FMF3032 Cyber-physical systems' safety and security 7.5 credits

Person- och cyber-säkerhet för cyber-fysiska system

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

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

Establishment

Course syllabus for FMF3032 valid from Autumn 2020

Grading scale

P, F

Education cycle

Third cycle

Specific prerequisites

Admitted to PhD studies

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

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

- Derive, explain, and evaluate safety and security aspects of CPS, and their relationships, according to best practice.
- Construct models of risks, hazards, threats, and CPS.
- Derive and specify safety and security properties to eliminate, reduce or deal with risks.
- Apply analysis methods and tools to models of CPS.
- Explain and compare different approaches to verifying and validating safety and security.

Course contents

Safety and security are increasingly important for the design of complex technological systems, as they are becoming more intelligent, always connected and influencing the societal infrastructure at all levels. There is a need for both citizens and professionals to have a broad awareness of safety, security and their relationship.

Citizens and experts shall be able to discuss the implications of safety and cybersecurity at different levels of society and industry; relate to best practice during the development of trustworthy cyber-physical systems (CPS) and the socio-technical systems they are used in; identify and define properties related to safety and cybersecurity in industrial and research projects; and use and adapt different tools and methodologies for analysing and verifying such properties as relevant for different industrial domains.

Therefore, the course consists of:

- A summary of the evolution of the associated concepts.
- Concepts and standards relevant to safety and cybersecurity at a societal level.
- Concepts, standards, tools, and methodologies for best practice engineering at a system design level.
- Concepts, standards, tools, and methodologies for best practice engineering at a software design level

Examination

- INL1 - Assignment, 3.0 credits, grading scale: P, F
- ÖVN1 - Exercises, 4.5 credits, grading scale: P, 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.

The examination is based on individual partial exam, group assignment and group presentation.

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.