NTNU

*Risikoanalyse: Teori og metoder, 2. utgave*

# Kapittel 3
# Farekilder og trusler

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

# Oversikt – kapittel 3

- Farekilder og trusler
- Menneskelige og organisatoriske faktorer
- Tekniske svikt og feil
- Fjerning og reduksjon av farekilder og trusler

# FAREKILDER OG TRUSLER

# Farekilder

Farekilder og trusler er sentrale begrep i en risikoanalyse.

Definisjon av farekilde:

- En egenskap, en tilstand eller et forhold som kan lede til en uønska hendelse.

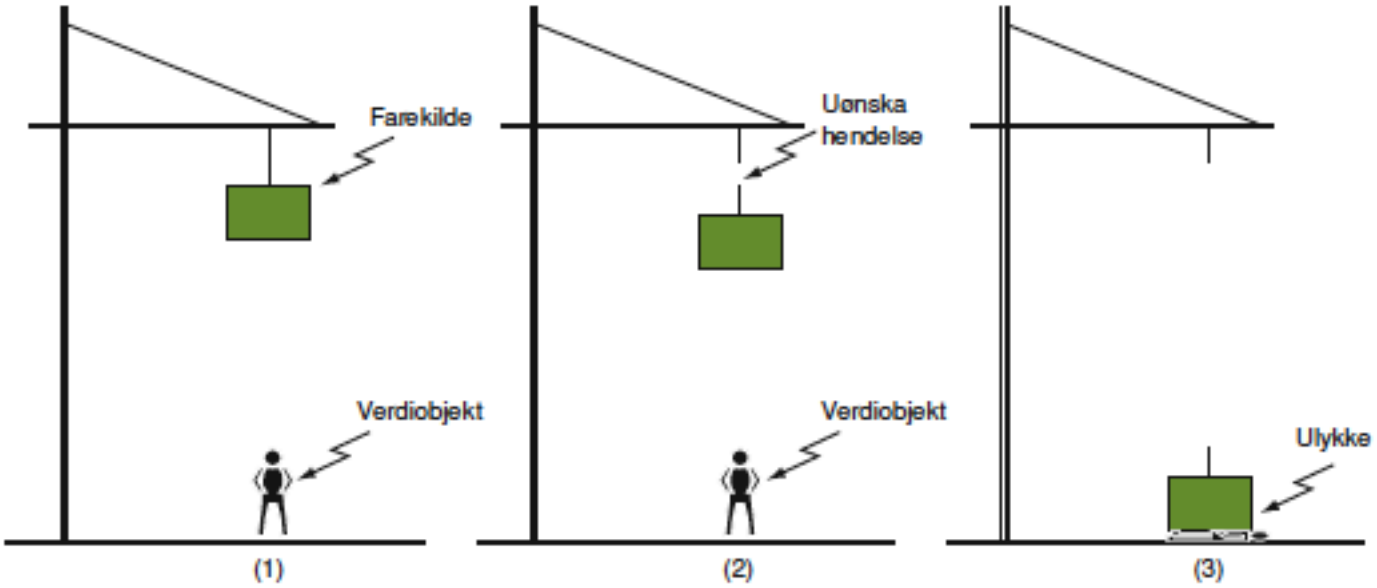
Farekilde brukes vanligvis om en mulig årsak til en utilsikta uønska hendelse.

En farekilde kan endre seg over tid.

Mange farekilder er knytta til energi.

For at en farekilde skal lede til en uønska hendelse må det normalt inntreffe en utløsende hendelse.

# Farekilde, uønska hendelse og ulykke:



# Trussel

Definisjon av trussel:

- En kategori av mulige (dvs. tenkelige) tilsikta uønska handlinger som kan påføre et system tap eller skade.

To typer:

- Fysiske og datatrusler

En trusselaktør er personer, forbund eller fremmed makt som tar sikte på å gjennomføre sikkerhetstruende virksomhet.

En trusselaktør må ha både intensjon og kapasitet til å utføre handlingen.

# Generisk liste

Mekanisk fare
Farlige stoff og materialer
Elektrisk fare
Termisk fare
Strålefare
Støyfare
Vibrasjonsfare

Fare pga. mangelfull ergonomi
Miljøpåvirkning – ytre
Miljøpåvirkning – indre
Organisatorisk
Villede/ondsinna handlinger

Lista er ikke uttømmende. Mer detaljerte lister finnes i flere standarder, bøker og retningslinjer.

# MENNESKELIGE OG ORGANISATORISKE FAKTORER

# Innledning

I samspillet mellom menneskelige-, tekniske- og organisatoriske (MTO) faktorer finner vi ofte avgjørende årsaker til ulykker.

Gransking av større ulykker viser at det sjelden bare er én årsak til ei ulykke.

Å hevde at 80–90 % av alle store ulykker kan tilskrives menneskelige feil, er en forenkling som skader arbeidet med å bedre sikkerheten.

# Menneskelige feilhandlinger

Definisjon av menneskelig feilhandling:

- En svikt i planlagte handlinger i forhold til å nå ønska resultat – uten innblanding av uforutsette hendelser*.

Menneskelige feilhandlinger kan ofte relateres til bakenforligggende årsaker som organisasjonens sikkerhetskultur, opplæring, det tekniske systemets utforming, vedlikehold, evne til å handtere stress o.l.

*Reason, J. (1997). Managing the Risk of Organizational Accidents. Ashgate, Aldershot, England.

# TEKNISKE SVIKT OG FEIL

# Feilrate

Tekniske enheter vil slutte å funksjonere på et eller annet tidspunkt. Denne hendelsen kaller vi en svikt.

Svikt er observerbare hendelser som vi kan anslå frekvensen av.

Definisjon av feilrate:

$$z(t) = \lim_{\Delta t \to 0} \frac{\Pr(t < T \leq t + \Delta t | T > t)}{\Delta t}$$

Dette uttrykker sannsynligheten for at enheten svikter i det korte tidsintervallet fra $t$ til $t + \Delta t$ når det er gitt at enheten har overlevd frem til tidspunktet $t$.

# Feiltilstand

Etter en svikt vil den tekniske enheten være i en feiltilstand i en kortere eller lengre periode. Enheten har da en feil.

En skjult svikt blir ikke oppdaga på det tidspunktet når en teknisk enhet svikter.

Feilmoder beskriver måten en enhet svikter på eller hvilken tilstand enhet har etter at den har svikta.

Systematiske feil er årsak til den systematiske svikten. Slike typer feil kan omfatte designsvakhet, feilmontering og programvarefeil.

# FJERNING OG REDUKSJON AV FAREKILDER OG TRUSLER

# Ulike strategier

Resultatet av risikoanalysen kan vise at vi bør redusere risikoen. Dette kan gjøres ved for eksempel å:

- Fjerne en farekilde
- Redusere en farekilde
- Skape avstand mellom farekilden og verdiene
- Redusere eksponering
- Utvikle mer robuste og/eller resiliente systemer

Definisjon av resiliens for tekniske enheter:

- Evnen en enhet har til å avgrense og absorbere skade og til å gjenvinne funksjonsevnen når enheten utsettes for en stor belastning.