Industriell IT-säkerhetstekniker

400 YH-krediter

Motsvarar ungefär 2 års studier

Hybridformat med träffar i Göteborg och Stockholm

Programmet är utformat för att möta en växande efterfrågan på expertis inom industrin, där digitalisering och ökande cyberhot skapar nya utmaningar. Genom att fokusera på praktiska färdigheter och avancerade säkerhetslösningar för IT- och OT-system förbereder programmet studenterna att skydda IT-infrastruktur, förhindra cyberintrång och hantera säkerhetsincidenter i industriella miljöer.

Om programmet

Programmet planeras att genomföras i ett hybridformat från Stockholm och Göteborg. Den kombinerar undervisning på plats med digitala föreläsningar, vilket gör det möjligt för sökande från närliggande områden och regioner samt huvudorterna att delta. För att bli antagen måste sökande ha en gymnasieexamen och godkända betyg i:

- Engelska 6
- Svenska 2
- Matematik 2

Kursöversikt som kommer att gälla vid beviljandebeslut från MYH

5 YH-poäng motsvarar en veckas heltidsstudier

Examensarbete	30
Härdning av industriella system	45
LIA, lärande i arbete (praktik)	80
Logghantering och incidentrespons i OT-miljö	35
Identitetshantering och åtkomstkontroll	30
Industriella nätverk och säkerhetsarkitektur	55
Introduktion till IT och OT i industriella miljöer	20
Molnteknologi inom industriell produktion	30
Penetrationstestning i industriella miljöer	30
Regelverk och standarder	30
Riskanalys och säkerhetsdesign	30
Summa:	**415**

Senast uppdaterad: 2026-08

Kursbeskrivningar

Examensarbete

Kursen ger de studerande möjlighet att fördjupa sig inom ett område som är centralt för utbildningen genom att utföra ett självständigt projekt. Examensarbetet ska ha en tydlig koppling till industriell IT-säkerhet och genomföras med professionell planering, korrekt dokumentation och hänsyn till formella regler och källkritik.

Kursens huvudsakliga innehåll:
• Val och avgränsning av projektområde inom industriell IT-säkerhet.
• Planering och genomförande av ett självständigt arbete.
• Tillämpning av metodik för informationsinsamling och analys.
• Korrekt dokumentation och presentation av resultat muntligt och skriftligt.

Härdning av industriella system

Kursen är utformad för att ge de studerande kunskaper och praktiska färdigheter i att säkra Linux- och Windows-baserade system som används i industriella OT-miljöer. Dessa system utgör ofta kritiska delar av produktionsinfrastrukturen, såsom SCADA-servrar, HMI-stationer, OPC UA-gateways och MES-system, vilket gör dem till attraktiva mål för cyberattacker.

Kursens huvudsakliga innehåll:
• Operativsystemens roll i OT-miljöer: Förstå hur Linux och Windows används i SCADA-, PLC- och produktionsnära system.
• Risker och utmaningar: Identifiera vanliga sårbarheter i äldre OS-versioner och förstå varför patchning ofta är eftersatt i industrin.
• Härdningsstrategier: Implementera best practice för att minska attackytor, inklusive tjänstehantering, rättighetshantering, och säkra konfigurationer.
• Patchning och uppdateringar: Metoder för att uppdatera system utan att störa produktionen, samt hantera livscykelutmaningar.
• ISA/IEC 62443-perspektiv: Tillämpa krav från standarden för säker konfiguration och systemhärdning i OT-miljöer.

LIA – lärande i arbete

Kursen ger de studerande möjlighet att tillämpa sina kunskaper i verkliga industriella miljöer. Arbetsuppgifterna ska ha direkt koppling till tidigare kursmoment och ge praktisk erfarenhet av att arbeta med IT-säkerhet i OT-kontext. Kursen förbereder de studerande för yrkesrollen som industriell IT-säkerhetstekniker genom att utveckla både tekniska färdigheter och professionellt agerande.

Kursens huvudsakliga innehåll:
• Praktiskt arbete med IT-säkerhet i industriella miljöer.
• Tillämpning av kunskaper från tidigare kurser i en verklig yrkesmiljö.
• Introduktion till arbetsprocesser, roller och ansvar på en arbetsplats.
• Dokumentation och rapportering av arbetsuppgifter enligt branschpraxis.
• Reflektion kring yrkesrollen, den egna prestationen och arbetsuppgifterna på arbetsplatsen.

Logghantering och incidentrespons i OT-miljö

Syftet med kursen är att ge de studerande kunskap och praktiska färdigheter i att övervaka, analysera och hantera säkerhetsincidenter i industriella miljöer samt att planera för återställning och kontinuitet vid störningar. Fokus ligger på insamling och analys av loggdata från kritiska system som PLC, HMI, SCADA och nätverksutrustning, utveckling av effektiva incidentresponsplaner och strategier för att säkerställa driften även vid cyberattacker eller systemfel.

Kursens huvudsakliga innehåll:
• Loggkällor i OT-miljö: Identifiera och samla in loggar från PLC, HMI, SCADA och nätverkskomponenter.
• Analys och övervakning: Använda verktyg för att analysera loggdata och upptäcka säkerhetsincidenter.
• Incidentrespons: Utveckla och implementera responsplaner som minimerar påverkan på produktionen.
• Disaster Recovery och kontinuitet: Återställning och backupstrategier för PLC-, SCADA- och HMI-system,
• Riskanalys och hotbild: Förstå vanliga sårbarheter och hot mot SCADA- och PLC-system som en del av incidenthantering.
• ISA/IEC 62443-perspektiv: Förstå standardens krav på övervakning, incidenthantering och kontinuitet i industriella miljöer.

Identitetshantering och åtkomstkontroll

Kursen handlar om hur identiteter och åtkomsträttigheter hanteras i industriella miljöer där IT och OT samverkar. Den fokuserar på både teoretiska principer och praktiska metoder för att implementera säkra lösningar som uppfyller branschstandarder och regulatoriska krav. De studerande får insikt i utmaningar som uppstår vid integration av moderna säkerhetslösningar med äldre OT-system och lär sig att tillämpa best practice för att minimera risker.

Kursens huvudsakliga innehåll:
• Principer för åtkomstkontroll: least privilege, rollbaserad åtkomst (RBAC), och segmentering.
• Autentisering i OT-miljöer: lokala konton, Active Directory-integration, multifaktorautentisering.
• Hantering av privilegierade konton och fjärradministration.
• Säkerhetsutmaningar vid identitetshantering i äldre system.
• ISA/IEC 62443-perspektiv: krav på identitet och åtkomstkontroll.

Industriella nätverk och säkerhetsarkitektur

Kursen ger de studerande en helhetsförståelse för hur industriella nätverk fungerar och hur man bygger en säker arkitektur för uppkopplade produktionssystem. Fokus ligger på kommunikationsprotokoll som används i OT-miljöer och designprinciper som minimerar attackytor. Brandväggar behandlas som en central komponent i segmentering och skydd av industriella nätverk.

Kursens huvudsakliga innehåll:
• Industriella kommunikationsprotokoll: Förstå och säkra protokoll som Modbus, OPC UA och Profinet.
• Säkerhetsutmaningar i OT-nätverk: Identifiera sårbarheter i kommunikation och nätverksdesign.
• Segmentering och zonindelning: Tillämpa Purdue-modellen och skapa konduiter för att isolera kritiska system.
• Brandväggar i OT-miljö: Konfigurera och administrera brandväggar för segmentering mellan zoner, trafikfiltrering och skydd av OT-protokoll.
• VPN och fjärråtkomst: Implementera säkra lösningar för fjärranslutning till produktionssystem.
• Säkerhetsarkitektur: Designa robusta nätverk för SCADA-, PLC- och MES-system enligt best practice.
• ISA/IEC 62443-perspektiv: Implementera krav på nätverkssegmentering och kommunikationskontroll i OT-miljöer.

Introduktion till IT och OT i industriella miljöer

Kursen ger de studerande en grundläggande förståelse för hur IT- och OT-system samverkar i industriella miljöer. Fokus ligger på skillnader mellan IT och OT, deras respektive roller i produktionen, samt de säkerhetsutmaningar som uppstår vid konvergensen mellan de olika områdena. Kursen introducerar centrala begrepp, arkitekturmodeller och komponenter som utgör basen för industriell digitalisering och cybersäkerhet.

Kursens huvudsakliga innehåll:
• Grundläggande begrepp inom IT och OT på svenska och engelska.
• Roller, funktioner och mål inom IT och OT: Individens och organisationens förutsättningar för säkerhet i IT- och OT-system.
• Industriella digitala system och komponenter: SCADA, PLC, HMI, MES och deras koppling till IT-infrastruktur.
• Kommunikationsprotokoll i OT-miljöer: översikt av Modbus, OPC UA, Profinet.
• Interoperabilitet och konvergens mellan IT- och OT-system
• Översiktlig introduktion till branschstandarder samt relevanta lagar och regler.

Molnteknologi inom industriell produktion

Kursen ger de studerande kunskap om hur molntjänster används i industriella miljöer och hur säker integration sker mellan OT-system och molnplattformar. Fokus ligger på arkitekturprinciper, säkerhetslösningar och riskhantering vid molnintegration. Kursen behandlar även regulatoriska krav och standarder som styr molnbaserade lösningar i industriella sammanhang.

Kursens huvudsakliga innehåll:
• Molnbaserade plattformar för övervakning, analys och styrning av industriella system.
• Säker arkitektur för hybridlösningar (OT–moln) och segmentering.
• VPN, kryptering och autentisering vid molnintegration.
• Risker och hotbilder vid molnanvändning i olika OT-miljöer.

• Compliance och regulatoriska krav (GDPR, NIS2) samt ISA/IEC 62443-perspektiv.

Penetrationstestning i industriella miljöer

Den här kursen ger de studerande praktisk erfarenhet av etisk hackning och säkerhetstestning i OT-miljöer. Fokus ligger på att förstå angriparens perspektiv och att utveckla förmågan att identifiera och åtgärda sårbarheter i industriella system. De studerande lär sig metoder och verktyg för penetrationstestning anpassade för SCADA-, PLC- och nätverksmiljöer, samt hur man implementerar försvarsåtgärder för att stärka säkerheten.

Kursens huvudsakliga innehåll:
• Vanliga sårbarheter i SCADA- och PLC-system: Identifiera svagheter i kommunikation, autentisering och konfiguration.
• Grundläggande och avancerade tekniker: Utföra penetrationstest mot virtuella PLC-, SCADA- och HMI-system.
• Angriparens perspektiv: Förstå vanliga attackvektorer och hur sårbarheter utnyttjas i OT-miljöer.
• Försvarsåtgärder: Implementera motåtgärder och härdningsstrategier baserat på testresultat.
• ISA/IEC 62443-perspektiv: Tillämpa standardens krav för säkerhetstestning och verifiering av systemhärdning.

Regelverk och standarder

Kursen behandlar juridiska och regulatoriska aspekter av industriell IT-säkerhet och ger de studerande en helhetsförståelse för hur lagar, standarder och branschkrav påverkar uppkopplade produktionssystem och OT-miljöer. De studerande lär sig om ansvar vid incidenter, dataskydd och hur standarder och regelverk som GDPR och NIS2 tillämpas i praktiken.

Kursens huvudsakliga innehåll:
• Regelverk och lagstiftning: Förstå GDPR, NIS2 och andra relevanta lagar som styr informationssäkerhet i industriella miljöer.
• Ansvar och roller: Identifiera ansvarsfördelning vid incidenter och säkerhetsbrister i OT-system.
• Compliance och riskhantering: Hur företag arbetar för att uppfylla juridiska krav och minimera risker.
• ISA/IEC 62443-perspektiv: Introduktion till standarden som ett branschkrav och dess koppling till juridiska och regulatoriska ramverk. Fokus på hur ISA/IEC 62443 används för att uppnå compliance och säkerhetsnivåer i industriella miljöer.

Riskanalys och säkerhetsdesign

Syftet med kursen är att ge de studerande en strategisk och metodisk grund för att identifiera, bedöma och hantera risker i industriella miljöer samt att omsätta dessa analyser till robusta säkerhetsarkitekturer. Kursen fokuserar på att skapa en helhetsförståelse för hur riskanalys styr designbeslut, hur ISA/IEC 62443 används för att definiera säkerhetsnivåer och hur zonindelning och konduitanalys implementeras som en del av en systematisk säkerhetsstrategi. Kursen belyser även mänskliga och organisatoriska faktorer som påverkar riskbilden och hur dessa kan hanteras för att stärka säkerhetskulturen. Därutöver får de studerande en genomgång av skillnaden mellan säkerhetsarkitektur och säkerhetsdesign, samt skillnaden mellan IT-arkitektur och säkerhetsarkitektur.

Kursens huvudsakliga innehåll:
• Metoder för riskbedömning i OT-miljöer (t.ex. HAZOP, FMEA, cyberriskanalys).
• ISA/IEC 62443 Security Levels (SL) och hur de används i design.
• Zon- och konduitanalys: skapa segmentering baserat på risk.
• Säkerhetskravspecifikationer och designprinciper.

- • Koppling till compliance och regulatoriska krav (GDPR, NIS2).
- • Mänskliga och organisatoriska faktorer: hur beteenden, rutiner och brister i organisationen kan skapa sårbarheter, inklusive strategier för att minska dessa risker.