



EL2850 Cyberfysisk säkerhet i tidskritiska system 7,5 hp

Cyber-Physical Security in Time-Critical Systems

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Fastställande

Kursplanen gäller från och med HT 2022 enligt skolchefsbeslut: J-2021-1918. Beslutsdatum: 2021-10-14

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik, Elektroteknik

Särskild behörighet

Kunskaper i linjär algebra, 7,5 hp, motsvarande slutförd kurs SF1624/SF1672/SF1684.

Kunskaper i flervariabelanalys, 7,5 hp, motsvarande slutförd kurs SF1626/SF1674/SF1686.

Kunskaper i sannolikhetsteori och statistik, 6 hp, motsvarande slutförd kurs SF1900/SF1912/SF1918/SF1922/SF1924.

Undervisningspråk

Undervisningspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten kunna

- formulera grundläggande teori och definitioner av viktiga begrepp inom säkerhet i cyberfysiska system i allmänhet och tidskritiska system i synnerhet
- tillämpa modell- och databaserade metoder för säkerhet i cyberfysiska system, särskilt för tidskritiska system.

Kursinnehåll

Kursen behandlar säkerhetsaspekter inom cyberfysiska system. Särskilt studeras tidskritiska system i kritisk infrastruktur och autonoma system där cyberattacker och fel kan ha fysiska konsekvenser. En stor del av kursen ägnas åt genomgång av grundläggande principer och angreppssätt för modellering, analys och detektering av fel och cyberattacker i dynamiska system. Speciellt studeras:

- Dokumenterade angrepp mot cyberfysiska system, systemarkitekturer, säkerhet och tillgänglighet, riskhantering och attackrymd inom cyberfysiska system.
- Modellbaserad kvantifiering av fysiska konsekvenser av fel och cyberangrepp, tidsdiskreta dynamiska system (linjära tillståndsmodeller), observatörer, stark observerbarhet och detekterbarhet.
- Modell- och databaserad fel detektering och felidentifiering, redundans, paritetsmetoder, observatörsbaserade metoder, inställning av tröskelvärde.
- Statistisk anomalidetektion, hypotestest, Neyman-Pearsons lemma, generaliserad likelihoodkvot (GLR), Bayes sats, principalkomponentanalys (PCA), detektion av abrupta processändringar, kumulativ summatest (CUSUM), maskininlärningsbaserade metoder.

Examination

- INL1 - Inlämningsuppgift, 2,5 hp, betygsskala: P, F
- INL2 - Inlämningsuppgift, 2,5 hp, betygsskala: P, F
- TEN1 - Skriftlig tentamen, 2,5 hp, betygsskala: A, B, C, D, E, FX, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.

- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.