Ausgewählte Kapitel der Systemsoftwaretechnik: Fehlertolerante Systeme

Peter Ulbrich

Lehrstuhl für Informatik 4
Verteilte Systeme und Betriebssysteme

Friedrich-Alexander-Universität
Erlangen-Nürnberg

Wintersemester 2014

https://www4.cs.fau.de/Lehre/WS14/MS_AKSS/

Überblick

Einführung: Fehlertolerante Systeme

Masterseminar AKSS

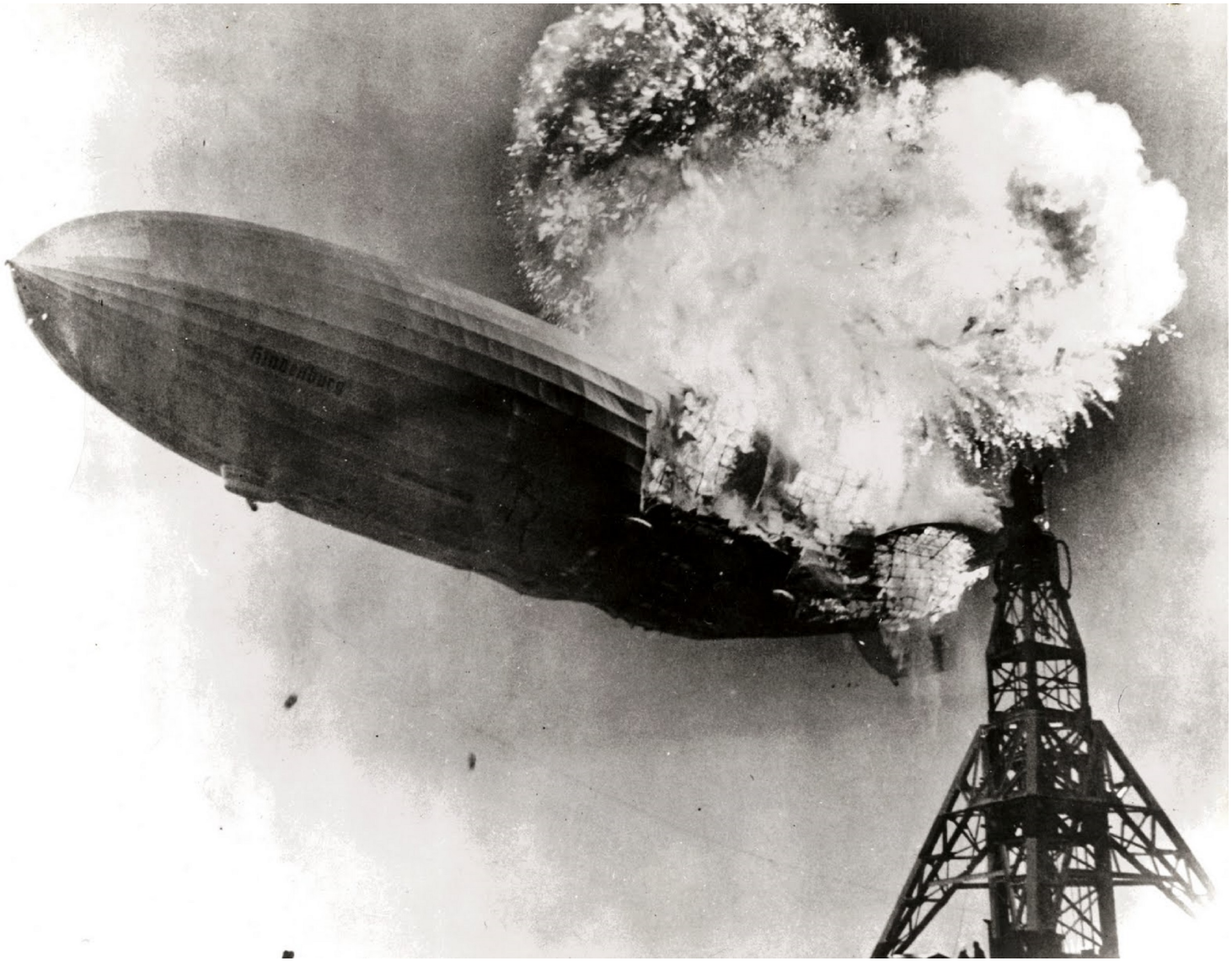
- Organisatorisches
- Seminarmodus
- Themen und Einteilung

Fachliteratur lesen und verstehen

Vortrag strukturieren, gestalten und vorbereiten

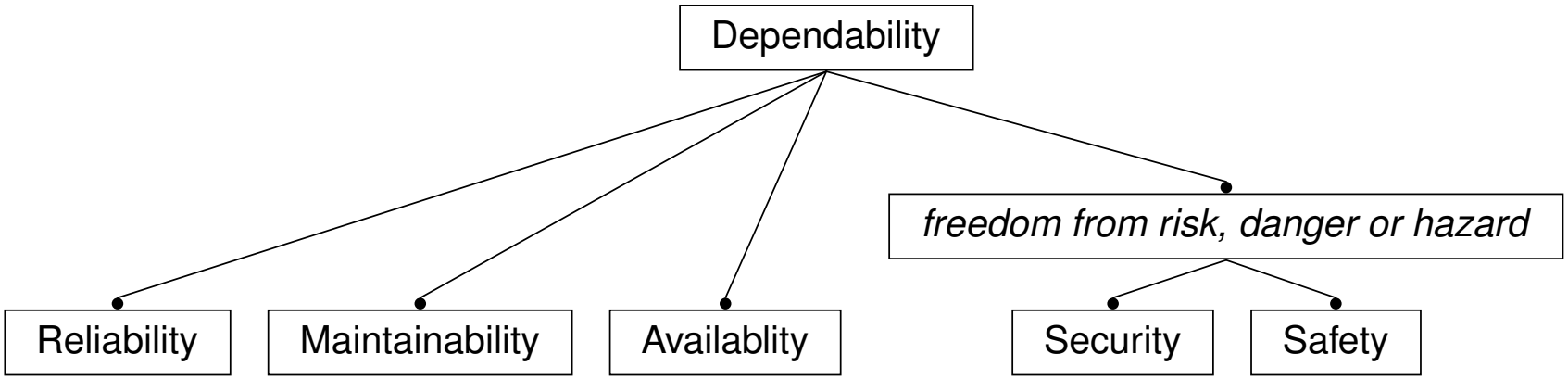
Fehlertoleranz – Motivation

Verlässlichkeit von Systemen?



LZ 129 (Hindenburg), 6. Mai 1937

„Verlässlichkeit“ ist ein vielschichtiger Begriff



The trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers. [6]

Zuverlässigkeit (engl. *reliability*)

$R(t)$ die Wahrscheinlichkeit, dass ein System seinen Dienst bis zum Zeitpunkt t leisten wird, sofern es bei $t = t_0$ betriebsbereit war

- Annahme: eine konstante Fehlerrate von λ Fehler/Stunde
- Zuverlässigkeit zum Zeitpunkt t: $R(t) = exp(-\lambda(t - t_0))$
  - mit $t - t_0$ gegeben in Stunden
- Inverse $1/\lambda$ ist die (engl. *mean time to failure*) (MTTF)

ultra-hohe Zuverlässigkeit $\mapsto \lambda \leq 10^{-9}$ Fehler/Stunde

- Beispiel: elektronisch gesteuerte Bremsanlage im Automobil
  - das Kfz sei durchschnittlich eine Stunde täglich in Betrieb
  - dann darf jährlich nur ein Fehler pro eine Million Kfz auftreten
- Beispiele: Eisenbahnsignalanlagen, Kernkraftwerküberwachung

Wartbarkeit (engl. *maintainability*)

$M(d)$ die Wahrscheinlichkeit, dass das System innerhalb Zeitspanne d nach einem reparierbaren Fehler wieder hergestellt ist

- Ansatz: konstante Reparaturrate von μ Reparaturen/Stunde
- die Inverse $1/\mu$ ist dann die *mean time to repair* (MTTR)

Fundamentaler Konflikt zwischen Zuverlässigkeit und Wartbarkeit:

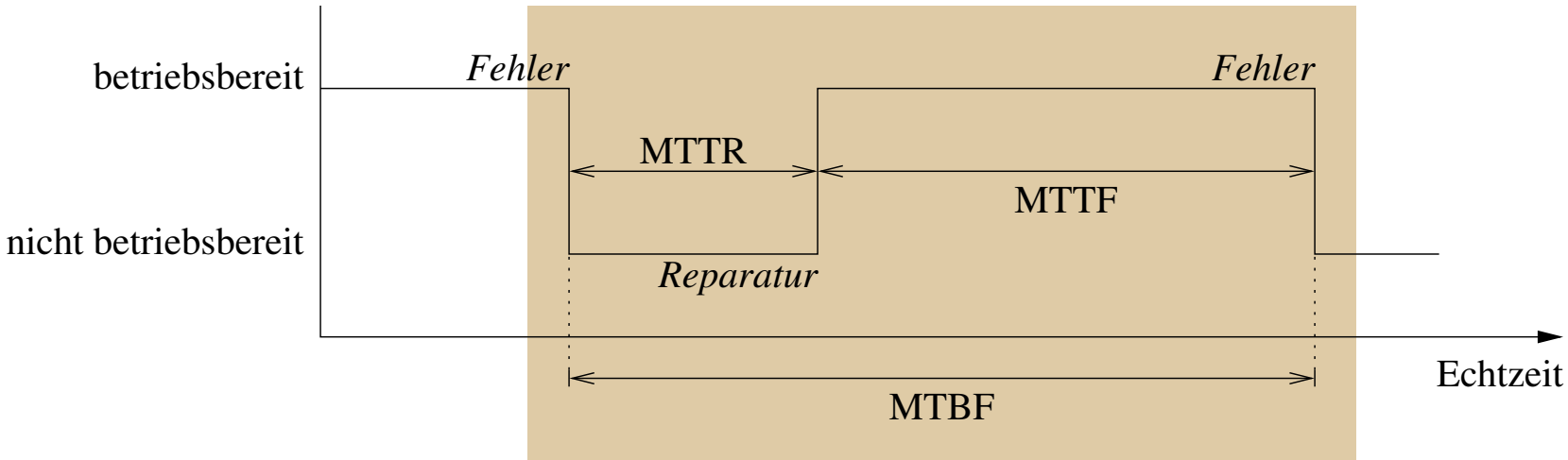
- ein wartbares System erfordert einen modularen Aufbau
  - kleinste ersetzbare Einheit (engl. *smallest replaceable unit*, SDU)
  - über Steckverbindungen lose gekoppelt mit anderen SDUs
  - dadurch ist jedoch eine höhere (physikalische) Fehlerrate gegeben
  - darüberhinaus verbuchen sich höhere Herstellungskosten
- ein zuverlässiges System ist aus einem Guss gefertigt...

Beim Entwurf von Produkten für den Massenmarkt geht die Zuverlässigkeit meist auf Kosten von Wartbarkeit.

Verfügbarkeit (engl. *availability*)

Maß zur Bereitstellung einer Funktion vor dem Hintergrund eines abwechselnd korrekt und fehlerhaft arbeitenden Systems

- Zeitanteil der Betriebsbereitschaft: $A = MTTF/(MTTF + MTTR)$
- $MTTF + MTTR$ auch kurz: *mean time between failures* (MTBF)



☞ hohe Verfügbarkeit bedeutet kurze MTTR und/oder lange MTTF

Verlässlichkeit unterscheidet sich je nach System

Je nachdem, wie kritisch sich ein einzelner Fehler auswirkt.

Hochverfügbare Systeme z. B. Telekommunikationstechnik

- müssen ihren Dienst möglichst ununterbrochen verrichten
- einzelne Fehler sind jedoch verkraftbar ($\rightsquigarrow$ fail-soft)
  - sie werden meist auf höheren Ebenen abgefangen (z. B. TCP/IP)

$\rightsquigarrow$ kurze Fehlererholung steht im Vordergrund

Langlebige Systeme z. B. Satelliten

- müssen auch nach Jahren noch funktionieren ($\rightsquigarrow$ fail-slow)
- eine Fehlerbehebung ist oft technisch nicht möglich

$\rightsquigarrow$ hohe Zuverlässigkeit steht im Vordergrund

Sicherheitskritische Systeme z. B. Flugzeuge, Kernkraftwerke, Eisenbahn, Industrieanlagen, Medizintechnik ...

- zuverlässig und ununterbrochene Funktion ($\rightsquigarrow$ fail-safe)
  - Diese Anlagen sind nur sinnvoll, wenn sie im Betrieb sind!
- hohe Ansprüche an Zuverlässigkeit und Verfügbarkeit

Sicherheit $\mapsto$ *Security* und *Safety*

security Schutz von Informationen und Informationsverarbeitung vor „intelligenten“ Angreifern

- allgemein in Bezug auf Datenbasen des Echtzeitsystems
  - Vertraulichkeit (engl. *confidentiality*)
  - Datenschutz (engl. *privacy*)
  - Glaubwürdigkeit (engl. *authenticity*)
- speziell z.B. Diebstahlsicherung: Zündungssperre im Kfz
  - Kryptographie (engl. *cryptography*)

safety Schutz von Menschen und Sachwerten vor dem Versagen technischer Systeme

- Zuverlässigkeit trotz bösartigen Fehlverhaltens
  - Kosten liegen um Größenordnungen über den Normalbetrieb
- Abgrenzung von unkritischen, gutartigen Fehlern
- oft ist Zertifizierung (engl. *certification*) erforderlich

Überblick

Einführung: Fehlertolerante Systeme

Masterseminar AKSS

- Organisatorisches
- Seminarmodus
- Themen und Einteilung

Fachliteratur lesen und verstehen

Vortrag strukturieren, gestalten und vorbereiten

- Verantwortliche

Daniel Lohmann	Volkmar Sieh	Peter Ulbrich
		
Raum: 0.049-113	0.053-113	0.037-113
lohmann@cs.fau.de	sieh@cs.fau.de	ulbrich@cs.fau.de

- Termin
  - Dienstag, 12:15–13:45, Raum 0.031-113
- Web-Seiten
  - Lehrveranstaltung: `https://www4.cs.fau.de/Lehre/WS14/MS_AKSS/`
  - Anmeldung: `https://waffel.cs.fau.de/signup/?course=205`
- Rückmeldungen und Fragen
  - Bitte Fragen stellen!
  - Auf Fehler aufmerksam machen!

- Schriftliche Ausarbeitung
  - Umfang mindestens 6 Seiten
  - ACM-Stil (zweispaltig, 9-Punkt), siehe:
    `http://acm.org/sigs/publications/proceedings-templates`
- **Abgabe der Ausarbeitung:**
  - Erste Fassung: spätestens zwei Wochen vor dem Vortrag
  - **Vortragsfassung: spätestens eine Woche vor dem Vortrag**
  - Finale Fassung: spätestens eine Woche nach dem Vortrag

  Hintergrund: Einarbeitung der Resonanz aus dem Vortrag
- Weitere Hinweise
  - Ausarbeitung unter Zuhilfenahme der Wissensbasis erstellen:
    `https://www4.cs.fau.de/Lehre/WS14/MS_AKSS/wissensbasis.pdf`
  - Ausarbeitung entweder auf Deutsch oder Englisch

- Vortrag
  - 30–40 min Vortrag *plus* anschließende Diskussion
  - Zur Vorbereitung *mindestens* einmal zur Probe halten
  - **Abgabe der Vortragsfolien:**
    - Erste Fassung: spätestens eine Woche vor dem Vortrag
    - Finale Fassung: spätestens einen Tag vor dem Vortrag
  - Grundlagen der Wissensbasis auch für den Vortrag anwenden
- Aktive Teilnahme
  - Vorbereitung anhand der Vortragsfassung des jeweiligen Vortrags
  - Anwesenheit
  - Beteiligung an den Diskussionen
- Vortragsevaluation
  - Die Seminarteilnehmer bewerten gegenseitig ihre Vorträge
  - Evaluationsbögen werden zu den Seminarterminen bereitgestellt

- Thema 1: Fehlertoleranz in verteilten Systemen (Volkmar)
- Thema 2: DRAM Speicherfehler im Betriebssystem – Problem und Gegenmaßnahmen (Daniel)
- Thema 3: Microrebooting — Feingranulare Fehlertoleranz in Betriebssystemkomponenten (Daniel)
- Thema 4: Redundanz und Replikation — Fehlertoleranz auf Systemebene (Peter)
- Thema 5: Wiederherstellung und Wiedereingliederung von Komponenten (Peter)
- Thema 6: Fehlertoleranz in Mehrkernsystemen (Peter)
- Thema 7: Fehlerinjektion — Wie testet man Fehlertoleranz? (Volkmar)
- Thema 8: Selbststabilisierende Betriebssysteme (Daniel)

Hinweis:
Weiterführende Literatur zu den einzelnen Themen siehe Web-Seite

Überblick

Fachliteratur lesen und verstehen

- Gründe, ein Papier zu lesen
  - Literaturanalyse relevanter verwandter Arbeiten
  - Begutachtung von zur Veröffentlichung eingereichten Beiträgen
  - [Weil es für das Masterseminar notwendig ist]
  - ...
- Mögliche Herangehensweise: Mindestens drei Lesedurchgänge mit jeweils unterschiedlichem Fokus
  - 1. Durchgang: Erster allgemeiner Eindruck
  - 2. Durchgang: Überblick über den Inhalt
  - 3. Durchgang: Detailliertes Verständnis
- Literatur

Srinivasan Keshav
How to Read a Paper
ACM SIGCOMM Computer Communication Review, 37(3):83–84, 2007.

1. Lesedurchgang

- Ziel: Verschaffen eines ersten allgemeinen Eindrucks
- Interessante Fragestellungen
  - In welche Kategorie (z. B. Analyse eines bereits existierenden Systems, Beschreibung eines Prototyps, etc.) fällt das Papier?
  - Was ist der wissenschaftliche Beitrag des Papiers?
  - Sind die getroffenen Annahmen dem ersten Anschein nach berechtigt?
  - Mit welchen anderen Papieren ist das Papier thematisch verwandt?
- Vorgehensweise
  - Detailliertes Lesen
    - Titel
    - Abstract
    - Einleitung
    - Schluss
  - Kurzer Blick auf
    - Überschriften
    - Referenzen

2. Lesedurchgang

- Ziel: Verschaffen eines Überblicks über den Inhalt
- Interessante Fragestellungen
  - Was ist der (komplette) Inhalt des Papiers?
  - Wie würde ich einem Anderen den Inhalt des Papiers erklären?
  - Enthält das Papier offensichtliche Fehler?
- Vorgehensweise
  - Detailliertes Lesen bzw. Betrachten
    - Abschnitte aus 1. Lesedurchgang
    - Restliche Abschnitte
    - Abbildungen, Graphen, etc.
  - Aussparen von Details (z. B. Beweisen)
  - Notizen
    - Zentrale Punkte
    - Relevante Referenzen
    - Unklare Stellen

3. Lesedurchgang, Anfertigung der Ausarbeitung

- Ziel: Detailliertes Verständnis des Papiers
- Interessante Fragestellungen
  - Was sind die wesentliche Beiträge des Papiers?
  - Sind die auf Basis der Annahmen gezogenen Schlüsse korrekt?
  - Werden Annahmen getroffen, die nicht explizit erwähnt sind?
- Vorgehensweise
  - Besonderes Augenmerk auf Details
  - (Gedankliches) Nachvollziehen der präsentierten Experimente
  - Heranziehen von referenzierten verwandten Arbeiten
- Vertiefung, Anfertigung der Ausarbeitung
  - Die wichtigsten verwandten Arbeiten im gleichen Modus bearbeiten
  - Ausarbeitung unter Zuhilfenahme der Wissensbasis erstellen:
    `https://www4.cs.fau.de/Lehre/SS14/MS_AKSS/wissensbasis.pdf`
  - Abgabetermine beachten

Überblick