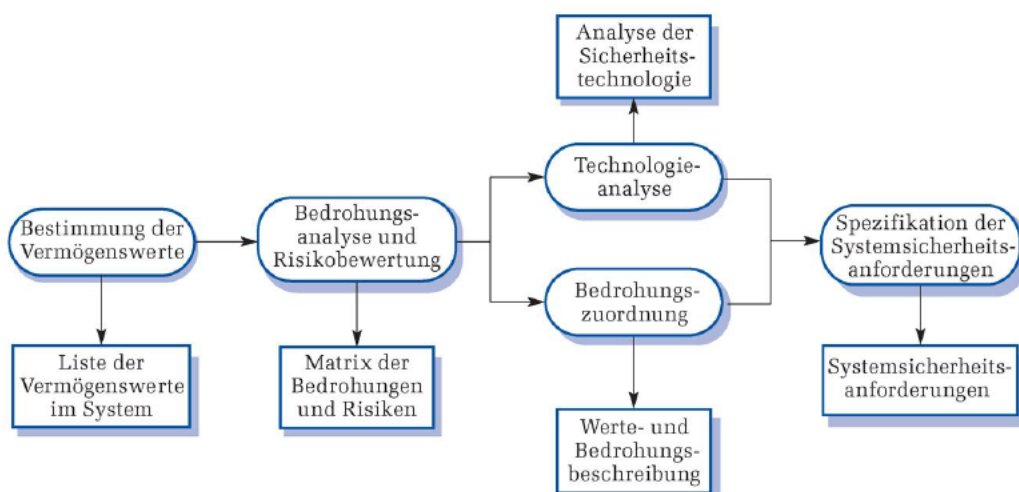


Abbildung 3.11: Sicherheit

## 3.16 Zuverlässigkeit

besteht aus Hardware-, Software- und Bedienerzuverlässigkeit.

**Extreme Zuverlässigkeitsanforderungen** lassen sich nicht testen!

Metrik	Erläuterung
POFOD Probability of failure on demand (Wahrscheinlichkeit eines Fehlers bei Anfrage)	Die Wahrscheinlichkeit, dass das System bei einer Dienstanforderung fehlschlägt. Eine POFOD von 0,001 bedeutet, dass eine von tausend Anforderungen zu einem Fehler führt.
ROCOF Rate of failure occurrence (Ausfallrate)	Die Frequenz, mit der ein unerwartetes Verhalten auftritt. Eine ROCOF von 2/100 bedeutet, dass pro 100 operativen Zeiteinheiten zwei Fehler zu erwarten sind. Diese Metrik wird manchmal auch Fehlerintensität (failure intensity) genannt.
MTTF Mean time to failure (Mittlere Zeit bis zu einem Ausfall)	Die durchschnittliche Zeit zwischen beobachteten Systemausfällen. Eine MTTF von 500 bedeutet, dass alle 500 Zeiteinheiten ein Ausfall erwartet werden kann.
AVAIL Availability (Verfügbarkeit)	Die Wahrscheinlichkeit dafür, dass das System zu einer gegebenen Zeit verfügbar ist. Eine Verfügbarkeit von 0,998 bedeutet, dass das System alle 1000 Zeiteinheiten wahrscheinlich in 998 Fällen verfügbar ist.

Abbildung 3.12: Zuverlässigkeit

Fehlerklasse	Beispiel	Metriken für Zuverlässigkeit
dauerhaft, nicht beschädigend	Das System funktioniert mit keiner der eingegebenen Karten. Die Software muss neu gestartet werden, um den Fehler zu beheben.	ROCOF 1 Vorfall/1.000 Tage
dauerhaft, nicht beschädigend	Die Magnetstreifendaten von einer unbeschädigten Karte können nicht gelesen werden.	ROCOF 1 pro 1.000 Transaktionen
dauerhaft, beschädigend	Ein Transaktionsmuster im Netzwerk verursacht eine Datenbankbeschädigung	Nicht messbar! Sollte während der Lebensdauer des Systems nicht vorkommen.

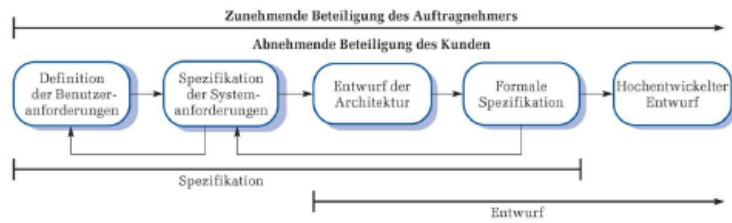
Abbildung 3.13: Zuverlässigkeit nach Sommervill

## 3.17 Formale Spezifikationsmethoden

An dieses Thema sind seit 1970 sehr hohe Erwartungen gerichtet aber der große Durchbruch blieb bisher aus. Gründe dafür sind die Entwicklung anderer Software-Engineering-Methoden, Marktveränderungen, beschränkte Einsetzbarkeit und mangelhafte Skalierbarkeit.

Erfolgreich verwendet wirds bei Raumfahrt-, und medizinischen Systemen sowie bei Überwachung des Luftverkehrs.

#### ◆ Linearer Prozess



#### ◆ Paralleler Prozess

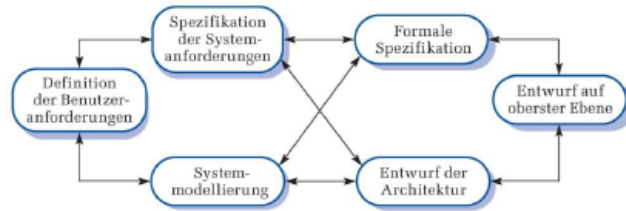


Abbildung 3.14: Formale Spezifikationsmethoden im Softwareprozess

#### Nutzung im Softwareprozess



## 4 Entwurf