

Course "Softwaretechnik"

Normales und radikales Vorgehen

Lutz Prechelt

Freie Universität Berlin, Institut für Informatik

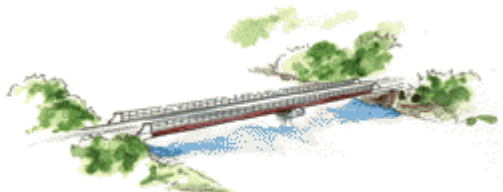
<http://www.inf.fu-berlin.de/inst/ag-se/>

- Fallstudie:
Tacoma Narrows Bridge
- "Normales Vorgehen",
"Radikales Vorgehen"
 - Beurteilung
- Wann/warum geht man radikal vor?
 - Unverstandene Anforderungen
 - Unverstandener Entwurf
- Wie geht man normal vor?
 - Arten von Wiederverwendung

- Verstehen, warum Ingenieurwesen auf erfahrungsgeleitetes Vorgehen angewiesen ist.
 - "Normales Vorgehen"
- Verstehen, warum man in seinem Vorgehen immer irgendwo von vorherigen Erfahrungen abweicht.
 - "Radikales Vorgehen"
- Einsehen, dass ingenieurmäßiges Vorgehen darin besteht, solche Abweichungen zu vermeiden/gering zu halten.
 - Radikales Vorgehen nur, wo unbedingt nötig!
- Ansätze für normales Vorgehen verstehen.

Fallbeispiel: Die Tacoma Narrows Bridge (TNB)

- 1938-1940: Brückenbau über den Puget Sound im Staat Washington
 - und zwar als Hängebrücke
 - wegen großer Spannweite
 - nicht verwechseln mit Gesamtlänge!



Balkenbrücke (bis ~200m)
 Girder bridge



Bogenbr. (bis ~150m)
 Arch bridge



Fachwerkbr. (bis ~500m)
 Truss bridge



Schrägseilbr. (bis ~500m)
 Cable-stayed bridge



Hängebr. (bis ~1000m)
 Suspension bridge

(<http://www.matsuo-bridge.co.jp/english/bridges/index.shtm>)

TNB: Chefingenieur

- Chefingenieur war Clark Eldridge
- Chefberater für die Konstruktion war ein Experte für Hängebrücken, Leon Moisseiff
 - Er hatte zuvor schon die Manhattan Bridge, Bay Bridge, George Washington Bridge und die Golden Gate Bridge maßgeblich mitgebaut
 - und war Spezialist für die Rechenmodelle



Golden Gate Bridge
1970m Länge
1280m Spannweite



Bay Bridge (west)
2820m Länge
700m Spannweite



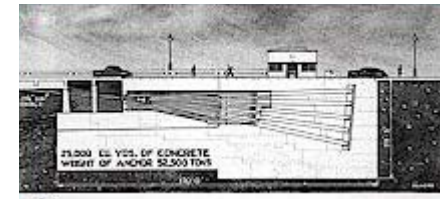
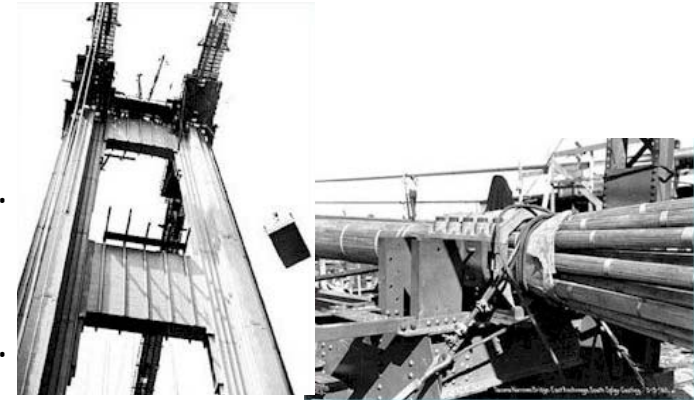
Tacoma Narrows B.
1520m Länge
850m Spannweite

Es gibt eine Vielzahl wichtiger Konstruktionsparameter für eine Hängebrücke:

- z.B. für die Einzelteile
 - Pylonverankerung, Pylon, Tragseilverankerung, Tragseil, Hängeseil, Fahrbahnunterbau, Fahrbahn
 - (jedes dieser Teile besteht natürlich wiederum aus einer Vielzahl von Teilen)
- jeweils diverse immer relevante Parameter
 - Material, Bauform, Verarbeitungsweise, Dimensionen
- und zusätzlich weitere spezielle (je nach Teil)
- Ferner globale Parameter

Die Tacoma Narrows Bridge hatte überwiegend ganz übliche Parameter für die Einzelteile:

- Übliche Pylonen
 - bezügl. Bauart, Größen, Materialien etc.
- übliche Seile
 - bezügl. Bauart, Größen, Materialien etc.
- eine übliche Verankerung
 - bezügl. Bauart, Größen, Materialien etc.
- eine übliche Fahrbahn
 - bezügl. Bauart, Größen (2 Fahrspuren, 2 Gehwege), Materialien
- einen weitgehend üblichen Unterbau
 - bezüglich Größen, Materialien

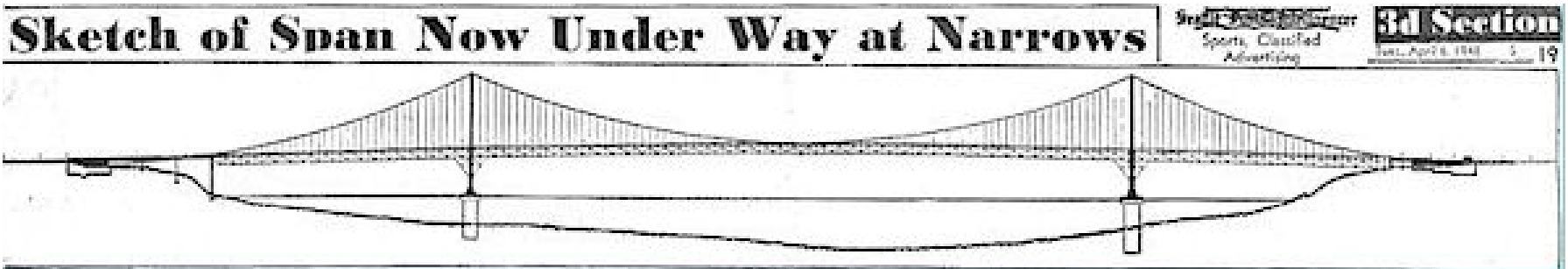


- Spannweite
 - Drittgrößte je gebaute (bis dahin)
 - Aber Moisseiff hatte die einzigen beiden größeren (Golden Gate, George Washington) mitgebaut
- Konstruktion des Fahrbahn-Unterbaus ("Tragwerk"):
 - Geschlossene Seitenwand statt Fachwerk
- Schlankheit
 - Tragwerk nur 12m breit und 2,40m hoch
 - Das Verhältnis Tragwerkhöhe: Spannweite war 1:350 (üblich war eher bis zu 1:90)
 - Das Verhältnis Tragwerksbreite: Spannweite war 1:72 (Golden Gate Bridge: 1:47)



TNB: Entscheidung über Parameter

- Der Entwurf wurde für die ungewöhnlichen Parameter von anderen Brückeningenieuren vor dem Bau kritisiert
 - Sie war ungewöhnlich leicht und flexibel für ihre Spannweite
 - geringe Breite, geringe Höhe des Tragwerks (also wenig Steifheit)
 - und Hängebrücken sind prinzipbedingt seitenwindempfindlich
- Aber Moisseiff bestand darauf, sie würde funktionieren
 - Er hatte ein Rechenmodell, nach dem sie Winden bis über 140 km/h standhalten sollte.
 - Die Geldgeber verlangten daraufhin die leichte Konstruktion



- Bau ging reibungslos vonstatten
- Eröffnung erfolgte im Juli 1940
- Schon während des Baus zeigte die Brücke starke Bewegungen bei Wind
 - Spitzname "Galloping Gertie"
- Nicht nur Querschwingungen, sondern achterbahnartige Längsschwingungen
 - Konstruktion war aber offenbar stark und flexibel genug, keine Schäden
- Am 7. November 1940 schaukelten sich die Schwingungen soweit auf, dass die Brücke zerbrach

TNB: Der Kollaps



TNB: Ursache für den Kollaps

- Keine Ursache: Die Windstärke
 - Sie war mit ca. 75 km/h noch weit im zulässigen Bereich
- Unfallhergang (Mechanismen):
 - Durch die Schwankungen rissen einige der Tragseile, was zur Überlastung der benachbarten Tragseile führte u.s.w.
- Unfallursache (Bedingungen):
 - Die Längsschwingungen, für die die Brücke nicht konstruiert war
- Unfallherkunft (Urgründe):
 - Herkunft: Das Rechenmodell von Moisseiff berücksichtigte nur Querschwingungen
 - Urgrund: Längsschwingungen waren vor TNB nie relevant gewesen, weil vergleichbar lange Brücken stets viel schwerer und steifer gebaut worden waren.
 - Ururgrund: Moisseiffs Konstruktion lag zu weit außerhalb des Bereichs, über den es Erfahrungen gab.

- 1948-1950 wurde eine neue Tacoma Narrows B. gebaut
 - Gleiche Spannweite
 - Fundamente wiederverwendet
 - Die Tragwerksbreite wurde um 50% erhöht
 - von 12m auf 18m
 - Die Tragwerkshöhe wurde um 300% erhöht
 - von 2,4m auf 10m
 - Das Tragwerk ist wieder ein offenes Fachwerk
- Die neue Brücke liegt damit für alle Parameter wieder im normalen Bereich:
 - Verhältnis Tragwerkshöhe: Spannweite sinkt auf übliche 1:85
 - Verhältnis Tragwerksbreite: Spannweite sinkt auf übliche 1:48 (wie bei Golden Gate B.)



- <http://www.lib.washington.edu/specialcoll/exhibits/tnb/default.html>
 - Hauptquelle, ausführliche Dokumentation mit vielen Bildern
 - ziemlich interessant!
- Vergleich der Parameter von TNB 1 und TNB 2
 - <http://www.nwrain.net/~newtsuit/recoveries/narrows/comp.htm>
- Englische Wikipedia:
 - Tacoma Narrows Bridge
 - Golden Gate Bridge
 - Bay Bridge
- Die längsten Brücken verschiedener Typen:
 - http://www.bernd-nebel.de/bruecken/1_einfuehrung/rekorde/rekorde.html

TNB: Zusammenfassung

- Die TNB war eine Konstruktion, die man zu beherrschen glaubte
 - Fast alle Eigenschaften waren wohlverstanden und wurden richtig gemacht
 - Materialien/Verarbeitung/Dimensionierung für Pylone, Tragwerk, Fahrbahn, Tragseil, Halteseile, Verankerung: alles bestens
 - Der weltbeste Experte hatte die Brücke konzipiert
- Sie entfaltete dann jedoch eine Eigenschaft (Längsschwingungen), mit der niemand gerechnet hatte
 - und die nicht von einem bestimmten Teil herrührte, sondern von deren Zusammenwirken ("**emergente Eigenschaft**")
- und die das Projekt komplett zunichte machte.
- Ursache: Man war in einer einzigen Hinsicht (Leichtheit) weit von dem abgewichen, was man aus vergleichbaren Projekten kannte.

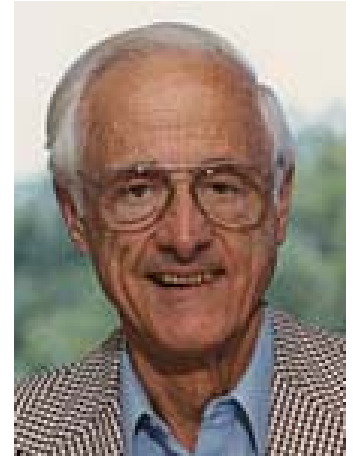
Die Moral von der Geschichte'

- Die emergenten Eigenschaften komplizierter Systeme lassen sich durch keine Theorie vorhersagen
 - Man versteht und beherrscht sie nur allmählich aufgrund von Erfahrung
- Etwas Neues ist also nur verstehbar/beherrschbar, wenn es Bekanntem stark ähnelt
- Deshalb ist erfolgreiches Ingenieurwesen davon abhängig,
 - immer möglichst viel so zu machen "wie üblich"
 - und nur möglichst wenig "neu" oder "ganz anders"
- denn ein Projekt soll ja zuverlässig und auf Anhieb klappen; nicht "nur allmählich aufgrund von Erfahrung" (s. oben)

- Etwas so zu machen "wie üblich" nennen wir **"normales Vorgehen"**
 - N1 Wir wissen, wie das geht. Wir tun es routinemäßig.
 - N2 Wir verstehen, worauf es dabei ankommt (Erfolgsfaktoren)
 - N3 Wir kennen die typischen Probleme dabei (Risikofaktoren)
 - N4 Wir verstehen, wofür das Vorgehen geeignet ist und wofür vielleicht nicht (Anwendbarkeitsbereich)
 - N5 Wir dürfen zuversichtlich sein, einen Erfolg zu erzielen
- Etwas "ganz anders" zu machen oder etwas "ganz Neues" zu tun nennen wir **"radikales Vorgehen"**
 - R1 Wir wissen nur *grob* (allgemein, nicht konkret), wie das geht
 - R2 Wir verstehen nur *teilweise*, worauf es dabei ankommt
 - R3 Wir wissen noch *nicht*, welche Probleme uns bevorstehen
 - R4 Wir verstehen höchstens *ansatzweise* Eignung und Grenzen
 - R5 Wir können allenfalls *hoffen*, einen Erfolg zu erzielen

Herkunft der Begriffe

- Die Unterscheidung wurde geprägt von Walter Vincenti, Professor für Luftfahrtwesen
 - Er nennt es "normal design", weil in aller Welt (außer bei den Softwareleuten) das Wort Design die Anforderungsdefinition mit einschließt
- Hier seine Formulierungen:
 - "[The engineer practicing normal design] knows at the outset how the device in question works, what are its customary features, and that, if properly designed along such lines, it has a good likelihood of accomplishing the desired task."
 - "[In radical design] how the device should be arranged or even how it works is largely unknown. The designer has never seen such a device before and has no presumption of success. The problem is to design something that will function well enough to warrant further development."
 - "What engineers know and how they know it", 1993



Anmerkung 1: Aspekte (nicht das Ganze) sind normal/radikal

- Jeder Aspekt eines Projekts ist entweder normal oder (mehr oder weniger) radikal
 - Jedes Einzelteil des Resultats (Produkt)
 - Jeder Arbeitsschritt auf dem Weg dahin (Prozess)
- Kein Ingenieurprojekt kommt ohne Anteile radikalen Vorgehens aus
 - irgendwas muss immer anders gemacht werden als gewohnt
- aber ein insgesamt "normales" Projekt hat nur wenige und kleine radikale Anteile/Aspekte.

Anmerkung 2: Lernziele in einem Ingenieurfach

1. Grundlagenwissen erwerben, um nötiges radikales Vorgehen besser bewältigen zu können
 - z.B. Informatikstudium: gesamtes Grundstudium
 - Allgemeines Wissen: Breit
 2. Erfahrungswissen und Urteilskraft erwerben, um möglichst oft normal vorgehen zu können
 - ...und radikalem Vorgehen wo immer möglich aus dem Weg gehen zu können
 - Bereichsspezifisches Wissen: Eng!
- Kurz gefasst:
 - Radikales Vorgehen ist der (einzig mögliche) Weg für Anfänger
 - Normales Vorgehen ist die Domäne der Profis

Anmerkung 3: Das Spannungsfeld

- Eigentlich ist also überall normales Vorgehen wünschenswert
- Aber das benötigt viel Erfahrung im jeweiligen Bereich
- Immer normal vorzugehen schließt also hochinnovative Projekte aus
 - denn bei einer Innovation hat man per Definition keine Erfahrung
- Deshalb gibt es ein Spannungsfeld zwischen
 - risikoarmen Projekten (wenig radikales Vorgehen nötig)
 - die können aber nicht sehr innovativ sein
 - innovativen Projekten (viel radikales Vorgehen nötig)
 - die sind aber stets riskant

Anmerkung 4: Der Umkehrschluss gilt nicht

- Zwar benötigt ein innovatives Vorhaben einen hohen Anteil radikalen Vorgehens
- aber deshalb heißt viel radikales Vorgehen noch längst nicht, dass man etwas Innovatives tut
- Softwareingenieure neigen bislang dazu, an Stellen radikal vorzugehen, wo das weder sinnvoll noch nötig ist:

Anmerkung 4 (2): "Wo bleibt da die Herausforderung?"

- "Das Wort 'Herausforderung' hat für Software-Entwickler eine geradezu religiöse Bedeutung.
Herausforderungen sind es, die unserer Arbeit Bedeutung geben und den Unterschied zwischen Eintönigkeit und dem Aufbruch zu neuen Ufern ausmachen.
Wir verwenden fast ebensoviel Kreativität darauf, nach Herausforderungen zu suchen, wie darauf, ihnen zu begegnen.
Deshalb neigen Entwickler dazu, selbst in der prosaischesten Aufgabe eine Notwendigkeit für Eleganz oder Prägnanz oder Schlankheit oder Geschwindigkeit oder Flexibilität zu entdecken, die über die spezifizierte Anforderung hinausgeht."

Tom DeMarco in

"Warum ist Software so teuer?", S.83
(auch in IEEE Software Nov. 1990)



Quellen radikalen Vorgehens

- Ziele, unverständene Anforderungen
 - Wir verstehen nicht gut genug, WAS für ein System wir überhaupt bauen müssen, um den Zweck zu erreichen
 - Was also das geplante Verhalten sein soll
 - Beispiel folgt
- Konstruktion, unverständener Entwurf
 - Wir verstehen nicht gut genug, WIE das System beschaffen sein muss, damit es sich wie geplant verhält.
 - meist wegen emergenter Eigenschaften (unerwartete Schwierigkeiten; Beispiel: Tacoma Narrows Bridge)
 - oder weil es einfach derartig viele Teile braucht (klar sichtbare Schwierigkeiten)
- Prozess, unverständene Methodik
 - Wir verstehen nicht gut genug die VERFAHREN, mit denen man zu korrekten Anforderungen und tragfähigem Entwurf gelangt

Beispiel für unverstandene Anforderungen

- Ziel: die Radbremsen und die Schubumkehr eines Verkehrsflugzeuges sollen nur nach der Landung ansprechen
 - vor der Landung müssen sie gesperrt sein.
 - Das arrangiert man natürlich per Software
- Daraus abgeleitete Anforderungen (Airbus A320):
 - Bremsenfreigabe = beide Haupträder drehen mit mindestens 80% der Bodengeschwindigkeit
 - gemessen durch Drehgeschwindigkeits-Sensor an jedem Rad
 - Schubumkehrfreigabe = beide Haupträder auf dem Boden oder ein Rad auf dem Boden und dreht mit mind. 72 Knoten
 - Bodenkontakt gemessen durch Gewichtsschalter am Fahrwerk
 - (in Wirklichkeit noch um einiges komplizierter)

<http://www.rvs.uni-bielefeld.de/publications/Incidents/DOCS/ComAndRep/Warsaw/leyman/analysis-leyman.html>

Anforderungen A320 Schubumkehr

- Ein Landeanflug:
 - Tower: 13 Knoten Wind von schräg vorn (also Seitenwind)
 - Pilot wählt deshalb genau gemäß Lehrbuch manuelle Landung und Anfluggeschwindigkeit 145 Knoten(Luft) statt normal 130
 - Tatsächlich sind aktuell 15-25 Knoten Rückenwind mit Böen
 - Landegeschwindigkeit(Luft) steigt auf 155 Knoten
 - Landung erfolgt zunächst auf nur einem Hauptrad (genau gemäß Lehrbuch für Seitenwindlandung)
 - Landebahn ist 3mm hoch mit Wasser bedeckt
→ Aquaplaning → Das Rad beschleunigt nur langsam
 - Hohe Geschwindigkeit → viel Auftrieb → langsames Landen
→ 9 Sekunden Verzögerung bis Freigabe Bremsen/Schubumkehr
→ Flugzeug schießt über Landebahnende hinaus
 - 2 Tote (Warschau, 14. Sept. 1993)



Anforderungen A320 Schubumkehr (2)

- Das computerisierte Steuersystem der A320 war korrekt implementiert und hat wie spezifiziert gearbeitet
 - Aber es war nicht gut genug vorhergesehen worden, wie es mit den Umweltbedingungen interagieren könnte
- Grund: die Anforderungen an die Schubumkehrsperre waren ein radikales Vorgehen:
 - R2 Wir verstehen nur *teilweise*, worauf es dabei ankommt
 - R3 Wir wissen noch *nicht*, welche Probleme uns bevorstehen

Wichtigster Ansatz für normales Vorgehen: Wiederverwendung

Wiederverwendung

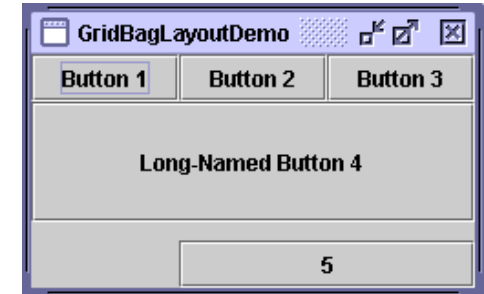
- von bewährten Komponenten
- von bewährten Entwurfsüberlegungen/Entwürfen
- von bewährten Anforderungen
- von bewährten Prozesselementen
- von bewährten Werkzeugen

(Die Übergänge sind fließend)

- Achtung: Wiederverwendung hat zwei Ziele
 - Senkung der Kosten
 - Senkung des Risikos
- Aus Sicht des normalen Vorgehens ist nur die Risikosenkung von Interesse
 - Die Kostensenkung gibt es quasi gratis dazu

Wiederverwendung von bewährten Komponenten

- Eine komplette Softwarekomponente benutzen, die man schon mehrmals zuvor in anderen Projekten für ähnliche Zwecke erfolgreich verwendet hat
 - z.B. eine Klasse, ein Modul, ein Subsystem
- Vorteile / Normalität:
 - N1 Wir wissen aus Erfahrung, wie man die Komponente benutzt
 - und brauchen es nicht erst mühsam zu erlernen
 - N3 Wir kennen die typischen Probleme dabei (Risikofaktoren)
 - z.B. Defekte, Seltsamkeiten
 - N4 Wir verstehen, wofür die Komponente geeignet ist und wo ihre Grenzen liegen (Anwendbarkeitsbereich)
 - Funktionalität, Qualitätsmerkmale, Kapazitätsverhalten, Leistungsgrenzen
 - N5 Wir dürfen zuversichtlich sein, ein an dieser Stelle gut funktionierendes System zu erhalten



Wiederverwendung von bewährten Entwurfsüberlegungen/Entwürfen

- Eine Softwarekomponente nach den gleichen Überlegungen konstruieren, wie man es schon mehrmals zuvor in anderen Projekten für ähnliche Zwecke erfolgreich getan hat
 - z.B. Einsatz eines Architekturmusters oder Entwurfsmusters
- Vorteile / Normalität:
 - N1 Wir wissen, wie man die Überlegungen anwendet.
 - N2 Wir verstehen, was das Wesen des Musters und seiner Nützlichkeit ausmacht (Erfolgsfaktoren)
 - N3 Wir kennen die typischen Stolperstellen beim Einsatz (Risikofaktoren)
 - N4 Wir verstehen, welche Ziele das Muster erreichen hilft und welche nicht oder wo es gar stört (Anwendbarkeitsbereich)
 - N5 Wir dürfen zuversichtlich sein, ein System mit den an dieser Stelle erwarteten Eigenschaften zu erhalten



Wiederverwendung von bewährten Anforderungen

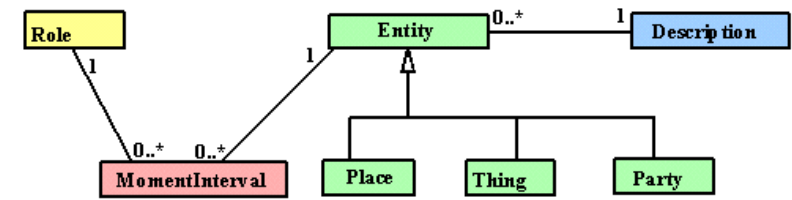
- Von einem System eine Gruppe von Eigenschaften fordern, die man bereits mehrmals zuvor in anderen Projekten für ähnliche Zwecke erfolgreich gemeinsam gefordert und umgesetzt hat

- z.B. Einsatz eines Analysemodells oder Problemrahmens

- Vorteile / Normalität:

- N1 Wir wissen, wie man diese Anforderungen hier formuliert.
- N2 Wir verstehen, was an den Anforderungen essentiell ist
 - und was anwendungsspezifisch wechselt (an Formulierung od. Inhalt)
- N4 Wir verstehen, welche Eigenschaften diese Anforderungen bewirken und welche nicht (Anwendbarkeitsbereich)
 - und können die Verträglichkeit mit anderen Anforderungen prüfen
- N5 Wir dürfen zuversichtlich sein, mit diesen Anforderungen ein gewisses angestrebtes Ziel auch zu erreichen
 - und keine Anforderung zu übersehen oder falsch zu formulieren

Business Modelling Stereotypes

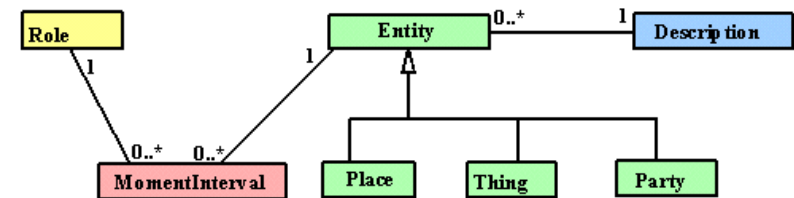


Wiederverwendung von bewährten Prozesselementen

- Im Projekt ein Verfahren verwenden, das man bereits mehrmals zuvor in ähnlichen Zusammenhängen für ähnliche Zwecke erfolgreich verwendet hat
 - z.B. Durchsichten, Testautomatisierung, Objektmodellierung
- Vorteile / Normalität:
 - N1 Wir wissen aus Erfahrung, wie das Verfahren gemacht wird
 - und brauchen es nicht erst mühsam zu erlernen
 - N2 Wir verstehen, worauf es dabei ankommt (Erfolgsfaktoren)
 - weil wir aus früheren Fehlern gelernt haben
 - N3 Wir kennen die typischen Probleme dabei (Risikofaktoren)
 - weil wir aus früheren Fehlern gelernt haben
 - N4 Wir verstehen, wofür das Verfahren geeignet ist oder nicht und was es erreichen kann oder nicht (Anwendbarkeitsbereich)
 - z.B. übertreiben wir es nicht

- Ein sprachliches oder technisches Hilfsmittel einsetzen, das man bereits mehrmals zuvor in anderen Projekten für ähnliche Zwecke erfolgreich eingesetzt hat.

- z.B. eine Notation/Sprache, einen Codegenerator



- Vorteile / Normalität:

- N1 Wir kennen uns bei der Verwendung aus
 - und machen deshalb wenig Fehler
- N2 Wir verstehen, worauf es dabei ankommt (Erfolgsfaktoren)
 - z.B. geschickte anstatt ungeschickte Benutzung
- N3 Wir kennen die typischen Probleme dabei (Risikofaktoren)
 - z.B. Schwächen der Notation, Defekte des Werkzeugs
- N4 Wir verstehen, wofür das Werkzeug geeignet ist und wofür schlecht oder gar nicht (Anwendbarkeitsbereich)
 - und werden deshalb beim Einsatzversuch nicht scheitern

- N5 Wir sind zuversichtlich, den gewünschten Effekt zu erzielen

Anmerkung 5: Nicht radikal, aber auch ungünstig

- Auch normales Vorgehen kann ungünstig sein:
nämlich unangemessen
- Beispiel:
 - Ich entwerfe und implementiere eine komplexe Komponente, die ich sehr gut verstehe, mit normalem Vorgehen,
 - z.B. bekanntem Entwurf und wiederverwendeten Anforderungen
 - obwohl mir eine gut geeignete wiederverwendbare Realisierung zur Verfügung steht.
- Solches Verhalten ist ineffizient (also teuer) und deshalb nicht ingenieurgerecht
 - ähnlich wie ein vermeidbares radikales Vorgehen

Zusammenfassung

- Normales Vorgehen bedeutet, etwas zu tun, das man gut kennt, versteht und beherrscht
 - Anwendungsweise, Erfolgsfaktoren, Risikofaktoren, Anwendungsbereich
- Radikales Vorgehen ist alles Übrige
- Wann immer möglich sollte man normales Vorgehen praktizieren
 - oder wenigstens anstreben
- Radikales Vorgehen ist dann akzeptabel, wenn es sich nicht umgehen lässt:
 - wegen Mangels an Personal mit dem passenden Wissen
 - wegen echter Innovation (d.h. überhaupt niemand könnte es normal tun)



Danke!