Module title
Formal Methods for Specification and Verification of Computer Systems

Module code	**Level**	**ECTS credits**	**Duration**
Tbd.	Bachelor (B.Sc.)	5	2 weeks block course
Module instructor	**Lecture type**	**Prerequisite(s)**	**Grading**
Vitaliy Mezhuyev, University Malaysia Pahang	Lectures + Guided Tutorial Sessions	Intermediate mathematical ability	Tbd.

Objectives
The module introduces Formal Methods (FMs), which are used for the specification and verification of safety-critical computer systems. FMs are presented with Z, TLA, and UPPAAL notations with appropriate tools and verification techniques. Using FMs, students will learn how to precisely specify computer systems and verify their properties. The module represents important properties of modern computer systems as real-time, concurrency, safety, liveness, fairness. The course exposes the student to rigorous and critical thinking skills.

Course Outcomes. By the end of the course, students will be able to:
Knowledge & Understanding: a) Demonstrate an understanding of the theory and principles of FMs; b) Chose when FMs are applicable in software development cycle; c) Transform informal requirements into the formal specifications of a system; d) Read formal specifications and then explain those clearly using informal means.
Skills & Abilities: a) Analyse a complex system and decompose it into abstracted views; b) Model the views by applying the mathematics, underlying the formal specification language; c) Write verification predicates to check the safety and liveness properties of the modelled system; d) Apply corresponding verification technique (checker or prover); e) Critically analyse the results of verification.

The course consists of the series of lectures, interspersed with guided tutorials. The tutorials will apply the techniques introduced in the lectures. Having learned and practised the techniques on small examples, students will participate in the project to specify a computer system using the Z, TLA or UPPAAL notations. This will constitute the single assignment for the module.

Content
1. **Introduction to Formal Methods**
   - 1.1. Formal specification notations and validation techniques
   - 1.2. Role of FMs in the software development cycle
   - 1.3. Benefits and drawbacks of FMs
2. **Z Notation.**
   - 2.1. Z Mathematical tool-kit and schema calculus
   - 2.2. Expression of states and operations
   - 2.3. CZT-IDE
3. **Temporal Logic of Actions (TLA)**
   - 3.1. Operators of TLA
   - 3.2. TLA specification of liveness and safety properties
   - 3.3. TLA model checker and a theorem prover
4. **UPPAAL timed automata**
   - 4.1. Introduction to UPPAAL notation
   - 4.2. Modelling real-time and concurrent behaviour
   - 4.3. Simulation and verification of the models
   - 4.4. Checking the statistical properties of computer systems

Textbook/teaching material
- Z Mathematical tool-kit http://staff.washington.edu/jon/z/toolkit.html
- Lesli Lamport. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers. https://lamport.azurewebsites.net/tla/book.html
- Gerd Behrmann, Alexandre David, and Kim G. Larsen. A Tutorial on UPPAAL. https://www.it.uu.se/research/group/darts/papers/texts/new-tutorial.pdf
- Course notes

Note: this is not the official course descriptor according to the “Studien- und Prüfungsordnung” (SPO)