

Anwendungssysteme Kompakt

Version vom 07. Oktober 2004

eine Zusammenstellung von Hannes Restel

basierend auf einem Script vom Prof. Dr. Lutz Prechelt

- Technische Sicht
 - was ist technisch machbar (Theorie)?
 - wie macht man es (Konstruktion)?
 - Ist interessiert an „Verfügungswissen“
- Wirkungsorientierte Sicht (Wirkungssicht)
 - warum ist es wünschenswert
 - was ist wünschenswert?
 - wie sollte man es machen?
 - wozu führt das? (Vermeidung von unerwünschten Wirkungen)
 - ist interessiert an „Orientierungswissen“
- Informatik sollte Gestaltungswissenschaft sein
- Informatik produziert direkt/indirekt starke Auswirkungen auf das Leben fast aller Menschen
- Informatik befasst sich mit Anwendungen und Auswirkungen von Computern auf Umwelt
- Diskrepanz: Sind Informatiker nur für Entwicklung oder auch für Auswirkungen von Technik verantwortlich?
- Verfügungswissen + Orientierungswissen + Konsequenz = Verantwortliches Handeln
- Trennung zwischen:
 - Technikfolgeabschätzung (mittels Orientierungswissen)
 - Technikfolgenbewertung (mittels persönlicher/gesellschaftl. Wertschätzungen)
- Schwierigkeit/Unmöglichkeit der Vorhersagbarkeit von Auswirkungen der Informatik auf Gesellschaft (Bsp: analog zur Einführung des Automobils, Pervasive Computing)
- Forderungen von Wendell Berry (1987):
 - „To make myself as plain as I can, I should give my standards for technological innovation in my own work. They are as follows:
 - 1. The new tool should be cheaper than the one it replaces.
 - 2. It should be at least as small in scale as the one it replaces.
 - 3. It should do work that is clearly and demonstrably better than the one it replaces.
 - 4. It should use less energy than the one it replaces.
 - 5. If possible, it should use some form of solar energy, such as that of the body.
 - 6. It should be repairable by a person of ordinary intelligence, provided that he or she has the necessary tools.
 - 7. It should be purchasable and repairable as near to home as possible.
 - 8. It should come from a small, privately owned shop or store that will take it back for maintenance and repair.
 - 9. It should not replace or disrupt anything good that already exists, and this includes family and community relationships.“

- BruttoInlandsProdukt = Konsum + Investition + öffentliche Ausgaben + Exporte – Importe
- VWL: Zwei grundsätzliche Wege zur BIP-Steigerung:
 - Steigerung der Eingaben
 - mehr Arbeitseinsatz
 - Erwerbsquote, Arbeitszeit, Bevölkerungsgröße
 - mehr Kapitaleinsatz
 - Investitionen in Maschinen, Infrastruktur etc.
 - Steigerung der Produktivität
 - Produktivität = produzierter Mehrwert pro Einsatz von Arbeit und Kapital
 - Arbeitsproduktivität: Mehrwert pro Arbeitseinsatz (Arb.zeit)
 - Kapitalproduktivität: Mehrwert pro Kap.einsatz (Geld, Zeit)
- Das faktische Kapital eines funktionierenden Unternehmens ist viel höher als das nominelle:
 - Durch einbehaltene Gewinne steigt das buchhalterische Eigenkapital über das nominelle Grundkapital an, mit dem das Unternehmen mal begann
 - Da auch Kunden, Know-How, Marktposition und vieles mehr einen Wert darstellen, ist der Gesamtwert eines guten Unternehmens viel höher als sein Eigenkapital
- Für Wachstum brauchen wir entweder
 - mehr Arbeit (nicht unbegrenzt wünschenswert) oder
 - mehr Kapital (Börse!) oder
 - höhere Produktivität
- Grober Überblick: Wirkungssicht ("Rausgucken") der Informatik:
 - Erkennen kontroverser Themenfelder (Auswirkungen der Informatik)
 - z.B. Wirtschaft, Arbeitsmarkt, Arbeitsleben, Gesellschaftl. Unterschiede, Computer-Analphabetismus, Ausbildung, Demokratisierung, Gleichberechtigung/Chancengleichheit), Sicherheitskritische Systeme, Militärische Sicherheit, Gesundheit/Gesundheitswesen, Privatsphäre und Verschlüsselung
 - Zuordnung der oben genannten Themenfelder in grobe Klassen:
 - private Lebensführung Einzelner
 - Berufsleben Einzelner
 - Wirtschaft
 - Gesellschaft
 - Beziehung zwischen Gesellschaften
 - Computer als Werkzeuge oder sozio-technische Systeme
 - Wir wollen lernen, beide Sichtweisen zugleich zu benutzen
 - Fragen stellen:
 - Ist technischer Fortschritt auch sozialer Fortschritt?
 - Welche Lehren für die Zukunft bietet die Vergangenheit?
 - Sind Informatiker/innen zugleich auch Soziologen und Moralphilosophen?

- Diagnosefragen:
 - Technik: Sind die technischen Aussagen haltbar?
 - Technikfolgenabschätzung: Sind die behaupteten Auswirkungen wahrscheinlich?
 - Technikfolgenbewertung: Sind die Wirkungen wirklich wünschenswert?
 - Technikfolgenabschätzung: Sind unerwünschte Nebenwirkungen zu erwarten?
 - Technikfolgenbewertung: Überwiegen diese vielleicht die positiven Wirkungen?
 - Prioritäten: Ist das alles überhaupt ein wichtiges Problem?

- Die "Code is law"-These (von Lessig):
 - Software und Standards ermöglichen oder verhindern gewisse Optionen, fast genau wie es Gesetze tun
 - Jedoch werden sie nicht demokratisch erschaffen
 - Die Konsequenzen sind nicht wünschenswert

- „Stille Post“
 - = Vereinfachungen und Verfälschungen von (Text-)Quellen zu einer Sachlage, wobei von einer bestehenden Quelle simplifiziert wird
 - also: Originalquellen lesen! (bzw: Originalquellen angeben)
 - Warum „Stille Post“:
 - Bequemlichkeit
 - Sachverstand fehlt
 - Jeder verfolgt ein eigenes Anliegen (Mikropolitik)
 - Stille Post in der Informatik:
 - (Akzeptable) Abwägungen werden von Außenstehenden (meist nicht-technischen Leuten) oft radikal anders (auch negativ) (um-)interpretiert

- Einige Definitionen zum Thema Risikomanagement:
 - Sicherheit (safety):
 - Zustand des Geschütztseins vor Unfällen
 - Unfall (accident):
 - Unerwünschtes, ungeplantes (aber nicht zwingend ganz unerwartetes) Ereignis, das zu einem Verlust führt
 - Risiko (risk):
 - Eine im Prinzip quantitative Größe. Produkt aus Eintrittswahrscheinlichkeit eines Unfalls und Schadenshöhe
 - Solche Berechnungen sind aber meist sehr dubios
 - Schwächer: Eine Möglichkeit, dass (oder wie) ein System unerwünschtes Verhalten zeigen kann
 - Verletzlichkeit (vulnerability):
 - Eine strukturelle Schwäche eines Systems, die zu unerwünschten Wirkungen (und dann Unfällen) führen kann
 - Bedrohung, Gefahr (threat, hazard):
 - Eine mögliche Einwirkung auf das System, die zusammen mit anderen zu einem Unfall führen kann
 - Versagen (failure):
 - Eine untolerierbare Abweichung eines Systems von seiner Spezifikation
 - Zuverlässigkeit (reliability):
 - Qualitativ: das Funktionieren eines Systems gemäß der Spezifikation unter allen vorgesehenen(!) Bedingungen
 - Quantitativ: Wahrscheinlichkeit des Nichtversagens

- Robustheit (robustness):
 - Fähigkeit eines Systems, auch unter unvorhergesehenen Bedingungen Unfälle auszuschließen
- Fehler (error):
 - Ein Ereignis beim Bau eines Systems, das zu einem Mangel führt oder führen kann
- Mangel, Defect (defect):
 - Eine strukturelle Unzulänglichkeit in einem System, die zu Versagen führt oder führen kann
- Schutz (security):
 - Die Widerstandsfähigkeit eines Systems gegen absichtliche Angriffe. Das System ist sicher (geschützt, secure), wenn die Angriffe ohne Unfall überstanden werden
 - Teilaspekt von Sicherheit
- Schwaches Glied (weak link):
 - Ein Ereignis, das die Funktionsfähigkeit eines Systems beeinträchtigt oder einen Unfall wahrscheinlich macht

- Arten von Risiken (gibt viele Arten, Risiken zu klassifizieren):
 - Nach Art der Abweichung:
 - Ein System zeigt eine erwünschte und erwartete Eigenschaft nicht
 - Ein System zeigt eine unerwünschte Eigenschaft
 - Nach Wahrscheinlichkeit/Häufigkeit des Eintretens:
 - sehr gering, gering, erheblich
 - Nach Höhe des Schadens:
 - vernachlässigbar, gering, erheblich, hoch, untragbar
 - Nach Art der Ursachen:
 - menschliches Versagen, technisches Versagen, beides eine Ursache, mehrere Ursachen
 - u.v.a.m.

- Arten von Schwächen und Bedrohungen (Die wichtigsten Klassen):
 - Software enthält Defekte (auch nach gründlichen Tests)
 - Bsp: Space Shuttle-Simulator, Erdbeben-Simulator (Abschalten von AKWs in USA)
 - Hardware und technische Einrichtungen versagen
 - Bsp: Telefonausfall New York 1991, kosmische Strahlung in RAMs, Geldautomaten-Ausfall 1993 in USA
 - Menschen sind fehlbar
 - insbesondere unter Stress
 - Bsp: frontaler Zugcrash 1993 in Berlin, Beinahe-Katastrofe SpaceShuttle 1986
 - Menschen sind unvorsichtig
 - insbesondere wenn sie sich sicher fühlen
 - Bsp: Titanic 1912, Chernobyl 1986, Osprey-Schwenkflügelflugzeug
 - Menschen sind oftmals ignorant (Wissen fehlt)
 - Bsp: Abkühlautomatismus Stahlwerk, U-Bahn ohne Fahrer, Namensverwechslung
 - Menschen sind manchmal böswillig
 - Kreditkartenbetrug, holländischer Bankangestellter betrügt Bank um 8,4Mio Dollar
 - Auch unwahrscheinliche Ereignisse treten gelegentlich ein
 - auch mehrere zugleich
 - Bsp: Kontoüberziehung Bank Of New York (32Mrd Dollar Schaden), McMuffin
 - Scheinbar unverbundene Ereignisse sind tatsächlich oftmals eng gekoppelt
 - Bsp: ARBAnet-Versagen 1986, Chicago 1990 (Telefonkabel durchtrennt)

- Hierarchische Sicht von Unfällen (Drei Ebenen):
 - Mechanismen (konkreter Hergang beim Unfall, rein deklarativ)
 - Bedingungen (Zustand des Systems bei Beginn des Unfalls, Hergangsverständnis)
 - Urgründe (root causes) (Allg. Bed. im Umfeld des Systems, die zu Bedingungen bei Unfallbeginn führten; Zur Vermeidung ähnlicher Unfälle in der Zukunft)

- Vorgehen zum Bau risikoarmer Systeme:
 - Gefahrenbestimmung
 - Risikoanalyse (lohnt Vorbeugung oder Abwehr finanziell?)
 - Entwurf (Gegenmaßnahmen zu Gefahren erfinden u. Umsetzen)
 - Entwurfssicherheitsprüfung (ggf. Entwurf nachbessern)
 - Bau
 - Abnahmesicherheitsprüfung (sehr konkret; Bau bewirkt Entwurfsänderungen)

- Tips zum Bau risikoarmer Systeme:
 - Sicherheit von vornherein!
 - System als Ganzes betrachten, nicht nur seine Teile
 - Da jedes System anders ist, nicht allein auf Erfahrungen/Standards verlassen
 - Qualitative statt quantitative Methoden verwenden
 - Eingestehen, dass immer Abwägungen und Konflikte auftreten
 - Bereits vorhandene Daten nutzen (historische Daten, Standards, öfftl. Checklisten, ...)
 - Untersuchen der Mensch-Maschine-Schnittstelle
 - jede möglichen Umstand in Betracht ziehen (Umwelteinflüsse, Hardwareversagen, ...)
 - Erweiterbarkeit von vornherein implementieren
 - Sichtbarmachung stillschweigender Annahmen
 - Problem: Sicherheit kostet Geld, Sicherheitsmaßnahmen kaum imponierend

- Beispiel für Sicherheit: Therac-25
 - Reproduktion der Umstände für Auftreten von Fehlern war sehr schwer (wegen Zeitbedingungen)
 - anfangs zu hohes Vertrauen in Sicherheit des Systems
 - voreiliger Glaube, die tatsächliche Ursache eines Unfalls lokalisiert zu haben
 - mangelnde Entschlossenheit bei Verfolgung der Probleme
 - keine Kontrollinstanzen vorhanden (nur ein Softwaretechniker)
 - kein redundantes Sicherheitssystem (Verzicht auf Hardware-Sicherheitsschaltkreise)
 - keine Dokumentation

- deshalb: Ratschläge an Ingenieure:
 - Systemarchitektur muss Sicherheit auch bei Softwarefehlern sicherstellen können
 - Vertraue Software so wenig wie möglich (Redundanz benutzen)
 - „KIS“: Keep It Simple
 - Testen und analysieren der Einzelteile
 - Einbauen von Protokollmechanismen in kritische Systeme
 - Dokumentation von Beginn an!!
 - Vermeiden von (ausschliesslich) quantitativen Risikoanalysen
 - Sicherheit geht vor Bequemlichkeit

- Privatsphäre (privacy):
 - Bereich, in dem eine Person selbst bestimmt (oder bestimmen können sollte), wem sie wann und warum welche Informationen über sich selbst zugänglich macht. (Prechelt)
 - „Goldene Regel“:
 - „Was Du nicht willst was man Dir tu, das füg' auch keinem Andern zu“
 - Privatsphäre im Grundgesetz festgehalten (Artikel: §2,§3,§4,§8,§9,§10,§11,§13,§14,§15)
 - Maßnahmen zum Schutz der Privatsphäre:
 - Physische Blockaden, Höflichkeitsregeln, Anonymität, Geheimhaltungsgebote, Informationelle Selbstbestimmung
 - Computerisierung bedroht Privatsphäre

- Schutz elektronischer Kommunikation (2 Bereiche):
 - Inhaltsdaten (kann man verschlüsseln)
 - Verkehrsdaten (Verbergung/Anonymisierung möglich)

- warnendes Beispiel zum (Nicht-)Datenschutz: Social Security Number (in USA)
 - SSN verfügt nicht über: Eindeutigkeit, Universalität, Identifikation
 - über SSN kann jeder sehr viele Daten über beliebige Person sammeln
 - dadurch hoher Mißbrauch der SSN

- Bundesdatenschutzgesetz (BDSG):
 - erstellt 1977, sinnvoll ab 1991 (Personen werden geschützt), geändert 14.1.2003
 - zum Inhalt siehe: www.datenschutz-berlin.de/recht/de/bdsg/bdsg03.htm
 - BDSG beschreibt, in welchen Fällen personenbezogene Daten erhoben, gespeichert und genutzt werden dürfen
 - Grundidee: Datensparsamkeit und informationelle Selbstbestimmung
 - die meisten Regeln sehr restriktiv, jedoch viele Ausnahmen/Abwägungsklauseln)
 - Beste Grundlage für legale Nutzung von Daten ist ausdrückliche Einwilligung unter Nennung des Zwecks an den Betroffenen

- Elektronisches Bezahlen:
 - Geld ist genormte, zertifizierte, meist gesetzlich festgeschriebene Standardtauschware (ein Konstrukt ohne Eigenwert welches Grundlage unserer Wirtschaftsweise ist)
 - Geld-Leistungsversprechen ist Scheck, Girokonto, Kreditkarte, Folge von Bits
 - Geld ist universelles Maß zur Beschreibung eines (abstrakten) Werts von Waren oder Dienstleistungen
 - Buchgeld: Guthaben bei einer Bank, welches kein phys. Gegenstück in Materialien hat
 - gar kein Geld: Wertpapiere
 - Geld ist: liquide, garantiert, anonym, inhaberbezogen (Tipp: „Gutgläubiger Erwerb“)
 - Elektronisches Geld (eGeld, eCash):
 - Datenpakete mit diskretem, weithin akzeptierten Wert
 - Problem: Fälschung (Entgegenwirken mit: Spezialhardware, Duplikation checken)
 - Anonymität möglich mit „Verdeckter digitaler Unterschrift“ (Chaum 1982)

- Elektronisches Bezahlsystem (eBS):
 - definiertes Verfahren (Protokoll), mit dem die Übertragung von Geld zwischen Personen arrangiert werden kann
 - Die meisten eBS kein eGeld in diesem Sinne (weil z.B. nicht anonym)
 - Bsp: Firstgate click&buy, PayPal (von ebay; Datenschutz kritisch), GeldKarte
 - diese sind kein eGeld, sondern Kreditsysteme, Geld mit Schattenkonten

- Trend (Zwei Tendenzen; im Jahre 2004):
 - Zahlungen über Mittler (Firstgate, PayPal)
 - Zahlung mit Mobiltelefon (Paybox)
 - Anonymität in vieler Hinsicht nicht gegeben
 - scheint aber kaum Jemanden zu stören...

- Entscheidungsprozesse:
 - Macht:
 - „Macht bedeutet jede Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht“ (Max Weber)
 - Ortman & Co.: „Macht ist Kontrolle relevanter Unsicherheitszonen in:“
 - Wahrnehmung und Formgebung
 - Kommunikation
 - Regeln und Sanktionen
 - Autorität und administrativem Handeln
 - Geld und wirtschaftlichem Handeln
 - Infrastruktur und Technik

 - Unternehmen:
 - konventionell aus BWL: Organisation kooperierender Personen, die alle einzig auf ökonomische Effizienz u. Unternehmenserfolg gerichtet agieren, d.h. rational handeln
 - mikropolitisch:
 - nach Burns: Unternehmen ist kooperatives System, das sich aus den benutzbaren Eigenschaften von Menschen zusammen setzt; bzw. ein soziales System, in dem Menschen um ihr Vorankommen wetteifern u. dabei Gebrauch von Anderen machen
 - nach Crozier: Organisation ist Gesamtheit miteinander verzahnter u. relativ autonom konstruierter „Spiele“, wobei die Regeln dieser „Spiele“ indirekt die Integration der Machtstrategien der Organisationsmitglieder bewirken

 - „Spiel“:
 - ist beschrieben durch Agieren einer Person u. seine Interaktion mit Anderen, wobei die Person die verwendeten Regeln in Grenzen selbst festsetzt, wobei das Spiel jedoch vielfältigen Einflüssen („Zwängen“) unterliegt
 - Mitspielen-Dürfen setzt tendenziell Erwarten-Erfüllen voraus
 - Regeln ändern sich kontinuierlich und sind meist implizit
 - Routinespiel (Mitarbeiter) vs. Innovationsspiel (Management)

 - Mikropolitik (nach Burns, 1995):
 - „... the exploitation of resources, both physical and human for the achievement of more control over others, and thus of safer, or more comfortable, or more satisfying terms of individual existence.“

 - These von Neuberger:
 - „Mikropolitik ist kein bedauerlicher und vermeidbarer Betriebsunfall oder ein unerklärliches Krebsgeschwür im ansonsten gesunden Organismus des Unternehmens, sondern ein unausweichlicher Bestandteil organisierten, sozialen Handelns.“

- Vier Annahmen Bosetzky's (1988):
 - Da in jeder Organisation nur ein Teil der theoretisch möglichen Machtmenge an Personen und Positionen gebunden ist, wird um den Rest gekämpft
 - Jede Organisation wird durch ihr gesellschaftliches Umfeld eingebunden, so dass sie ausserorganisatorischen Machtpotentialen (z.B. geliehene Autoritäten) unterworfen ist
 - In jeder Organisation gibt es Solche, die nach Macht und Einfluss streben, und Solche die kein Interesse daran haben
 - Erhöhung des Machtpotentials des Einzelnen ist meist nur dadurch möglich, dass er Koalitionen bildet oder sich ihnen anschliesst und sich mikropolitisch verhält

- Fallstudie: Versicherungsfirma, welche Gehaltsabrechnungssoftware kauft
 - Am Anfang von Entscheidungsprozessen steht die Wahrnehmung eines Problems
 - Entscheidungsprozesse sind kontingent (d.h. sie könnten auch anders ausgehen)
 - viele Entscheidungen werden implizit getroffen u. zentrale Alternativen gar nicht erst diskutiert
 - wichtige Entscheidungen werden getroffen, obwohl Konsequenzen kaum erforscht
 - Verhalten entsteht aus einem Gemisch von gemeinsamen u. persönlichen Interessen
 - Interaktion solcher Verhalten führt zu „Entscheidungskorridoren“
 - wichtig für Softwareentwickler:
 - EDV- und Fachabteilung leben in verschiedenen Vorstellungswelten
 - Gestaltung einer Softwarelösung bewirkt meist weit reichende Entscheidungen
 - Betriebliche Software ist ein Machtfaktor

- Beispiel für integrierte unternehmensweite Software-Systeme: mySAP ERP

- Gesunde/Kranke Unternehmen:
 - bei gesunden Unternehmen sind Machtspiele erheblich schwächer ausgeprägt
 - kranke Unternehmen sind von außen schwer zu erkennen
 - Ratschläge (in einem gesunden Unternehmen):
 - selbst stets konstruktiv verhalten
 - Egoismen O.k., wenn sie Unternehmen nicht schaden
 - Eigenes Wohlverhalten sichtbar machen („Klappern“)
 - Fremdes Fehlverhalten monieren („Stimme der Vernunft“ sein)

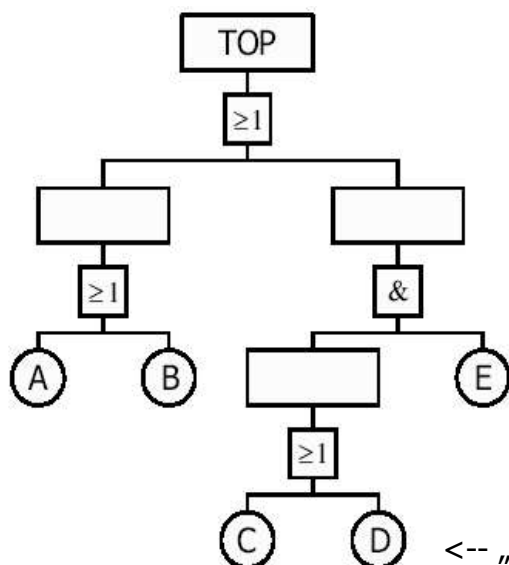
- Möglichkeiten zur Reformation eines Systems (nach dem Selbstgestaltungsgrad sortiert):
 - Organisationsentwicklung:
 - Erfolgreiche Steuerung und Gestaltung von inneren Veränderungsprozessen
 - kulturelle Identität bleibt erhalten
 - Gruppen, Personen, Akteure werden in Entwicklung/Umsetzung von Lösungsprozessen (Veränderungen) einbezogen
 - Veränderungsmaßnahmen laufen kontinuierlich, prozesshaft u. evolutionär ab
 - Veränderung durch interne Reflexion
 - sozial aufwendig
 - langwierig
 - Transformations Management:
 - aktive Verknüpfung von inneren u. äusseren Transformationsideen
 - punktuelle/differenzierbare Einbindung der Betroffenen, aber auch Umsetzung gegen Betroffene
 - Change Management:
 - Ideen, Steuerung u. Gestaltung kommt von ausserhalb des Systems

- kaum Einbeziehung der Betroffenen
 - sehr dynamisch, sprunghaft
 - Veränderungsprozess wird beschleunigt
 - Widerstände in Implementierungsphase wahrscheinlich
- Benutzbarkeit (von z.B. User Interfaces von Software):
 - Benutzbarkeit bedeutet, dass eine Software ihre Benutzer gut dabei unterstützt, die gewünschten Arbeitsgänge zu erledigen
 - Verständlichkeit
 - Erlernbarkeit
 - Bedienbarkeit
 - Benutzbarkeit ist ein Teilaspekt von Brauchbarkeit (i.e. sind überhaupt die richtigen Anforderungen realisiert?)
 - Vier Entwicklungsprinzipien für gute Benutzbarkeit (von Gould und Lewis):
 - Direkter Kontakt zu Benutzern
 - mittels Interviews, Beobachtung, Umfragen, Zusammenarbeit mit (End-)Benutzer
 - Frühes und fortlaufendes Benutzbarkeitstesten
 - Erforschung und Verwirklichung des Feedback von echten Benutzern
 - Iterativer Entwurf
 - mehrere Zyklen von Entwicklung, Benutzbarkeitstest, Bewertung, Entwurfsänderung; Vorsicht: Korrekturen rufen meist neue Probleme hervor!
 - Integrierter Entwurf
 - Benutzbarkeits-Aspekte laufen zeitlich und inhaltlich parallel („in einer Hand“) ab
 - Parallelentwicklung von Benutzerschnittstelle, Lehreinheiten, Hilfe/Dokumentation
 - Fallstudie: Große Softwarefirma welches CAD-Programm entwickelt
 - hatten Probleme -> „Superentwerfer“ löste diese in einem Jahr u. verschwand dann
 - danach: Marketing/Vertrieb/Entwicklung arbeiten unabgestimmt an einander vorbei
 - die Vier Entwicklungsprinzipien wurden verletzt, da u.a. HW,SW,Doku,Training getrennt
 - Ratschläge an Softwareorganisationen:
 - Trage Mitarbeitern möglichst nur Dinge auf, die sie gut können
 - Sorge für kurze Kommunikationspfade
 - Sorge für zentrale Entscheidungsinstanz
 - Hindere Mitarbeiter nicht daran, genau das zu tun was nötig ist
 - Ergebnisse von Benutzbarkeitsprüfungen (und deren häufigste Fallen)
 - Defekte (Funktion tut nicht was sie soll)
 - Funktionslücken (benötigte Funktionalität nicht vorhanden)
 - Verständnisprobleme (Lernprobleme für Benutzer, Darstellung uneindeutig)
 - Bedienschwierigkeiten (umständliche Benutzung, Bedienweise provoziert Fehler)
 - Diese Fehler-Zuordnungen können mehrdeutig sein!
 - Email
 - simplex: Kommunikation nur in eine Richtung
 - halbduplex: Kommunikation (nur abwechselnd) in beide Richtungen
 - (voll)duplex: Kommunikation in beide Richtungen zugleich
 - email ist asynchron, halbduplex, kurze Latenzzeit, dauerhaft(?), reproduzierbar, weiterleitbar, duplizierbar, beliebig viele Teilnehmer, automatisch durchsuchbar, z.T. Unpersönliche Adressaten (z.B. in Mailinglisten)

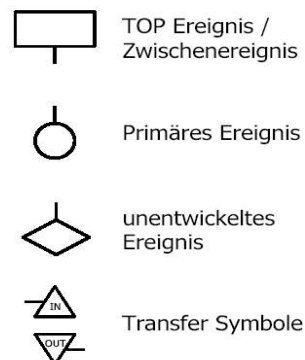
- Email hat positive (meist technisch-organisatorischer Art) und negative Wirkungen (meist sozialer Art)
- negative Wirkungen sind emergente (d.h. plötzlich auftauchende) Eigenschaften
 - entstehen aus Kombination von inhärenten Eigenschaften (Technik) und Mikropolitik von beteiligten Personen (Ziele, Persönlichkeitseigenschaften)
 - Bsp: Informationsüberflutung, Verrohung der Umgangsformen, Schludrigkeit bei Informationsangaben führt zu unnötigen „Diskussionen“ per email, Vermeiden von persönlichen Kontakten, Dokumentationswahn
- Tips für Benutzung von Email:
 - gut geeignet, wenn Präzision verlangt ist, viele Beteiligte eingebunden sind, Distanz/Zeit überbrückt werden muss, dokumentiert werden muss
 - schlecht geeignet, wenn Interaktion (Diskussion) nötig, Emotionen transportiert werden müssen, es gilt Beziehungen herzustellen/zu pflegen, Präzision/Schriftlichkeit unerwünscht sind
- „Netiquette“ für Email: <http://www.netplanet.org/netiquette/email.shtml>

Anhang: Fehlerbaumanalyse (fault tree analysis; FTA)

- FTA wird angewandt, wenn:
 - (Auswirkungen von Komponentenversagen bekannt) AND (Gefahrenursache unbekannt)
 - dient der Ursachenermittlung von Systemversagen
 - ist eine deduktive (ableitende) Top-Down-Methode
 - Vorgehensweise:
 - Ereignis (TOP-Ereignis), was nicht eintreten soll, wird vorgegeben
 - in einer Baumstruktur wird beschrieben, welche untergeordneten Ereignisse wie eintreten müssen, damit das jeweilige übergeordnete Ereignis eintritt.
 - Das zuunterst liegende Ereignis eines Astes wird Primäreignis genannt
 - dann folgt eine qualitative/quantitative Analyse mit anschließender Dokumentation
- Fehlerbaum entspricht einer logischen Gleichung -> ermöglicht Bestimmung von:



- Minimal Cut Sets (MCS): $\{\{A\}, \{B\}, \{C, E\}, \{D, E\}\}$
- Single Point Failures (SPF): $\{\{A\}, \{B\}\}$
- Common Mode Failure: Ursache, welche gesamtes System betrifft (z.B. Erdbeben)



<-- „D“ ist Primäreignis (Basiseignis)