EL2850 Cyberfysisk säkerhet i tidskritiska system 7,5 hp

Cyber-Physical Security in Time-Critical Systems

Fastställande

Kursplanen gäller från och med HT 2025 enligt grundutbildningsansvarigs beslut: HS-2025-0552Beslutsdatum: 2025-04-02

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Elektroteknik, Datalogi och datateknik

Särskild behörighet

Färdigheter i grundläggande programmering, 3 hp, motsvarande slutförd kurs

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

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

Kunskaper i sannolikhetsteori och statistik, 6 hp, motsvarande slutförd kurs

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

Undervisningsspråk

Undervisningsspråk 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 tidsdiskreta dynamiska system i synnerhet

– tillämpa modell- och databaserade metoder för säkerhet i cyberfysiska system, särskilt för tidsdiskreta dynamiska system.

Kursinnehåll

Kursen behandlar säkerhetsaspekter inom cyberfysiska system. Särskilt studeras cyberfysiska system som kan modelleras som dynamiska system, med tillämpningar inom kritisk infrastruktur och autonoma system där cyberattacker och fel kan ha fysiska konsekvenser. Vi introducerar tidsdiskreta dynamiska system med hjälp av linjär algebra. En stor del av kursen ägnas åt genomgång av grundläggande principer och angreppssätt för modellering, analys och detektering av fel och cyberattacker i tidsdiskreta dynamiska system. Speciellt studeras:

– Dokumenterade angrepp mot cyberfysiska kritiska infrastrukturer, systemarkitekturer, säkerhet och tillgänglighet, riskhantering och attackrymd inom cyberfysiska system.

– Modellbaserad kvantifiering av fysiska konsekvenser av fel och cyberangrepp, falsk datainjektion och DoS-attacker, tidsdiskreta linjära tillståndsmodeller, observatörer (UIO), stark observerbarhet och detekterbarhet.

– Modell- och databaserad feldetektering och felidentifiering, redundans, paritetsmetoder, observatörsbaserade metoder, inställning av tröskelvärde.

– Statistisk anomalidetektion, hypotestest, Neyman-Pearsons lemma, generaliserad likelihoodkvot (GLR), Bayes sats, detektion av abrupta processändringar, kumulativ summatest (CUSUM), maskininlärningsbaserade metoder (PCA, SVM, etc.).

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.

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

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.