HÖGSKOLAN VÄST

COURSE SYLLABUS

Course code: **SFC600**

Cyber-physical Systems Security, 7,5 HE credits

Säkerhet för cyberfysiska system, 7,5 hp

Established: 2021-10-07
Established by: Department of Engineering Science
Applies from: H22

Learning outcomes

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

Knowledge and understanding

- describe various types of cyber-physical systems and their application areas.
- explain general security architecture principles.
- identify vulnerabilities, threats, attack models affecting cyber-physical systems and choose countermeasures.
- explain protocols and standards used in cyber-physical security.
- understand variation among cyber-physical security solutions when applied to different types of cyber-physical systems.

Skills and abilities

- differentiate between physical, logical, and organizational security.
- select proper tools and methods to counteract threats to cyber-physical security.
- integrate recent development in the area of cyber-physical security into existing systems.

Values and attitudes

- understand the impact cyber-physical systems have on society.
- demonstrate an understanding of personal responsibility as a cybersecurity expert for cyber threat mitigation.

Entry requirements

Bachelor of Science in Computer science, Computer engineering, Information technology, Electrical engineering, or equivalent. The degree must include at least 30 HE credits computer science or equivalent comprising at least 7,5 HE credits in programming and 7.5 HE credits in data communication. Verified knowledge of English corresponding to the course English 6 in the Swedish Upper Secondary School (high school) or equivalent. Recommendations regarding English described at hv.se/en/education/degree-programmes/application-admission/admission-requirements/english-language-requirement/

The forms of assessment of student performance

Individual written exam. Assignment in group with oral presentation.

Course contents

The course focuses on main cybersecurity aspects of areas such as

- Internet of Things (IoT)
- Industrial Internet
- Smart Cities
- Smart Grid and "Smart" Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances).

The students are introduced to the concepts of general security architecture, network security, and cyber physical security. Importance of continuous assessment of security threats and the countermeasures is emphasized. Notion of physical, logical, and organizational security is provided. Leading industrial communication standards are covered both theoretically and practically.

Other regulations

Course grading: F/Fx/E/D/C/B/A - Insufficient, Insufficient- more work required before the credit can be awarded, Sufficient, Satisfactory, Good, Very Good, Excellent
Course language: The teaching is conducted in English.

General rules pertaining to examination at University West are available at www.hv.se.

If the student has a decision/recommendation on special support due to disability, the examiner has the right to examine the student in a customized examination form.

Cycle

Second cycle

Progressive specialization

A1N - second cycle, has only first-cycle course/s as entry requirements

Main field of study

Computer Engineering