Proseminar
Berüchtigte Fehler in Softwaresystemen
Vorbesprechung

Joost-Pieter Katoen & Thomas Noll

Software Modeling and Verification Group

14. Oktober 2008

Seminarthema

Thema des Proseminars

Analyse gravierender Fehler in (Hard- und) Softwaresystemen

- Was ist passiert? Beschreibung
  - des Systems
  - des aufgetretenen Fehlers,
  - der unmittelbaren Folgen
  - des Gesamtschadens
  - der organisatorischen/technischen Konsequenzen
- Was waren die Ursachen?
  - technische Fehler
  - Versagen von Test/Validierung
  - Planungs-/Managementfehler
  - ...
- Mit welchen Maßnahmen hätte der Fehler verhindert werden können?

Zielsetzung

Ziele des Proseminars

- Selbständiges Einarbeiten in ein neues Thema
- Literaturrecherche
- Darstellen des Inhalts in einer wissenschaftlichen Ausarbeitung
- Verständliches Präsentieren

Anforderungen Ausarbeitung

Ausarbeitung

- selbständiges Verfassen einer ca. 15-seitigen Ausarbeitung
- vollständiges Literaturverzeichnis
- korrektes Zitieren
- Plagiarismus:
  Die nicht gekennzeichnete Übernahme fremder Inhalte führt zum sofortigen Ausschluss.
- Schriftgröße 11pt, übliche Seitenränder
- Sprache Deutsch oder Englisch
- Korrekte Sprache wird vorausgesetzt:
  $\geq$ 10 Fehler pro Seite $\Longrightarrow$ Abbruch der Korrektur

Anforderungen Vortrag

Vortrag

- 30-minütiger Vortrag
- Zielgruppengerechte Präsentation der Inhalte
- übersichtliche Folien:
  - $\leq$ 15 Textzeilen
  - sinnvoller Einsatz von Farben
- Vortrag in Deutsch oder Englisch

Bibliothekseinführung

Einführung in die Literaturrecherche

- Einweisung in themenspezifische Literaturrecherche
- Dauer: ca. zwei Stunde
- Teilnahme für BSc-Studierende verpflichtend
- Terminabsprache: `biblio@cs.rwth-aachen.de`, Tel. 80-21025

Deadline

Deadlines

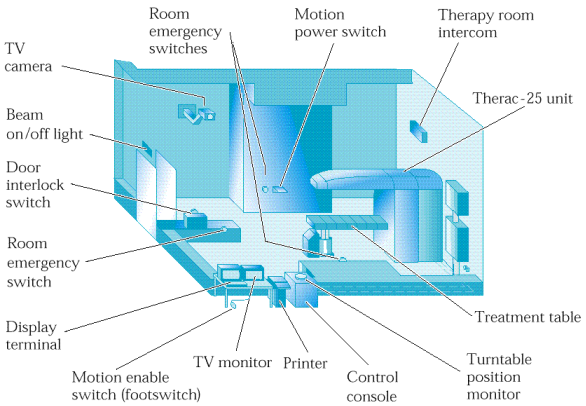
Folgende Termine sind einzuhalten:

- 17. November: Gliederung vorlegen
- 1. Dezember: erste Fassung der Ausarbeitung
- 19. Dezember: endgültige Fassung der Ausarbeitung
- 5. Januar: endgültige Fassung der Folien
- 15./16. Januar: Blockseminar

Destruction of Mariner 1 Spacecraft (1962)

- Venus-Raumsonde der NASA, gestartet Juli 1962
- Unerwartetes Manöver 5 min nach Start $\Rightarrow$ Selbstzerstörung
- Ursache: Codierungsfehler (Übertragung einer mathematischen Formel in Programmtext)

Therac-25 Radiation Overdosing (1985-87)



- Gerät zur Behandlung mit Röntgenstrahlen
- Zwischen 1985 und 1987 mindestens sechs Fälle von Überdosierung (ca. 100-fache Dosis)
- Drei Todesopfer
- Ursache: Entwurfsfehler in Steuerungssoftware (*race condition*)

AT&T Telephone Network Outage (1990)

- Januar 1990: Störung in New York City bewirkt 9 h-Ausfall von großen Teilen des US-Telefonnetzes
- Schaden von mehreren 100 Mio US$
- Ursache: Programmierfehler (falsche Interpretation von `break` in C)

Patriot-Scud Tracking Error (1991)

- Februar 1991 während Zweitem Golfkrieg (*Operation Desert Storm*)
- Patriot-Abwehrrakete fängt angreifende Scud-Rakete nicht ab
- 28 Todesopfer
- Ursache: ungenaue Kursberechnung mit Anhäufung von Rundungsfehlern

Sinking of Sleipner A Offshore Platform (1991)

- Versank im August 1991 während vor Stavanger (Norwegen)
- Entstehung eines Lecks in einem Ballasttank
- Ursache: Kombination von
  - Planungsfehler (zu ungenaue Approximation in Finite-Elemente-Analyse)
  - Konstruktionsfehler (Verankerung der Verstärkung in einem kritischen Bereich)

Pentium Division Bug

- Genauigkeitsverlust bei Fließkomma-Divisionen mit bestimmten Operanden
- Auswirkungen auf Normalanwender umstritten
  (Auftreten im Mittel ca. einmal je neun Milliarden FDIV-Operationen)
- Geschätzter Schaden: 400 Mio US$
- Ursache: Umsetzung eines Softwarebugs (Divisionsalgorithmus) in Hardware

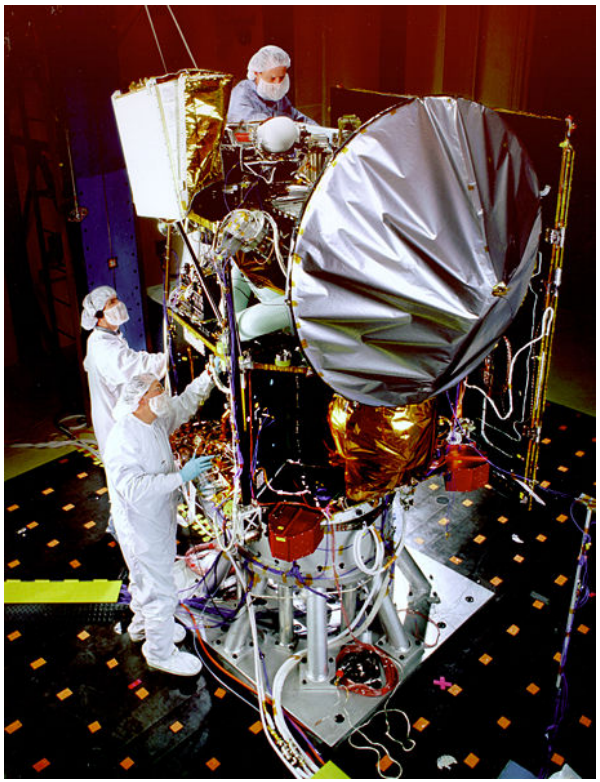
Chinook Helicopter Disaster (1994)

- Hubschrauberabsturz am *Mull of Kintyre* (Schottland) im Juni 1994
- 29 Todesopfer
- Ursache nicht vollständig geklärt
  - Nachlässigkeit der Piloten
  - Fehler im *Full Authority Digital Engine Control (FADEC)*-System

Ariane 5 Crash (1996)

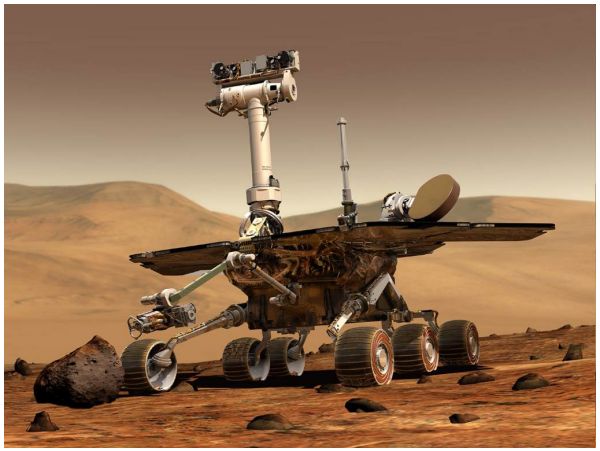
- Absturz der europäischen Ariane 5-Rakete beim Jungfernflug im Juni 1996
- Schaden: mehr als 500 Mio US$
- Ursache: Spezifikations- und Entwurfsfehler in der Software für das Trägheitsnavigationssystem (Konvertierung von 64-Bit-Gleitkommazahlen in 16-Bit-Integerzahlen)

Loss of Mars Climate Orbiter (1999)



- Mars Climate Orbiter: erster interplanetarer Wettersatellit
- Start im Dezember 1998, Verlust im September 199 nach Eintritt in Mars-Umlaufbahn
- Schaden laut NASA: 125 Mio US$
- Ursache: Verwechslung von metrischen und englischen Einheiten in der Software zur Bahnsteuerung

Mars Rover Overload (2004)



- Landung von Mars Rover Spirit im Januar 2004
- Steuerungssoftware durchläuft endlosen Reset-Zyklus
- Ursache: Maximalzahl der Dateien in Flash-Speicher nicht beachtet