#### Oppgavetekst

I en kjemisk prosess blir flere stoff blandet i en reaktor. I denne oppgaven skal vi betrakte rørledningen som forsyner reaktoren med et av disse stoffene. Hvis for mye av stoffet blir tilført blandingen, vil blandingen komme ut av balanse og trykket i reaktoren vil øke. Dette er en kritisk hendelse og et instrumentert sikkerhetssystem (SIS) er derfor installert for å unngå en slik kritisk situasjon. En skisse av sikkerhetssystemet er vist i Figur 1.

Tre strømningsgivere (“Flow transmitters”) er installert i rørledningen. Når minst to av disse oppdager og varsler for høg strømning, sendes et signal til den logiske enheten (“logic solver”) som igjen sender et signal om at de to nedstengningsventilene (“shutdown valves”) i rørledningen skal lukkes. I tillegg er tre trykkgivere (“pressure transmitters”) installert i reaktoren.



Figur 1 Instrumentert sikkerhetssystem (SIS).

Når minst to av disse oppdager og varsler for høgt trykk, sendes et signal til den logiske enheten som igjen gir beskjed om at de to nedstengningsventilene skal lukkes og stoppe tilførselen av stoffet til reaktoren. En ikke-planlagt nedstengning av reaktoren kan lede til farlige situasjoner, og utilsiktet nedstengning (“spurious shutdown”) bør derfor unngås.

De tre strømningsgiverne er av samme type og er, som vist i Figur 1, koplet opp som et 2-av-3 (2oo3) system. De tre trykkgiverne er også av samme type og koplet opp som et 2oo3 system. Den logiske enheten sender et lukkesignal til de to nedstengningsventilene så snart den mottar et signal fra enten strømningsgiverne eller trykkgiverne. Hovedlogikken i den logiske enheten er derfor satt opp som et 1-av-2 (1oo2) system. Det er tilstrekkelig at en av de to nedstengningsventilene, som er av samme type, kan lukkes for å stoppe tilførselen av stoffet til reaktoren. Nedstengningsventilene er da et 1oo2 system. 2oo3 voteringsenhetene for strømnings- og trykkgiverne er fysisk plasser i den logiske enheten selv om de er tegnet som egne enheter i Figur 1.

De to nedstengningsventilene er åpne i normal produksjon og er installert for å stoppe tilførselen av stoffet dersom høg strømning eller høgt trykk er “oppdaget” av giverne. Systemet er et passivt sikkerhetssystem og kritiske feil blir bare oppdaget ved periodisk funksjonstesting (“proof testing”). Hele systemet blir funksjonstestet samtidig etter jevne intervall – med testintervall τ = 6 måneder.

I oppgave 1 og 2 antar vi at alle enheter i systemet er stokastisk uavhengig.

Skriv ned eventuelle ekstra antakelser du må gjøre for å svare på spørsmålene nedenfor.

#### Oppgave 1

1. Tegn pålitelighetsnettverket for hele sikkerhetssystemet med hensyn på systemets hovedfunksjon som sikkerhetsbarriere.
2. Forklar kortfattet hvorfor en 2oo3 konfigurasjon for giverne (“transmitters”) er valgt for dette sikkerhetssystemet (SIS).

Den logiske enheten er ikke i stand til å foreta diagnostisk testing – slik at alle komponentene i systemet bare kan ha to feilmoder: farlige uoppdagede (“dangerous undetected - DU”) feil og sikre (“safe - S”) feil. Tida som går med til periodisk funksjonstesting og mulig reparasjon hvis feil oppdages, oppfattes i første omgang å være neglisjerbar.

Sviktintensitetene (“failure rates”) for de ulike komponentene er gitt i Tabell 1.

Tabell 1 Sviktintensiteter for komponentene i sikkerhetssystemet i Figur 1.

|  |  |  |
| --- | --- | --- |
| Komponent | DU-sviktintensitet (timer-1) | Sikker sviktintensitet (timer-1) |
| Strømningsgiver (FT) | 1.2 ⋅ 10-5 | 1.5 ⋅ 10-5 |
| Trykkgiver (PT) | 1.7 ⋅ 10-5 | 5.0 ⋅ 10-6 |
| Logisk enhet (LS) | 1.5 ⋅ 10-8 | 6.0 ⋅ 10-7 |
| Nedstengningsventil (V) | 2.0 ⋅ 10-6 | 2.5 ⋅ 10-5 |

1. Finn sannsynligheten for feil ved behov (“failure on demand - PFD”) for hver enkelt komponent i sikkerhetssystemet (bruk gjerne tilnærmingsformler)
2. Finn strukturfunksjonen for systemet. Diskuter hvordan du kan lage «moduler», og i hvilken grad du trenger å «multiplisere ut» alle leddene.
3. Finn sannsynligheten for at hele sikkerhetssystemet overlever et testintervall uten at noen typer svikt inntreffer.
4. Finn sannsynligheten for sikkerhetssystemet overlever et testintervall med hensyn på sikkerhetskritisk system-svikt.

#### Oppgave 2

1. Tegn et feiltre for situasjonen i oppgave 1. Definer selv topp-hendelsen slik at du kan sammenligne resultatet fra pålitelighetsnettverket med feiltreanalysen.
2. Finn de minimale kuttmengdene.
3. Finn sannsynligheten for at hele sikkerhetssystemet overlever et testintervall med hensyn på sikkerhetskritisk system-svikt ved å ta utgangspunkt i de minimale kuttmengdene. Sammenlign svaret med oppgave 1f).

#### Oppgave 3

Vi vil nå finne PFD for systemet.

1. Forklar hva som menes med PFD, og hva som menes med PFD(*t*)
2. For å finne PFD vil vi beregne PFD(*t*) for hhv *t* = 1, 3 og 5 måneder. Gjør dette ved å ta utgangspunkt i enten feiltreanalysen eller pålitelighetsnettverket, og finn gjennomsnittsverdien for de tre tidspunktene som et anslag for den totale PFDen.

En annen tilnærming for å finne PFD er å beregne PFD for hvert «system», dvs strømningsgiver, trykkgiver, logisk enhet og nedstengningsventiler.

1. Finn PFD hvor hvert system, og bruk dette til å finne PFD for hele systemet. Sammenlign med oppgave 3b).
2. I oppgave 1c) ble det beregnet PFD-verdier for hver komponent. Hvorfor kan vi ikke sette inn disse verdiene direkte med utgangspunkt i de minimale kuttmengdene?

Strømningsgiverne er utsatt for fellesfeil (“common cause failures - CCF”) med hensyn på DU-feil (CCF-DU) og vi antar at disse kan modelleres ved en beta-faktor modell med betafaktor *β*DU,FT = 0.10. På samme måte er også trykkgiverne utsatt for CCF-DU som også kan modelleres ved en beta-faktor modell med *β*DU,PT = 0.08. Strømningsgiver-delsystemet og trykkgiver-delsystemet antas å være uavhengige. De to nedstengningsventilene er også utsatt for CCF-DU som kan modelleres ved en beta-faktor modell med *β*DU,V = 0.20.

1. Forklar hva som menes med betafaktormodellen, og oppdater PFD-beregningene når du tar med fellesfeil.

#### Oppgave 4

Når den logiske enheten mottar et enkelt signal om høg strømning eller høgt trykk fra en giver, blir kontrollrommet varslet og en reparatør blir sendt til reaktoren for å kontrollere og rette opp feilen. Når det er et falskt sikkert signal (S-feil), trenger reparatøren i gjennomsnitt 24 timer på å finne og reparere feilen. For å forenkle analysen vil vi kun se på trykkgiverne. Vi antar at S-feilene er stokastisk uavhengig av hverandre.

1. Finn antall timer per år systemet er nede pga S-feil som følge av svikt i trykkgiverne.
2. Finn den totale frekvensen av S-feil som følge av svikt i trykkgiverne

#### Oppgave 5

Vi har så langt kun betraktet farlige uoppdagede (DU) feil. For strømnings- og trykkgiverne finnes også mulighet for såkalt «selvtest». Slike selvtester kan utføres med korte tidsintervaller, slik at farlige feil som kan oppdages ved en selvtest i praksis oppdages umiddelbart. Slike feil kalles farlige oppdagede feil (dangerous detected, DD). Når en farlig feil oppdages, tar det i snitt 24 timer å finne og reparere feilen.

For å forenkle analysen vil vi kun se på trykkgiverne. Vi antar at raten av farlige oppdagede feil er ti ganger høyere enn farlige uoppdagede feil gitt i Tabell 1. Videre vil vi forenkle å betrakte et 1-av-2 (1oo2) system av trykkgivere i motsetning til 2oo3 systemet vi har analysert til nå.

Vi vil benytte Markov-analyse til å analysere 1oo2 systemet hvor vi ser bort fra fellesfeil.

1. Finn PFD-bidraget fra DU-feilene ved å benytte en Markovmodell, hvor du ser bort fra DD-feilene.
2. Finn PFD-bidraget fra DD-feilene ved å benytte en Markovmodell, hvor du ser bort fra DU-feilene.
3. Finn den totale PFDen ved å lage en felles Markovmodell for DD- og DU-feil. Du kan her anta at dersom en trykkgiver har en DU-feil, kan en DD-svikt ikke inntreffe, og tilsvarende dersom en trykkgiver har en DD-feil, kan en DU-svikt ikke inntreffe. Det betyr at du i Markovmodellen har 6 tilstander: 0DD/0DU, 1DD/0DU, 0DD/1DU, 1DD/1DU, 2DD/0DU, 0DD/2DU. Hvorfor blir PFD nå større enn summen av PFD for a) og b).