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.

Establishment

The official course syllabus is valid from autumn semester 2025 according to the decision of Director of First and Second Cycle Education: HS-2025-0552Date of decision: 2025-04-02

Grading scale

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

Education cycle

Second cycle

Main field of study

Electrical Engineering, Computer Science and Engineering

Specific prerequisites

Skills in basic programming, 3 credits, equivalent to the completed course

DD1337/DD1310-DD1319/DD1321/DD1331/DD1333/DD100N/ID1018/CK1310/BB1000/SF1511/SF151

Knowledge in linear algebra, 7.5 higher education credits, equivalent to completed course SF1624/SF1672/SF1684.

Knowledge of probability theory and statistics, 6 credits, equivalent to completed course

SF1900/SF1912/SF1918/SF1922/SF1924/SF1935.

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:

– formulate basic theory and definitions of important concepts in safety and security in cyber-physical systems in general and discrete time systems in particular

– apply model and data-based methods for safety and security in cyber-physical systems particularly for discrete time systems.

Course contents

The course covers safety and security aspects in cyber-physical systems. In particular, cyber-physical systems that can be modelled as dynamic systems are studied, with applications in critical infrastructure and autonomous systems where cyber-attacks and failures can have physical consequences. We introduce discrete-time dynamical systems using linear algebra. A large part of the course is devoted to presentation by basic principles and methods for modelling, analysis and detection of errors and cyberattacks in dynamic system. 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 faults and cyber-attacks, false data injection and DoS attacks, discrete-time linear state models, observers (UIO), 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.

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.