

Verlässliche Systemsoftware

Peter Ulbrich

Lehrstuhl für Informatik 12 – Arbeitsgruppe Systemsoftware

Technische Universität Dortmund

<https://sys.cs.tu-dortmund.de>

Wintersemester 2021/22

Verlässliche Systemsoftware

Lehrveranstaltungskonzept & Organisation

Peter Ulbrich

Lehrstuhl für Informatik 12 – Arbeitsgruppe Systemsoftware

Technische Universität Dortmund

<https://sys.cs.tu-dortmund.de>

Wintersemester 2021/22



Die Lehrveranstaltung ist grundsätzlich für alle Studiengänge offen. Sie verlangt allerdings gewisse Vorkenntnisse.



- **Systemprogrammierung**, Grundlagen der Informatik
- **C / C++**, Java
- Ein gewisses Maß an **Durchhaltevermögen**
- Freude an systemnaher und **praktischer Programmierung**

Wir arbeiten mit eingebetteten Systemen!

Die meisten sind überrascht, wie viel Spaß das macht :-)

1 Vorwort

2 Die Veranstaltung

■ Lernziele

3 Organisatorisches

■ Die Beteiligten

■ Vorlesung und Übung



Technik (von eingebetteten Systemen) **begeistert**

- Neue Verfahren und Architekturen zu entwickeln, ist spannend!
- Mikrokerne schotten Programme **räumlich** voneinander ab
- Verschlüsselungsalgorithmen garantieren **Datensicherheit**
- Zusteller begrenzen den **zeitlichen** Einfluss
 - Nicht-periodischer Aktivitäten auf periodische Arbeitsaufträge
- ...

Das ist jedoch nur die halbe Miete

- Erfordert möglichst fehlerfreie Implementierungen
- Implementierung muss mit Laufzeitfehlern umgehen können
- Verfahren und Architekturen müssen **korrekt** arbeiten!

Wie lassen sich Ausnahmen vermeiden bzw. behandeln?



Im Fokus dieser Veranstaltung: **Software**

1 **Zuverlässige (robuste) Software entwickeln**

- Robustheit gegenüber externen Fehlern (zur Laufzeit)
 - Wie erkenne und toleriere ich solche Fehler?
- Wie testet man, ob man korrekt mit solchen Fehlern umgeht?
- Hier „forschen“ wir (hoffentlich auch zusammen mit euch)

2 **Software zuverlässig entwickeln**

- Wie kommt man zu einer möglichst fehlerfreien Implementierung?
- Welche Werkzeuge helfen mir dabei?
 - Was tun diese Werkzeuge eigentlich?
 - Welche Grenzen haben diese Werkzeuge demzufolge?
- Hier „lernen“ wir zusammen mit euch



Zuverlässige (robuste) Software entwickeln

- Maskieren von Fehlern durch Redundanz
 - Replizierte Ausführung
 - Homogene und heterogene Redundanz
- Härtung von Datenstrukturen und Kontrollfluss
 - Informationsredundanz
 - In Daten mithilfe von z.B. Prüfsummen
 - In Berechnungen/Kontrollfluss mithilfe arithmetischer Codierung
- Evaluierung von Fehlertoleranzmaßnahmen
 - Fehlerinjektion und Testen

Anknüpfungspunkte für den praktischen Einsatz aufzeigen

- Niemand braucht das 1001. Fehlertoleranzprotokoll!
 - Das den gegenwärtigen Stand der Kunst nicht reflektiert
 - Obendrein vielleicht fehlerhaft ist



Software zuverlässig entwickeln

- Typische **Laufzeitfehler** in C/C++-Programmen suchen und finden
 - Nullzeiger, Ganzzahlüberläufe, nicht initialisierte Speicherstellen, ...
 - Durch Testen oder mittels statischer Analysewerkzeuge
- **Testüberdeckung**: Wie gut hat man getestet?
 - die Testüberdeckung für ein gegebenes Programm messen
 - Gibt es Zusammenhänge zwischen der Testüberdeckung, der Testfallanzahl und anderen Metriken?
- **Design-by-contract**: statische, werkzeug-gestützte Verifikation
 - Formulierung/Verifikation von Nachbedingungen für kleine C-Programme
 - Mithilfe von Werkzeugen (AbsInt Astrée) wie sie auch Airbus einsetzt



Vorurteile gegenüber formalen Methoden abbauen

- Keine **unverwendbaren Monster** mehr
 - Vollbringen aber auch **keine Wunder**
 - Ihre Anwendung ist noch immer mühsam, aber sie lohnt sich



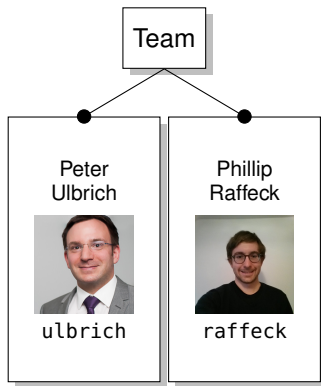
1 Vorwort

2 Die Veranstaltung

- Lernziele

3 Organisatorisches

- Die Beteiligten
- Vorlesung und Übung



■ Wissensvermittlung

- Stoff der **Vorlesung** \rightsquigarrow Folien, Videoaufzeichnung und Screencasts
- Stoff der **Tafelübung** \rightsquigarrow Folien und Screencasts

■ Praktische Arbeit

- Übungs- und Programmieraufgaben
- In Präsenz oder Distanz

■ Interaktion

- Vorlesung und Tafelübung \mapsto Wöchentliche Diskussions- und **Fragestunde**
- Rechnerübung \mapsto **Helpdesk**



Termine und technische Umsetzung im Fluß (Moodle prüfen!)



Termine

- Montags, 16:00-18:00 (c.t.)

Ausnahmen

- 01.11. (Allerheiligen)

■ Inhalt

- Aktueller Stoff der Vorlesung und Tafelübung
- Laufende Übungsaufgaben
- Allgemein fachliche sowie ethische Fragestellungen

■ Ziele

- Diskussion und Reflexion des Stoffes
- Beantwortung von Fragen
- Besprechung der Lernziele der Übungsaufgaben

■ Technik

- Videokonferenz mit BBB



Termine

- Dienstags, 14:00-16:00 (c.t.)

Ausfälle

- siehe Moodle

■ Inhalt & Ziele

- Laufende Übungsaufgabe
- Lösen konkreter Probleme bei der Umsetzung der Aufgaben

■ Auf Zuruf

- In Präsenz im Labor der Arbeitsgruppe (E07)
- Individuelle Videokonferenzen (Screensharing)



Termine und technische Umsetzung im Fluß (Webseite prüfen!)



[2] Fehlertoleranz in Software:

M. Lyu, editor. *Software Fault Tolerance*, volume 3 of *Trends in Software*.

John Wiley & Sons, Inc., 1995.

<https://www.cse.cuhk.edu.hk/~lyu/book/sft/>



[3] Der „Klassiker“ für transiente Hardwarefehler:

S. Mukherjee. *Architecture Design for Soft Errors*.

Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008



[1] Weiters Buch zu transienten Hardwarefehlern:

O. Goloubeva, M. Rebaudengo, M. S. Reorda, and M. Violante. *Software-Implemented Hardware Fault Tolerance*. Springer-Verlag, New York, NY, USA, 1 edition, 2006

