Safety Critical Systems *Safety Critical Systems*	Modulnummer: ME-707.04

Master					Zugeordnet zu Masterprofil	Basis	Ergänzung
Pflicht/Wahl	☐						
Wahl	☒	Basis	☐	Ergänzung ☒	Sicherheit und Qualität (SQ)	☐	☒
Sonderfall	☐				KI, Kognition, Robotik (KIKR)	☐	☐
					Digitale Medien und Interaktion (DMI)	☐	☐

Modulbereich: Praktische und Technische Informatik

Modulteilbereich: 707 Sichere Systeme

Anzahl der SWS	V	UE	K	S	Prak.	Proj.	Σ	Kreditpunkte: 6	Turnus
	2	2	0	0	0	0	4		i. d. R. angeboten alle 2 Jahre

Formale Voraussetzungen: -

Inhaltliche Voraussetzungen: Technische Informatik 2

Vorgesehenes Semester: ab 1. Semester

Sprache: Deutsch/Englisch

Ziele:

- Über ein fundiertes Sicherheitsbewusstsein (“Safety Awareness”) für Computer-gestützte Steuerungssysteme verfügen
- Einfache Sicherheitsmechanismen umfassend prüfen können
- Einfache Sicherheitsmechanismen selbstständig entwerfen können
- Über Spezialkenntnisse in Bezug auf Sicherheit in den Domänen Bahnsteuerung, Luftfahrt und Automobilbereich verfügen
- Verständnis für Methoden des Sicherheitsnachweises erwerben. Kenntnis der einschlägigen Normen und Zertifizierungsanforderungen haben
- Verständnis für die gesellschaftlichen und wirtschaftspolitischen Rahmenbedingungen, die zur Bildung von Regeln, Normen und Gesetzen für den Einsatz sicherheits-relevanter Systeme führen

Inhalte:

1. Der Begriff der Zuverlässigkeit (Dependability)
2. Standards und Vorgehensmodelle für sicherheits-relevante Systeme
3. Modellierung sicherheits-relevanter Systeme
4. Hazard-Analyse und Risiko-Abschätzung
5. Entwurfskriterien für sicherheits-relevanter Systeme
6. Validation, Verifikation und Test sicherheits-relevanter Systeme
7. Entwicklung von Sicherheitsnachweisen (“Safety Cases”)
8. Spezialthemen aus den Gebieten
    - Zertifizierung von Avionik-Systemen
    - Modellprüfung von Bahnsteuerungen
    - Spezifikationsformalismen für sicherheits-relevante Systeme

Unterlagen (Skripte, Literatur, Programme usw.):

- J. C. Laprie (ed.): Dependability: Basic Concepts and Terminology. Springer 1992.
- Nancy G. Leveson: SAFEWARE: SYSTEM SAFETY AND COMPUTERS. Addison-Wesley ISBN: 0-201-11972-2.
- Nancy G. Leveson: A Systems-Theoretic Approach to Safety in Software-Intensive Systems.. IEEE Trans. on Dependable and Secure Computing, January 2005.
- N. Storey: Safety-Critical Computer Systems. Addison Wesley Longman 1996.
- M. R. Lyu: Software Reliability Engineering. McGraw-Hill 1995.
- Jens Braband: Risikoanalysen in der Eisenbahn-Automatisierung. Edition Signal+Draht, EurailPress, Hamburg, 2005.

Form der Prüfung: i.d.R. Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung		
Arbeitsaufwand	Präsenz 56 h Übungsbetrieb/Prüfungsvorbereitung 124 h Summe 180 h	
Lehrende: Prof. Dr. J. Peleska		Verantwortlich: Prof. Dr. J. Peleska