

# Kapittel 10

## Årsaks- og frekvensanalyse

Ingrid Bouwer Utne og Marvin Rausand  
ingrid.b.utne@ntnu.no

# Oversikt – kapittel 10

- Feiltreanalyse
- Bayesianske nettverk



# FEILTREANALYSE



NTNU

# Hva er feiltreanalyse?

- Kan brukes til å bestemme årsakene og sannsynligheten/frekvensen til en uønsket hendelse.
- Kan også brukes til å analysere påliteligheten til de proaktive og reaktive barrierene som er installert.
- Kan være kvalitativ, kvantitativ eller begge deler.
- Er et logisk diagram som illustrerer sammenhengen mellom en uønsket hendelse (kalt Topp-hendelsen) og årsakene til denne hendelsen.

# Hensikt og anvendelse

En feiltreanalyse kan blant annet gi svar på følgende spørsmål:

- Hvilke kombinasjoner av feil og hendelser kan føre til topphendelsen?
- Hva er sannsynligheten for at topphendelsen vil inntreffe?
- Hvor ofte vil topphendelsen inntreffe?
- Hvilke komponentfeil og/eller hendelser har størst betydning for om topphendelsen vil inntreffe eller ikke?

Feiltreanalyse kan brukes både i pålitelighets- og risikoanalyser



NTNU

# Metodebeskrivelse

Feiltreanalysen består av fem trinn:

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

Forberedelser og rapportering er beskrevet i kap. 8 i boka.

# 1. Definisjon av problem

Hensikten med dette trinnet er å:

- Gi en klar definisjon av topphendelsen som skal analyseres
- Fastlegge randbetingelsene for analysen

Beskrivelsen av topphendelsen bør gi svar på spørsmålene:

- Hva: Gi en klar beskrivelse av hva topphendelsen innebærer, hvilken hendelse eller ulykke
- Hvor: Beskriv hvor topphendelsen inntreffer
- Når: Si når topphendelsen inntreffer

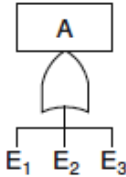
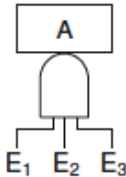
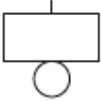
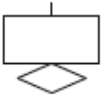
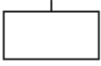


Definisjon av randbetingelser inkluderer fysiske avgrensninger, startbetingelser, ytre belastninger og detaljeringsnivå for analysen.

## 2. Konstruksjon av feiltreet

- Start med topphendelsen
- Regler:
  - Beskrivelse av inngangshendelser:
    - Til alle inngangshendelsene, både normal- og sekundærinngangene, knytter du et kommentarrektangel. I kommentarrektanglene beskriver du nøyaktig hva feilen/hendelsen består i, hvor og når den inntreffer.
  - Vurdering av inngangshendelser.
    - Utstyrfeil kan du dele i tre typer: primære feil, sekundære feil og kommandofeil.
  - Portene skal «fullføres».
  - Portene skal ikke knyttes sammen.



# Feiltre- symboler

	Symbol	Beskrivelse
Logiske porter	ELLER-port 	Utgangshendelsen $A$ inntreffer hvis minst én av inngangshendelsene $E_i$ inntreffer. Antall inngangshendelser er vilkårlig.
	OG-port 	Utgangshendelsen $A$ inntreffer bare hvis samtlige inngangshendelser $E_i$ inntreffer. Antall inngangshendelser er vilkårlig.
Inngangshendelser	Inngangshendelse 	Symbol for komponent i primær feiltilstand, oppstått under normal drift. Hendelsen krever ingen videre analyse
	Sekundærhendelse 	Symbol for sekundær feiltilstand oppstått på grunn av ekstreme miljøforhold, mangelfullt vedlikehold o.l. Årsakene til hendelsen er ikke undersøkt nærmere
Beskrivelse	Kommentarrektangel 	Benyttes for å gi utfyllende informasjon
Overføringssymboler	Overføring-ut 	Overføringssymboler for videre utvikling av en årsakskjede. Brukes når samme grein inngår flere steder i feiltreet, og når feiltreet må tegnes over flere sider.
	Overføring-inn 	

### 3. Bestemmelse av minimale kuttmengder

- En kuttmengde i et feiltre er en mengde av inngangshendelser som ved å inntreffe (samtidig) sikrer at topphendelsen inntreffer.
- En kuttmengde sies å være minimal hvis den ikke kan reduseres uten å miste status som kuttmengde.
- For enkle feiltre kan de minimale kuttmengdene bestemmes direkte fra feiltreet uten noen formell prosedyre/algoritme. For litt mer kompliserte feiltre trenger vi en algoritme (dataprogram).



## 4. Kvalitativ analyse

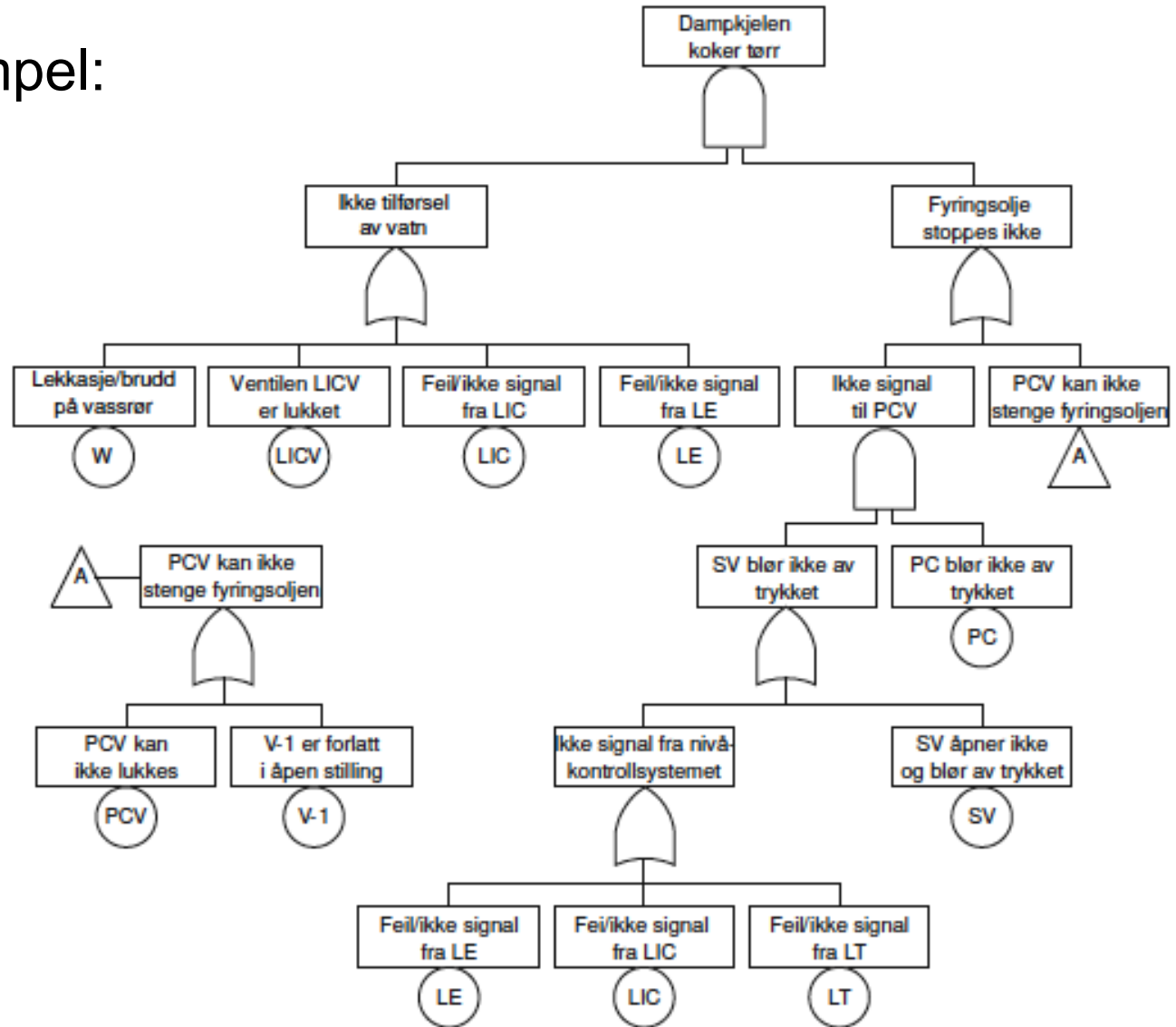
- Ved kvalitativ analyse av feiltreet er det vanlig å ta utgangspunkt i de minimale kuttmengdene.
- Betydninga av en kuttmengde er blant annet avhengig av hvor mange inngangshendelser kuttmengden er sammensatt av.
  - En kuttmengde med bare én hendelse er i utgangspunktet viktigere enn kuttmengder med to eller flere hendelser.
- Mulig rangering av kuttmengde:
  - Menneskelige feilhandlinger
  - Aktiv utstysrfeil
  - Passiv utstysrfeil



NTNU

# Feiltre

Eksempel:





## 5. Kvantitativ analyse

Vanligvis vil du ønske å beregne:

- Sannsynligheten for at topphendelsen i feiltreet vil inntreffe i løpet av en gitt tidsperiode. I mange tilfelle kan det være like aktuelt å finne frekvensen topphendelsen vil inntreffe med.
- Den pålitelighetsmessige betydninga til inngangshendelsene (her må du ta hensyn til både plasseringen i feiltreet og sannsynligheten for at hendelsen vil inntreffe).
- Usikkerheten i anslaget for sannsynligheten/frekvensen.



## 5. Kvantitativ analyse (ii)

Sannsynlighet for hver inngangshendelse:

$$q_i(t) = \Pr(\text{inngangshendelse nr. } i \text{ inntreffer ved tidspunkt } t)$$

Sannsynlighet for at minimalt kuttsett  $j$  feiler ved tidspunkt  $t$ :

$$\check{Q}(t) = \prod_{i \in K_j} q_i(t)$$

Sannsynlighet for topphendelsen:

$$Q_0(t) = \Pr(\text{topphendelsen inntreffer ved tidspunkt } t)$$

Tilnærma verdi:

$$Q_0(t) \approx 1 - \prod_{j=1}^k (1 - \check{Q}(t))$$

## 5. Kvantitativ analyse (iii)

Hovedutfordringen er å bestemme sannsynlighetene for inngangshendelsene. Tre vanlige situasjoner:

1. Komponent  $i$  blir ikke reparert når den feiler:

$$q_i(t) = 1 - e^{-\lambda_i t}$$

2. Komponent  $i$  blir reparert når feil inntreffer:

$$MTTF_i = \frac{1}{\lambda_i} \text{ og } q_i(t) \approx \frac{MTTR_i}{MTTF_i + MTTR_i}$$

3. Komponent  $i$  testes periodisk med testintervall  $\tau_i$  :

$$q_i(t) \approx PFD_i \approx \frac{\lambda_i \tau_i}{2}$$



# Pålitelighetsmessig betydning

- Inngangshendelsene har ulik betydning for om topphendelsen skal inntreffe eller ikke.
- Det mest kjente målet for «pålitelighetsmessig» betydning er Birnbaums mål, som er definert slik:

$$I^B(i|t) = \frac{\delta Q_0(t)}{\delta q_i(t)}$$

- Sannsynlighetene for alle inngangshendelsene unntatt  $i$  holdes fast, og at vi ser på hvor mye  $Q_0(t)$  endrer seg ved en liten endring i  $q_i(t)$ . Denne endringen måles ved den deriverte av  $Q_0(t)$  med hensyn på  $q_i(t)$ .



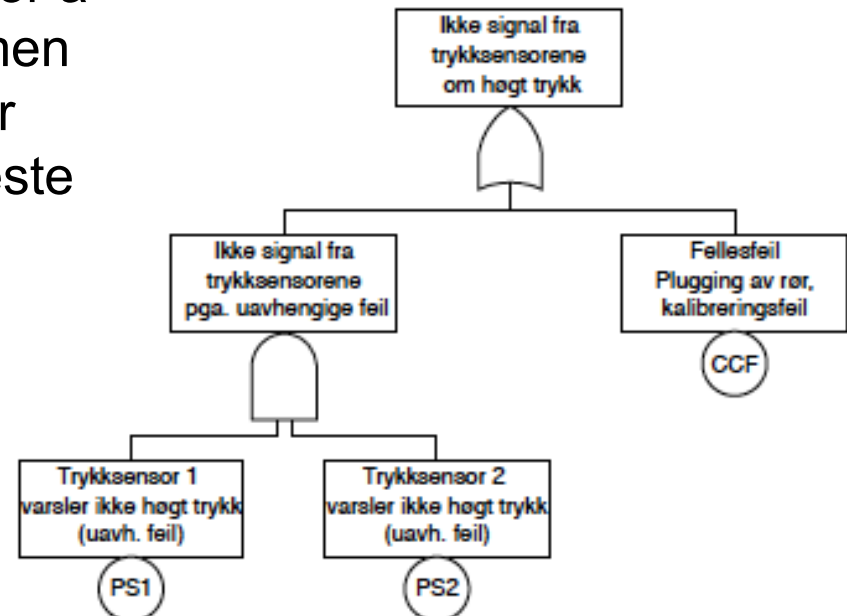


# Avhengige feil

Tilnæringsformelen for topphendelsen på slide 14 er gyldig når inngangshendelsene er uavhengige.

- Betingelsen om uavhengighet er ofte ikke oppfylt, f.eks. for barrierer med en viss grad av redundans. Slike system er gjerne utsatt for avhengige feil/fellesfeil.

Det er utvikla flere metoder for å anslå effekten av fellesfeil, men mange av disse metodene er svært kompliserte. Det enkleste er trolig å foreta en eksplisitt modellering av fellesfeilene i feiltreet, som vist i figur.



# Fordeler

- Gir et klart og oversiktlig bilde av hvilke kombinasjoner av utstysrfeil og andre hendelser som kan lede til topphendelsen.
- Er enkelt å forklare til personer som ikke på forhand er skolert i feiltreanalyse.
- Feiltreanalyse er den mest brukte analysemetoden i årsaksanalyse og metoden er godt dokumentert.
- Den/de som utfører analysen blir tvunget til å forstå systemet til bunns.
- Mange svakheter i systemet derfor blir avdekka og korrigert mens feiltreet konstrueres.

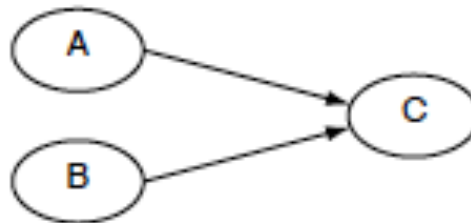
# Begrensninger

- Gir et statistisk «bilde» av de feilkombinasjonene som kan resultere i topphendelsen.
- FTA ikke er en velegna metode for å analysere system med dynamiske egenskaper (f.eks. er det vanskelig å behandle et standby-system med omkopling, periodisk testing og vedlikehold med FTA).
- Et anna problem er behandling av avhengige feil.

# **BAYESIANSKE NETTVERK**

# Hva er et bayesiansk nettverk?

- Er en grafisk nettverksmodell som illustrerer hvordan et system kan funksjonere eller feile.
- Er svært fleksible og kan erstatte både feiltre og hendelsestre.
- Er spesielt godt egna til årsaksanalyser.
  - Årsakene til en uønska hendelse kan lett beskrives med piler fra årsaker til den uønska hendelsen. I noen sammenhenger kalles «årsakene» risikopåvirkende faktorer (RIF).





# Hensikt og anvendelse

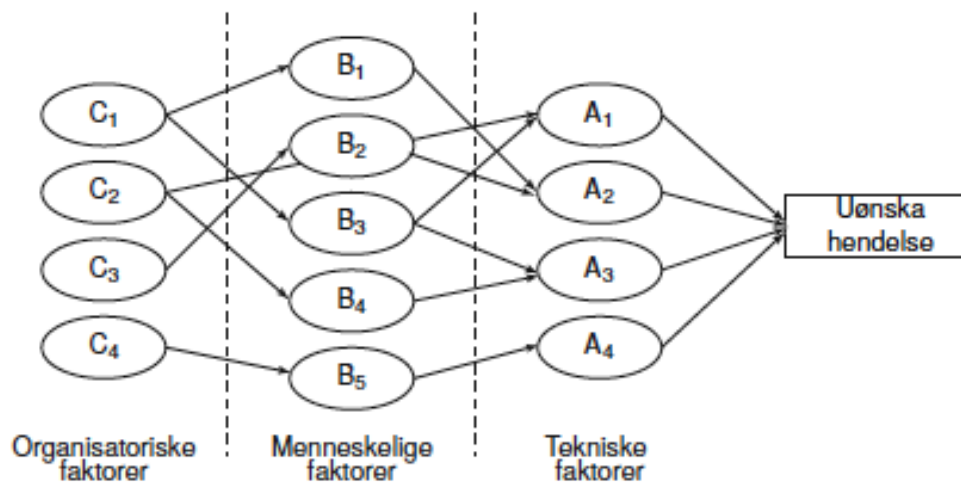
- Bayesianske nettverk er et nyttig hjelpemiddel til å avdekke hvilke risikopåvirkende faktorer som kan påvirke uønska hendelser og ulykker.
- Nettverket viser hvordan RIF-ene påvirker hverandre og vil kunne gi ideer til risikoreducerende tiltak.
- Bayesianske nettverk kan også brukes til kvantitative analyser. Dette krever at du setter opp CPT\*-er for hver av nodene i nettverket. Disse kan brukes til å anslå sannsynligheten for at den uønska hendelsen inntreffe.

\*CPT – Conditional probability table

# Metodebeskrivelse

RIF-ene deles noen gang inn i grupper som danner grunnlag for utviklingen av nettverket (figur), f.eks:

- Tekniske
- Menneskelige
- Organisatoriske
- Miljømessige
- Sosiale
- Knyttet til lovverket



Både kvalitativ og kvantitativ analyse.

# Kvantitativ analyse

- En tilfeldig variabel  $X_i$  knyttes til hver node.
- Variabelen kan ha to eller flere tilstander, feks.:

$$X_i = \begin{cases} 1 & \text{Det regner} \\ 0 & \text{Det regner ikke} \end{cases}$$

- For hver av nodene må du sette opp en betinga sannsynlighetstabell (CPT).
- For de nodene som ikke har foreldrenoder, må du anslå sannsynlighetsfordelingen for de tilhørende variablene ut fra tilgjengelige data og ekspertvurderinger (bayesianske sannsynligheter).





# Kvantitativ analyse (ii)

- For de nodene som har foreldre må du anslå sannsynlighetsfordelingen til variabelen for de ulike kombinasjonene av tilstander til foreldrenodene.
- For å utføre beregninger må det antas at to noder vil være uavhengige når vi kjenner tilstandene til alle foreldrenodene deres.
- Kvantitative analyser av nettverket kan utføres ved gjentatt bruk av Bayes regel – som er hovedgrunnen til at metoden kalles bayesianske nettverk.



# Fordeler og begrensninger

- Gir en god oversikt over aktuelle RIF-er og koplingene mellom dem.
- Er godt egna som underlag for å diskutere hvilke RIF-er som påvirker en uønska hendelse, og kan brukes som underlag for en idédugnad.
- Er en fleksibel metode der du kan ta inn mange ulike typer RIF-er.
- Kvantitative analyser av bayesiansk nettverk kan bli svært arbeidskrevende, sjøl for forholdsvis små nettverk.
- Kvantitative analyser krever bruk av dataverktøy og omfattende opplæring.