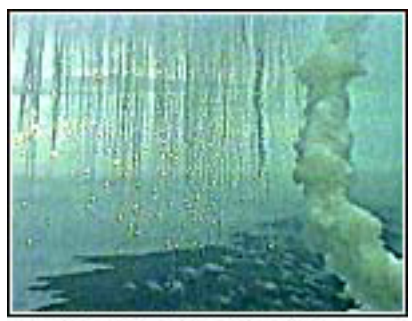
Warum soll man testen?

- Explosion der Ariane 5 am 4. Juni 1996



Smoke from the explosion
June 4, 1996 (AP Photo)

- Verlust von nichtversicherten Geräten für 500 Mio. US $

Chronologie

- Normaler Flug bis T+36 Sekunden nach dem Start
- T+36.7: Fehler des Backup-„Inertial Reference System“
- T+36.75: Fehler des aktiven „Inertial Reference System“
  - Diagnoseinformation zum Hauptcomputer übertragen
- Hauptcomputer interpretiert Diagnosedaten als Flugdaten
  - Hauptcomputer weist Triebwerke an, eine große Korrektur vorzunehmen
- Rakete bricht aufgrund der aerodynamischen Kräfte auseinander
  - Selbstzerstörung wird in einer Höhe von 4 km automatisch eingeleitet

Erklärung

- Fehler im „Inertial Reference System“:
  - Konversion von float auf int führt zu Überlauf
  - „Operand-Error“ wird nicht abgefangen
  - Fehler tritt bei aktivem und Backup-System gleichzeitig auf
  - aktives System kann nicht mehr auf Backup-System umschalten
- Softwarefehler übernommen von Ariane-4:
  - Es geht um die Horizontalbeschleunigung der Rakete, um die Rakete zu stabilisieren, falls der Start abgebrochen wird.
  - Der Softwareteil ist eigentlich nur vor dem Start notwendig und sollte eine Minute nach dem Start abgeschaltet werden.
  - Bei der wesentlich größeren Ariane-5 ist die Horizontalbeschleunigung aber schon innerhalb der ersten Minute außerhalb des ursprünglichen Wertebereichs (wegen der anfänglich größeren Gesamtbeschleunigung und anderen Flugbahn).

Folgerungen

- Während des Flugs soll nur Software laufen, die benötigt wird.
- Vollständige Simulation vor dem Flug.
- Hohe Abdeckung erreichen (= alles testen).
- Alle impliziten Annahmen erkennen.
- Review durch externe Experten durchführen lassen.
- Beim Review die Gründe für Entscheidungen substanziell besprechen, nicht nur den Code inspizieren.
- Rechtfertigungen genauso überprüfen wie den Code.
- Code mit den Rechtfertigungen und Spezifikationen konsistent halten.
- Nichts unbedacht übernehmen.