Matteo Kuschel

TSO-Data gmbh

Zwischenprüfung

-

Lernzettel

Inhalt

[Inhalte 3](#_Toc127286017)

[Projektmanagement 4](#_Toc127286018)

[Allgemein 4](#_Toc127286019)

[Merkmale 4](#_Toc127286020)

[Phasen 4](#_Toc127286021)

[SMART 4](#_Toc127286022)

[Visualisierung 4](#_Toc127286023)

[Netzplan 4](#_Toc127286024)

[Gantt-Diagramm 4](#_Toc127286025)

[EPK 4](#_Toc127286026)

[Amortisation 4](#_Toc127286027)

[Qualitätsmanagement 4](#_Toc127286028)

[Programmierung 5](#_Toc127286029)

[Codestrukturierung 5](#_Toc127286030)

[PAP(Programmablaufplan) 5](#_Toc127286031)

[Struktogramm 6](#_Toc127286032)

[Pseudocode 6](#_Toc127286033)

[Anwendungsfalldiagramm 7](#_Toc127286034)

[Klassendiagramm 7](#_Toc127286035)

[Lastenheft/Pflichtenheft 7](#_Toc127286036)

[Software 8](#_Toc127286037)

[Softwarearten 8](#_Toc127286038)

[Softwarelebenszyklus 9](#_Toc127286039)

[Kriterien für Softwarequalität 9](#_Toc127286040)

[IT-Sicherheit 11](#_Toc127286041)

[Schutzziele 11](#_Toc127286042)

[ISMS (Informationssicherheits-Managementsystem) 11](#_Toc127286043)

[Übersicht 11](#_Toc127286044)

[Bausteine 12](#_Toc127286045)

[Kreislauf 12](#_Toc127286046)

[Strukturanalyse 13](#_Toc127286047)

[Schutzbedarfsfeststellung 13](#_Toc127286048)

[Modellierung 13](#_Toc127286049)

[Risikoanalyse 13](#_Toc127286050)

# Inhalte

* Projektmanagement
  + Merkmale, Phasen, SMART
  + Netzplan, Gantt-Diagramm, EPK
  + Amortisation
  + Geschäftsprozesse, Aufbauorganisation
  + Marktformen
  + Marketing
  + Qualitätsmanagement (ISO9000)
  + Vertragsarten, Vertragsstörungen, Mängel, Mängelarten
* Elektrotechnik
  + Einheiten
  + Größen (Spannung, Strom, Leistung, Arbeit, Wirkungsgrad, Kosten)
  + USV, Ladungsmenge, Akkus
* Programmierung
  + PAP, Struktogramm, Pseudocode
  + UML (Use Case Klassendiagramm)
  + Lastenheft/Pflichtenheft
  + DIE, Softwarearten, Softwarelebenszyklus, Kriterien für Softwarequalität
  + Compiler, Linker, Interpreter
  + Prozeduale vs. Objektorientierte Programmierung
  + Variablen, Datenstrukturen, Kontrollstrukturen, Funktionen, Klassen, Vererbung
  + Debugging, Fehlersuche
  + Einfache ER-Modelle, SELECT-Abfragen
  + Abnahmeprotokoll, Benutzerdokumentation, Kundendokumentation, Programmdokumentation
* IT-Sicherheit
  + Schutzziele, IT-Grundschutz nach BSI, IT-Sicherheitsmanagement
  + Strukturanalyse, Schutzbedarfsfeststellung, Modellierung
  + Bedrohungen, Malware, Phishing, Passwortregeln usw.
  + Maßnahmen (Backup (!), RAID, Verschlüsselung Authentifizierung, Firewall)
* Hardware und Software
  + Hardwareprodukte, Softwareprodukte
  + Virtualisierung, Cloudlösungen
  + Netzwerkkomponenten (WLAN, LAN, Router, Switch, AP, Netzwerkprotokolle, Funktechniken)
  + Kenngrößen, Leistungsdaten usw.
  + Anschaffungskosten, Betriebskosten

# Projektmanagement

## Allgemein

### Merkmale

Phasen

SMART

## Visualisierung

### Netzplan

### Gantt-Diagramm

### EPK

## Amortisation

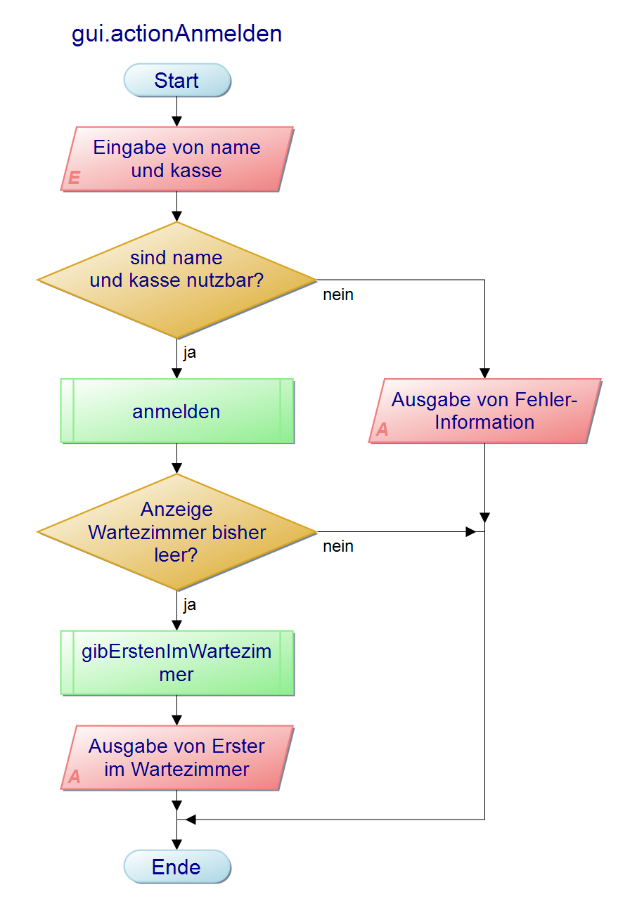
## Qualitätsmanagement

## 

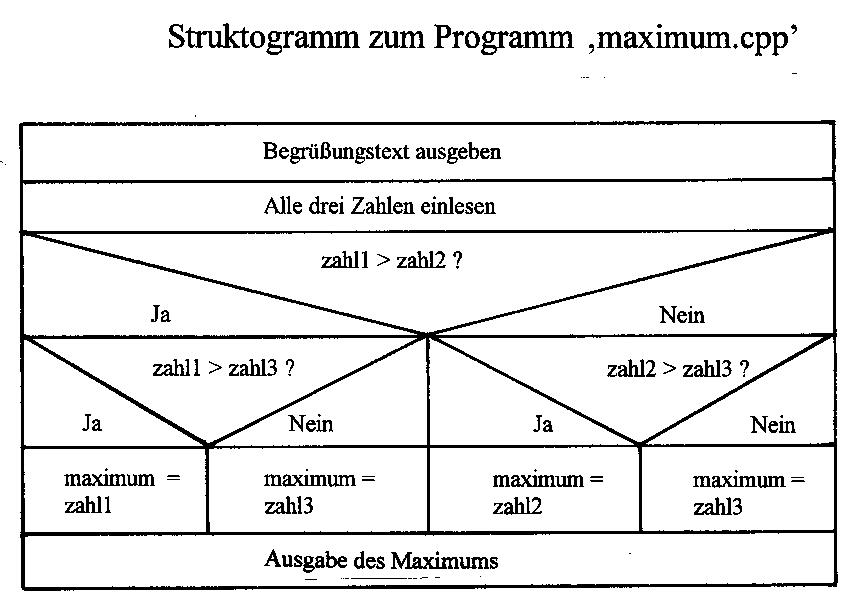
# Programmierung

## Codestrukturierung

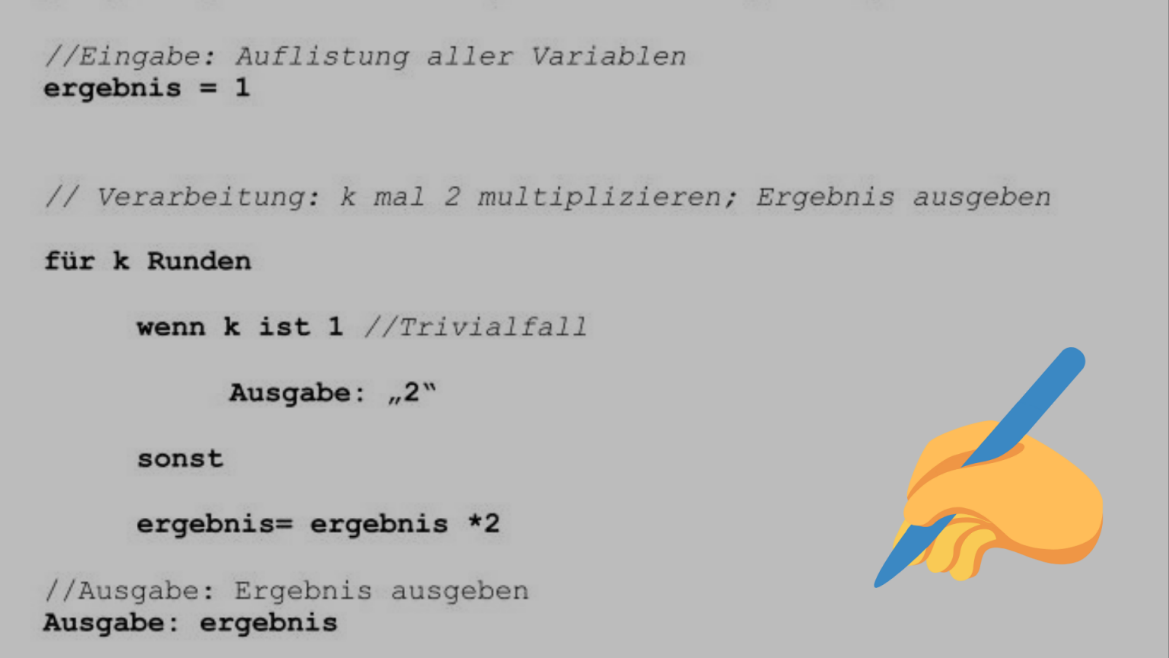
### PAP(Programmablaufplan)



### Struktogramm



### Pseudocode

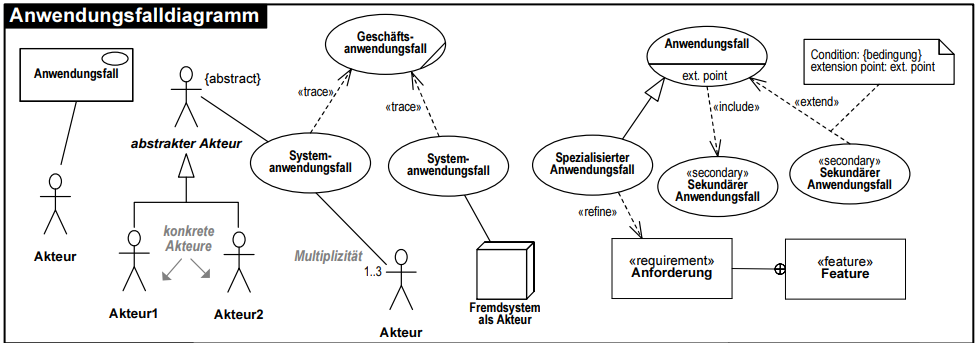


UML

[Notationsübersicht UML 2.5 (oose.de)](https://www.oose.de/wp-content/uploads/2012/05/UML-Notations%C3%BCbersicht-2.5.pdf)

### Anwendungsfalldiagramm

* Muss vom Programmierer und Auftragsgeber verstanden werden
* Akteure
  + Nutzt das System, ist aber nicht Bestandteil vom System
* Abstrakte Akteure
  + Nicht wirklich real
* Use-Case
  + Können in Beziehung zueinanderstehen (extend, include)
  + Extend benötigt Bedingung
* Fremdsysteme als Akteure möglich



### Klassendiagramm

## Lastenheft/Pflichtenheft

* Lastenheft (Standpunkt des Kunden)
  + Kunde beschreibt seine Anforderungen an das Projekt
* Pflichtenheft (Antwort aufs Lastenheft)
  + Darstellung wie das Projekt umgesetzt werden soll

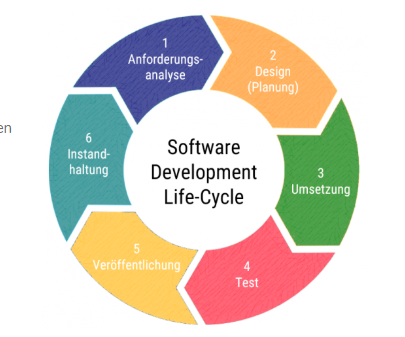
## Software

* Sammelbegriff für Software und die zugehörigen Daten

## Softwarearten

* Systemsoftware
  + Software, die sämtliche Abläufe des Rechners steuert
  + Schnittstelle zwischen Hard- und Software
  + Z.B. Betriebssysteme (Windows, MacOS) oder Software für wissenschaftliches Rechnen
* Standardsoftware
  + Software mit einem klar definierten Anwendungsbereich, die als vorgefertigtes Produkt erworben werden kann
  + Z.B.: Word, Excel, Powerpoint
* Anwendungssoftware
  + Software, die Aufgaben ausführen, die nichts spezifisch mit der Systemsoftware zu tun haben
  + Z.B.: Bildbearbeitung, E-Mail-Programme, Webbrowser, Textverarbeitung
* Branchensoftware
  + Software, die speziell auf die Anforderungen einer Branche abgestimmt ist
  + Z.B.: ERP oder CRM
* Individualsoftware
  + Software, die für einen Kunden individuell angefertigt wurde
  + Z.B.: Homepage, Wissensdatenbank für einen Verlag
* Open-Source-Software
  + Code kann öffentlich eingesehen, genutzt und verändert werden
* Proprietary Software
  + Möglichkeiten der Nutzung und Anpassung stark eingeschränkt

## Softwarelebenszyklus



* Anforderungsanalyse
  + Problem analysieren und Anforderungen bestimmen
* Design (Planung)
  + Anforderungen analysieren und Lösungswege überlegen
* Umsetzung
  + In Programmiersprache überführen (Coden)
* Test
  + Anforderungen testen
* Veröffentlichung
  + Software bereitstellen
* Instandhaltung
  + Anwender nutzen die Software

## Kriterien für Softwarequalität

|  |  |  |
| --- | --- | --- |
| Qualitätsmerkmale | Kenngrößen | Maßnahmen |
| Funktionalität | Liste der Anforderungen | Passende Absprache der Anforderungen an die Software |
| Effizienz | Ladezeit bei einer bestimmten Anforderung | Unnötigen Code vermeiden, Datenbankzugriffe effizient gestalten |
| Kompatibilität |  | Vorher Gedanken machen, womit die Software kompatibel sein muss |
| Benutzbarkeit | Kundenzufriedenheit | Absprache mit Kunden, Feedback einholen |
| Zuverlässigkeit | Ausfallzeiten | Fehlerquellen bei Ausfällen bestimmen und beheben |
| Sicherheit |  |  |
| Wartbarkeit | Lesbarkeit | Funktionen vernünftig benennen |
| Portabilität |  |  |

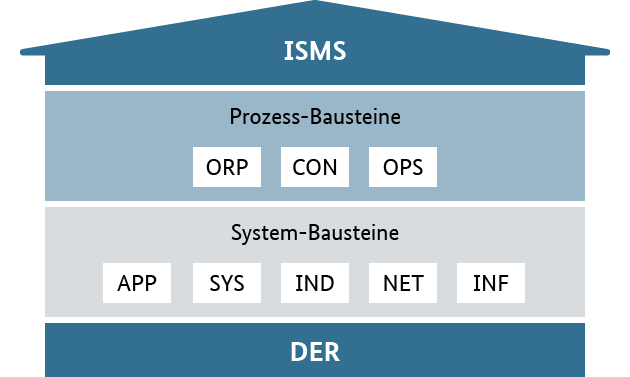
### IT-Sicherheit

## Schutzziele

* Kurz: **Verfügbarkeit**, **Integrität**, **Vertraulichkeit**
* **Verfügbarkeit**
  + Verhinderung von Systemausfällen
  + Daten müssen innerhalb eines bestimmten Zeitraums verfügbar sein
* **Integrität**
  + Datenänderungen müssen nachvollziehbar sein, dürfen nicht unbemerkt verändert werden
* **Vertraulichkeit**
  + Daten dürfen nur von Leuten gelesen werden, die die Berechtigung dafür haben

## ISMS (Informationssicherheits-Managementsystem)

### Übersicht



### Bausteine

* **ORP**: Organisation und Personal
  + Informationssicherheit auf organisatorischer und personeller Ebene
    - Verantwortlichkeiten
    - Mitarbeiterschulungen
    - Mitarbeiterverantwortung
    - ..
* **CON**: Konzeption
  + Allgemeines Konzept
    - Verschlüsselung
    - Datenschutzkonzept
    - Datensicherungskonzept
* **OPS**: Betrieb
  + Umsetzung von IT-Sicherheit
    - System-Administration
    - Schutz vor Schadprogrammen
* **APP**: Anwendungen
  + Schutz der Daten, die durch Anwendungen verarbeitet werden
    - Hinweise für Anwender von Office-Produkten
    - Sicherheitsanforderungen bei Webbrowsern
* **SYS**: IT-Systeme
  + Datenschutz bei internen und externen IT-Systemen
* **IND**: Industrie
  + a
* **NET**: Netzwerk
  + IT-Sicherheit bei internen Netzwerken
* **INF**: Infrastruktur

### Kreislauf

Ein Bild, das Text, Visitenkarte enthält.

Automatisch generierte Beschreibung

Schutzbedarfsanalyse

* Allgemein
* Bestandteile
  + Strukturanalyse
  + Schutzbedarfsfeststellung
  + Modellierung
  + Risikoanalyse

### Strukturanalyse

* Auflistung von
  + Geschäftsprozessen
  + Anwendungen
  + Zuordnungen von Geschäftsprozessen und Anwendungen
  + IT-Systemen
  + Zuordnungen von Geschäftsprozessen und IT-Systemen
  + Räume

### Schutzbedarfsfeststellung

* Bei den Komponenten der Strukturanalyse schauen, wie viel Schutz für sie benötigt wird
* Angabe für alle drei Schutzziele (normal, hoch, sehr hoch)

### Modellierung

* Objekte den Bausteinen zuordnen

### Risikoanalyse

* Zielobjekte zusammenstellen
  + Mindestens einen hohen oder sehr hohen Schutzbedarf in einer der drei Schutzzielen
* Risiken identifizieren und Bausteine finden
* Risiken einstufen
  + Häufigkeit und möglich Schäden
* Risiken behandeln