Qualitätssicherung von Software

Prof. Dr. Holger Schlingloff

Humboldt-Universität zu Berlin
und
Fraunhofer FIRST

Kapitel 1. Einleitung

Ursache, Wirkung und Folge

- Standardwerk zur Terminologie: J.C. Laprie, A. Avizienis, H. Kopetz: Dependability: Basic Concepts and Terminology. Springer-Verlag (englisch, deutsch, französisch)

Irrtum (error)	Ursache
➔ Fehlzustand (fault)	Wirkung
➔ Ausfall (failure)	Folge

- Ausfall kann Fehlerursache für weiteren Fehler sein!

Klassifikation von Fehlern (1)

- **Intention (Art)**
  - **zufälliger Fehler =** zufällig auftretender oder erzeugter Fehler
  - **absichtlicher Fehler =** in böswilliger Absicht erzeugter Fehler
- **Idee, phänomenologischer Ursprung**
  - **physikalischer Fehler =** Fehler aufgrund eines physikalischen Phänomens
  - **logischer Fehler =** auf menschlicher Unzulänglichkeit basierende Fehlerursache, Denkfehler

Klassifikation von Fehlern (2)

- **Raum**
  - **externer Fehler =** von der Beeinflussung des Systems durch seine physikalische Umgebung oder vom Zusammenwirken mit seiner menschlichen Umgebung hervorgerufene Fehlerursache
  - **interner Fehler =** Teil des Systemzustandes, der bei Aufruf durch eine Rechenaktivität einen Fehler hervorruft

- **Zeit, Entstehungsphase**
  - **Betriebsfehler =** während der Nutzung des Systems auftretender Fehler
  - **Entwurfsfehler, Konstruktionsfehler =** während der Entwicklung oder der Modifikation oder der Erstellung der Betriebsprozeduren entstandener Fehler

Klassifikation von Fehlern (3)

- **Dauer**
  - **permanente Fehler** = Anwesenheit ist nicht von einer punktuellen Bedingung abhängig
  - **Temporäre oder transiente Fehler** = nur während einer bestimmten Zeit vorhanden

➔Unterscheidung reparierbar oder nicht!

temporäre interne Fehler werden auch intermittierende Fehler genannt

jeder Fehler kann als permanenter Entwurfsfehler verstanden werden

Klassifikation von Ausfällen

- Wert- oder Zeitausfälle
- verfrüht oder verspätet
- konsistent oder inkonsistent
- kritisch oder unkritisch
- Stillstand oder Livelock
- Auslassungsausfälle, Totalausfälle
- ...

Kapitel 1. Einleitung

Korrektheit, Sicherheit, Zuverlässigkeit...

- ANSI 72983: „Grad der Übereinstimmung zwischen Spezifikation und Programm“
  - vgl. Definition von Qualität!
  - ungeeignete Definition (ein wenig schwanger...)
- Korrektheit bedeutet Abwesenheit von Fehlern
- Software ist korrekt, wenn sie genau das in der Spezifikation festgelegte funktionale Verhalten zeigt
  - also nicht: Wartbarkeit, Effizienz, Funktionalität, ...
  - als Qualitätsmaß schlecht geeignet
- Üblicherweise sind mehrere verschiedene korrekte Implementierungen einer Spezifikation möglich

Sicherheit

„Sicher“ ist sicher ein vielstrapaziertes Wort...

- ISO 8402: „Zustand, in dem das Risiko eines Personen- oder Sachschadens auf einen annehmbaren Wert begrenzt ist“
- Ein System heißt sicherheitskritisch, wenn es beim Ausfall großen Schaden verursachen kann
  - „großer Schaden“: Der Ausfallverlust übersteigt die regulären Betriebsgewinne um ein Vielfaches
- Stillstand ist nicht immer sicher...
  - fail-safe, safe-stop, fail-silent, ...

- Security = Informationssicherheit / Geschütztheit
  - Security = Schutz vor böswilligen Schäden
  - Safety = Schutz vor unbeabsichtigten Schäden

- Formale Definitionen von Sicherheit existieren
  - safety = „nothing bad will ever happen“
  - liveness = „something good will eventually happen“

Zuverlässigkeit

- Zuverlässigkeit (Reliability) ist ein Maß für die Fähigkeit des Systems, funktionstüchtig zu bleiben; Wahrscheinlichkeit, dass das System während einer bestimmten Zeitdauer *t* nicht versagt
- Grad der Vertrauenswürdigkeit in die vom System erbrachte Leistung
- MTTF: mean time to failure
- Überlebenswahrscheinlichkeit R(t): Wahrscheinlichkeit, dass das System nach t Zeiteinheiten noch nicht ausgefallen ist

Verlässlichkeit

- Verlässlichkeit (Dependability) wird oft synonym oder als Erweiterung für Zuverlässigkeit verwendet
- DIN 40041: Zuverlässigkeit ist die Beschaffenheit bezüglich der Eignung, während oder nach vorgegebenen Zeitspannen bei vorgegebenen Arbeitsbedingungen die Zuverlässigkeits-Anforderungen zu erfüllen
- Teile: Verfügbarkeit, Funktionsfähigkeit, Sicherheit
- Vertraulichkeit ist Teil der Informationssicherheit

Verfügbarkeit

- MTBF: mean time between failures;
  MTTR: mean time to repair
- Verfügbarkeit (availability) misst die Wahrscheinlichkeit, mit der ein reparierbares System zu einem beliebigen Zeitpunkt funktioniert: MTBF / (MTBF + MTTR)

Robustheit und Fehlertoleranz

- Robustheit = Eigenschaft des Systems, auch in ungewöhnlichen (unspezifizierten) Situationen bestmögliche Funktionalität zu erbringen
- Fehlertoleranz = Eigenschaft des Systems, auch beim Auftreten von bestimmten Fehlern (Fehlzuständen) die geforderte Funktionalität zu erbringen


It's clearly a case of a failure in the graphics software.
or the wrong printer driver