

# Hält Doppelt besser?

Redundanzkonzepte und einige Fehler in der Anwendung

„Uns kann nichts passieren, weil alle Systemkomponenten doppelt/mehrfach ausgelegt sind...“

## Kann die augenscheinliche Sicherheit trügen?



Wilhelm Uhlenberg  
wu@sv-uhlenberg.de

Vortrag zum Frankfurter Treffen von DECUS 22.9.2006

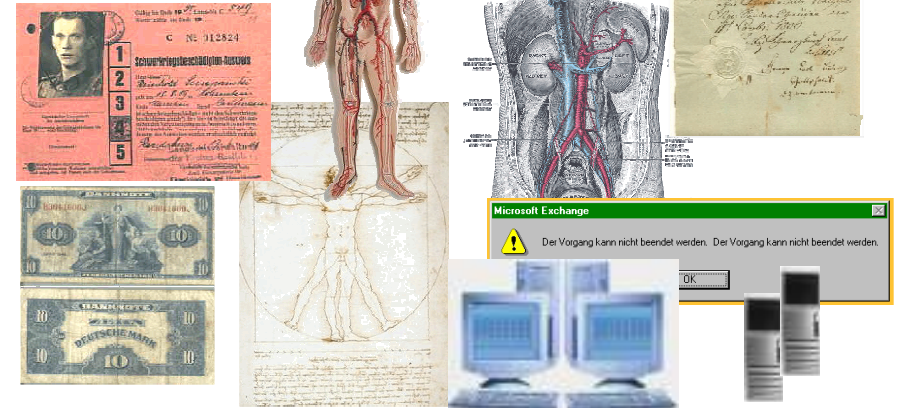
- DECUS Frankfurter Treffen 22.9.2006 -

<http://www.sv-uhlenberg.de/>

1

# Wie sieht Redundanz aus?

## Verschiedene Zielrichtungen..

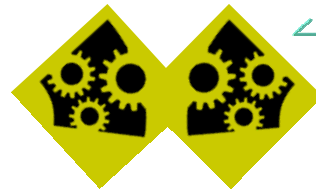


<http://www.sv-uhlenberg.de/>

- DECUS Frankfurter Treffen 22.9.2006 -

2

# Missverständnisse?



## Redundanz – was ist das?

- Vom Wortstamm: „im Überfluss vorhanden sein“  
(Quelle: Wiki <http://de.wikipedia.org/wiki/Redundanz>)

- Vom Verständnis: mehr Mittel benutzen, einsetzen als die  
Nach DIN 40041, Teil 4 (Verfügbarkeit, Zuverlässigkeit): „Vorhandensein von mehr als für die Ausführung der vorgesehenen Aufgaben an sich notwendigen Mittel.“

- Biologische Redundanzen
  - ◆ Augen, Ohren, Nieren, Lungen, Arme, Beine
  - ◆ Aber komplexe Systeme: Gehirnhälften? Herzkammern?
- Die Ambivalenz der Redundanz
  - Segen, Reichtum, Förderer ODER
  - Last, Ballast, Inkonsistenz, Hindernis.
  - Zielrichtungen, warum Redundanzen sinnvoll sind

<http://www.sv-uhlenberg.de/>

- DECUS Frankfurter Treffen 22.9.2006 -

3

# Zielrichtungen

## Was soll erreicht werden

- Ausfallsicherheit
- Verfälschungssicherheit
- Reaktionssicherheit
- Funktionssicherheit
- Versorgungssicherheit
- Zustandssicherheit
- Erhöhung der Verständlichkeit
- ...



<http://www.sv-uhlenberg.de/>

- DECUS Frankfurter Treffen 22.9.2006 -

4



## Technische Redundanz

- Geliebt als Gangreserve
- Gehasst als Datenzergliederung (Mehrdeutig)
- Geliebt als Sicherungsprinzip
- Gehasst als Kostenfaktor
  
- Segen und Fluch je nach Nutzungskontext
  - Ambivalenz als Risikofalle

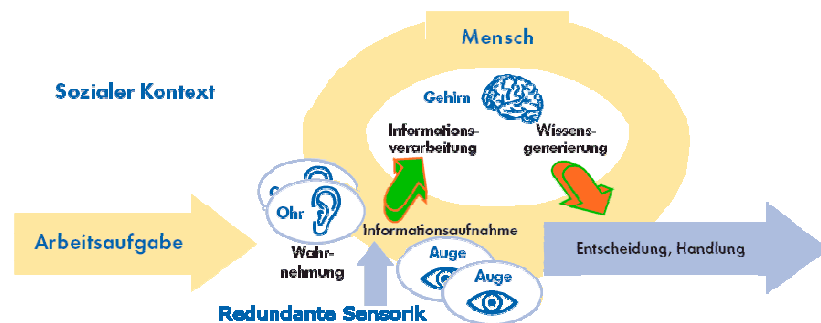


## Copyright(obligation) Natur?

- Evolutionsgesteuerte Organismen bilden
  - Echte statische Redundanzen
  - Nie etwas wie „Standby“.
  - Performante Gemeinschaften
    - ◆ Mit zwei Beinen läuft man stabiler und schneller...
- Sollte dies als Vorlage dienen?
  - Oft zu teuer und zu komplex, aber bewährt und gut!
- Ein wesentlicher Unterschied zwischen Menschen und Computern (auch Maschinen) ist immer noch die stark differierende Fähigkeit Redundanzen zu erwarten und verarbeiten zu können.



## Bio-Redundanz, wo?



## Selbstversuch

- Können Sie das noch verstehen?

### „Die Bedroung

Wie weit kann das geen? Wann werden die Aussetzer bedrolic? Wann greift der Scleandrian auf wirklich lebenswichtige Funktionen unserer Gesellschaft über? Ab welchem Punkt sind die Sicereitssysteme betroffen? Das Scilmme daran ist die Gewönung. Kaum at man sic abgefunden mit den systematic auftretenden Felern, da taucen mitten im Saz vielleic schon neue auf. Wo vorer noc was war, da is plözlic gar nics mer.“

...  
(Auszug auf einer Glosse in PC-Professional 9/2000)

## Redundanz, wofür?



- **Strukturelle Redundanz**
  - Erweiterung des Systems um zusätzliche Objekte.  
z.B. gleichartige Rechner, Baugruppen, Speicherkomponenten, Sensoren, Bussysteme...
- **Funktionelle Redundanz**
  - Erweiterung des Systems um zusätzliche (sichernde, rettende) Funktionen
- **Informationsredundanz**
  - z.B. durch zusätzliche Bitpositionen wie Prüfbits, Polynombildung, CRC usw.
- **Zeitredundanz**
  - z.B. Wiederholungen fehlgeschlagener Operationen

## Erkenntnisse



- **Erste Grunderkenntnis:**
  - Von einem Betriebsmittel, Information ist mehr vorhanden als reduziert auf die Kernaufgabe tatsächlich benötigt wird.
- **Mehr**, ist immer aufwendiger zu verstehen, zu verwalten, zu installieren, pflegen, warten, bezahlen.....
- **Technische (strukturelle) Redundanzen haben mindestens 3 Ausprägungen**
  - Statische Redundanz
  - Dynamische Redundanz
  - Mischformen (Hybride)

## Kleine Anatomiekunde (1)



- **Statische Redundanz**
  - Kommt biologischen Systemen nahe
  - Immer sind alle Komponenten aller Instanzen zeitgleich aktiv und synchron und gleichberechtigt an der Funktionserfüllung beteiligt.
  - Fehlertolerierende oder –maskierende Strukturen
  - Mitlaufende Reserve („hot standby“)
    - ◆ Gefahr der trügerischen Sicherheit wenn identisch
- **Vorteil: Sofortige (unterbrechungsfreie) Funktionsübernahme bei Ausfall.**
- **Nachteil: Kosten und tatsächliche Synchronität der Teilsysteme**

## Kleine Anatomiekunde (2)



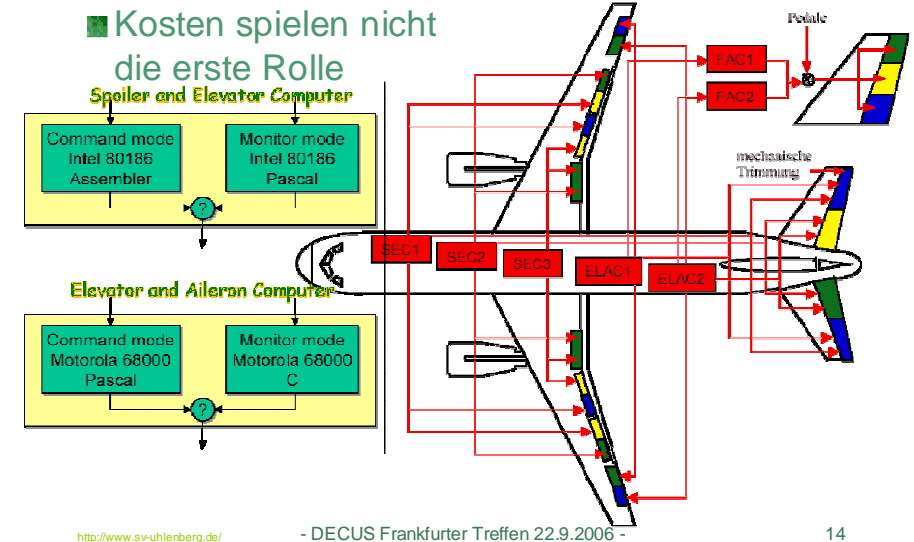
- **Dynamische Redundanz**
  - Zuschalten von Reserveeinheiten bei Erkennen eines Ausfalls
  - Übernahme der Funktionserfüllung nach einer tolerablen Totzeit.
  - Fehlertolerierende oder –maskierende Strukturen
  - Beigestellte Reserve („cold“ standby)
    - ◆ Gefahr: Standby-System weicht vom Ausfallsystem ab (Historie, Daten) und trügerische Sicherheit wenn identisch.
- **Vorteil: kostengünstig realisierbar. Kein Verschleiß während echter Passivzeiten.**
- **Nachteil: Gesamtleistung ist im Fehlerfall meist beeinträchtigt. Totzeit oft nicht deterministisch. Trägheit. Kapitalbindung ohne permanenten Bedarf.**

## Kleine Anatomiekunde (3)



- Anwendungsspezifische Ausprägungen der Redundanz
  - Ungenutzte Redundanz (Doppel steht passiv in der Ecke)
  - Fremdgenutzte Redundanz (Hintergrundaufgaben im Passivbetrieb)
  - Gegenseitig nutzbare Redundanz (funktionstüchtige Subsysteme übernehmen gegenseitige Aufgaben der defekten)
  - Aktive-Redundanz (funktionsbeteiligte, heiße Redundanz)
  - Standby-Redundanz (passive Redundanz)
- Funktions-, Algorithmus-, Software- und Hardware-Diversität bei den Redundanzkomponenten erreicht größte mögliche Sicherheit und maximale Kosten.

## Wenn Sicherheit regiert: „A320“



## Verwirrung total?



- Was ist los, wenn bei Zweien jeder was anderes behauptet? (Glaubenskrieg)
- Dann doch lieber Demokratie (Wahlausschuss)
- Eine Erkenntnis war bisher oft, dass man am besten aus Fehlern lernen kann - also
- Gab es Fehler aus denen man lernen kann?
  - GE XA/21 Energy Management&Control System
  - Ariane 5 Jungfernflug
  - Bell V-22 Osprey Schwenkflügel-flugzeug



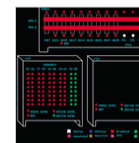
## Gelebte Praxis (1)



- Sind Automaten/Konzepte den Situationen angepasst?

- General Electric XA/21 Leitsystem/Netzführung zur Lastverteilung in elektrischen Netzen.

XA/21™ System

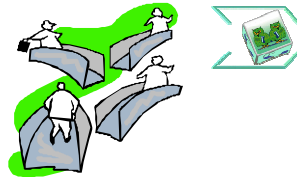


- ◆ Redundanz wird von den Anwendern als äußerst wichtig für die Versorgungssicherheit angesehen.
- ◆ Nur redundante Konfigurationen hatten bis Anfang 2004 einen Software-Fehler mit Auswirkungen.

- (race condition bei einer globalen Datenstruktur, wenn Alarmmeldungen einer bestimmten Häufigkeit und Reihenfolge eintreffen und synchronisiert wurden).

- Redundanzauswirkung: 14.8.2003 16:10 bis 15.8.2003 21:03 Dunkelheit an der Nordostküste USA (60 Mio. Einw.).

## Gelebte Praxis (2)



### ■ Doppelte Komponenten == Ausfallsicherheit?

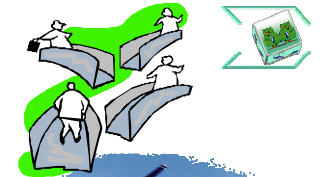
- Ariane Jungfernflug 4.6.1996.
  - ◆ Redundanz ist als systemimmanentes Konzept Standard.
  - ◆ 37 Sekunden Steigflug bis Probleme zu Fehlsteuerungen der Boosterdüsen führten.



(Messwert der horizontal Beschleunigung war außerhalb des erwarteten Bereiches im SRI. Überlauf-Verarbeitung führte zu einer nicht abgefangenen Exception im Primärsystem und anschließend gleichermaßen im identischen Redundanzpartner. Grund: Software aus Ariane 4 übernommen (ungeprüft?). Funktion war zum Zeitpunkt des Steigfluges NICHT mehr erforderlich!).

- Redundanzauswirkung: Schaden > 5 Mrd. US\$ (4 Satelliten der Traglast gehen verloren, Programmstopp A501, Rufverlust, Zeitverzug).

## Gelebte Praxis (3)



### ■ Wenn Doppelt nicht immer reicht, dann doch lieber dreifach!

### ■ Bell-Boeing V-22 Osprey Schwenkflügelzeug (5 Prototypen in 1991)



- Eine 3fach-Redundanz wird an den Gyro (Raten) Sensoren bewusst eingesetzt, um Richtung und Beschleunigung sicher zu erfassen.



- ◆ Fertigungsfehler: 2 der 3 Sensoren waren falsch herum (verpolt) verdrahtet worden.

- Die zwei fehlerhaften Sensorwerte überstimmten den richtigen und der Absturz aufgrund von instabiler Fluglage war die Folge.

- Redundanzauswirkung: Geheim, da Militärprogramm

## Was zeigt die Praxis?



### ■ Die selektive Wahrheit ... (haben wir was gelernt?)

- Alte Gefahrenquellen: Menschen machen Fehler, besonders unter Stress
- Neue Gefahrenquellen durch Komplexität
  - ◆ Verführung des Probierens; nicht alle Permutationen des Gesamtsystems bedacht
  - ◆ Langzeiteffekte oft nicht erkannt oder vernachlässigt
- Empfindlichkeit komplexer elektronischer Systeme gegenüber Umfeld und untereinander steigt aufgrund ihrer Anzahl
- Menschliche Redundanzen untergraben die maschinelle Konsistenz
- Risikofallen
  - ◆ Maßnahmen zur Risikominderung steigern oft Komplexität



## Risikofallen – ein Grund?



- Wissensdefizite
- Denkgewohnheiten
- Motivationslagen
- Prozesse der Gruppendynamik, Soziale Fallen
- Kognitive Fallen
  - Gefahr der Checklisten
  - Generalisieren von Regeln („Doppelt hält besser“)



Ingenieursglaube an die prinzipielle Beherrschbarkeit von Technik führt zu ihrer Unbeherrschbarkeit. Paradox.

## Gründe



- Bei vielschichtigen Problemen ist oft das abbildende Modell bereits zu einfach.
  - Tendenz zur Beherrschbarkeit führt zu Verkürzungen
- Bei komplexen Zusammenhängen werden die „einfachen“ Grundregeln als trivial angesehen und vernachlässigt (als gegeben vorausgesetzt).
  - Verliebtheit und Konzentration auf nur das was Spaß macht (fordert)
- Konzepte werden durch Kosten nachträglich diktiert (revidiert), wenn sie aus dem Ruder laufen.
  - Schnelle Vereinfachungen, Abkürzungen aufgrund von Kostendruck.
- Eitelkeiten
  - Menschliche Schwingungen sorgen für unbewusste Inkonsistenzen

## Anregungen



- **Kernfrage:** Ist ein Ausfall wirtschaftlich und sicherheitstechnisch über eine definierte Zeitspanne tragbar (zu verantworten)?
- Alternative „**Nein**“: Statische Redundanz mit diversitären Software- und Hardware-Komponenten implementieren. Folge: Kosten anfangs ebenfalls erheblich!
- Alternative „**Ja**“:
  - Zeitspanne der Reaktionsmöglichkeit bestimmt das Standby-Konzept.
    - ♦ Skala: Beschaffung ausgefallener Komponenten über Neubestellung erlaubt oder unterhalb der menschlichen Informationsverarbeitungszeit (<10 Sekunden).
- Alternative „**Vielleicht**“: Nachdenken und Rat einholen.
- Alternative „**Manchmal**“: Wahrscheinlichkeiten bewerten.
- Alternative „**Ich weiß nicht so recht**“: Ich auch nicht!

# Fazit

## Redundanzen geben und nehmen zunächst mehr als man unter normalen Umständen braucht.

Ein Nutzeffekt im Ernstfall kann sich ins Gegenteil verkehren, wenn die eingebaute steigende Komplexität zu zusätzlichen Gefährdungsquellen führt, die wiederum nur mit steigender Komplexität beherrschbar wären.

Vortragsauszug

<http://www.sv-uhlenberg.de/index-Dateien/downloads.htm>

## Danke für die Zeit

## Referenzen / Quellen

- Prof. Dr.Ing. Dr.med. Volkmar Miszlok  
[http://www.miszlok.de/Lectures/L01\\_Redundancy/Redundancy\\_deutsch.htm](http://www.miszlok.de/Lectures/L01_Redundancy/Redundancy_deutsch.htm)
- Wikipedia <http://de.wikipedia.org/wiki/Redundanz>
- K. Beck, Test-Driven Development by Example, Addison-Wesley, 2003
- Herbert Klaeren, Die artifiziellen Paradiese der Informatik
- Klaus Eppel: Erhöhung der Zuverlässigkeit von Rechnersystemen (Datacom 09/91)  
<http://www.improve-mtc.de/Veroffentlichungen/Zuverlässigkeit1/zuverlässigkeit1.html>
- Gunhild Lütge: Amoklauf der Maschinen. Die Zeit. 2. April 1993, S. 23–24, Prof. Dr. Klaus Pommerening, Johannes-Gutenberg-Universität Mainz, IT-Sicherheit in der Medizin,  
<http://www.uni-mainz.de/~pommeren/Artikel/stmed.pdf>, 22.06.2003
- Dirk Spöri, Uni Freiburg, Informatik Fachbereich, Vortrag aus 2002 „Pleiten, Pech und Pannen der Informatik“
- EN ISO 13849-2:2003, *Sicherheit von Maschinen . Sicherheitsbezogene Teile von Steuerungen Teil 2: Validierung (ISO 13849-2:2003)*.
- "eigensichere" elektrische Ausrüstungen (siehe EN 50020);
- Ergonomische Anforderungen and Maschinenschnittstellen, siehe EN 614-1, ISO 6385, EN 13861 und IEC 61310-1.
- Konstruktion elektrischer Ausrüstungen von Maschinen siehe IEC 60204-1:1997
- IEC 60050-191:1990, *International electrotechnical vocabulary . Chapter 101: Dependability and quality of complex systems*



# Referenzen / Quellen

- Informatik Informatik im Cockpit: Pilot contra Computer  
<http://kbs.cs.tu-berlin.de/publications/presentations/He260399.pdf>
- DIN 40041-4, Zuverlässigkeit, Verfügbarkeit, Fehlertoleranz
- S. Montenegro: Prinzipien der Fehlertoleranz; S. Montenegro: Fehlertoleranz und Industrie Computer beide über  
<http://www.first.gmd.de>
- BG-Information „Einrichten von Software – Leitfaden und Check für Benutzer“ (SP 2.11/3) (BGI 852-3)
- Praktische Beispiele fehlertoleranter Systeme  
<http://www.morawek.at/roman/papers/fehlertoleranz/>
- Forum On Risks To The Public In Computers And Related Systems  
<http://catless.ncl.ac.uk/Risks>
- Aufbau des Osprey Helikopters <http://www.ausairpower.net/TE-V-22A-Osprey.html>