### Course Description

**Department**

07 Computer Science and Mathematics

**Course title**

Functional Safety

**Hours per week (SWS)**

4

**Number of ECTS credits**

5

**Course objective**

Students who successfully complete this module will have:

- competence on methods and tools to assess a given systems conformity to functional safety requirements as well as to develop a new system taking safety aspects into account.
- competence on the basic concepts (e.g. fault avoidance, risk assessment, software and hardware safety) of functional safety with respect to state-of-the-art industry standards.

**Prerequisites**

Basic knowledge in programming languages and statistics

**Recommended reading**

- J Bürcsök - Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme, 2011, VDE-Verlag
- HL Ross - Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitsebenszyklus und bewährten Managementsystemen, 2014, Carl Hanser Verlag

**Teaching methods**

Lectures and Hands-On Training (Lab sessions)

**Assessment methods**

Written Exam (90 minutes, 100%)

**Language of instruction**

English

**Name of lecturer**

Prof. Dr.-Ing. Martin Hobelsberger

**Email**

martin.hobelsberger@hm.edu

**Link**


**Course content**

Software-intensive systems are already a big part of our daily life and are increasingly influencing or even supervising it. Often, human lives depend on a safe and reliable execution of a systems functionality. Examples for such systems are airbag control units, aircraft autopilots, robots used in chirurgical proceedings or, in near future, autonomously driving cars.

In those systems reliability and safety play a crucial role in the development process. To guarantee and analyze a reliable and safe execution of functions under normal operation and even control the system in case of faults and failures, functional safety methods are applied. Application scenarios can be found for example in domains like automotive, avionic, industrial automation or medical devices.

In this lecture different aspects on reliability and safety are presented and you will learn to analyze systems, identify weaknesses and, as a result, what suitable counter-measures to implement. Among others, the following topics will be discussed:

- Risk assessments methodologies (e.g. failure probability based on ISO 61508) and state-of-the-art methods to analyze a system (e.g. FMEA, FTA, FHA, ETA)
- Functional safety metrics like failure probability or fault tolerance
- Mathematical methods to analyze a systems reliability and safety
- Methods to supervise, detect and control systematic and transient system failures.
- Design patterns and programming guidelines
- Discussion, comparison and classification of state-of-the-art standards from different domains (e.g. ISO 13849, IEC 62061, IEC 61508, IEC 61511, ISO 26262) regarding content, guidelines, regulations and application in a software development process.

**Remarks**

30 hours for lectures, 30 hours for lab sessions, 45 hours for preparing and documenting in-class and lab assignments, 45 hours for reviewing classes and preparing for the exam