Proseminar
Berüchtigte Fehler in Softwaresystemen
Einführungsveranstaltung

Thomas Noll

Software Modeling and Verification Group

21. Oktober 2009

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 zur 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 Stunden
- Teilnahme für BSc-Studierende verpflichtend
- Terminabsprache: `biblio@cs.rwth-aachen.de`, Tel. 80-21025

Deadline

Deadlines

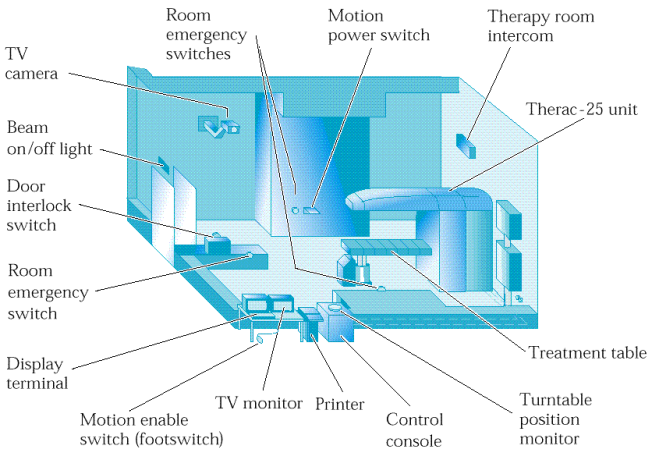
Folgende Termine sind einzuhalten:

- 4. Dezember: Gliederung vorlegen
- 18. Dezember: erste Fassung der Ausarbeitung
- 15. Januar: endgültige Fassung der Ausarbeitung
- 29. Januar: endgültige Fassung der Folien
- 9./10. Februar: Blockseminar

(1) Destruction of Mariner 1 Spacecraft (1962)

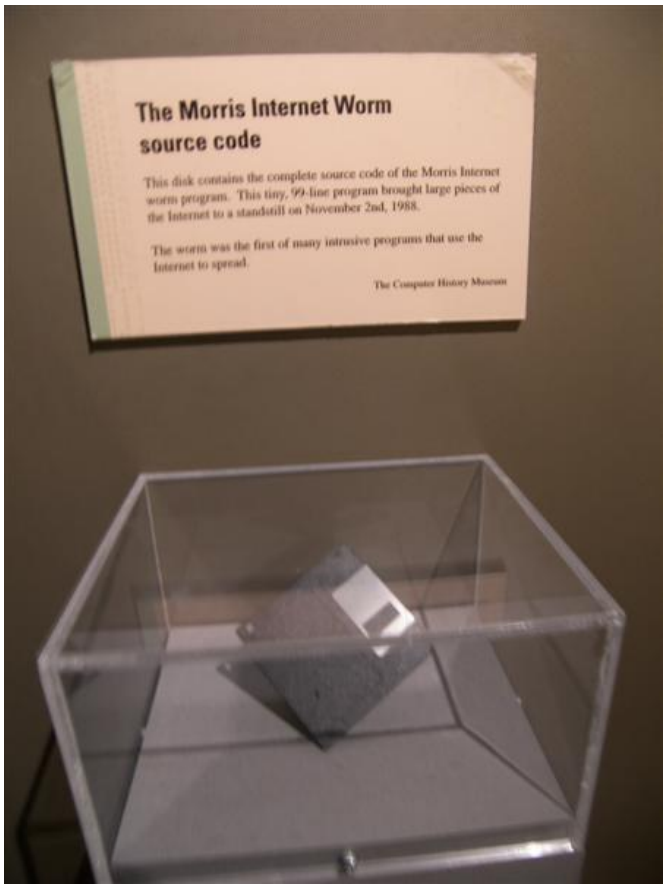
- Venus-Raumsonde der NASA, gestartet Juli 1962
- Unerwartetes Manöver 5 min nach Start $\Rightarrow$ Selbstzerstörung
- Ursache: Codierungsfehler (Übertragung einer mathematischen Formel in Programmtext)

(2) 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*)

(3) Morris Internet Worm (1988)



- Erster über Internet verbreiteter Computerwurm
- Einsatz bei *Denial of Service*-Attacken
- Basierend auf *Buffer overflow*

(4) 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)

(5) 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

(6) Crash of Lufthansa Flight 2904 (1993)

- 14. September 1993: Lufthansa-Flug 2904 (Airbus A320-211) verunglückt bei Landung in Warschau
- Zwei Todesopfer
- Ursachen: starke Scherwinde, Nässe (Aquaplaning), hoher Aufsetzdruck (12 t) vor Freigabe des Bremssystems

(7) 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

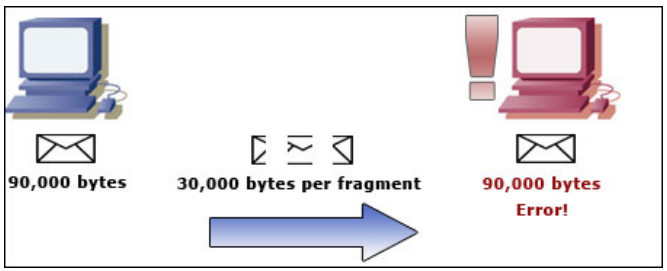
(8) Chinook Helicopter Disaster (1994)

- 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

(9) Altona Railway Software Glitch (1995)

- Totalausfall des neuen, voll computerisierten Eisenbahn-Stellwerks in HH-Altona
- Fehler schwer reproduzierbar (4 Ausfälle in 2 Tagen)
- Ursache: Stacküberlauf verursacht durch Programmierfehler eine Endlosschleife

(10) Ping of Death (1995/96)

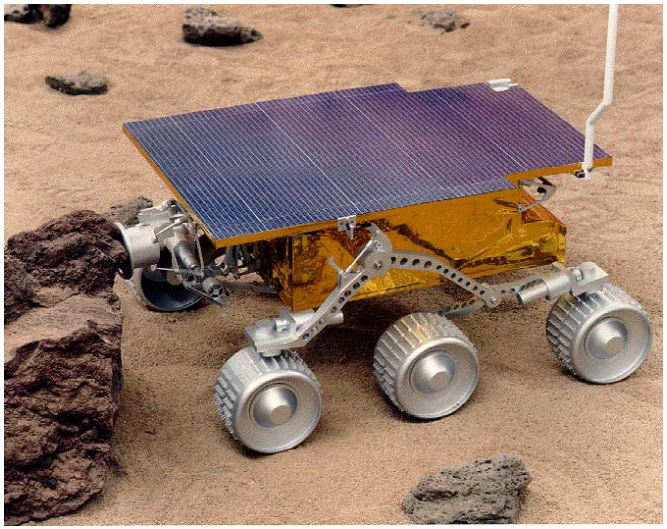


- Maximale Paketgröße in TCP/IP: 65536 bytes
- *Denial of Service*-Attacke durch Übergröße *Internet Control Message Protocol* (ICMP) Pakete (`ping`)
- Inkorrekte Implementierungen können System abstürzen, einfrieren oder rebooten lassen

(11) Ariane 5 Crash (1996)

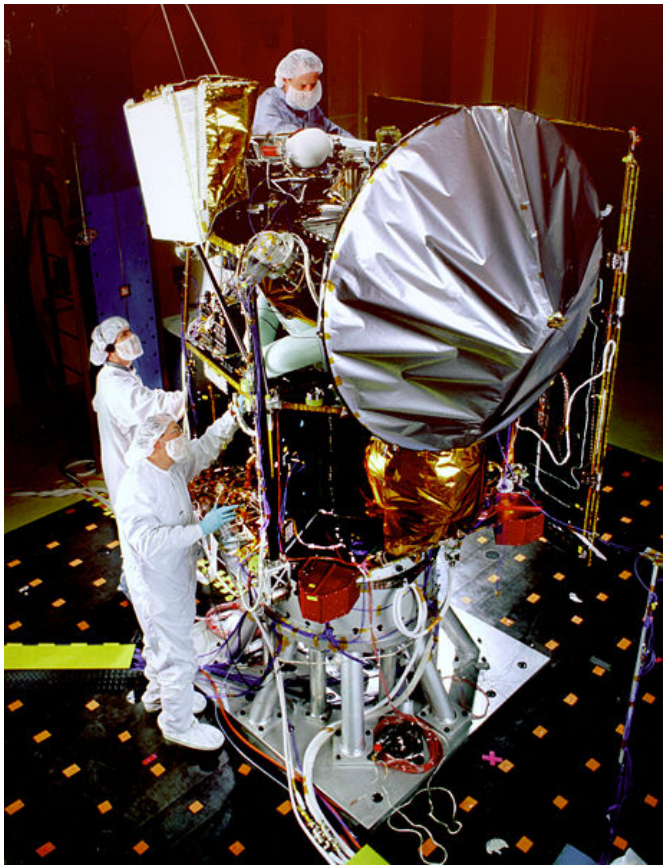
- Absturz der europäischen Ariane 5-Rakete beim Jungfernflug im Juni 1996
- Schaden: mehr als 500 Mio US$
- Ursache: Spezifikations- und Entwurfsfehler in der Software für das Trägheitsnavigationssystem (Konvertierung von 64-Bit-Gleitkommazahlen in 16-Bit-Integerzahlen)

(12) Mars Pathfinder System Resets (1997)



- Marssonde der NASA mit Roboterfahrzeug
- Landung am 4. Juli 1997
- Auftreten sporadischer Resets des Datenerfassungssystems
- Ursache: *priority inversion* (Warten eines Tasks mit hoher Priorität auf Ergebnisse eines Tasks mit niedriger Priorität)

(13) Loss of Mars Climate Orbiter (1999)

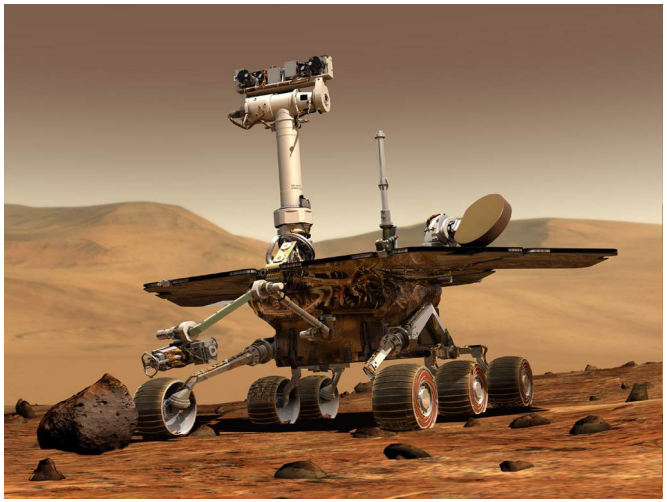


- Mars Climate Orbiter: erster interplanetarer Wettersatellit
- Start im Dezember 1998, Verlust im September 199 nach Eintritt in Mars-Umlaufbahn
- Schaden laut NASA: 125 Mio US$
- Ursache: Verwechslung von metrischen und englischen Einheiten in der Software zur Bahnsteuerung

(14) Radiation Overdosing at Nat. Cancer Institute, Panama (2000/01)

- Strahlungsbehandlung von Krebspatienten im
- Verstrahlung von 28 Patienten; davon mind. 18 Todesopfer
- Ursache: Fehler bei der automatischen Kalkulation der Behandlungszeit (Berücksichtigung von Abschirmungen)

(15) 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

(16) Toyota Prius Recall (2004/05)

- Hybridfahrzeug (Benzin/elektrisch) von Toyota
- Rein elektrisch bei niedrigen Geschwindigkeiten oder im Schubbetrieb
- 13 Fälle von spontanen Motorabschaltungen bei Autobahngeschwindigkeit
- Ursache: Softwarefehler