Omtale av TTK2 - Pålitelighet av sikkerhetskritiske funksjoner

Faglærer: Mary Ann Lundteigen

Semester: Høsten 2026

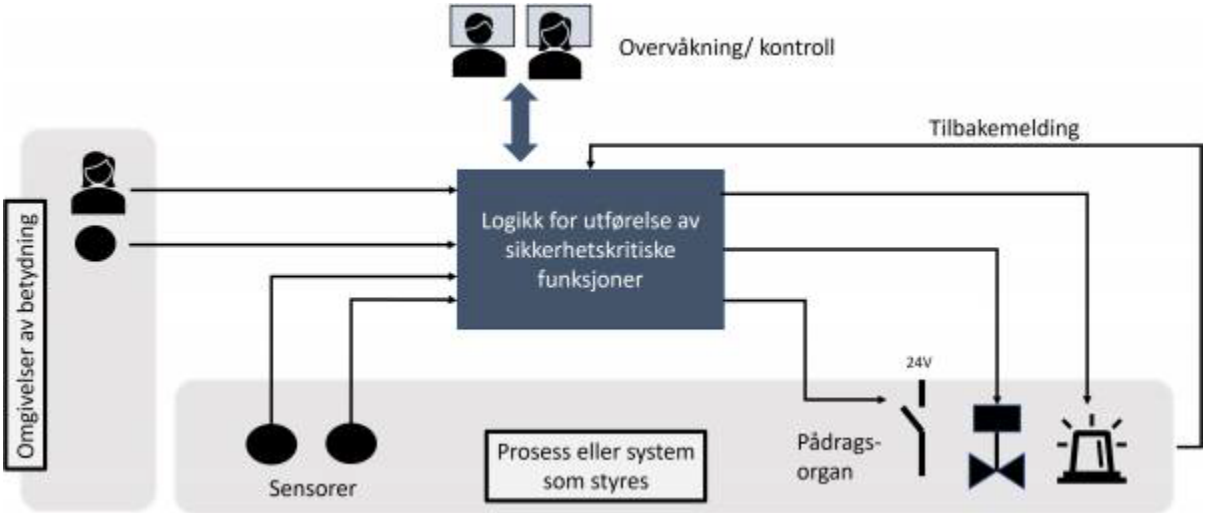
Informasjon om emnet: https://www.itk.ntnu.no/emner/fordypning/TTK2

1 Bakgrunn og motivasjon

På kybernetikkstudiet lærer man å lage styringssystemer for mange ulike anvendelser. Fokus rettes primært mot å få systemene til å virke, og mindre på hva som skal til for at systemene *svikter*. Ei heller er det mye fokus på hvilke ekstra krav og føringer som gjelder for systemer som er sikkerhetskritiske, og der feil kan medføre ulykker og skade på personer og miljø. For eksempel:

- Hvilke krav stilles til spesielt kritiske funksjoner i dynamiske posisjoneringssystemer, slik at man forhindrer eller stanser en situasjon der fartøyet plutselig akselererer mot en kai eller et nærliggende fartøy?
- Hvilke krav stilles til utvikling og oppfølging i drift for å sikre at et nødavstegningssystem er i stand til å fjerne alle usikrede elektriske tennkilder ved en gasslekkasje i et prosessanlegg?

Sentralt for begge disse problemstillingene er gjennomføring av pålitelighetsanalyser.



Sikkerhetssystemer og sikkerhetskritiske funksjoner, som nevnt ovenfor, har til oppgave å oppdage farlige situasjoner og utføre aksjoner som forhindrer ulykker eller begrenser omfanget. Slike sikkerhetsfunksjoner implementeres etter hovedregelen med egne dedikerte sikkerhetskontrollere og instrumentering, uavhengig av reguleringssystemene.

Når sikkerhet er et tema, stiller myndighetene krav til både dem som designer og dem som har fått installert sikkerhetssystemer. Et av disse kravene er å ha kontroll over pålideligheten. Pålitelighetsanalyse er derfor en helt sentral del av designutvikling og bruk av systemer som har betydning for sikkerheten.

Men dere spør dere kanskje: Jaha, men er pålitelighetsanalyse relevant for oss som går på kybernetikk? Min erfaring er at mange med kybernetikkbakgrunn vil ha noe med pålitelighetsanalyse å gjøre. Kanskje skal selskapet ditt oppnå en sertifisering og leie inn eksperter for å utføre de nødvendige pålitelighetsanalysene. Ekspertene vil stille spørsmål om mange detaljer som har betydning for påliteligheten, og de vil levere en rapport der de presenterer resultatene sine. Da er det jo fint å ha en basiskunnskap om hvorfor de spør det de spør, og hva resultatene de presenterer faktisk betyr.

2 Innhold og fokus

I temaet vil vi ha fokus på å lære metoder som ligger nær det industrien bruker for å utføre pålitelighetsanalyser av sikkerhetsfunksjoner. Emnet bygger på tematikk belyst i TTK 4175 Instrumenteringssystemer og sikkerhet, men her tas det grundigere slik at det ikke er en forutsetning å ha gjennomført det nevnte faget: Tema som dekkes er:

- Hva er sikkerhetsfunksjoner innenfor ulike typer anvendelser og hvilke krav stilles til dem? Her bruker vi eksempler som er relevante ut fra deltagernes fokus i fordypningsprosjektet.
- Hvilke mål for pålitelighet brukes for sikkerhetsfunksjoner
- Pålitelighetsanalysemetoder (hver metode blir mest sannsynlig en egen forelesning/seminar) - hva kjennetegner de, hvordan brukes de, og hva er eventuelt forskjellene?:
    - Pålitelighetsblokkskjema
    - Feiltreanalyse (FTA)
    - Markov analyse
- I noen grad også: Pålitelighetsdata – ulike type datakilder. Hva skal/bør en bruke når?

3 Programvare

Pålitelighetsnettverk (seminar 2)	Ikke avhengig av noe programvare. Faglærer viser eventuelt noen eksempler kodet i JupyterLab.

Feiltreanalyse	Vi bruker CARA-FT. Finnes i to varianter, begge utviklet av utviklet av Professor Jørn Vatn (NTNU):
	• Web-basert: Tilgjengelig her https://jvatn.folk.ntnu.no/eLearning/FTA/
	• PC versjon (fungerer ikke på MAC): Kan lastes ned her: https://jvatn.folk.ntnu.no/eLearning/CaraFaultTree/CARAFaultTree.htm
	
	PS: Det er noen «issues» når en kjører den web-baserte versjonen og her er noen nyttige tips:
	
	• Run as «**Inprivate window**» (CTRL+SHIFT+N)
	• As needed: Delete cashed images and files with CTRL+SHIFT+DEL.
	  • For at least 24 hours, or more considering when tool as used last time.
	  • Make sure that all AND and OR gates have unique Ids (must be updated manually when sections of the tree is copied). Refresh page afterwards!
	• For decimals in data entries (basic events): Use «.», not «,»

Markov analyse	Vi bruker en Excel-fil med makroer implementert i Visual Basic. Utviklet av Professor Jørn Vatn (NTNU), med noe involvering i senere tid av professor Mary Ann Lundteigen. Malen kan lastes ned her. https://jvatn.folk.ntnu.no/eLearning/commonFiles/MarkovGeneral.xlsm Merknad 1: Denne excel-filea har innebygget kode, dvs. at denne fila kan utføre spesielle beregninger som ikke finnes i «blanke» Excel-filer. Det er alltid en risiko forbundet med Excel-filer som har innebygget kode eller makroer. En fil som har innebygget kode og/eller makroer betegnes i Excel som en *makrofil*. Slike filer har etternavn .xlsm For å bruke denne fila anbefales at du lagrer den på PC eller Mac på et eget *klarert område*. Se følgende lenke for hvordan du kan opprette et slikt klarert område (gjelder PC): Legge til, fjerne eller endre en klarert plassering i

		Microsoft Office - Støtte for Microsoft Du kan f.eks. lage en mappe under "Dokumenter" som heter NTNU hvor du legger filene du bruker. I "klareringssenteret" sier du at dette er et område du stoler på.
	Merknad 2:	Dersom du har en jobb-PC kan det hende at firmaet du jobber i har svært strenge regler for å laste ned Excel-filer. Dersom du ikke får lastet ned og kjørt makroene i denne fila, anbefales at du kontakter dataansvarlig i firmaet du arbeider i.

4 Tilgang til slides og annet materiale

I utgangspunktet deles alt av materiale og informasjon om tidspunkt for seminarene på:

- Se https://www.itk.ntnu.no/emner/fordypning/ttk2

CANVAS (eller Blackboard) blir ikke benyttet da det ikke lages egne sider for dette for emner, kun for den overordnede emnekoden TTK 4555.

5 Øvingsoppgaver (miniprosjekt)

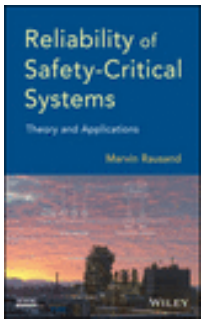
Studentene gjennomfører et miniprosjekt bestående av 5 oppgaver med deloppgaver. Det er disse oppgavene som er utgangspunktet for utspørringen på muntlig eksamen. Jobber dere med disse underveis i semesteret er forberedelsene til muntlig eksamen gjort samtidig. Informasjon om miniprosjektet er beskrevet i en egen fil som publiseres med link fra https://www.itk.ntnu.no/emner/fordypning/ttk2. Det meste av øvrig materiell deles også via herfra.

6 Vurderingsform

Fordypningsemner har muntlig eksamen i slutten av november eller starten av desember. For TTK2 blir utspørringen basert på 5 oppgaver som dere kan jobbe med i løpet av semesteret. Temaer relevant for oppgavene belyses i de enkeltvise seminarene samt ved å lese pensum. Man kan

samarbeide så mye man ønsker i utførelsen av oppgavene, men man er selv ansvarlig for å kunne svare ut alle spørsmål på eksamen, da muntlig eksamen er individuell.

7 Pensum



Pensum er miniprosjektet, med teori i dokumentet er miniprosjektet er presentert, samt slides og utvalgte kapitler i boka «Reliability of Safety-Critical Systems» er tilgjengelig online via ORIS for NTNU-studenter (se nedenfor for detaljer).

Noen kan finne det nyttig å også se gjennom deler av kapittel 6, 8, 9 og 10 i kompendiet for emnet TTK 4175, fordi det utdyper noen temaer som er kortfattet forklart i forbindelse med miniprosjektet. Imidlertid er disse kapitlene ikke oppført som pensum.

Seminar	Hovedtema	Del av pensum	Stikkord for sentrale tema
1 & 2	Introduksjon	2.1-2.8, 3.1-3.5.8	Stikkord: • Funksjonell sikkerhet – functional safety • Instrumentert sikkehetsfunksjon - Safety instrumented function (SIF) • Delsystemer • Redundans og votering • Sentrale begrep knyttet til feilanalyse: Feil/svikt, feilmode, feilårsak • Typer feil – farlige (D – dangerous) vs sikre (S) feil, tilfeldige (random) vs systematiske feil • Deteksjonsmetoder for feil – detektert vs udetektert (DU vs DD feil) • Avhengig feil med felles årsak (“fellesfeil”) - common cause failure (CCF) • Hardware feiltoleranse (HFT) • Operasjonsmodi – mode of operation (low, high, continuous) • Sikker tilstand – safe state • SIF trigger hendelse (demand, demandrate og demand duration) • Integritetsmål for sikkerhet - Safety integrity level (SIL) • Type testing – diagnostikk og funksjonstesting – diagnostics and functional/proof testing

			• Typer pålitelighetsmål - Probability of failrue on demand (PFD), Probability of having a dangerous failure per hour (PFH) • SIF sin rolle for å forhindre ulykker: Farlig hendelse (hazardous event HE), frekvens av farlige hendelser (HEF) og barrierer
2	Pålitelighets-blokkskjema	8.1-8.3.7 10.5	Læringsmål: • Pålitelighetsblokkskjema og kobling til formler for PFD/PFH • Sette opp formler for delsystemer i et SIF med ulik type votering • Beregne pålitelighet. Implementere kode for utvalgte systemer i Python. Stikkord: • Oppetid og nedetid for en SIF • PFD for delsystemer vs PFD for hele SIFen • Parametre som inngår og sentrale antagelser • Inkludering av fellesfeil • Beregne PFD for en SIF delsystem med ulike voteringer • Betydning av ikke å ta med reparasjonstid • Beregne PFH for ulike voteringer • Refleksjon av PFD vs PFH
3	Feiltre	5.3, 8.6	• Feiltre symboler • Feiltre vs RBD • Modellering i feiltre – med og uten fellesfeil (CCF) • Minimale kuttsett • “Upper bound” • Beregne PFD og PFH med feiltre basert på minimale cut • Sammenligne med PFD og FPH utregnet med CARA Fault tree
4	Markov	5.5, 8.7	Markov tilstandsdiagram – hvilke tilstander modelleres inn? • Typer feil man kan velge å inkludere • Typer reparasjon • Demand tilstand og demand varighet (duration) • Farlig hendelsestilstand (HE – hazardous event) • Inkludere fellesfeil • Hva er svikttilstander for delsystemet)? “Steady state” sannsynligheter vs PFD/PFH