Modul INF-MSc-415: Verlässliche Systemsoftware (VSS)

Englischer Modultitel: Dependable System Software

Studiengänge: Masterstudiengang Informatik, Masterstudiengang Angewandte Informatik

Turnus	Dauer	Studienabschnitt	Credits	Aufwand
nach Ankündigung	1 Semester	2.–3. Semester	6	180 (90/150)

1 Modulstruktur

Nr.	Element / Lehrveranstaltung	Typ	Credits	SWS
1	Verlässliche Systemsoftware	V	3	2
2	Übung zu Verlässliche Systemsoftware	Ü	3	2

2 Lehrveranstaltungssprache: deutsch

3 Lehrinhalte

Viele Rechensysteme sind in Bereiche des täglichen Lebens eingebettete, die hohe Anforderungen an die funktionale Sicherheit dieser Systeme stellen. Beispiele hierfür sind Fahrerassistenzsysteme in modernen Automobilen, medizinische Geräte, Prozessanlagen in Kernkraftwerken oder Chemiefabriken oder Flugzeuge. Fehlfunktionen in diesen Anwendungen ziehen mitunter katastrophale Konsequenzen nach sich - Menschen können ernsthaft verletzt oder sogar getötet werden, Landstriche können unbewohnbar gemacht oder zumindest großer finanzieller Schaden verursacht werden.

Dieses Modul betrachtet Methoden und Werkzeuge, die uns helfen können, einerseits zuverlässig Software zu entwickeln (also Fehler im Programm zu entdecken und zu vermeiden), und andererseits zuverlässige Software zu entwickeln (also Abstraktionen, die auch im Fehlerfall ihre Gültigkeit behalten). Hierbei steht weniger die Vermittlung theoretischer Grundkenntnisse auf diesen Gebieten im Vordergrund, also vielmehr

- die praktische Anwendung existierende Werkzeuge und Methoden
- sowie die Erfahrung und das Verständnis ihrer Grenzen.

Auf diese Weise soll ein Fundament für die konstruktive Umsetzung verlässlicher Systeme gelegt werden.

4 Kompetenzen

Studierende, die das Modul erfolgreich abgeschlossen haben:

- nennen die Konzepte und die Taxonomie verlässlicher Systeme, unterscheiden Software- und Hardwarefehler und klassifizieren Fehler (Defekt, Fehler, Fehlverhalten).
- stellen Fehlerbäume auf.
- organisieren Softwareentwicklungsprojekte mittels der Versionsverwaltung git.
- vergleichen die verschiedenen Arten der Redundanz als Grundvoraussetzung für Fehlererkennung und -toleranz.
- entwickeln fehlertolerante Systeme mittels Replikation.
- diskutieren die Fehlerhypothese und die Sicherstellung von Replikdeterminismus.
- erläutern die Vor- und Nachteile softwarebasierter Replikation und den Einsatz von Diversität.
- wenden Informationsredundanz zur Härtung von Daten- und Kontrollflüssen an.
- bewerten die Effektivität der arithmetischen Codierung von Programmen und verallgemeinern diesen Ansatz auf die verschiedenen Implementierungsebenen (Maschinenprogramm zu Prozessinkarnation).
- interpretieren den Einfluss der Ausführungsplattform (Hardware, Betriebssystem) auf die Leistungsfähigkeit der Fehlererkennung.
- konzipieren eine fehlertolerante Ausführungsumgebung für ein softwarebasiertes TMR-System basierend auf ANBD-Codierung.
- nennen die Grundlagen der systematischen Fehlerinjektion.
- überprüfen die Wirksamkeit von Fehlertoleranzmechanismen mittels Fehlerinjektion auf der Befehlssatzebene.
- entwickeln Testfälle für die Fehlerinjektion mittels des fail* Werkzeugs.
- setzten Messergebnisse in Relation zu dem tatsächlichen Fehlerraum.
- beschreiben die Grundlagen der Fehlererholung (Vorwärts- bzw. Rückwärtskorrektur) und Reintegration fehlgeschlagener Knoten.

	• fassen die Grundlagen des dynamischen Testens zusammen. • unterscheiden Black-Box und White-Box Testverfahren. • konzipieren und implementieren Testfälle. • überprüfen die Testüberdeckung anhand grundlegender Überdeckungskriterien (Anweisungs- bis Bedingungsüberdeckung). • geben die Grundlagen der statischen Programmanalyse wieder. • nennen die Funktionsweise von Hoare- WP-Kalkül. • verifizieren einfache Funktionen mittels des FramaC Werkzeugs zur statischen Analyse von C Programmen. • beschreiben den Korrektheitsnachweis mittels abstrakter Interpretation und unterscheiden die konkrete von der abstrakten Programmsemantik. • erläutern die Funktionsweise von Sammel- und Präfixsemantiken. • erstellen einen Korrektheitsbeweis einfacher Funktionen mittels des Astrée Werkzeugs zur abstrakten Interpretation von C Programmen. • bewerten die Verlässlichkeit kommerzieller, sicherheitskritischer Systeme anhand von Fallstudien (Sizewell B, Airbus A320). • erschließen sich typische Probleme und Fehlerquellen bei der Programmierung von eingebetteten Systemen im Allgemeinen. • klassifizieren Fallstricke und Mehrdeutigkeiten in der Programmiersprache C99 im Besonderen. • können in Gruppen kooperativ und effektiv arbeiten. • können ihre Entwurfs- und Implementierungsentscheidungen kompakt präsentieren und argumentativ vertreten. • reflektieren ihre Entscheidungen kritisch und leiten Alternativen ab. • können offen und konstruktiv mit Schwachpunkten in der Konzeption wie Umsetzung umgehen.
5	**Prüfungen** *Modulprüfung:* Klausur oder mündliche Prüfung BOSS-NR. ???? *Studienleistung: –keine–*
6	**Prüfungsformen und -leistungen** ☒ Modulprüfung ☐ Teilleistungen
7	**Teilnahmevoraussetzungen** *Erfolgreich abgeschlossen:* –keine– *Vorausgesetzte Kenntnisse:* grundlegende Programmierkenntnisse in C/C++
8	**Modultyp und Verwendbarkeit des Moduls** Vertiefungsmodul im Masterstudiengang Informatik und Masterstudiengang Angewandte Informatik Forschungsbereich Verteilte und eingebettete Systeme
9	**Modulbeauftragte/r** Prof. Dr. P. Ulbrich **Zuständige Fakultät** Informatik Beschluss Fakultätsrat 17.02.2021