Verlässliche Systeme

11. Kapitel
Havarien – Fallstudien

Prof. Matthias Werner
Professur Betriebssysteme

11.1 Motivation

- Bei „Verlässlichen Systemen“ geht es um den Umgang mit **unerwarteten/unerwünschten Ereignissen**
- Wir haben in diesem Semester u. a. über
  - ...Begriffe und Maße aus dem Bereich der verlässlichen Systeme
  - ...Modellierung
  - ...Störungsverhalten
  - ...Diagnose
  - ...Entwurfsmuster und Algorithmen zur Erhöhung von Verlässlichkeit
  - ...Verifikation
  - ...Software-Fehlertoleranz

  diskutiert
- Wollen zum Abschluss betrachten, was im wahren Leben™ schief gehen kann

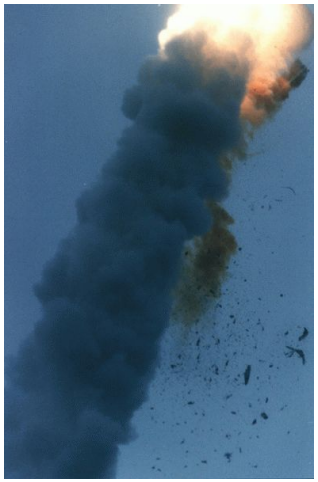
Fallstudien

- Betrachten zwei Fallstudien:
  - Fehlstart der ersten Ariane 5 Rakete
  - Ausfall der Feuerwehrleitzentrale in Berlin in der Neujahrsnacht 2000

11.2 Ariane 501

Ereignis

- Am 4. Juni 1996 endete der erste Flug einer **Ariane 5** (Flug V88) nach 40 Sekunden mit einer Explosion
- Verlustkosten für Rakete und Last (vier Forschungssatelliten): ca. 290 Mio €
- Die Entwicklung der Ariane 5 dauerte 10 Jahre und kostete ca. 4 Mrd. €
- Der Flug war nicht versichert



Hintergrund

- Die Ariane 5 war eine Neuentwicklung
- Einige Komponenten wurden von der Ariane 4 übernommen, u. a. das Trägheitsnavigationssystem (*inertial navigation system*, **INS**)
  - Alle neuen Komponenten wurden ausführlich getestet, **jedoch aus Kostengründen nicht als Gesamtsystem**
  - Als „alte“ Komponente galt das INS als „bewährt“ und wurde nicht erneut getestet
  - Die Software des INS ist in ADA programmiert, was als besonders tauglich für kritische Anwendungen gilt
  - Das INS ist einfach-redundant ausgelegt ➡ ein identisches System im **hot stand-by**
- Das INS besitzt eine **Kalibrierungsroutine**, die im Ruhezustand (vor dem Start) permanent einen Meßabgleich vornimmt
- Um einen evtl. Startabbruch besser behandeln zu können, läuft diese Routine auch eine Weile nach dem Start weiter

Ablauf

- Die Ariane 5 hat eine andere Flugbahn als die Ariane 4 ➡ die Horizontalgeschwindigkeit ist größer als (für die Ariane 4) erwartet
- Der 64-Bit-Gleitkommawert wird im INS in eine 16-Bit-Integerzahl konvertiert
- Es kommt zu einer Ausnahme wegen **Überlauf** ➡ **Operand Error**
- Das Stand-by-INS fällt aus gleichem Grund bereits 50ms früher aus
- Die Ausnahmemeldung (Diagnosemeldung) wird an den **On Board Computer** (OBC) weitergereicht
- Der OBC interpretiert die Diagnosedaten als Flugdaten und berechnet falsche Steuerinformation
- Falsche Flugsteuerung führt zu einer Überlastung ➡ Booster löst sich ➡ automatische Selbstzerstörung

Nachspiel

- Aus den Empfehlungen der Untersuchungskommission zur Aufklärung des Vorfalls
  - Es soll keine Software-Funktion laufen, die aktuell nicht benötigt wird
  - Testen soll unter realistischen Bedingungen stattfinden
  - Kritische Software soll auf
    - implizite Annahmen
    - Wertebereiche der Variablen/Kommunikationskanäle

    überprüft werden
  - Umgebungsbedingungen (Flugbahndaten) sollen bei Spezifikation und Test direkt berücksichtigt werden

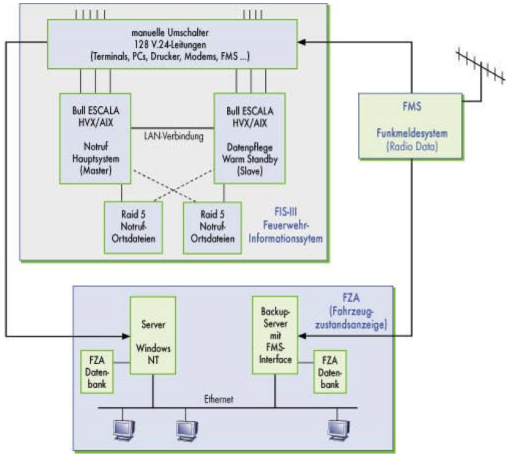
11.3 Ausfall des Berliner Feuerwehrleitsystem

Ereignis

- Am 1. Januar 2000 (Millenniumsneujahr) fällt das im Vorjahr aufgerüstete **Feuerwehr Informationssystem III** (FIS III) vollständig aus
- Als hochkritisches System ist FIS III redundant mit mehreren Rückfallebenen ausgelegt
- Innerhalb von etwa 2 Stunden wurden **alle Rückfallebenen** durchlaufen
- Konkrete Kosten sind schwer abschätzbar
- Folgen u.a.:
  - In der ersten Stunde des Jahres wurden 148 von 337 besetzten Fahrzeugen überhaupt nicht eingesetzt
  - An einem Einsatzort trafen über 20 Fahrzeuge ein, die voneinander nichts wussten
  - Auf einen gegen 1.30 Uhr eingetroffenen Notruf wegen „plötzlicher Bewusstlosigkeit“ wurde über zwei Stunden nicht reagiert, so dass die Polizei nur noch den Tod eines Mannes feststellen konnte

Hintergrund

- FIZ-III ist ein speziell für die Berliner Feuerwehr entwickeltes System mit einem **warm standby** System
- Zusatzkomponenten:
  - **Digitales Funkmeldesystem** (FMS), erlaubt automatische Übermittlung von Einsatzort und Status („Auf dem Weg zum Einsatzort“, „Einsatz“, „Einsatz beendet“, „Wagen nicht bereit“)
  - **Rechnergestützte Fahrzeugzustandsanzeige** (FZA): Grafische Aufarbeitung der aktuellen Einsätze
- Im Normalbetrieb übergibt FMS die Daten an FIS-III, von dort werden sie an die FZA weitergereicht



Hintergrund (Forts.)

- Eigentlich sollte zum Jahreswechsel längst das Leitsystem „IGNIS“ zur Verfügung stehen
- Ende 1998 zeichnete sich ab, dass Termin nicht haltbar war ➡ Das alte FIS-III wurde für 700000 € Y2K-fähig gemacht
  - Neue HW, neues OS, Simulator für altes OS, Überarbeitung der COBOL-Programme
- Y2K-Tests am 6.12. und 9.12. zeigten keine Probleme ➡ Freeze
- Datum des FZA wurde auf 1993 gesetzt
- Kurz vor Jahresende Ergänzung durch Zeitserver

Ablauf

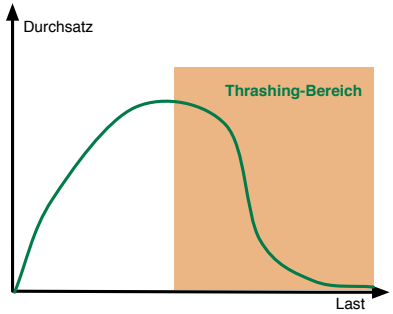
- **00.04 Uhr**: Formatfehler bei einstelligen Daten (`01:13:99` vs. `1:13:99`) führt zu Fehlermeldung
- **Rückfallebene 1:** Umschalten auf *warm stand-by* System
- Redundantes System produziert gleiche Meldung
- FIZ-III wird neu gestartet ➡ fährt nicht hoch, da falsche Konfiguration
- **Rückfallebene 2:** Übergang auf Vorgängersystem FIS-II
- **00:20 Uhr**: FIZ-II wurde hochgefahren
  Dieses befindet sich in einem anderem Gebäude, so dass Entgegennahme von Notfallmeldungen und Koordinierung an unterschiedlichen Orten stattfinden
- Kommunikation mit ausgedruckten Meldungen, die per FAX übermittelt werden
- FMS wird direkt an die FZA gekoppelt

Ablauf (Forts.)

- FAX hat Papierstau ➡ Nutzung von Boten
- Drucker des FIS-II können bis zu 70 Einsätzen/h ausgeben, zu Silvester waren es ca. 500 Einsatzanforderungen/h
- Manuelles Notmanagement verstärkt Inkonsistenzen in der Planung ➡ **Abschaltung** des FIS-II
- **Rückfallebene 3:** Manuelles Dispatchen, lediglich unter Nutzung rechnergestützte Fahrzeugzustandsanzeige (FZA)

Ablauf (Forts.)

- Personal war für Rückfallebene 3 nicht geschult und entsprechend überfordert
- Durch FMS/FZA-Rekonfiguration und die hohe Kommunikationsfrequenz kommt es zu einer Sättigung des Ethernets, verstärkt durch Kaskadeneffekte



Ablauf (Forts.)

- Falsche Darstellung des Zustandes lässt Koordinierung vollständig zusammenbrechen ➡ Abschaltung der FZA
- **02:09 Uhr** Rückfallebene 4: Dezentraler Einsatz, „Streife Fahren“
- Den einzelnen Fahrzeugen wurde aufgetragen, in ihrem Einsatzgebiet auf Brandereignisse und Rauchentwicklung zu achten
- Eingeschränkte Wirksamkeit durch
  - Starken Nebel
  - Feuerwerksrauch

Nachspiel

- Im November 2000 wurde IGNIS probeweise in Betrieb genommen; der Regelbetrieb startete im April 2001
- Der Bericht an das Abgeordnetenhaus sprach von einer „Verkettung unglücklicher Umstände“

Literatur

[Ari96] Ariane 501 Inquiry Board. *ARIANE 5 Flight 501 Failure*. Techn. Ber. ESA, 1996

[Sie00] Richard Sietmann. „Dumm gelaufen? – Anatomie eines Computer-GAUs“. In: *c't - Magazin für Computertechnik* 13 (2000), S. 216–226