DD2460 Software Safety and Security 7.5 credits

Programvarusäkerhet

This is a translation of the Swedish, legally binding, course syllabus.

Establishment

Grading scale

A, B, C, D, E, FX, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

knowledge and skills in Programming, 6 credits, equivalent to completed course DD1337/DD1310-DD1319/DD1321/DD1331/DD1333/DD100N/ID1018/ID1022.

Knowledge in Algorithms and Data Structures, 6 credits, equivalent to completed course DD1338/DD1320-DD1328/DD2325/ID1020/ID1021.

Knowledge in Computer Security, 6 credits, equivalent to completed course DD2391/DD2395.

Intended learning outcomes

After passing the course, the student should be able to:

- explain safety and security aspects for systems,
- construct models of systems,
- specify and analyse safety and security properties,
- apply analytical tools on software systems,
- evaluate and compare different approaches to verification and validation of software systems,

in order to

- as citizen and expert be able to discuss software safety and security,
- in professional life and/or research projects be able to formally express safety and security related properties,
- be able to use and adapt various tools and technologies to verify such properties.

Course contents

- Part I. Introduction to safety and security.
- Part II. Temporal logics, modeling, model checking, formal specification. Tool: NuSMV.
- Part III. System modeling with Event-B. Tool: Rodin.
- Part IV. Concurrency, network programming. Tool: Java Pathfinder.
- Part V. Memory safety, fuzzing Tools: memory checker, fuzzer.

Examination

- LAB2 - Laboratory work, 5.0 credits, grading scale: A, B, C, D, E, FX, F
- ÖVN2 - Group presentation and report, 1.5 credits, grading scale: A, B, C, D, E, FX, F
- TEN2 - Examination, 1.0 credits, grading scale: A, B, C, D, E, FX, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

If the course is discontinued, students may request to be examined during the following two academic years.

Ethical approach

- All members of a group are responsible for the group's work.

- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.

Additional regulations

This course contains group projects and labs. Course registration after the official registration period is not possible, since we need to create the groups in the beginning of the course.