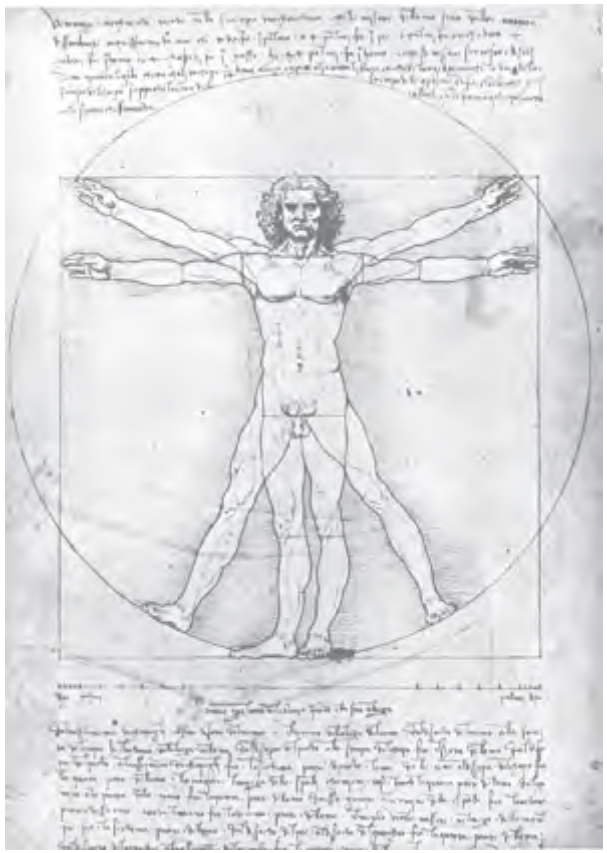


Systems Engineering als Schlüsseldisziplin in Projekten mit funktionaler Sicherheit

ThomasFranzen
SystemBeratung

Mittelstraße 25/1
88471 Laupheim
Fon: 07392 - 9393525
Fax: 07392 - 9393526
Mailto: tf@thomasfranzen.com

Beispiele nicht sicherer Systeme

Windscale (Sellafield) 1957, 2005, 2014

Apollo 13 1970

Ariane 5 1996

Functional Safety

Tschernobyl 1986

Fukushima 2011

Wie es zu diesem Vortrag kam

Immer mehr Systeme müssen unter dem Aspekt funktionaler Sicherheit entwickelt werden.

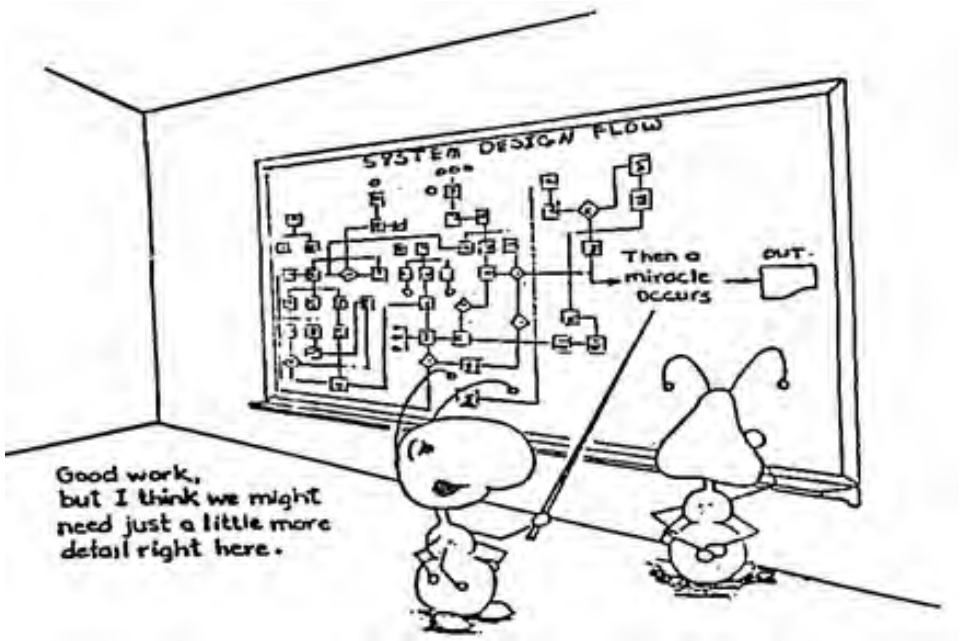
Die Systeme kommen aus den Bereichen:

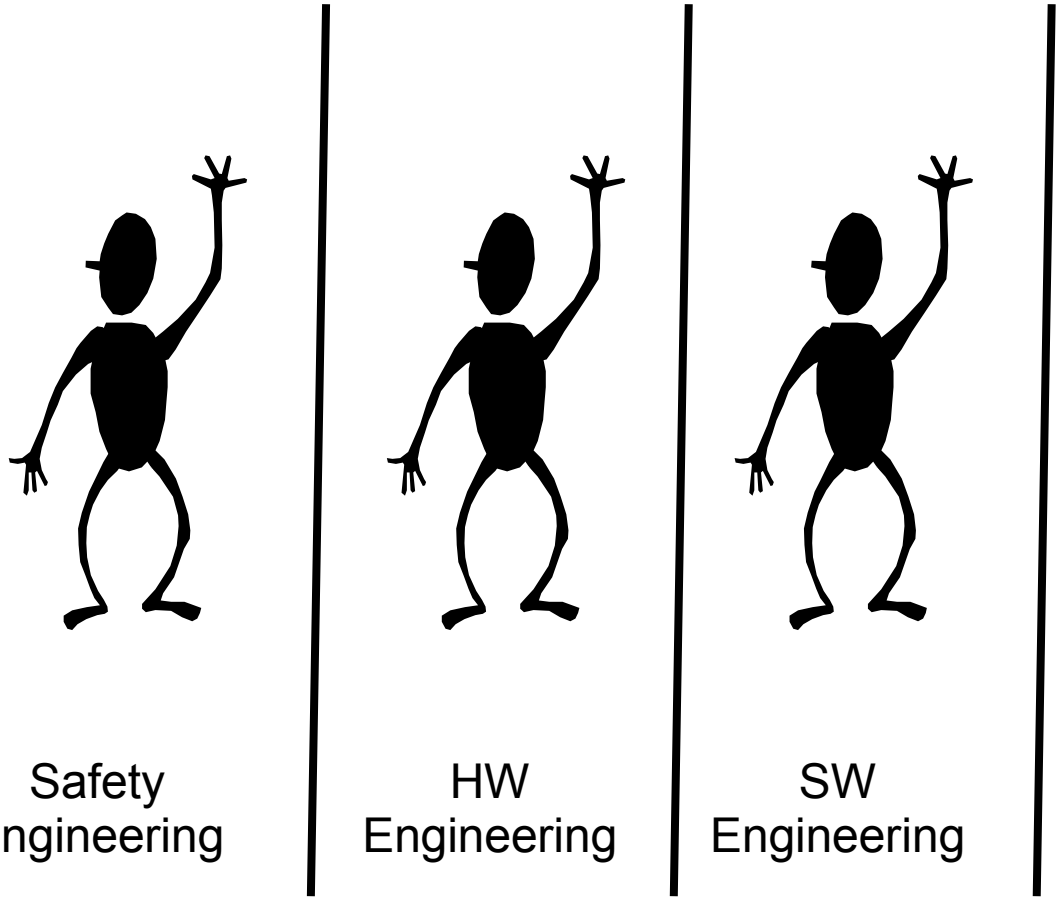
· Automotive
· Eisenbahn
· Avionik
· Medizintechnik

Daraus folgt, dass sich immer mehr KMUs mit dem Thema „funktionaler Sicherheit“ auseinandersetzen müssen.

In vielen KMUs ist System Engineering als eigenständige Disziplin noch nicht integriert.

Mangelnde System Engineering Kompetenz macht den Projekterfolg fraglich.




Safety Engineering
HW Engineering
SW Engineering
Das System

Systems Engineering (~~auch Systems Design oder Systems Design Engineering~~) ist ein interdisziplinärer Ansatz, um komplexe technische Systeme in großen Projekten zu entwickeln und zu realisieren. Systems Engineering ist nötig, da gerade in großen komplexen Projekten Punkte wie zum Beispiel Logistik und Koordination schwerer zu handhaben sind und zu massiven Problemen bei der Abwicklung des Projekts führen können.

Quelle: Wikipedia

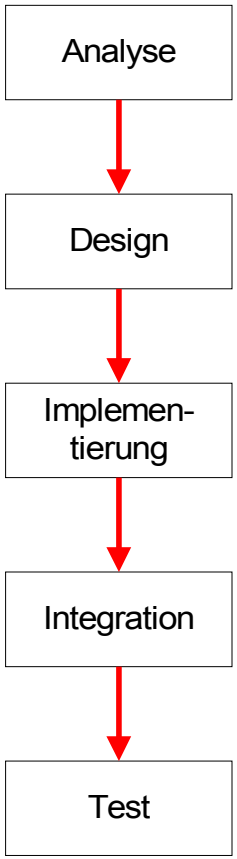
Was ist Systems Engineering?

System Engineering ist ein interdisziplinärer Ansatz, um komplexe technische Systeme in Projekten zu entwickeln und zu realisieren.

Die wesentlichen (primären) Prozesse des System Engineerings sind:

· Analyse
· Design
· (Implementierung)
· Integration
· Test

Unter Prozess versteht man in diesem Kontext: Vorgehensweise, Verfahren.



Aufgabe des System Ingenieurs ist auch die Gestaltung.

Gestaltet werden:

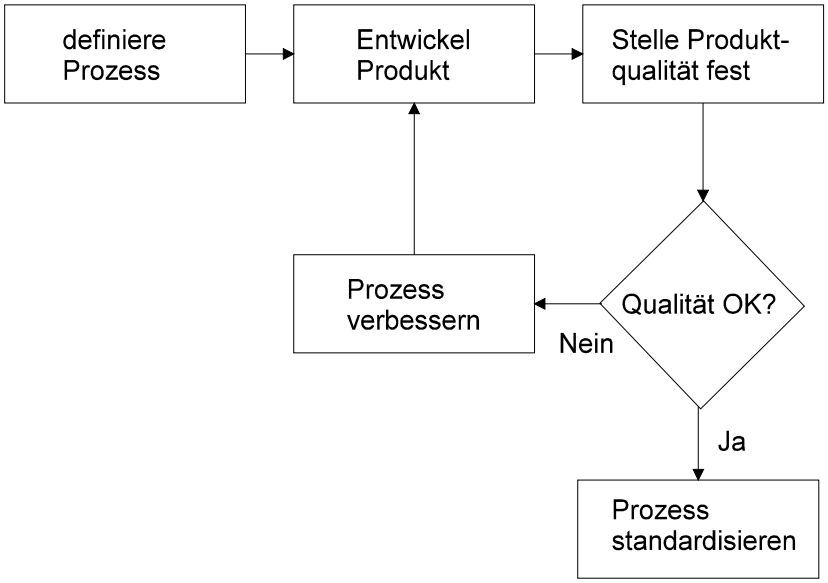
· Prozesse
· Methoden
· Design

... und letztendlich wird das System gestaltet.

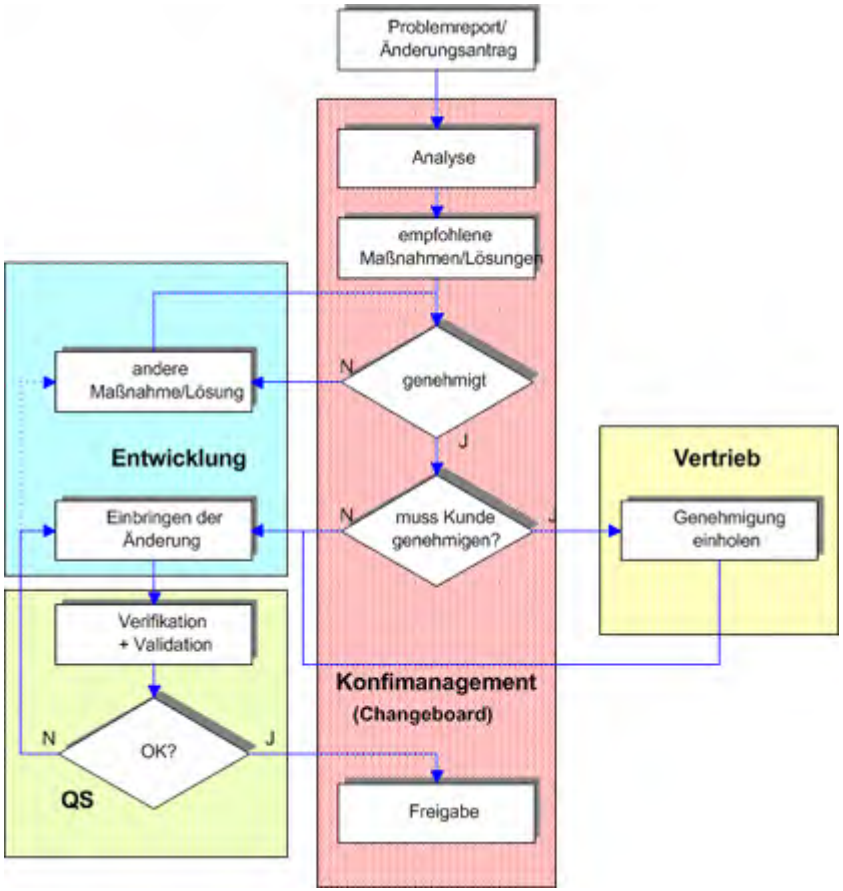
Für die Entwicklung funktional sicherer Systeme werden folgende Voraussetzungen an die entwickelnde Organisation gestellt:

1. Die Organisation kann nach dem V-Modell entwickeln
2. Die Organisation besitzt ein funktionierendes QM + KM System, das mindestens den Anforderungen aus ISO 9001 entspricht
3. Die Organisation besitzt ein funktionierendes System Engineering
4. Requirements Engineering und Management sind eingeführt
5. Test Engineering Prozesse sind eingeführt
6. HW + SW Engineering werden beherrscht
7. Erfahrung in der Entwicklung sicherheitskritischer Systeme ist ein Vorteil

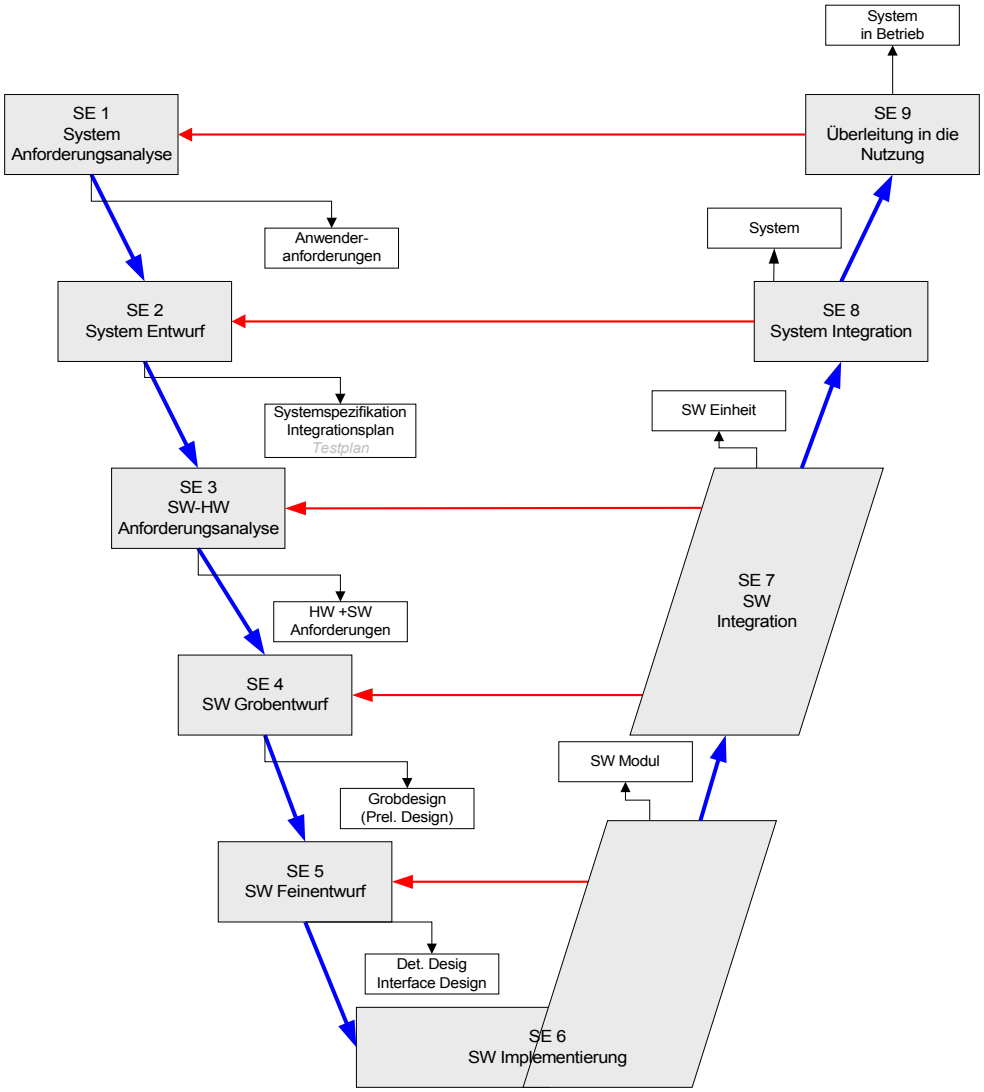
QM + KM System

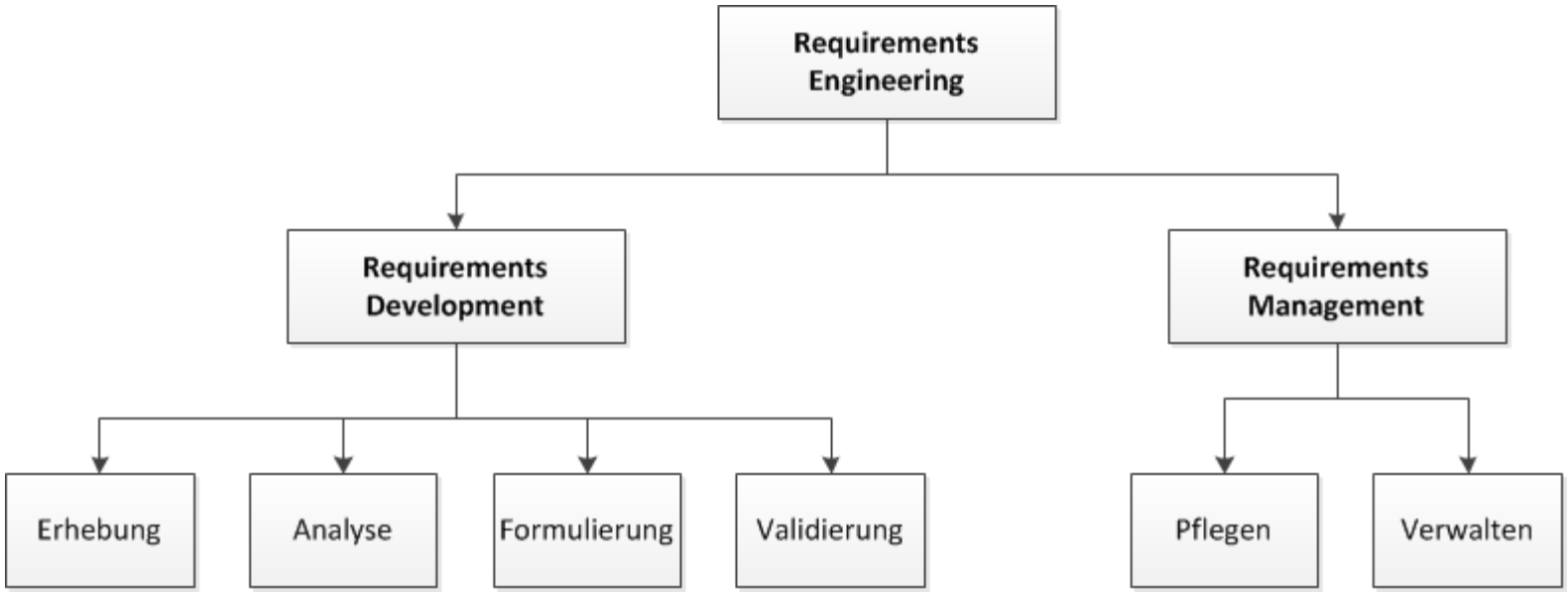


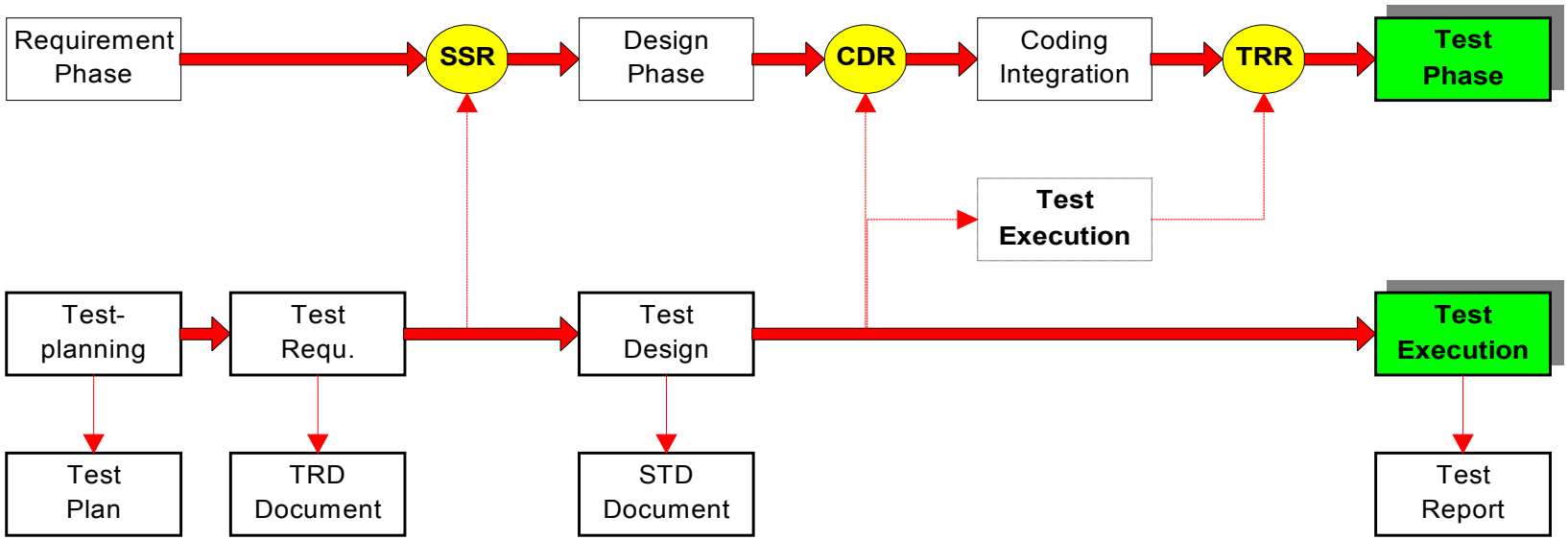
Functional Safety



V-Modell

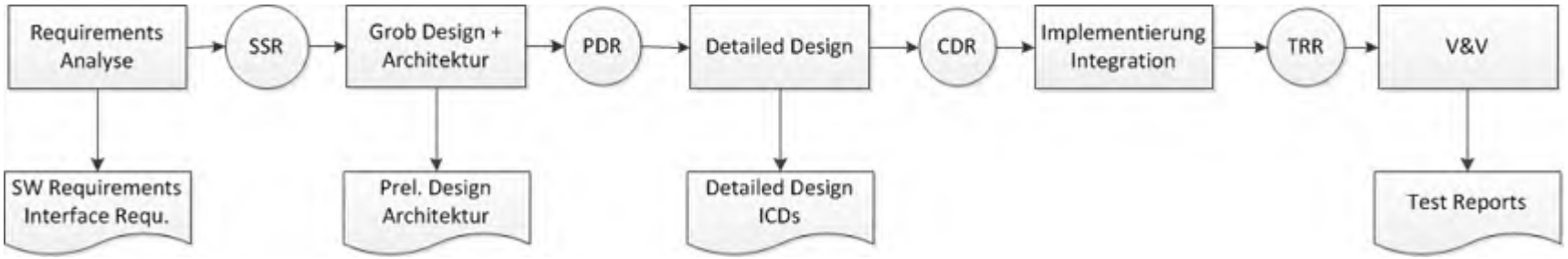

System
in Betrieb
SE 1
System
Anforderungsanalyse
SE 9
Überleitung in die
Nutzung
Anwender-
anforderungen
System
SE 2
System Entwurf
SE 8
System Integration
Systemspezifikation
Integrationsplan
Testplan
SW Einheit
SE 3
SW-HW
Anforderungsanalyse
SE 7
SW
Integration
HW +SW
Anforderungen
SE 4
SW Grobentwurf
SW Modul
Grobdesign
(Prel. Design)
SE 5
SW Feinentwurf
Det. Desig
Interface Design
SE 6
SW Implementierung


Requirements Engineering
Requirements Development
Requirements Management
Erhebung
Analyse
Formulierung
Validierung
Pflegen
Verwalten

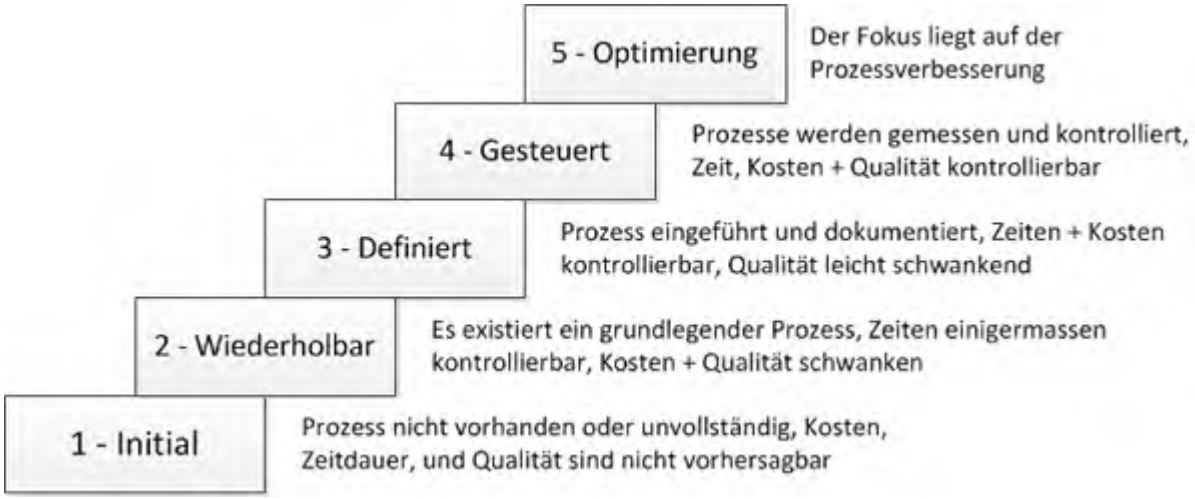


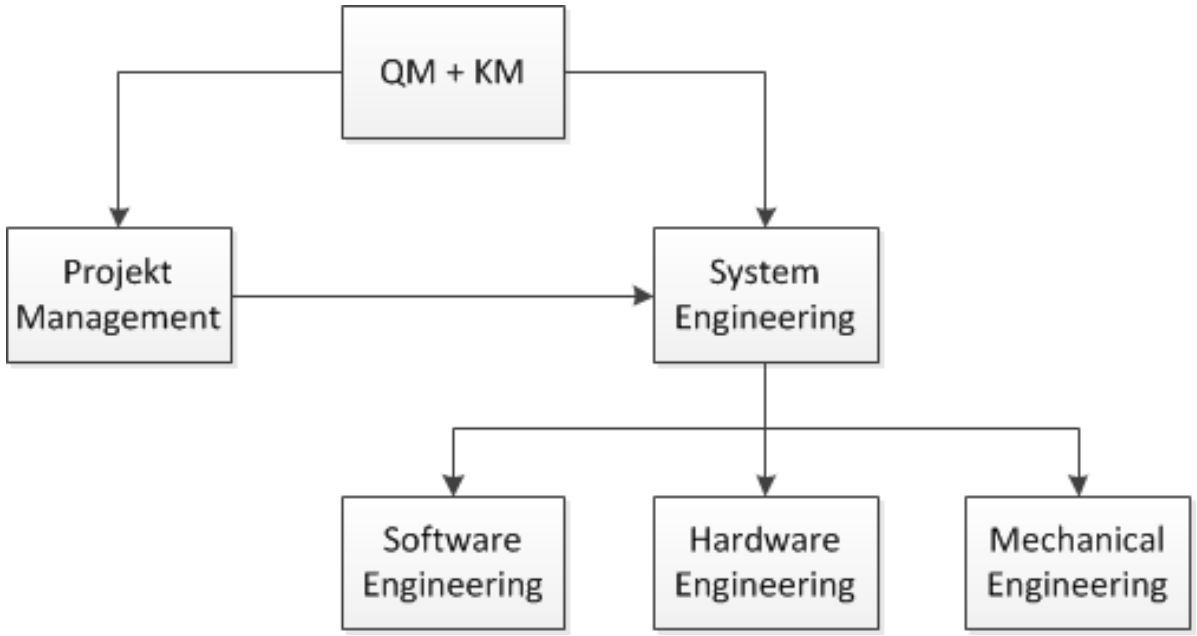
SSR: Software Specification Review
CDR: Critical Design Review
TRR: Test Readiness Review

TRD: Test Requirement Definition
STD: Software Test Description

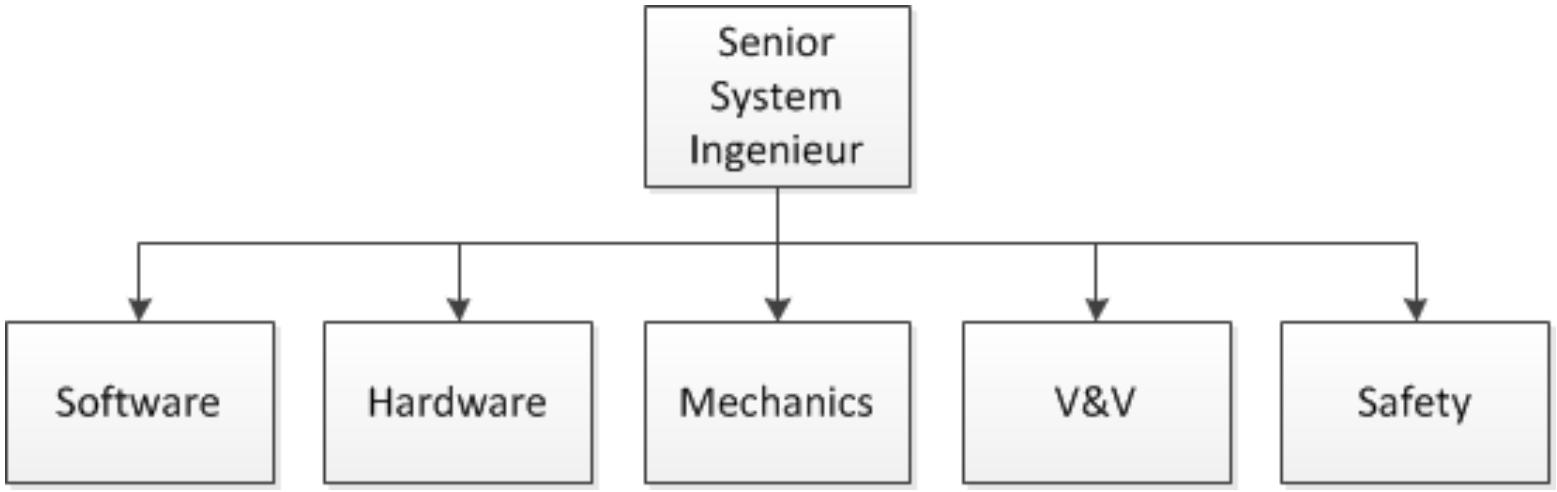


Ihre Organisation sollte SW auf mindestens CMM Level 3 entwickeln können, ansonsten kann es Schwierigkeiten mit der Zertifizierung des Systems geben.





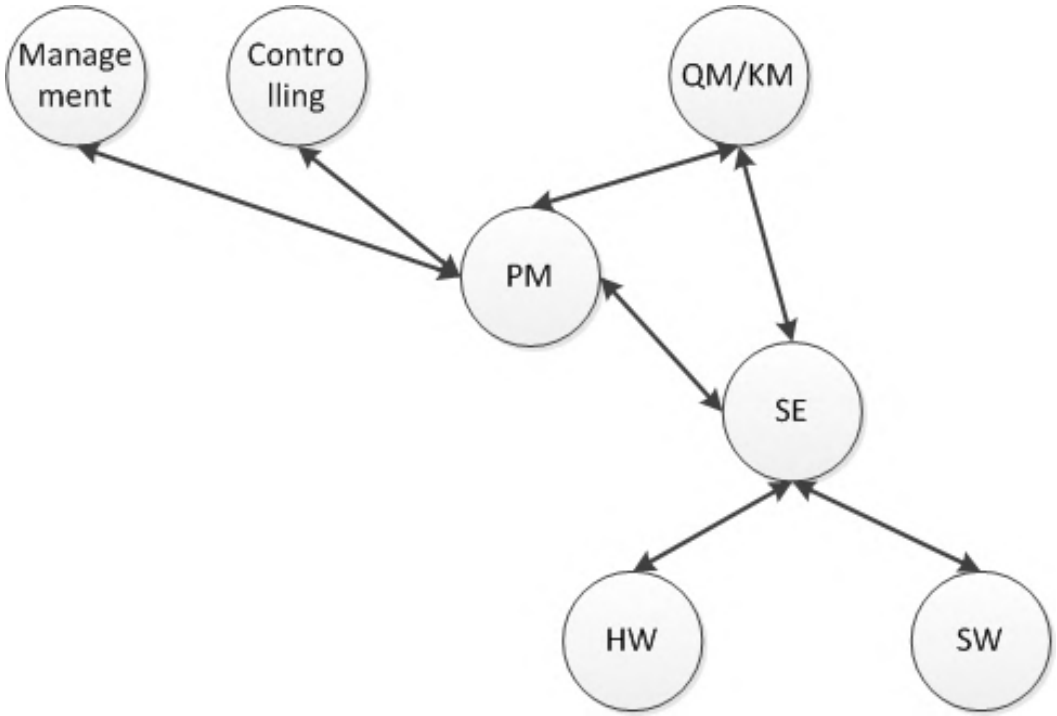
Das System Engineering ist verantwortlich für die Systementwicklung bis zur Auslieferung des Systems.

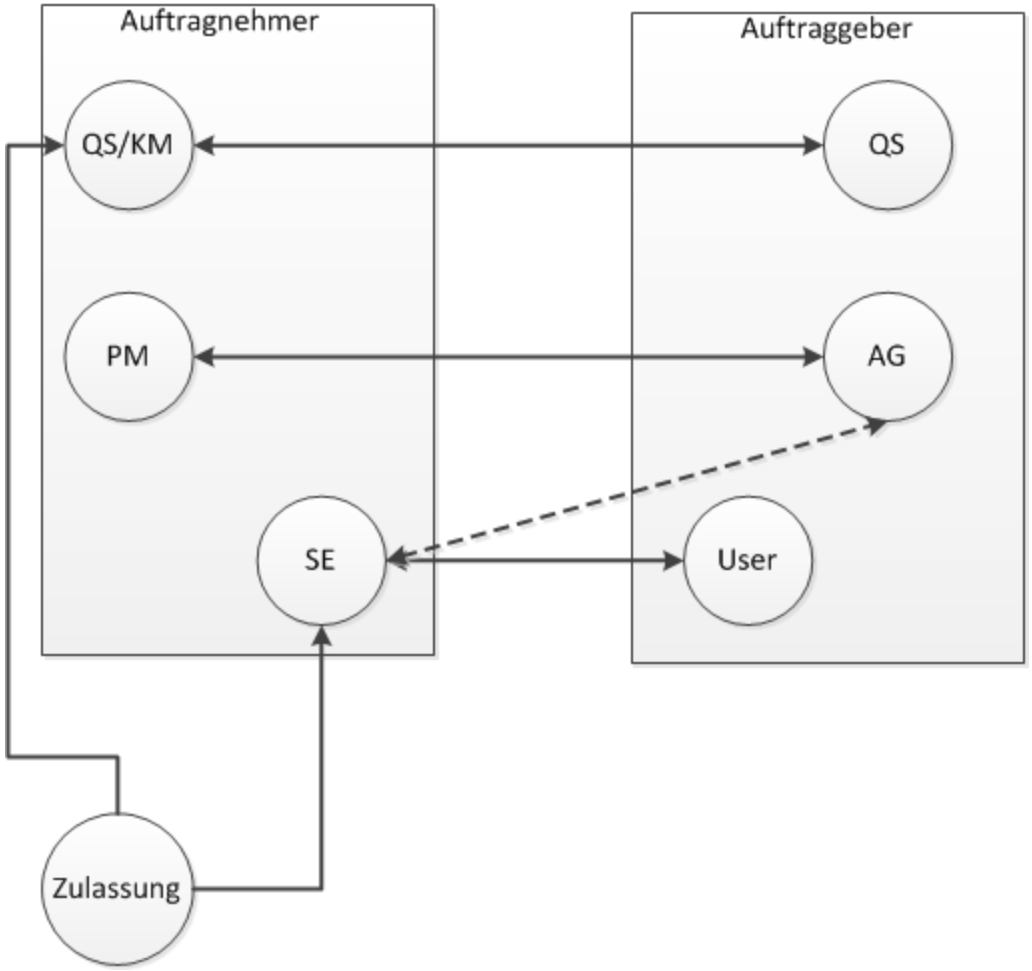


Inwieweit die Rollen auf unterschiedliche Personen aufgeteilt werden, hängt von den Kompetenzen und der Projektgröße ab.

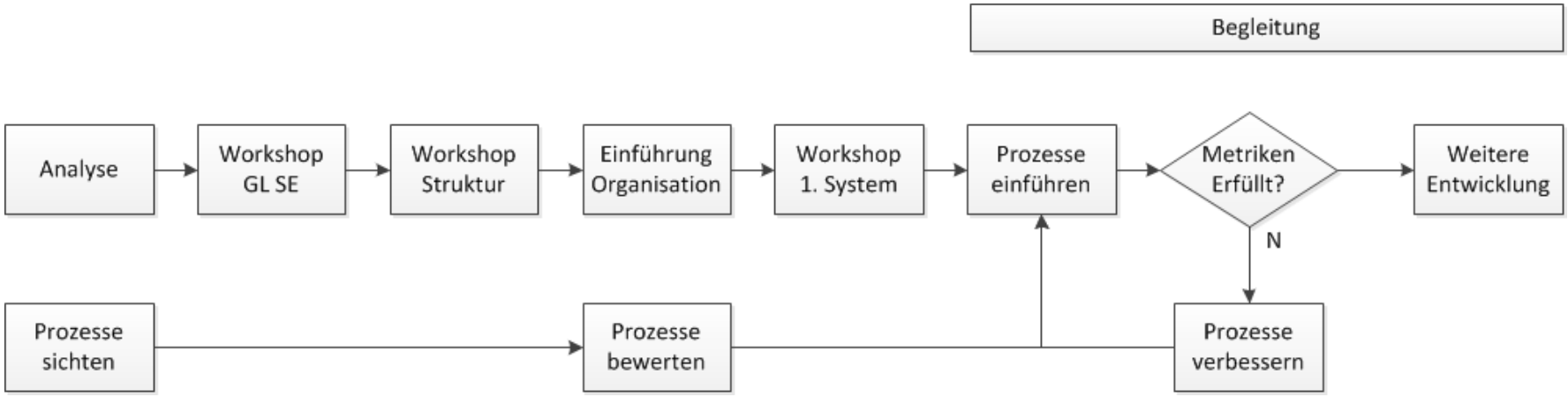
Hinweis: hier erfolgt die Systementwicklung, d.h. es werden keine HW, SW oder Mechanik entwickelt!

Rolle	Aufgaben/Verantwortlichkeiten
Senior SE	Gesamtsystem, SystemSpec, Systemarchitektur, Systemdesign, Schnittstellen extern, Umwelt, EMV
Software SE	Software, Spezifikation (SRS), IRS, Tayloring
Hardware SE	Hardware, Spezifikation
Mechanics SE	Mechanik, Spezifikation, Umwelt
V&V SE	Systemtestplan, Subsystemtestpläne, Testspez., ATPs, evtl.: Integrationsplan, Integration
Safety SE	Safety, Safetyarchitektur, Safetyplan


Manage
ment
Contro
lling
QM/KM
PM
SE
HW
SW


Auftragnehmer
Auftraggeber
QS/KM
QS
PM
AG
SE
User
Zulassung

Beispiel Einführung SE in einer Organisation



Wie geht es weiter?

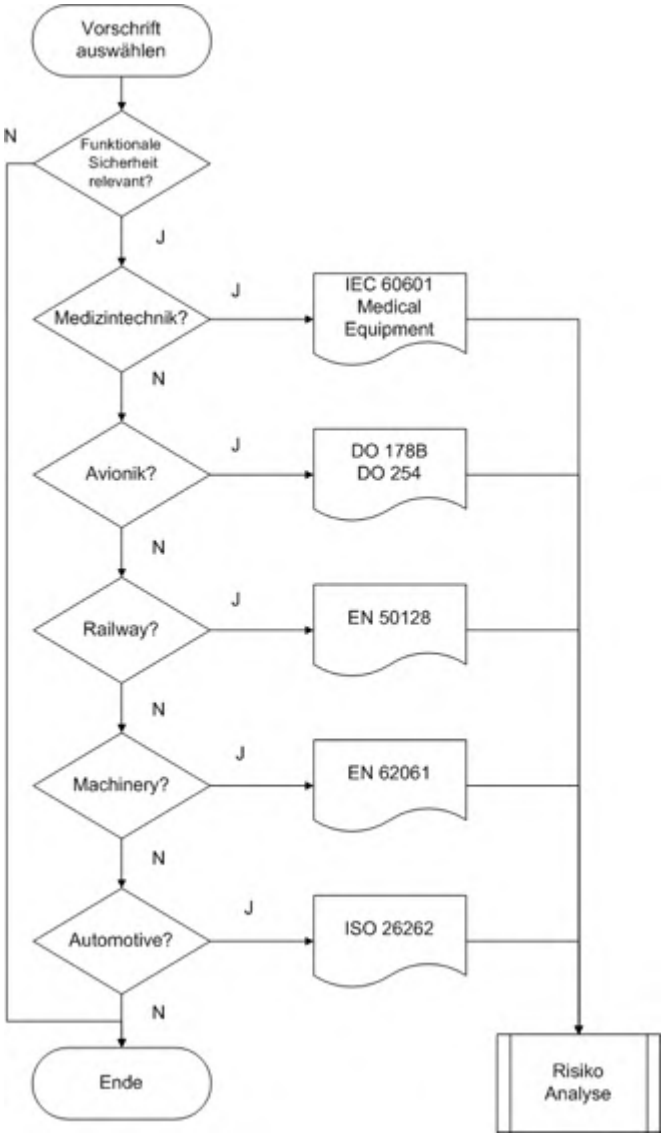
Sie sind zurück in Ihrem Unternehmen und wollen feststellen ob Sie Sicherheitskritische Systeme entwickeln können?

O.K.

Auf welchem Gebiet? Avionik? Medizintechnik? Sonstige?

Überlegen Sie bis zu welchem Level Sie entwickeln wollen.

SIL2? SIL3? DAL A?



Welche Voraussetzungen erfüllt Ihre Organisation?
Welche Defizite ergeben sich?

1. Die Organisation kann nach dem V-Modell entwickeln
2. Die Organisation besitzt ein funktionierendes QM + KM System, das mindestens den Anforderungen aus ISO 9001 entspricht
3. Die Organisation besitzt ein funktionierendes System Engineering
4. Requirements Engineering und Management sind eingeführt
5. Test Engineering Prozesse sind eingeführt
6. HW + SW Engineering werden beherrscht
7. Erfahrung in der Entwicklung sicherheitskritischer Systeme ist ein Vorteil

O.K. Sie haben 90%, haben aber noch nie ein sicherheitskritisches System entwickelt und gerade einen Auftrag für eine SW Entwicklung nach DAL A angenommen. Volumen 500.000 €.

Mit welchem Lehrgeld müssen Sie rechnen?

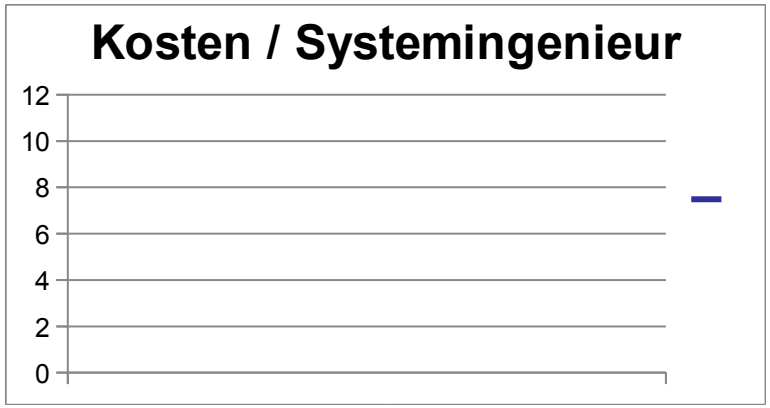
Holen Sie sich fehlende Kompetenzen für einen definierten Zeitraum von extern. Z.B. externe Mentoren. Zeitraum 6 – 12 Monate.

Ihre Mitarbeiter meinen das brauchen sie nicht, das können sie selber.

O.K. siehe vorherige Folie.

Wollen es aber einführen!

Was kostet Sie das?



Was noch?

Hängt von der vorhandenen Infrastruktur und den beherrschten Prozessen ab.