Module Specification

Analysis and Verification of Concurrent Systems

Version: 2023-24, v2.0, 06 Jul 2023

Contents

Part 1: Information

Module title: Analysis and Verification of Concurrent Systems

Module code: UFCFYN-15-M

Level: Level 7

For implementation from: 2023-24

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: This module will introduce you to the basic theory and principles of concurrent systems, and their use in designing computer programs, with a special focus on formal description, analysis, and correctness.

Features: Not applicable

Educational aims: In particular, you will study the safety and liveness properties of concurrent algorithms and protocols or policies, proving properties using assertional

reasoning and model checking techniques. This module will focus on, and allow you to examine conventional testing methods as well as formal approaches, exploring the emerging challenges and limitations. This module will highlight how formal approaches enable reasoning from logical or mathematical specifications of the behaviours of concurrent processes, and how they offer rigorous proofs that all system behaviours meet some desirable property.

Outline syllabus: Theory and concepts of concurrent systems: concurrency primitives for shared memory and distributed implementations of concurrency, and their use in solving some common problems in concurrent programming. (A)

Testing and formal verification techniques: concepts of static vs. dynamic testing, traditional testing vs. formal verification, test case design, path testing, statement and branch coverage, formal specification and verification using the model checking technique. (A, B)

Formal specification: concepts of formal specifications expressed in languages with formally defined syntax and semantics. Model-based specifications, specifying system behaviour by constructing a model in terms of well defined mathematical constructs. Property-based specifications, specifying system behaviour in terms of properties that must be satisfied considering process algebra (CSP). (A, B)

Tool support and case study: throughout the module, an emphasis will be given to formal approaches, tool support and the application of techniques in domains such as computer/mobile security. The module will provide practical experience in using modern verification tools such as FDR and Casper. (B)

Part 3: Teaching and learning methods

Teaching and learning methods: The module is delivered through a combination of formally scheduled sessions and independent learning. The scheduled learning includes lectures, tutorials, demonstrations and practical sessions. The independent learning will constitute the remaining study time and will be spent on self-directed

study, support of the coursework, and preparation for the summative coursework demonstration.

Practical exercises will allow the students to gain familiarisation with the tools and techniques required for the specification and verification of safety and liveness properties of concurrent systems.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Demonstrate in-depth understanding of the concepts, problems, and techniques of concurrent programming

MO2 Evaluate approaches and techniques to develop safe and secure concurrent systems

MO3 Distinguish, contrast, and apply the concept of traditional testing and formal verification

MO4 Demonstrate the application of formalisms to specify system properties using process algebra (CSP).

MO5 Use tools and analysis techniques to study and reason about critical properties of the concurrent systems, including security protocols

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/modules/ufcfyn-15-m.html

Part 4: Assessment

Assessment strategy: At both first sit and resit, the summative assessment for this module is a coursework assignment:

The coursework assignment assesses, via a case study, the students' application of practical skills in modelling and reasoning about the critical properties of concurrent systems. Students will be required to submit a portfolio containing documents for the modelling and verification of the system's properties, including the system encoding, a log of the analysis, and the results of verification. The case study will be related to automated analysis and verification of security protocols. Students will be required to reflect on their the work within the context of general concurrent systems security vulnerabilities.

Students will have the opportunity for formative feedback during practical lab sessions.

Assessment tasks:

Portfolio (First Sit)
Description: Case study portfolio
Weighting: 100 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Portfolio (Resit)
Description: Case study portfolio
Weighting: 100 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Part 5: Contributes towards

This module contributes towards the following programmes of study: