Repetisjon – Pålitelighet

Jørn Vatn, Institutt for maskinteknikk og produksjon, NTNU. September 2025.

Ved å gå gjennom notatet er man godt forberedt dersom det kommer oppgaver på pålitelighet. Merk at notatet dekker mer enn det vi fikk tid til på forelesningene. På eksamen vil det kun bli spurt om det som ble gjennomgått på forelesningene.

Begreper og definisjoner

Def: Pålitelighet = En enhets evne til å utføre en påkrevd funksjon, under gitte miljø- og operasjonelle betingelser for en gitt tidsperiode

Kommentar: Fokus er å yte en funksjon. En enhet kan ha flere funksjoner.

Def: **Svikt** (failure) = Opphør av mulighet til å utføre krevd funksjon

Def: **Feil** (fault) = Tilstanden at evnen til å utføre krevd funksjon er opphørt

Def: **Feilmode** (failure mode) = effekten av en svikt slik den observeres på enheten som har sviktet (sett utenfra, dvs relativt til funksjonen den skal utføre)

Def: **Feilmekanisme** = fysiske, kjemiske eller andre prosesser som forringer enheten, og leder til svikt

Def: Tid til svikt (TTF = Time-To-Failure) = Tiden fra en enhet settes i drift til den svikter.

Tid til svikt er en tilfeldig størrelse. Ofte benyttes symbolet T om tid til svikt. Viktige begrep:

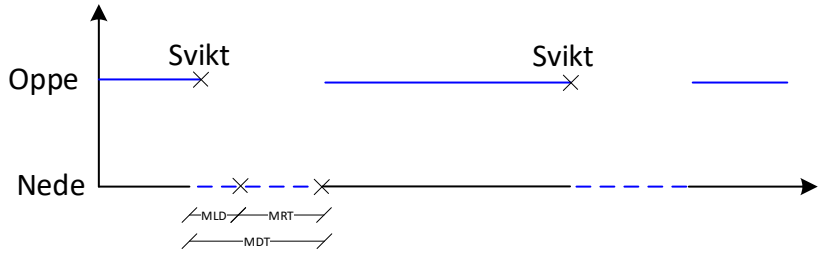
- **Fordelingsfunksjon**, $F(t) = \Pr(T \leq t)$ = Sannsynlighet for at enheten svikter før tidspunkt *t*. F eks $F(8760) = \Pr(T \leq 8760) = 0{,}1$ betyr at det er 10% sjanse for at enheten svikter før ett år er gått (*t* = 8760).

- **Overlevelsessannsynligheten**, $R(t) = \Pr(T > t) = 1 - F(t)$ angir sannsynligheten for at enheten overlever tid t. F eks $R(8760) = \Pr(T > 8760) = 0{,}9$ betyr at det er 90% sjanse for at enheten overlever ett år ($t = 8760$) etter at den er satt i drift.
- **Sviktintensitet** $z(t)$ angir sannsynligheten for at en enhet med alder t og som fortsatt fungerer, svikter i et lite tidsintervall (sannsynligheten divideres med lengden av intervallet). Ofte betegnes sviktintensiteten for (den lokale) badekarskurven.
- **Midlere tid til svikt** (Mean Time To Failure), $\mathrm{MTTF} = \mathrm{E}(T)$ (Bokstave E står for «Expected»)

Def: **Midlere nedetid** (MDT = Mean Down Time) = Forventet tid det tar fra en enhet svikter, til den er ferdig reparert, og satt i drift.

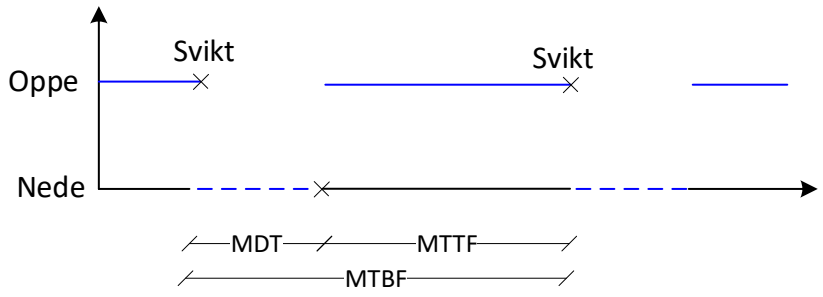
Def: **Midlere logistisk forsinkelse** (MLD = Mean Logistic Dealy) = Forventet tid fra en svikt inntreffer til man kan starte aktiv reparasjon, dvs vente på deler, rykke ut, feildiagnostisering osv.

Def: **Midlere (aktiv) reparasjonstid** (MRT = Mean Repair Time) = Forventet tid det tar å utføre reparasjonen etter at en svikt har inntruffet.



Vi har at: $\mathrm{MDT} = \mathrm{MLD} + \mathrm{MRT}$

Def: **Midlere tid mellom svikt** (MTBF = Mean Time Between Failure) = Midlere tid mellom en enhet svikter til den svikter neste gang. $\mathrm{MTBF} = \mathrm{MTTF} + \mathrm{MDT}$.



For enheter som svikter, blir reparert til så god som ny, for deretter å svikte igjen osv, innfører vi begrepet utilgjengelighet (U = Unavailability). Utilgjengeligheten er det samme som sannsynligheten for at enheten ikke virker på et vilkårlig tidspunkt. Formel for U (som må huskes) er:

$$U = \mathrm{MDT}/(\mathrm{MTTF}+\mathrm{MDT}) \qquad (1)$$

Merk at både MDT og MTTF påvirkes av mange forhold, f eks mengden forebyggende vedlikehold, antall reservedeler på lager, beredskap osv. I ligning (1) må vi derfor sette inn MDT og MTTF verdier som representerer status på disse forhold. Ofte benyttes symbolet $\mathrm{MTTF_E}$ for å angi den *effektive midlere tid til svikt* med et gitt forebyggende vedlikehold. $\mathrm{MTTF_E}$ er betydelig større enn MTTF uten vedlikehold, som betegnes $\mathrm{MTTF_N}$, N = "Naked". I dette kurset har vi ikke presentert metoder for å beregne effektiv MTTF som funksjon av hvilket vedlikehold vi gjør. MTTF-verdiene vi kan estimerer fra data vi henter ut fra vedlikeholdsstyringssystemet (f eks SAP) vil gjenspeile gjeldende vedlikeholdsstrategi. Det er viktig å kunne si noe om hvordan MTTF-verdien vil påvirkes av en endringer i vedlikeholdet, men dette er ikke et tema i dette kurset.

For enheter som har skjult funksjon kan man foreta en funksjonstest for å avdekke skjult feil(tilstand). Ofte er tid det tar å reparere en slik enhet mye kortere enn tid mellom funksjonstest. Dersom tid mellom funksjonstest betegnes τ og enheten har konstant sviktintensitet = $\lambda = 1/\mathrm{MTTF}$ kan vi finne utilgjengeligheten ved:

$$U = \lambda\tau/2 = \tau/(2\cdot\mathrm{MTTF}) \qquad (2)$$

I denne situasjonen er det vanlig å bruke betegnelsen PFD i stedet for utilgjengelighet. PFD står for probability of failure on demand, og oversettes til norsk som sannsynligheten for at enheten ikke er tilgjengelig ved en forespørsel.

☐ Jeg husker ligning (1), eller kan resonere meg fram til den (fra en figur jeg tegner)

☐ Jeg satser på at ligning (2) blir oppgitt på eksamen, men jeg vet hvordan jeg bruker ligningen.

☐ Jeg forstår de viktigste begrepene, og kan spesielt redegjøre for MTTF, MDT og sviktintensitet («badekarskurven»)

Levetidsfordelinger

For å beskrive levetider (tid til svikt) benyttes ofte ulike klasser av levetidsfordelinger. De vanligste er:

- *Eksponensialfordelingen*. Denne karakteriseres ved at sviktintensiteten er konstant, dvs $z(t) = \lambda$. For eksponensialfordelingen gjelder at en gammel komponent statistisk sette er like god som en ny komponent. Eksponensialfordelingen er den enkleste fordelingen å jobbe med, og benyttes derfor ofte som en forenkling. For komponenter som er underlagt et forebyggende vedlikeholdsprogram kan eksponensialfordelingen være en rimelig tilnærming. For eksponensialfordelingen er overlevelsessannsynligheten lik $R(t) = \mathrm{e}^{-\lambda t}$, og sviktintensiteten er $z(t)$ = konstant.
- *Weibulfordelingen*. Denne fordelingen er ofte benyttet dersom sviktintensiteten øker.

 Jeg kan redegjøre for hvorfor det ikke har noen hensikt å foreta forebyggende utskifting av komponenter hvor tid til svikt kan beskrives ved eksponensialfordelte.

FMEA/FMECA - Kritikalitetsanalyse

Feilmode og effektanalyse (FMEA) og Feilmode, effekt og kritikalitetsanalyse (FMECA) er metoder for å:

- Identifisere de mulige feiltilstandene (feilmodene) til hver enkelt komponent i et teknisk system,
- Bestemme årsakene til feiltilstandene, samt
- Bestemme feiltilstandens innvirkning på systemet som helhet
- Bestemme alvorligheten av de ulike feileffektene

I systemanalysen deles systemet inn i delsystemer som analyseres separat. Et funksjonsdiagram viser hvordan delsystemene henger sammen og for hvert delsystem identifiseres alle komponenter. FMEA/FMECA skjemaet fylles ut med basis i komponentene.

Selve skjemaet består av fire hovedblokker:

1. Beskrivelse av komponenten (ID, operasjonell tilstand og funksjon)
2. Beskrivelse av feilmoder knyttet til hver funksjon (dvs det kan være flere rader per funksjon)
3. Beskrivelse av effekt av feilen
4. Tilleggsinformasjon i form av frekvens/sannsynlighet, tydeliggjøring av konsekvenser, feilårsaker, feilmekanismer osv

Dersom vi tar med «C»'en i FMECA vil analysen også være en *kritikalitetsanalyse*. Kritikalitetsklassifisering av feilmoder (og tilhørende utstyr) er viktig for å:

- Etablere et grunnlag for et forebyggende vedlikeholdsprogram
- Bestemme behov for reservedeler
- Bestemme behov for beredskap og tid for sikkerhetskritisk feil må utbedres
- Avgjøre hva som er *sikkerhetskritisk* etterslep

Kritikalitetsklassifisering bør inneholde både *sannsynligheten* for svikt og *konsekvensen* dersom en svikt inntreffer. I noen få sammenhenger er det kun konsekvensen som er avgjørende, f eks når man skal vurderer tid til utbedring og hva som er sikkerhetskritisk etterslep i korrigerende vedlikehold. Det er vanskelig å fange alle forhold som påvirker kritikaliteten i en analyse, f eks kompetansekrav til operatører og driftspersonell.

Ut over disse generelle betraktningene diskuterte vi ikke FMEA/FMECA på kurset.

Strukturfunksjon og pålitelighetsblokkdiagram

For *binære* systemer innfører vi to typer tilstandsvariable (et binært system er et system hvor komponentene kun antar to verdier (fungerer eller i feiltilstand), og systemet også har kun to tilstander (fungerer eller i feiltilstand)). En tilstandsvariabel innføres for komponentene, og en for systemet. For komponent nummer *i* setter vi $x_i = 1$ dersom komponenten fungerer og 0 ellers. For systemet setter vi $\phi(\mathbf{x}) = 1$ om systemet fungerer, og 0 ellers. ϕ betegnes *strukturfunksjonen*, og er en funksjon av tilstanden

til komponentene. $\mathbf{x}$ er en vektor av *x*-ene. Matematisk benytter vi ofte tallverdier for indeksen, mens for et konkret system, benytter vi forkortelser, f eks x_{Pu} er tilstandsvariabelen for en pumpe.

For å illustrere funksjonaliteten til et system tegnes ofte et pålitelighetsblokkdiagram (RBD = Reliability Block Diagram). Diagrammet synliggjør hvordan det er mulig å gå fra venstre gjennom fungerende komponenter og komme helt til høyre i diagrammet.

For å etablere strukturfunksjonen til et pålitelighetsblokkdiagram tar vi ofte utgangspunkt i de to basisreglene som gjelder for serie- og parallellstrukturer. Dvs for en seriestruktur av *n* komponenter gjelder at

$$\phi(\mathbf{x}) = x_1 \cdot x_2 \cdot \ldots \cdot x_n \qquad (3)$$

og tilsvarende for en parallellstruktur (redundans) gjelder:

$$\phi(\mathbf{x}) = 1-(1-x_1)(1-x_2)\ldots(1-x_n) \qquad (4)$$

Merk at ligning (4) kan forenkles om vi kun har to komponenter ($n = 2$)

$$\phi(\mathbf{x}) = 1-(1-x_1)(1-x_2) = x_1 + x_2 - x_1x_2 \qquad (5)$$

For å jobbe med strukturfunksjonen er det viktig å beherske reglene for parentesregning. Når vi skal multiplisere to parentesuttrykk med hverandre er regelen at vi for det første parentesuttrykket systematisk går gjennom alle ledd, og for hvert lett multipliserer vi med hvert ledd i det andre uttrykket og legger sammen etter hvert. Her må vi huske på reglene for pluss og minus. ” + · + = +”, ” ÷ · ÷ = +”, ” + · ÷ = ÷”¸ og ” ÷ · + = ÷”. Eksempel $(3a+4)(2b-3) = 3a\cdot 2b + 3a\cdot(-3) + 4\cdot 2b + 4\cdot(-3) = 6ab - 9a + 8b - 12.$

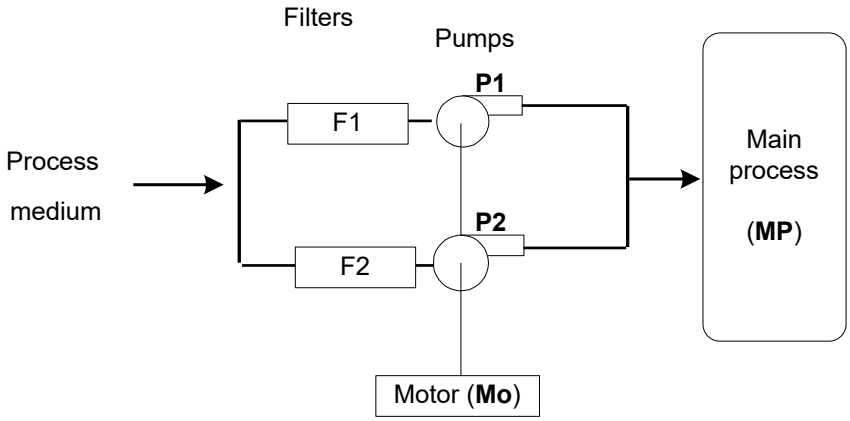
☐ Jeg husker formlene for serie- og parallellstrukturer

☐ Jeg kan finne moduler, og bruke reglene for serie- og parallellstrukturer

For sammensatte strukturer kan vi lage moduler av delstrukturer. Reglene for serie- og parallellstrukturer gjelder også om noen komponenter er «moduler». Se eksemplet som følger senere.

Strukturfunksjonen er en deterministisk funksjon (dvs uten sannsynligheter). Vi er ofte interessert i å finne påliteligheten til et system representert ved et pålitelighetsblokkdiagram. Vi benytter symbolet p_S for påliteligheten til et system (dvs sannsynligheten for at systemet fungerer). Noen ganger ønsker vi å understreke at påliteligheten er en funksjon av komponentpålitelighetene, og skriver da $p_S = h(\mathbf{p})$, hvor $\mathbf{p}$ er en vektor av komponentpålitelighetene. Sammenhengen mellom p_S og pålitelighetene kommer vi tilbake til.

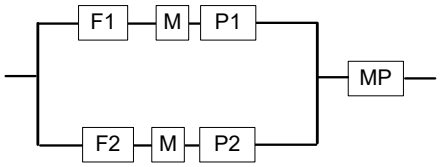
Nedenfor følger en «kokebok» i 7 punkter som viser hovedgangen i analyse ved bruk av pålitelighetsblokkdiagram. Kokeboken er supplert med et eksempel. Dette eksemplet er litt mer komplisert enn hva du kan forvente på eksamen.



Figur 1 Skisse av prosess-system med pumper

1 - "Oversett" fysisk system til pålitelighetsblokkdiagram

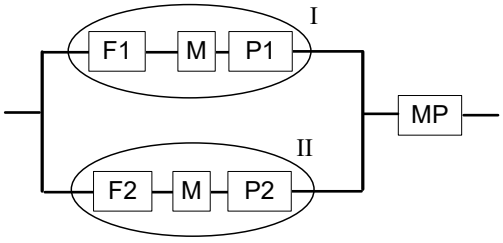
Beskrivelsen av det fysiske systemet kan være som følger. Prosessmediet pumpes ved hjelp av to redundante pumper inn i en tank der den kjemiske hovedprosessen foregår. Hver pumpe har et eget filter (sil) for å skille ut grovpartikler. Pumpene drives av en felles motor.



Figur 2 Pålitelighetsblokkdiagram

2 - Finn strukturfunksjonen

Dvs finn $\phi(\mathbf{x})$, som funksjon av x-ene ved å sette sammen resultat for serie- og parallellstrukturer



Figur 3 Strukturfunksjon med moduler

For den øverste grenen får vi for modul I

$\phi_I(\mathbf{x}) = x_{F1}x_{P1}x_{Mo}$

For den nederste grenen får vi for modul II

$\phi_{II}(\mathbf{x}) = x_{F2}x_{P2}x_{Mo}$

Disse to grenene settes sammen med reglene for parallellstruktur, og så multipliserer vi uttrykket med x_{MP} for hovedprosessen som ligger i serie:

$\phi(\mathbf{x}) = (1-(1-x_{F1}x_{P1}x_{Mo})(1-x_{F2}x_{P2}x_{Mo}))x_{MP}$

3 - Multipliser ut strukturfunksjonen (løse opp parenteser)

$\phi(\mathbf{x}) = x_{F1}x_{P1}x_{Mo}x_{MP} + x_{F2}x_{P2}x_{Mo}x_{MP} - x_{F1}x_{F2}x_{P1}x_{P2}x_{Mo}^2x_{MP}$

4 - Stryk potenser i x-ene

Vi ser at for motoren har vi en potens i uttrykket, og den stryker vi fordi vi alltid kan og skal stryke potenser for *binære* variable. Vi får da til slutt:

$\phi(\mathbf{x}) = x_{F1}x_{P1}x_{Mo}x_{MP}+x_{F2}x_{P2}x_{Mo}x_{MP}-x_{F1}x_{F2}x_{P1}x_{P2}x_{Mo}x_{MP}$

5 - Finn p_i-ene ved formler for tilgjengelighet

Følgende pålitelighetsparametere antas. Kolonne 2-3 er data som ofte oppgitt, mens kolonne 4-5 er beregnet. Vi trenger spesielt p her.

Komponent	MTTF	MDT	$U = q$ = MDT/(MDT+MTTF)	p=1-U
P1 /P2	1460	16	0,01084	0,98916
F1 /F2	1460	4	0,00273	0,99727
Mo	17520	24	0,00137	0,99863
MP	26280	48	0,00182	0,99818

6 - Bytt ut x-ene med p-er i strukturfunksjonen for å finne systemtilgjengeligheten $p_S = h(\mathrm{p})$

$p_S = h(\mathbf{p}) = p_{F1}p_{P1}p_{Mo}p_{MP}+p_{F2}p_{P2}p_{Mo}p_{MP}-p_{F1}p_{F2}p_{P1}p_{P2}p_{Mo}p_{MP} = 0{,}9966297$

□ Jeg forstår gangen i en pålitelighetsblokkdiagramanalyse

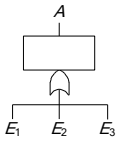
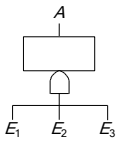
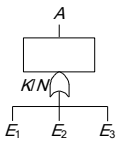
□ Jeg har trening i å løse ut parenteser, og stryke potenser

□ Når jeg har gjort dette, kan jeg finne påliteligheten ved å bytte ut x-ene med p-er og sette inn tallverdier

Feiltreanalyse (FTA = Fault Tree Analysis)

Et feiltre er et logisk diagram som illustrerer sammenhengen mellom en uønsket hendelse i et system og årsakene til denne hendelsen

For å konstruere et feiltre benytter vi følgende symboltyper:

	SYMBOL	BESKRIVELSE
LOGISKE PORTER	"ELLER" port 	ELLER-porten indikerer at utgangshendelsen *A* inntreffer hvis minst en av inngangshendelsene E_i inntreffer.
	"OG" port 	OG-porten indikerer at utgangshendelsen *A* inntreffer hvis alle inngangshendelsene E_i inntreffer.
	"KooN" port 	KooN-porten indikerer at utgangshendelsen *A* inntreffer hvis K eller flere av inngangshendelsene E_i inntreffer.
	"Basis"-hendelse 	Symbol for komponent i primær feiltilstand, oppstått under normal drift.

Gangen i en feiltreanalyse er i hovedtrekk:

1. Definisjon av problem og randbetingelser
2. Konstruksjon av feiltreet
3. Bestemmelse av minimale kutt- og stimengder
4. Kvalitativ analyse av feiltreet
5. Kvantitativ analyse av feiltreet

I dette kurset introduserte vi kun feiltre som en alternativ metode til pålitelighetsblokkdiagram for å beregne upålitelighet og pålitelighet til systemer. Det kan være greit å vite om at feiltreanalysen er en tilgjengelige analyse, men detaljene her er ikke pensum i dette kurset.

Hendelsestreanalyse (ETA = Event Tree Analysis)

I en hendelsestreanalyse modellerer vi mulige hendelsesforløp etter at en uønsket hendelse har inntruffet. Hendelsesforløpet illustreres grafisk, hvor vi tar inn tidsaskepktet, avhengigheter og dominoeffekter. Resultater fra en hendelsestreanalyse er:

- Kvalitativ beskrivelse av hendelsesscenariene
- Kvantitativ beregning av frekvenser for hver av slutthendelsene
- Anbefalte risiokreduserende tiltak
- Kvantitativ beregning av effekt av tiltak

Hendelsestreanalyse er heller ikke aktuelt for eksamen, men det er viktig å vite at slike analyser er mye benyttet når vi analyserer risiko. Da er vi opptatt av å se hva som kan skje etter en uønsket hendelse, og analysen hjelper oss i å forstå hvilke sikkerhetsbarrierer vi har, og effekten av disse.

RCM - Reliability Centred Maintenance

RCM er primært en metode for å etablere et forebyggende vedlikeholdsprogram. Metoden er sporbar, slik at man forholdsvis enkelt kan justere vedlikeholdsprogrammet ved endring av forutsetninger. Det er ikke noe standardoppsett for RCM, men følgende trinn kan være en naturlig start:

1. Forberedelser
2. Valg av system, systemavgrensninger
3. Funksjonell feilanalyse (FFA)
4. Utvelgelse av kritiske enheter (MSI)
5. Datainnsamling og analyse
6. Feilmode og effekt analyse (FMEA/FMECA)
7. Bestemmelse av vedlikeholdsaktiviteter (RCM-logikk)
8. Intervalloptimalisering
9. Kontinuerlig oppdatering - RCM prosessen

I sesjonen jeg hadde ble RCM ikke diskutert.

HAZOP - Hazard and Operability Analsysis

HAZOP ble kun introdusert i form av noen korte beskrivelser. Selv om det neppe kommer til eksamen, kan det likevel være lurt å kjenne hovedelementene i analysen. En HAZOP utføres vanligvis i prosjekteringsfasen av et *prosessanlegg.* I en slik fase er fokus på det *tekniske systemet*. Metoden kan også benyttes for andre faser, f eks vedlikehold. Da er ofte fokus knyttet til feil ved gjennomføring av *oppgaver*. Et viktig element i HAZOP-analysene er idé-dugnad (”brainstorming”). Prosessen styres av *ledeord*, og *prosessparametere*.

Ledeord	Mening
Ingen	Benektelse av formålet
Mindre	Kvantitativ minking
Mer	Kvantitativ økning
Del av	Kvalitativ minking
Motsatt	Motsatt av formålet
Andre enn	Fullstendig substitusjon

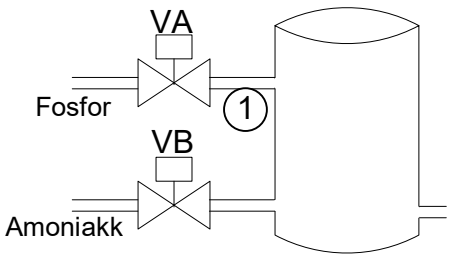
Ledeordene kombineres med prosessparametere (trykk, temperatur, flyt osv), f eks

Ledeord + prosessparameter	Avvik (faresituasjon)	Konsekvens
Ingen & Strøm	Ingen strøm	uttørking
Mer & Strøm	Mer strøm	oversvømmelse
Mer & Trykk	Mer trykk	overtrykk

Viktige trinn i prosessen:

1. Del systemet inn i spesifikke punkter (tar ofte utgangspunkt i tegninger, f eks P&ID)
2. Repiter for alle punkter
    a. Kombinasjon av ledeord og parameter ==> avvik
    b. For hvert avvik vurderes
        i. konsekvens
        ii. årsak (er)
        iii. forslag til løsning
3. Dokumenter resultatene

Eksempel på resultat hvor vi har en tank som får tilførsel av ammoniakk og fosfor:



Figur 4 Eksempel på system som analyseres med HAZOP

Ledeord	Avvik	Konsekvenser	Årsaker	Foreslått løsning
Ingen	Ingen strøm-ning	Overskudd av ammoniakk i reaktor. Utslipp til arbeidsområde.	1. Ventil A feiler til/i lukket tilstand 2. Fosforsyrelageret er tomt. 3. Tett rør, sprekk i røret	Automatisk lukking av ventil B ved tap av strøm fra fosforsyrelageret
Mindre	Mindre strøm-ning	Overskudd av ammoniakk i reaktor. Utslipp til arbeidsområde. Finn ut mer	1. Ventil A delvis lukket. 2. Delvis tett, eller lekkasje i rør	Automatisk lukking av ventil B ved tap av/redusert strøm fra fosforsyrelageret. Settpunkt bestemmes av giftighet og strømningsberegninger.
Mer	Mer strømning	Overskudd av fosforsyre. Ingen fare i arbeidsområdet		

Som det fremgår av analysen er HAZOP egnet til å studere prosessforstyrrelser som følge av tekniske svikt.