

WCM repetisjon – Sikkerhet, pålitelighet og vedlikehold

Jørn Vatn, Institutt for maskinteknikk og produksjon, NTNU. Oktober 2017.

Ved å gå gjennom notatet er man godt forberedt til den mer kvantitative delen av eksamen i WCM. Notatet dekker ikke alle aspekter diskutert på Storefjell, men det aller viktigste mht eksamen er tatt med her. Det er også noen avkrysningsspørsmål for å sjekke at det viktigste er forstått. Hver enkelt kan huke av etter som det jobbes med notatet.

En liste av forkortelser og viktige symboler er gitt til slutt i notatet.

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 forringere 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 størrrelse. Ofte benyttes symbolet T . 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** $\lambda(t)$ 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), $MTTF = E(T)$

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

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

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

Vi har at: $MDT = MLD + MRT$

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

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

$$U = \frac{MDT}{MTTF + MDT} \quad (1)$$

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 $MTTF_E$ for å angi den *effektive feilraten* med et gitt forebyggende vedlikehold. $MTTF_E$ er betydelig større enn $MTTF$ uten vedlikehold (betegnes ofte $MTTF_N$, $N = \text{"Naked"}$)

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 = $\lambda = 1/MTTF$ kan vi finne utilgjengeligheten ved:

$$U = \lambda\tau/2 \quad (2)$$

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 («den lokale badekarskurven»)

Levetidsfordelinger

For å beskrive levetider benyttes ofte ulike klasser av levetidsfordelinger. De vanligste er:

- *Eksponensialfordelingen*. Denne karakteriseres ved at sviktintensiteten er konstant, dvs $\lambda(t) = \lambda$. For eksponensialfordelingen gjelder at en gammel komponent statistisk sett 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 viktintensiteten = $\lambda(t) = \lambda =$ konstant. Overlevelsessannsynligheten er $R(t) = e^{-\lambda t}$.
- *Weibullfordelingen*. Denne fordelingen er ofte benyttet dersom sviktintensiteten øker. Formen på sviktintensiteten er $\lambda(t) \propto t^{\alpha-1}$ (\propto er proporsjonalitetssymbolet). α er aldringsparameteren. For enheter som blir dårligere med alderen (økt sviktintensitet) vil α være større enn 1. Typiske verdier er i området 2-4.

- Jeg kan redegjøre for hvorfor det ikke har noen hensikt å foreta forebyggende utskifting av komponenter med eksponensialfordelte svikttider.
- Dersom jeg kjenner feilraten i eksponensialfordelingen kan jeg beregne overlevelsessannsynligheten. F eks dersom $\lambda = 0.1$, og $t = 3$ er $R(t=3) = e^{-\lambda t} = e^{-0.3} \approx 0.74$.
- For Weibullfordelingen vet jeg at dersom aldringsparameteren er > 1 har vi økende sviktintensitet.

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.

NORSOK-Z008 er en standard for olje- og gassvirksomheten som støtter opp under kritikalitetsklassifisering.

- Jeg skjønner hovedtrekkene i FMEA/FMECA og kan resonere meg fram til fornuftige kolonner
- Jeg vet hvilke faktorer som bør inngå i et kritikalitetsmål, og vet hva et slikt mål kan benyttes til

Strukturfunksjon og pålitelighetsblokkdiagram

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

Ofte er vi kun interessert i å se på den funksjonelle sammenhengen mellom strukturfunksjonen og komponenttilstandene, og da dropper vi ofte symbolet t .

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

$$\phi(\mathbf{x}) = x_1 \cdot x_2 \cdot \dots \cdot x_n \quad (3)$$

og tilsvarende for en parallellstruktur (redundans) gjelder:

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

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

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

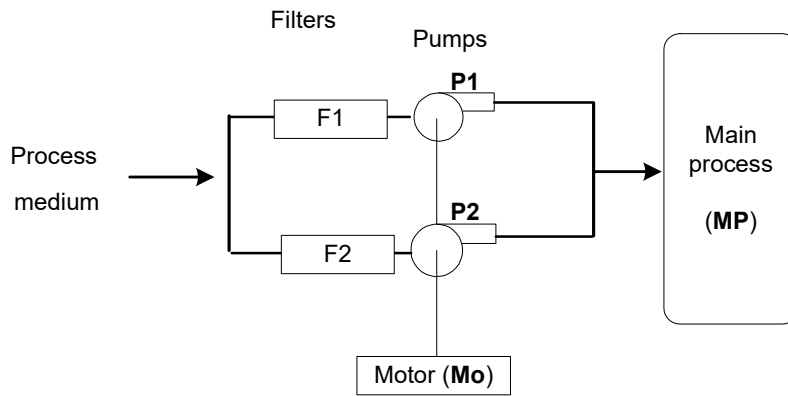
For å jobbe med strukturfunksjonen er det viktig å beherske reglene for parentesregning. Når vi skal multiplisere to parentesuttrykk med hverandre er regelen at vi for det første parentesuttrykket systematisk går gjennom alle ledd, og for hvert ledd multipliserer vi med hvert ledd i det andre uttrykket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

- 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 pålitelighetsblokkdiagram. Vi benytter symbolet ps 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 $ps = h(\mathbf{p})$, hvor \mathbf{p} er en vektor av komponentpålitelighetene.

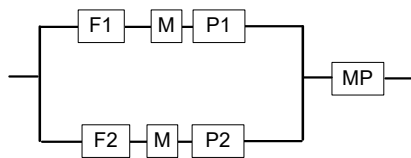
Nedenfor følger en "kokebok" i 7 punkter som viser hovedgangen i analyse ved bruk av pålitelighetsblokkdiagram. Kokeboken er supplert med et eksempel.



Figur 1 Skisse av prosess-system med pumper

1 - "Oversett" fysisk system til pålitelighetsblokkdiagram

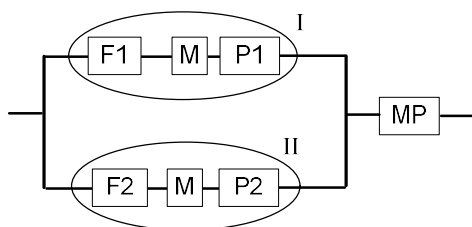
Beskrivelsen av det fysiske systemet kan være som følger. Prosessmediet pumpes ved hjelp av to redundante pumper inn i en tank der den kjemiske hovedprosessen foregår. Hver pumpe har et eget filter (sil) for å skille ut grovpartikler. Pumpene drives av en felles motor.



Figur 2 Pålitelighetsblokkdiagram

2 - Finn strukturefunksjonen

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

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

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 | $q = \text{MDT}/(\text{MDT} + \text{MTTF})$ | $p = 1 - U$ |
|-----------|-------|-----|---|-------------|
| 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 $p_S = h(\mathbf{p})$

$$p_S = h(\mathbf{p}) = p_{F1}p_{P1}p_{Mo}p_{MP} + p_{F2}p_{P2}p_{Mo}p_{MP} - p_{F1}p_{F2}p_{P1}p_{P2}p_{Mo}p_{MP} = 0.9966297$$

7 - Viktigheten av komponent nr i finnes ved å derivere systempåliteligheten mhp p_i

For å finne viktigheten av en komponent kan man se hvor mye systempåliteligheten vil bedre seg dersom vi bedrer komponentpåliteligheten marginalt. Dette betyr i matematiske termer å derivere systempåliteligheten $p_S = h(\mathbf{p})$ mht p_i . Dvs

$$I^B(j) = \partial h(\mathbf{p}) / \partial p_j$$

(6)

(Dette målet betegnes Birnbaums mål for pålitelighetsmessig betydning)

Dette gir for eksemplet:

$$I^B(P1) = p_{F1}p_{Mo}p_{MP} - p_{F1}p_{F2}p_{P2}p_{Mo}p_{MP} = 0.0134604$$

$$I^B(P2) = p_{F2}p_{Mo}p_{MP} - p_{F1}p_{F2}p_{P1}p_{Mo}p_{MP} = 0.0134604$$

$$I^B(F1) = p_{P1}p_{Mo}p_{MP} - p_{F2}p_{P1}p_{P2}p_{Mo}p_{MP} = 0.0133509$$

$$I^B(F2) = p_{P2}p_{Mo}p_{MP} - p_{F1}p_{P1}p_{P2}p_{Mo}p_{MP} = 0.0133509$$

$$I^B(Mo) = p_{F1}p_{P1}p_{MP} + p_{F2}p_{P2}p_{MP} - p_{F1}p_{F2}p_{P1}p_{P2}p_{MP} = 0.9979969$$

$$I^B(MP) = p_{F1}p_{P1}p_{Mo} + p_{F2}p_{P2}p_{Mo} - p_{F1}p_{F2}p_{P1}p_{P2}p_{Mo} = 0.9984468$$

Dette viser følgende:

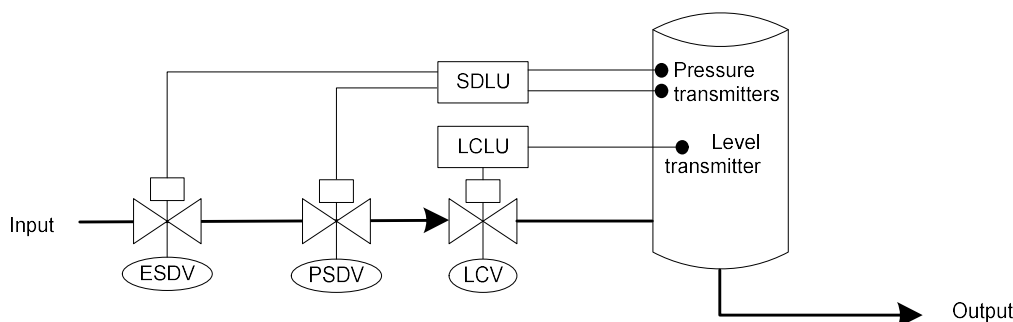
Komponenter i serie er viktigere enn komponenter i parallell (høyere verdier). Merk at motoren egentlig er i serie, selv om vi har vist den i begge grenene i parallellstrukturen. For komponenter som ligger i serie slik at en komponentsvikt alltid gir systemsvikt, gjelder at den komponenten med lavest pålitelighet den viktigste. F eks er MP viktigere enn Mo fordi MP har lavere pålitelighet. For komponenter som er i parallell, er den komponenten som har høyest pålitelighet den viktigste.

Merk at det er lite sannsynlig at mål for viktighet (Birnbaum) kommer på eksamen.

- 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

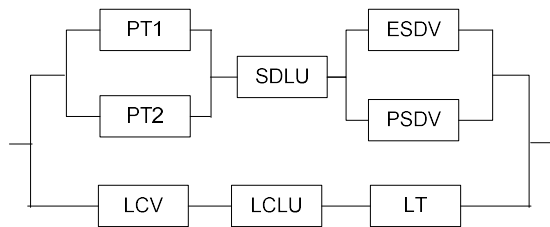
Hvilken systemfunksjon betraktes?

Betrakt følgende system:



Det primære kontrollsystemet består av en nivåventil (LCV), en logisk enhet (LCLU), og en nivåtransmitter (Level transmitter=LT). I tilfelle dette systemet feiler å regulere prosessen, vil et nedstengingssystem forsøke å stenge input. Nedstengingssystemet består av to redundante trykktransmittere (Pressure transmitters = PT), en kontrollenhet (SDLU), og to redundante ventiler (ESDV og PSDV).

Dersom vi betrakter systemets funksjon å *sørge for at trykk i tanken ikke blir for høyt*, kan vi lage følgende pålitelighetsblokkdiagram:

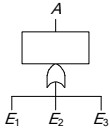
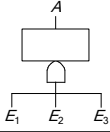
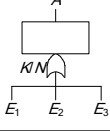



Komponentene i diagrammet representerer her feilmodene som går på nedstengning, f eks for ventilene er feilmoden "Fail To Close". Dersom vi betrakter systemets funksjonen å *sørge for "produksjon"*, vil alle komponentene komme i *serie*. Da vil felmodene typisk bli utilsiktet aktivering, f eks for ventilene er feilmoden "Spurious Closure".

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

Noen kommentarer følger til hvert trinn:

Definisjon av problem og randbetingelser

Hjelpespørsmål for å definere "TOPP"-hendelsen

- **Hva:** F eks brann
- **Hvor:** I kontrollrom
- **Når:** Under normal drift

Med disse hjelpespørsmålene blir det ofte lettere å konstruere feiltreet, dvs det blir klart hvilken situasjon vi analyserer.

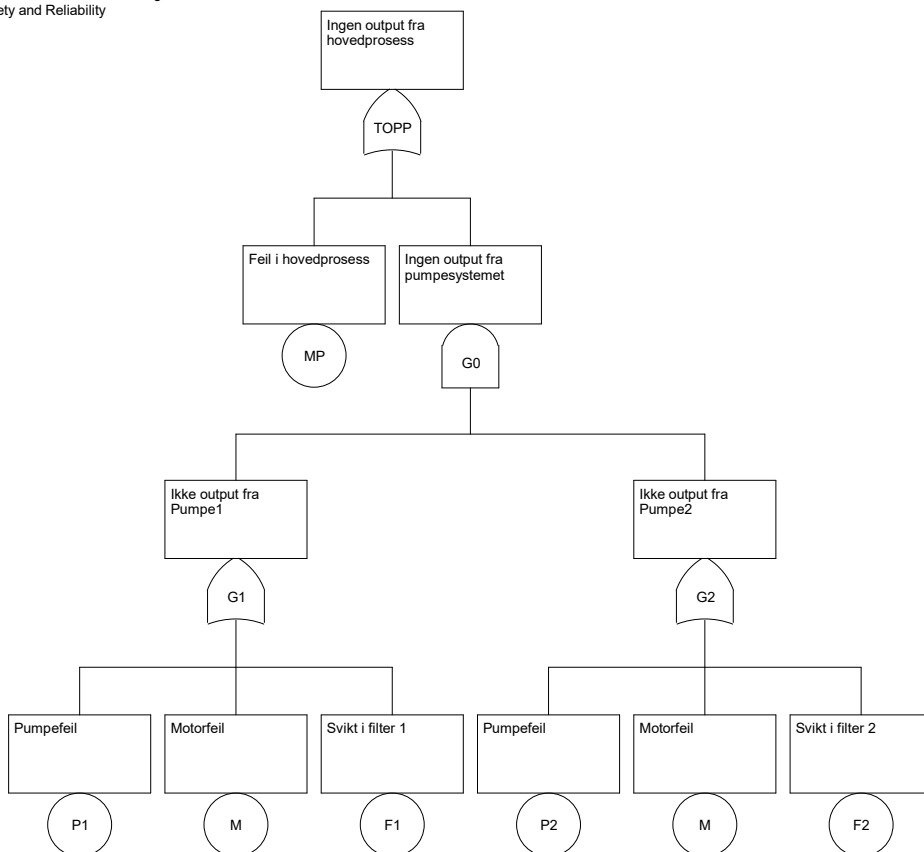
Jeg bruker hjelpespørsmålene hva, hvor og når for å definere TOPP-hendelsen presist.

Konstruksjon av feiltreet

- Start med "TOPP"-hendelsen
- Spør hvilke hendelser som er de direkte årsaker til "TOPP"-hendelsen
- Kople disse sammen med en "OG"/"ELLER"-port
- Hver av hendelsene behandles nå på samme måte, og man arbeider seg suksessivt ned til "basishendelsene"

Nedenfor vises feiltreet for eksemplet ovenfor. Vi starter på toppen. Direkteårsakene til "ingen output" er enten at hovedprosessen har sviktet, eller at det ikke kommer inn prosessmedium til hovedprosessen. Vi bruker ELLER port her fordi det er nok at en av disse svikter for å gi TOPP-hendelsen. Fortsetter slik med at vi ikke får output fra pumpe systemet. Direkteårsakene her er at det verken kommer fra den ene eller den andre pumpen. Bruker her en OG port fordi vi har antatt at det er tilstrekkelig at det kommer prosessmedium fra den ene (redundant system). Dvs feil kun dersom begge "grenene" feiler. Fortsetter videre etter samme prinsipp.

CARA Fault Tree version 4.1 (c) Sydvest Software 1999
Licenced to: SINTEF Industrial Management
Dept of Safety and Reliability



Jeg starter med TOPP-hendelsen, og ser etter direkteårsaker. Jeg forstår forskjellen mellom OG-porter og ELLER-porter.

Bestemmelse av minimale kutt- og stimengder

En kuttmengde i et feiltre er en mengde av basishendelser som ved å inntreffe sikrer at TOPP-hendelsen inntreffer. En kuttmengde sies å være minimal hvis den ikke kan reduseres uten å miste status som kuttmengde.

En stimengde er en mengde av basishendelser som ved ikke å inntreffe sikrer at TOPP-hendelsen ikke inntreffer.

Vi bruker som oftest de minimale kuttmengdene. På eksamen kan vi finne kuttmengdene ved direkte inspeksjon:

- Start fra toppen
- Ved ELLER-port, ta med hendelser lenger ned fra hver gren inn til porten. For hver hendelse får vi en ny kuttmengde
- Ved OG-port, ta med hendelser lenger ned fra hver gren inn til porten. Alle hendelsene vi tar med oss "opp" blir i en kuttmengde
- Kan bli veldig stort dersom vi har mange OG porter
- Eliminer ikke-minimale kuttmengder

Fra eksemplet:

Ta først med

{MP}

Deretter går vi videre med G0 porten. Da dette er en OG port må vi ta med en fra hver side. Etter som vi får ELLER porter lenger ned må vi ta med alle kombinasjoner, en fra hver hovedgren som gir:

{P1, P2}, {P1, M}, {P1, F2}, {M, P2}, {M, M}, {M, F2}, {F1, P2}, {F1, M}, {F1, F2}

Vi ser at $\{M, M\} = \{M\}$, og har da totalt følgende kuttmengder:

{MP}, {P1, P2}, ~~{P1, M}~~, {P1, F2}, ~~{M, P2}~~, {M}, ~~{M, F2}~~, {F1, P2}, ~~{F1, M}~~, {F1, F2}

hvor ikke minimale kuttmengder er strøket over. Totalt får vi da følgende *minimale* kuttmengder:

{MP}, {P1, P2}, {P1, F2}, {M}, {F1, P2}, {F1, F2}

Kvalitativ analyse av feiltreet

Vi lister kuttene i stigende orden. De minimale kuttmengder med få element er de viktigste:

Cut set(s) with 1 component (Total: 2)

{M}
{MP}

Cut set(s) with 2 components (Total: 4)

{P1, P2}
{P1, F2}
{F1, P2}
{F1, F2}

Jeg kan finne kuttmengdene for enkle feiltrær. Jeg kan også eliminere ikke-minimale kuttmengder om jeg har slike.

Kvantitativ analyse av feiltreet

Følgende systemmål er av interesse:

- $Q_0(t)$ = Sannsynligheten for at TOPP-hendelsen er inntruffet ved tid t (utilgjengelighet)
- $F_0(t)$ = Frekvens av TOPP-hendelsen ved tid t
- $R_0(t)$ = Sannsynligheten for at TOPP-hendelsen ikke har inntruffet i $[0, t>$

For å beregne systemmålene kreves pålitelighetsdata for basishendelsene

- feilrater ($\lambda_j = 1/MTTF$)
- reparasjonstider ($MDT = 1/\mu_j$)
- testintervall ved funksjonstest (τ_j)

Vi viser kun beregning av $Q_0(t)$, hvor vi dropper tidsangivelsen (t). Trinnene i beregningen er nå:

Trinn 1

Finn feilsannsynlighetene per komponent. For enheter som repareres med en gang svikt inntreffer benytter vi:

$$q_i = \lambda_i MDT_i$$

(7)

Merk at dette er en tilnærming av ligning (1), hvor $q_j = U$. For enheter som funksjonstestes får vi tilsvarende:

$$q_i = \lambda_i \tau_i / 2$$

(8)

For eksemplet ovenfor får vi (med mer nøyaktig formel for q_i)

| Komponent | MTTF | MDT | $q = \text{MDT}/(\text{MDT}+\text{MTTF})$ |
|-----------|-------|-----|---|
| P1 /P2 | 1460 | 16 | 0.01084 |
| F1 /F2 | 1460 | 4 | 0.00273 |
| M | 17520 | 24 | 0.00137 |
| MP | 26280 | 48 | 0.00182 |

Jeg kan finne q_i -ene på samme måte som jeg fant de i pålitelighetsblokkdiagrammet, evt gjøre det enda litt enklere med formelen $q_i = \lambda_i \text{MDT}_i$.

Trinn 2

For hver kuttmengde beregner vi sannsynligheten for at kuttmengden er i feiltilstand. Denne sannsynligheten finner vi ved å multiplisere sammen alle feilsannsynlighetene for basishendelsene som inngår i kuttmengden. Fra eksemplet får vi:

| Kuttmengde | Bidrag per kutt | \check{Q}_j |
|------------|------------------------|---------------|
| {M} | q_M | 0.001370 |
| {MP} | q_{MP} | 0.001820 |
| {P1,P2} | $q_{P1} \times q_{P2}$ | 0.000011 |
| {P1,F2} | $q_{P1} \times q_{F2}$ | 0.000003 |
| {F1,P2} | $q_{F1} \times q_{P2}$ | 0.000030 |
| {F1,F2} | $q_{F1} \times q_{F2}$ | 0.000007 |

Trinn 3

Vi kan nå legge sammen alle bidragene (kolonnen for \check{Q}_j), og får $Q_0 = 0.003241$. Ved å beregne $h(\mathbf{p})=1-Q_0$ får vi $h(\mathbf{p}) = 0.996759$ som svarer rimelig med svaret fra pålitelighetsblokkdiagrammet.

Jeg kan finne bidragene til Q_0 fra hvert kutt, og så summere disse for å finne Q_0

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 tidsaspekttet, avhengigheter og dominoeffekter. Resultater fra en hendelsestreanalyse er:

- Kvalitativ beskrivelse av hendelsesscenariene
- Kvantitativ beregning av frekvenser for hver av slutthendelsene
- anbefalte risikoreduerende tiltak
- Kvantitativ beregning av effekt av tiltak

For å systematisere hendelsestreanalysen benyttes følgende trinn:

1. Identifiser og definer den initierende hendelsen (uønsket hendelse)
2. Identifiser barrierer og fysiske forhold som skal modelleres i hendelsestreet
3. Konstruer hendelsestreet
4. Beskriv mulige hendelsesforløp som leder til slutthendelsene
5. Bestem frekvensen av den initierende hendelsen og sannsynlighetene i hendelsestreet
6. Beregn frekvenser for slutthendelsene i hendelsestreet
7. Sammenstilling og presentasjon av resultater

Kvantitativ analyse av hendelsestre (punkt 6)

Vi trenger følgende størrelser

- f = Frekvens av initierende hendelse
- q_i = Sannsynligheten for at barrieren feiler (fiasko)
- $p_i = 1 - q_i$ = Sannsynligheten for at barrieren virker etter hensikten

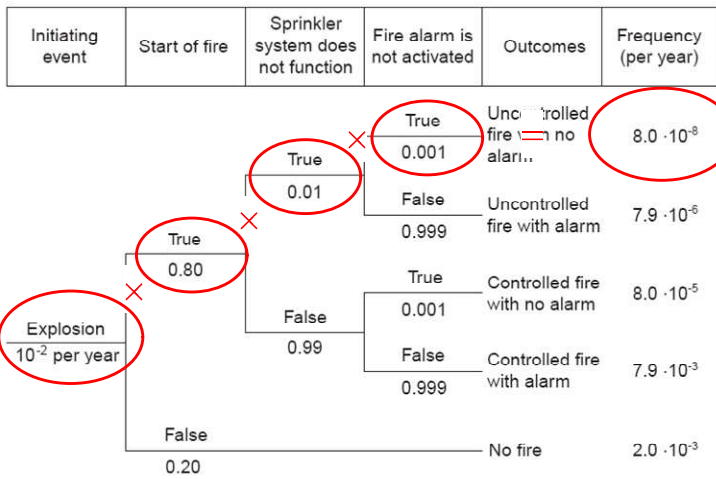
Oftest representerer barrierene skjulte funksjoner, slik at vi kan benytte følgende formel:

$$q_j = \lambda_j \tau_j / 2 \tag{9}$$

for å finne feilsannsynlighetene.

For å finne slutfrekvensene (dvs frekvensene til slutthendelsene lengst til høyre i treet) multipliserer vi frekvensen av initierende hendelse med alle sannsynlighetene vi treffer på fram til slutthendelsen, dvs q_i for "fiasko-utgangene", og p_i for "suksessutgangene". Eksempel følger nedenfor.

Det er enkelt å regne på hendelsestrær, utfordringen er å sette opp barrierene i riktig rekkefølge



– Adapted from IEC 60300-3-9

Hendelsestreanalyse kontra feiltreanalyse

En feiltreanalyse benyttes primært til å analysere årsakene til uønskede hendelser, eller årsakene til en svikt i en barriere. For feiltreanalysen er det bare en "utgangshendelse", dvs TOPP-hendelsen.

Feiltreanalyse er derfor uaktuelt dersom det er flere utfall. Hendelsestreanalysen benytter vi når vi skal analysere hendelsesforløpet etter en uønsket hendelse (dvs den initierende hendelsen i hendelsestreet).

En hendelsestreanalyse vil ha flere utganger. Hver gren i hendelsestreet representerer et mulig utfall gitt at den uønskede hendelsen har inntruffet. Typisk vil vi tegne et hendelsestre for et system hvor flere barrierer aktiveres en etter en etter en kritisk situasjon. Alvorligheten av hendelsesforløpet vil typisk øke jo færre barrierer som fungerer (dvs opp til høyre i eksemplet ovenfor).

Jeg er stø i valget av ETA kontra FTA. Med kun et utfall, er FTA naturlig, mens ved mange utfall er ETA eneste tilnærming.

Dersom det er knyttet en tallverdi for tap til hver sluttkonsekvens (f eks antall drepte) kan jeg finne forventet tap (f eks forventet antall drepte) ved å multiplisere slutfrekvens med tap for hver sluttkonsekvens, og så summere alle bidragene.

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. Utvalgelse av kritiske enheter (MSI)
5. Datainnsamling og analyse
6. Feilmode og effekt analyse (FMEA/FMECA)

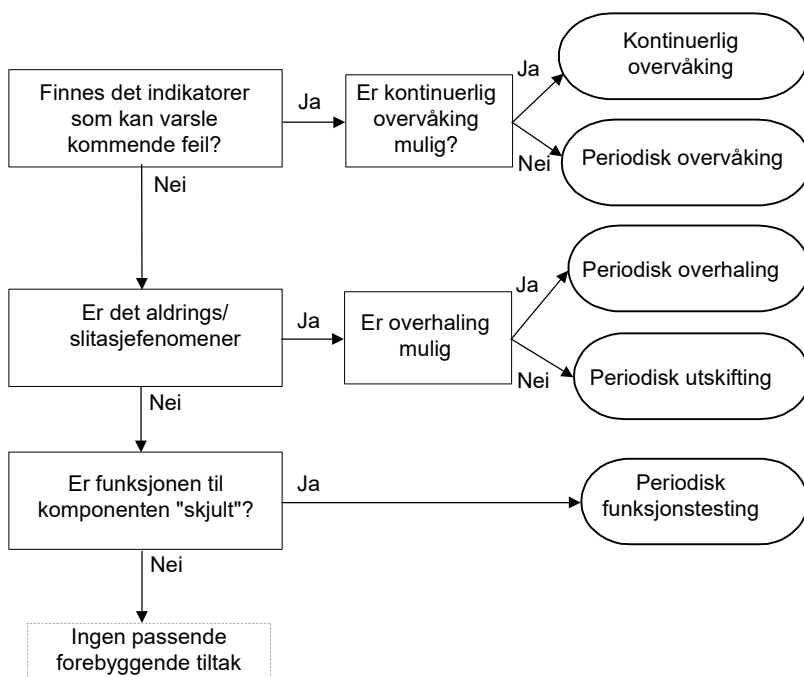
7. Bestemmelse av vedlikeholdsaktiviteter (RCM-logikk)
8. Intervalloptimalisering
9. Kontinuerlig oppdatering - RCM prosessen

FFA og FMECA er viktige skjemateknikker for å analysere funksjon og feilmoder til systemet, evt komponentene til systemet. I denne analysen begrenser man antall komponenter/feilmoder ved at kun de med høy kritikalitet (på en eller annen skala) blir tatt med i det videre arbeidet.

- Jeg vet at en FFA finner delsystemets funksjoner, og feilmoder (som ofte betegnes funksjonsfeil).
- Jeg vet at basert på kritiske systemfeilmoder identifiseres relevante komponenter for videre analyse (MSI=Maintenance Significant Items).
- For enkle systemer kan jeg utføre en FMECA, og vurdere relevansen av de ulike kolonnene i skjemaet.

RCM - Beslutningslogikk

For de mest kritiske feilmodene (fra FMECAen) foretas nå en analyse av hvilke vedlikeholdsaksjoner som kan være relevante. Til dette benyttes RCM beslutningslogikk. Det finnes heller ingen standard beslutningslogikk, men en enkel og for de aller fleste situasjoner tilstrekkelig logikk gjengis nedenfor:



- Jeg forstår spørsmålene, og kan for rimelige enkle systemer benytte logikken. F eks tilstandskontroll (kontinuerlig eller periodisk) er naturlig dersom det finnes indikatorer som kan varsle kommende feil.

□ Jeg vil kunne huske hovedtrekkene i en slik logikk fordi jeg skjønner gangen i logikken. Først vurderer vi om tilstandskontroll er mulig, hvis ikke, er neste valg aldersbestemt utskifting/overhaling, og til slutt er det bare funksjonstest som er mulig (ved skjult funksjon).

Intervalloptimalisering

RCM beslutningslogikk gir type vedlikehold. Men logikken sier ikke noe om hvor mye vedlikeholds som bør gjennomføres. Intervalloptimalisering betyr å finne tid mellom hver vedlikeholdsoppgave. Jo mer vedlikeholds som gjøres (kortere intervall) jo lavere effektiv feilrate kan man forvente, og i utgangspunktet lavere produksjonstap osv. Men vedlikehold koster slik at man må balansere innsatsen. For å optimere vedlikeholdsintervallene trenger vi som minimum:

1. Effektiv feilrate, $\lambda_E(\tau)$,
2. Kostnad for å utføre en FV, C_{PM}
3. Kostnad for å utføre en KV, C_{CM}
4. Sannsynlighet for at vi får systemsvikt gitt komponentsvikt
5. Konsekvens av systemsvikt
 - a. Sikkerhet (kroneverdi)
 - b. Punktlighet/tilgjengelighet (kroneverdi)
 - c. Materielle tap (havari med mer, kroneverdi)

Effektiv feilrate, $\lambda_E(\tau)$, er sannsynlighet for svikt per tidsenhet (ubetinget feilrate) gitt at vi foretar vedlikehold med tid mellom hver gang vedlikehold utføres lik τ (vedlikeholdsintervall).

Vi beskriver gangen kun i situasjonen med aldring, dvs vedlikeholdsaktiviteten er enten periodisk overhaling eller periodisk utskifting, se RCM logikk ovenfor.

Hvis man har gode (nok) erfaringsdata, kan sviktintensiteten, $z(t)$, estimeres, og den effektive feilraten $\lambda_E(\tau)$, beregnes numerisk. Dette er ofte vanskelig i praksis. I mangel på gode data kan man følge denne oppskriften:

1. Anslå midlere tid til feil, $MTTF$, uten vedlikehold (= $MTTF_N$, $N = \text{«Naked»}$)
2. Anslå grad av aldring, liten, middels, sterk
3. Effektiv feilrate er nå gitt ved:

Lav aldring: $\lambda_E(\tau) = 0.79 \tau / MTTF_N^2$

Middels aldring: $\lambda_E(\tau) = 0.71 \tau^2 / MTTF_N^3$

Sterk aldring: $\lambda_E(\tau) = 0.67 \tau^3 / MTTF_N^4$

- Dersom jeg får oppgitt MTTF uten vedlikehold og grad av aldring, kan jeg beregne effektiv feilrate ut fra formlene ovenfor.
- Jeg satser på at disse formlene evt oppgis på eksamen.

For å finne optimalt intervall beregnes forventede kostnader per tidsenhet

$$C(\tau) = C_{PM}/\tau + \lambda_E(\tau) [C_{CM} + Pr(S) \times C_S + Pr(P) \times C_P \times MDT + \dots] \quad (10)$$

Hvor C_{PM} er kostnader per forebyggende vedlikeholdsaktivitet (perventive maintenance), C_{CM} er kostnadene ved å reparere en feil (corrective maintenance), $Pr(S)$ er sannsynligheten for at komponentsvikt leder til en hendelse kritisk for sikkerhet. C_S er tilhørende kostnad gitt sikkerhetshendelse inntreffer. $Pr(P)$ er sannsynligheten for at en komponentsvikt leder til produksjonstap (punktlighetstap osv). C_P er kostnaden per time systemet er nede, og MDT er midlere nedetid til komponenten.

For å finne minimale kostnader per tid kan man derivere ligning (10) mht τ og sette lik 0. Alternativt kan man beregne kostnadene i ligning (10) for ulike τ -verdier, og se hvilken τ som gir laveste forventede kostnader.

- Jeg skjønner gangen i å sette opp kostnadsfunksjonen. $C(\tau)$ angir forventede kostnader per tidsenhet.
- Jeg pugger aldri slike formler, men resonerer meg fram til uttrykket. Jeg starter med totale FV kostnader per tid, og setter disse til C_{PM}/τ . Så ser jeg på hva som skjer ved feil. Utenfor parentesen har jeg raten av svikt som funksjon av intervallet, dvs $\lambda_E(\tau)$. Inne i parentesen har jeg alltid C_{CM} da jeg alltid må reparere enheten som har sviktet. Med en viss sannsynlighet får jeg systemsvikt, enten i form av sikkerhet, eller produksjonstap. For å finne forventet kostnad her multipliserer jeg sannsynligheten med konsekvensen gitt sikkerhet, eller produksjonstap.
- Derivasjon er ikke min sterke side, men jeg er i stand til å beregne kostnadsfunksjonen for utvalgte verdier av τ (intervallet).
- På WCM eksamen er det ikke aktuelt å finne optimale intervaller, men jeg kjenner til tilnærmingene slik at jeg kan bruke slike metoder i min egen bedrift for å optimalisere vedlikeholdet, evt argumentere for at noen andre kan gjøre slike analyser.

HAZOP - Hazard and Operability Analysis

HAZOP teknikken ble ikke gjennomgått på Storefjell. Det kan 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:

| Ledeord | Avvik | Konsekvenser | Årsaker | Foreslått løsning |
|---------|------------------|--|--|---|
| Ingen | Ingen strømning | 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 strømning | 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/reduert strøm fra fosforsyrelageret. Settpunkt bestemmes av giftighet og strømningsberegninger. |
| Mer | Mer strømning | Overskudd av fosforsyre. Ingen fare i arbeidsområdet | | |

Jeg kan kombinere ledeord med prosessparametere og vurdere tilhørende avvik.

MORT

MORT (Management oversight and risk tree) er et omfattende rammeverk for både sikkerhetsstyring og ulykkesgransking. MORT ble utviklet på 1970-tallet av William G. Johnson for det amerikanske atomenergibyrået. Den underliggende ulykkesmodellen er basert på barrieretenkning og har vært viktig for utviklingen av sikkerhetsområdet selv om metoden i dag er lite brukt fordi den er svært omfattende og arbeidskrevende.

MORT er basert på generiske faktorer i et sikkerhetsprogram hvor disse kobles sammen logisk ved hjelp av feiltre-symboler. Et eget spørsmålsbatteri finnes for systematisk å kunne undersøke en bestemt situasjon eller en hendelse som har inntruffet med hensyn på ledelsesfaktorer.

MORT var en av de første analyseteknikkene som fokuserte på energi- og barriereanalyse. Senere er det utviklet mange andre analyseteknikker for barriereanalyse, f.eks. BORA (Barriere og operasjonell risikoanalyse) og PDS (Pålitelighet av datamaskinbaserte sikringssystemer).

Jeg vet at MORT har vært viktig for å utvikle sikkerhetstenkningen. Metoden brukes i liten grad i dag, men *barriereanalysen* er tatt videre i andre analyseteknikker.

Sikkerjobbanalyse - SJA

En sikker jobbanalyse gjennomføres for å:

- Avdekke farekilder
- Avdekke farlige bevegelser, stillinger, aktiviteter og arbeidsmåter
- Gi innspill til å håndtere farer
- Bevisstgjøre involverte parter på farer og trusler før en kritisk jobb skal utføres

Metodebeskrivelse - SJA

0. Innledning
1. Velg ut og avgrens arbeidsoppgaven
2. Bryt arbeidsoppgaven ned i deloppgaver
3. Identifiser farer for hver deloppgave
 - Farekilder
 - Farefulle arbeidsmåter
 - Andre farlige forhold
4. Vurder risikoen
5. Foreslå risikoreducerende tiltak

Noen stikkord

En arbeidsoppgave består vanligvis av en sekvens av deloppgaver. Arbeidsoppgaven skal brytes ned i korte og handlingsrettede deloppgaver hvor rekkefølgen også angis.

- Beskriv *hva* som skal gjøres, og ikke hvordan

- Bruk verb som: "Sett inn", "installer", "løft", "åpne", osv

Som et minimum bør følgende forhold vurderes mht å avdekke farekilder og uønskede hendelser:

- Er det fare for å slå seg, bli truffet av, eller komme i skadelig kontakt med en gjenstand?
- Kan en arbeider bli klemt inni, ved, eller mellom gjenstander?
- Er det mulighet for å skli/snuble?
- Kan arbeideren falle fra ett nivå til et annet (evt. til samme nivå)?
- Er arbeidsmiljøet skadelig for sikkerhet og helse?
- Er det giftig gass, damp, lukt eller støv til stede?
- Er det mulig å bli eksponert for varme, kulde, støy eller ioniserende stråling?
- Er det brennbare, eksplosive eller elektriske farekilder?

Hver farekilde og uønsket hendelse avdekket må vurderes mht. frekvens og konsekvens for å fastsette en risikoindeks:

- Hva kan gå galt?
- Hva er konsekvensene?
- Hvordan kan det skje?
- Kan det være andre risikopåvirkende faktorer?
- Hvor sannsynlig er det at den uønskede hendelsen vil inntreffe
- Hvilke barrierer finnes for å forhindre den uønskede hendelsen?

Vurderingen av risikomomentene gjør det mulig å prioritere risikoreduserende tiltak. Tiltakene kan omfatte:

- Utstyr og hjelpemidler
- Fast verneutstyr
- Arbeidsrutiner og metoder. Kan arbeidet gjøres på en annen måte?
- Fjerne behovet for deloppgaver
- Forbedre arbeidsinstrukser, utdanning osv.
- Ha instrukser klare for ekstraordinære situasjoner
- Personlig verneutstyr

Eksempel

Skifte til sommerdekk på bilen:

| Nr. | Deloppgave | Fare/årsak | Mulige konsekvenser | Risiko | | | Risikoreduserende tiltak | Ansvarlig |
|-----|----------------------|-------------------|--|--------|-------|-----|--|----------------|
| | | | | Frekv. | Kons. | RPN | | |
| 1 | Hente dekk fra loft | Klatre i stige | Ramle i stige | L | M | M | Sikre underlag for stige | Mannen i huset |
| | | Potensiell energi | Miste dekk i hode på den som tar i mot | L | M | M | Avklar arbeidsoperasjon før dekk heises ned | Kona |
| 2 | Jekke opp bil | Dårlig sikring | Jekk ut av posisjon, bil faller ned | L | H | M | Sjekke underlag | Kona |
| | | | Bil ruller | M | H | H | Sette på parkbrems | Kona |
| | | Teknisk svikt | Jekk svikter, bil faller ned | L | H | M | Unngå å ligge under bilen, pass på fotstilling | Mannen i huset |
| 3 | Løsne opp hjulskruer | | | | | | | |
| 4 | Skru ut hjulskruer | | | | | | | |
| 5 | Løfte av vinterhjul | | | | | | | |
| 6 | Sette på sommerhjul | | | | | | | |
| 7 | Skru inn skruer | | | | | | | |
| 8 | Jekke ned bil | | | | | | | |

RPN = Risk Priority Number

Trinn 2 – 8 utføres for alle 4 hjul

Her kan man tenke seg at jobben gjøres mht på å lage en god arbeidsbeskrivelse, både for sommer og vinter. Merk at noen aktiviteter slik som å avklare prinsippene for løfteoperasjonen i forhold til at dekkene er på hemsen vanskelig kan beskrives i prosedyrer. Hensikten med SJA her, er å bli bevisst på risikoen, og at involverte parter blir enige der og da om hvordan det er sikkert å utføre deloppgaven.

SJA kan her være nyttig både som et grunnlag for å lage prosedyrer for gjennomføring av en arbeidsoppgave, men også som grunnlag for forberedelser til selve jobben.

Jeg vet at SJA kan benyttes både til å analysere rutineoppgaver og å gjøre en konkret analyse før en kritisk jobb.

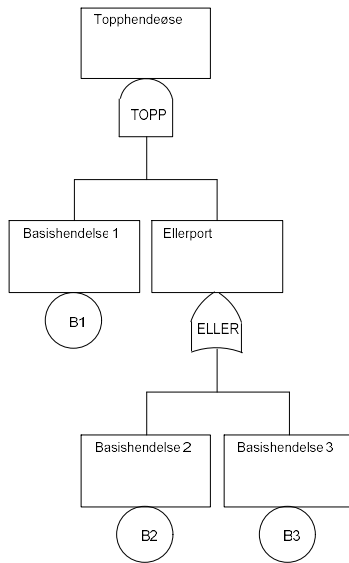
Jeg vet at for å identifisere farer må jobben brytes ned i hensiktsmessige deloppgaver

Jeg vet at det finnes sjekklister som understøtter analysen

Eksempler, minimale kuttmengder

Eksempel 1:

CARA Fault Tree version 4.1 (c) Sydvest Software 1999



Vi starter fra TOPPEN, og bruker «regelen» Ved OG-port, ta med hendelser lenger ned fra hver gren inn til porten. Alle hendelsene vi tar med oss "opp" blir i en kuttmengde

Her er TOPP= «OG-port». Vi må da ta med hendelser fra hver gren, dvs «B1»-greina, og «ELLER» greina. Det blir i utgangspunktet en kuttmengde:

{B1 , ELLER}

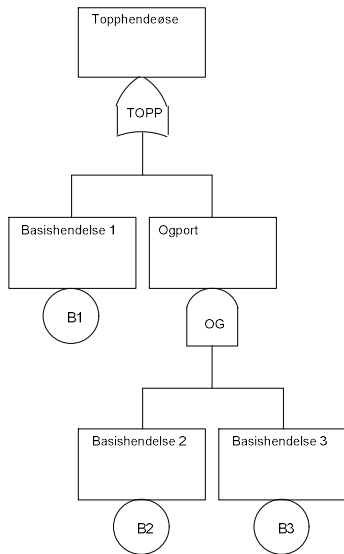
Men vi må gå videre med «ELLER» greina, og får da ved å bruke «regelen»: Ved ELLER-port, ta med hendelser lenger ned fra hver gren inn til porten. For hver hendelse får vi en ny kuttmengde

Her er ELLER= «ELLER-port», og vi må ta med B2 og B3 som nå gir nye kuttmengder. Men ELLER-porten er fortsatt knyttet til {B1} via «foreløpig kutt» {B1,ELLER}. Vi får da to nye kuttmengder for denne ELLER-porten:

{B1 , B2}

{B1 , B3}

Eksempel 2:



Vi starter fra TOPPEN, og bruker «regelen»: Ved ELLER-port, ta med hendelser lenger ned fra hver gren inn til porten. For hver hendelse får vi en ny kuttmengde

HER er TOPP= «ELLER-port». Tar fortsatt med fra hver gren under TOPP, men nå lager vi ett kutt for hver gren, dvs:

{B1}
{OG}

Så bruker vi «regelen»: Ved OG-port, ta med hendelser lenger ned fra hver gren inn til porten. Alle hendelsene vi tar med oss “opp” blir i en kuttmengde

Her er OG= «OG-port». Vi må da ta med hendelser fra hver gren under OG porten. Det blir i utgangspunktet en kuttmengde:

{B2 , B3}

Denne kuttmengden erstatter nå {OG} ovenfor, slik at vi totalt får ved å ta med {B1} som vi alt har:

{B1}
{B2 , B3}

Forkortelser og notasjon

$F(t) = \Pr(T \leq t)$ = Fordelingsfunksjon, T = levetid

$R(t) = \Pr(T > t) = 1 - F(t)$ = Overlevelsessannsynlighet.

$z(t)$ = Sviktintensitet = den lokale badekarskurve

MTTF = Midlere tid til svikt (Mean Time To Failure)

λ benyttes generelt om feilrate, og spesielt når sviktintensiteten er konstant, da har vi $\lambda = 1/\text{MTTF}$

MLD = Midlere logistisk forsinkelse (Mean Logistic Delay)

MRT = Midlere (aktiv) reparasjonstid (Mean Repair Time)

MDT = Midlere nedetid (Mean Down Time), $\text{MDT} = \text{MLD} + \text{MRT}$

MTBF = Midlere tid mellom svikt (Mean Time Between Failure), $\text{MTBF} = \text{MTTF} + \text{MDT}$.

U = Utilgjengelighet (Unavailability), $U = \text{MDT}/(\text{MTTF} + \text{MDT})$

A = Tilgjengelighet (Availability), $A = \text{MTTF}/(\text{MTTF} + \text{MDT})$

τ = Vedlikeholdsintervall, f eks intervall for periodisk bytte eller periodisk funksjonstest

PFD = Sannsynlighet for at enheten ikke er tilgjengelig når den etterspørres (probability of failure on demand), $\text{PFD} = \lambda\tau/2$

$x_i(t)$ = Tilstand til komponent i ved tid t

p_i = pålitelighet til komponent i , typisk sannsynlighet for at komponenten er funksjonsdyktig

q_i = Sannsynlighet for at komponent i er i feiltilstand, $q_i = 1 - p_i$

$\phi(\mathbf{x}, t)$ = Strukturfunksjon = Tilstand til systemet ved tid t

$p_s = h(\mathbf{p})$ = Systempålitelighet, dvs en funksjon av komponentpålitelighetene

$Q_0(t)$ = Sannsynligheten for at TOPP-hendelsen er inntruffet ved tid t (utilgjengelighet)

$F_0(t)$ = Frekvens av TOPP-hendelsen ved tid t

$R_0(t)$ = Sannsynligheten for at TOPP-hendelsen ikke har inntruffet i $[0, t]$

$\lambda_E(\tau)$ = Effektiv feilrate = Forventet antall svikt per tidsenhet som funksjon av τ

α = Aldringsparameter i Weibullfordelingen ($\alpha = 2$ = svak aldring, $\alpha = 4$ = sterk aldring)