EL2850 Cyber-Physical Security in Time-Critical Systems 7.5 credits

Cyberfysisk säkerhet i tidskritiska 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

The official course syllabus is valid from the autumn semester 2022 in accordance with the decision from the head of school: J-2021-1918.Decision date: 14/10/2021

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering,Electrical Engineering

Specific prerequisites

Knowledge in algebra and geometry, 7.5 higher education credits, equivalent to completed course SF1624.

Knowledge in multivariable analysis, 7.5 higher education credits, equivalent to completed course SF1626.

Knowledge in probability theory and statistics, 6 higher education credits, equivalent completed course SF1900/SF1912/SF1918/SF1922/SF1924.

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 shall be able to

- formulate basic theory and definitions of important concepts in safety and security in cyber-physical systems in general and time-critical systems in particular
- apply model and data-based methods for safety and security in cyber-physical systems particularly for time-critical systems.

Course contents

The course covers safety and security aspects in cyber-physical systems. Particularly, time-critical systems in critical infrastructure and autonomous systems are studied, where cyberattacks and errors can have physical consequences. A large part of the course is devoted to the presentation of basic principles and methods for modeling, analysis and detection of errors and cyberattacks in dynamic systems. In particular, the following is studied

- Documented attacks against cyber-physical systems, system architectures, safety and accessibility, risk management and attack-space in cyber-physical systems.
- Model-based quantification of physical consequences of errors and cyberattacks, discrete-time dynamic systems (linear state models), observers, strong observability and detectability.
- Model and data-based error detection, fault identification and redundancy, parity space methods, observer based methods, setting of threshold.
- Statistical anomaly detection, hypothesis testing, Neyman-Pearson's lemma, generalised likelihood ratio (GLR), Bayes' theorem, principal component analysis (PCA), detection of abrupt process changes, cumulative sum test (CUSUM), machine-learning based methods.

Examination

- INL1 - Assignment, 2.5 credits, grading scale: P, F
- INL2 - Assignment, 2.5 credits, grading scale: P, F
- TEN1 - Written exam, 2.5 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.

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.