FEL3360 Cyber-Physical Security of Networked Control Systems 3.0 credits

Cyberfysisk säkerhet i nätverkade reglersystem

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

Establishment

Course syllabus for FEL3360 valid from Spring 2019

Grading scale

P, F

Education cycle

Third cycle

Specific prerequisites

Language of instruction

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

Intended learning outcomes

The goal of the course is to introduce and survey some recent results in security and fundamental limitations of cyber-physical systems. After the course, the student should be able to:

- Describe attacks spaces and adversary models for NCSs;
- Define and compute security metrics for NCSs;
- Perform impact analysis for common attack scenarios; and
- Perform risk management and implement simple defense mechanisms.

Course contents

Industrial control systems and SCADA; Confidentiality, Integrity, and Availability; Attack space; Power systems models; Bad Data Detection algorithms; Security Index; Mixed integer linear program; Denial of service attack; Zero dynamics attack; Covert attack; Replay attack; Bias injection attack; Risk analysis (threat identification, likelihood assessment, impact assessment); Risk treatment (prevention, detection, mitigation); Model-Based Fault Diagnosis

Examination

- EXA1 - Examination, 3.0 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.

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

Other requirements for final grade

To obtain the 3 credits, the student must achieve 80% on the home-work problems. The content of FEL3360 partially overlaps that of FEL3361, and one can only obtain a final grade in one of theses courses.

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.