Sikkerhets- og pålitelighetsteknikk
Kortfattet orientering

Forfatter: Ragnar Hartmann, Statkraft Engineering as

30.10.95

Innholdsfortegnelse.

1. Hensikt og målsetting.

Manuskriptet er laget i tilknytning til et kurs om luker, ventiler, rør og varegrinder og skal gi en kortfattet presentasjon av faget sikkerhets- og pålitelighetsteknikk. Hensikten blir å gi en viss forståelse av hva sikkerhets-/risikoteknikk kan tilby ifm. vannveisutstyr, men ikke kvalifisere for analysearbeid.

Målgruppen blir personell ved vannverk og i kraftforsyning. Spesielle forkunnskaper er ikke påkrevet. For den som føler behov for å vite mer om emnet enn det som fremgår av mauskriptet, anbefales EnFO-kurset "Risikoanalyser for kraftverk og vassdrag".

Det antas at sikkerhets- og pålitelighetsteknikk på sikt vil få en bredere plass i norsk kraftforsyningen enn det det har i dag. Ved pågående revisjon av Damforskritene synes det som om ny utgave vil innvitere til, eller kanskje til og med kreve, bruk av kjente sikkerhets- og pålitelighetstekniske metoder. Det er dessuten et faktum at enkelte kraftselskaper i såvel inn- som utland allerede har tatt de nevnte metodene i bruk.

Et problem for moderne sikkerhets- og pålitelighetsteknikk er at faget i sin terminologi benytter ord kjent fra dagligtale, men med en noe annen betydning. Dette gir i enkelte tilfeller problemer når det kommuniseres med grupper eller enkeltpersoner utenfor fagmiljøet. I det følgende vil man derfor også forsøke å definere enkelte av de mest brukte uttrykk. For dette er [4] lagt til grunn.

2. Historikk.

Sikkerhets- og pålitelighetsteknikk kan karakteriseres som et nytt teknisk fag. Menneskers funderinger omkring emnet er derimot urgamle. Aktuelle problemstillinger har angått såvel enkeltmennesker som nasjoner. Eksempler på vanlige spørsmål kan være "om man skal gifte seg", "om man skal foreta en farefull, men kanskje lønnsom reise", "om nasjonen skal ruste seg til krig", osv. I de enkleste samfunn ble slike spørsmål besvart av shamaner. Oltidens kulturriker hadde prester som "leste" i stjernene eller i offerdyrs innvoller. I vår tid blir kanskje en av utfordringene at matematiske manipulasjoner ikke må overta der det okkulte har veket plass.

Moderne sikkerhets- og pålitelighetsteknikk vokste for alvor frem etter siste verdenskrig. Amerikanske analyser ifm. våpensystemer var viktige, men et arbeid tyskerne gjennomførte ifm. utviklingen av V1-bomben, kan også fremheves. Sentralt står imidlertid en studie som amerikanerne gjennomførte for risikovurdering av kommersiell kjernekraft. Rapporten "The Reactor Safety Study", også kallt "Rasmussen-rapporten", forelå i 1974 og la føringer for mange av de arbeider som etter dette er utført på ulike områder.

I Norge ble sikkerhets- og pålitelighetsteknikk tidlig knyttet opp mot oljevirksomheten i Nordsjøen. Teknikken har dessuten vært benyttet for studier ifm. kjemisk industri. Omfattende nasjonal virksomhet gjennom mer enn 20 år gjør at norsk fagmiljø nå ikke står tilbake for det internasjonale, heller tvert i mot.

Norsk kraftforsyning har på sin side vært noe tilbakeholden ifm. sikkerhets- og pålitelighetsteknikk. Enkelte risikoanalyser er imidlertid utført. Det synes nå som om erfaringene fra disse har inspirert deler av bransjen til å vise større åpenhet til de muligheter som sikkerhets- og pålitelighetsteknikk gir.

3. Definisjoner.

Definisjonene er i hovedsak hentet fra [4].

Konsekvens: En av de mulig følger av en uønsket hendelse, dvs. skader på liv og helse, miljø og/eller materielle verdier.

Kritikalitet: Dette er en størrelse som angir kombinasjonen av konsekvenshendelsers hyppighet og feileffektgradering. Linjen i figur 8.1 kan oppfattes å angi ulykker med lik kritikalitet.

Pålitelighet: Begrepet er synonymt med funksjonssannsynlighet, sannsynlighet for at en enhet opprettholder sin funksjonsevne under gitte forhold for en gitt tidsperiode.

Pålitelighetsanalyse: Analyse for å beregne tilgjengelighet eller funksjonssannsynlighet for et teknisk eller et menneske-maskin-system.

Risiko: Dette angir både mulighet for og følgene av uønskede hendelser.

Risikoanalyse: Metode for systematisk gjennomgang av et system i den hensikt å fastslå den totale risiko i systemet vha. å identifisere og kategorisere farer, og å fastslå risiko for mennesker, miljø og materielle verdier.

Sannsynlighet: Kvantitativ angivelse av muligheten for at en hendelse skal inntreffe. Referanse [4] gir dette en mer spesifikk matematisk beskrivelse, se også kapittel 6.

Ulykke: Uønsket hendelse som medfører tap av liv, personskade, store miljøskader eller stort økonomisk tap.

4. Moderne pålitelighets- og risikoanalyse.

Pålitelighets- og risikoanalyse kommer til anvendelse ifm. uoversiktelige systemer hvor ulike hendelser kan inntreffe, og hendelsene beheftes med usikkerhet. Hovedmål for analysene blir klargjøring av problemkomplekser slik at man i neste omgang gis grunnlag for nødvendige beslutninger. Er det på den annen side ingen usikkerhet, blir det heller ikke behov for å gjennomføre analyse.

Metoder ved pålitelighets- og risikoanalyser kan være ulike. Stikkord blir:

- Grovanalyse.
- Konsekvensanalyse.
- FMEA: "Failure Modes and Effect Analysis".
- FMECA: "Failure Modes, Effects and Criticality Analysis".

- HTA: Hendelsestreanalyse.
- FTA: Feiltreanalyse.
- GFUA: Grafisk feilutviklingsanalyse.
- HAZOP: "Hazard and Operability" studie.
- MORT: "Management Oversight and Risk Tree".
- SMORT: "Safety Management and Organization Review Technique".
- THERP: "Technique for Human Error Rate Prediction".

Flere av metodene er nærmere beskrevet i kapittel 9. "Populært" kan det imidlertid hevdes at samtlige har som mål å klargjøre: "Det som ikke skal skje". Følgende tre spørsmål blir som regel alltid sentrale: "Hva kan gå galt ? / Hvor sannsynlig er det ? / Hva blir konsekvensene ?" Usikkerheten fremstår da som et vesentlig element. Sannsynlighet blir et kvantitativt mål for denne.

Det er hevdet at det i risikofaget har dannet seg to "skoler", den klassiske og Bayesianerne. Førstnevnte baserer pålitelighetsvurdering på erfaringsdata, dvs. statistikk. Det hevdes at tilgjengelighet og funksjonssannsynlighet ved dette fremkommer som "objektiv sannhet". Bayesianerne mener derimot at det ikke finnes noen "objektiv" tilgjengelighet eller funksjonssannsynlighet. I stedet må disse størrelser fastlegges subjektivt og tuftes på "beste" vurdering gjort av spesialister, mao. eksperters konsensus.

5. Kvalitet og nytteeffekt ved pålitelighets- og risikoanalyse.

Hovedmålet for en risikoanalyse er som nevnt å bli underlag for avgjørelse. Denne skal kanskje tas i en bedriftsledelse, men analysen kan også være viktig for meneskene andre steder i bedriften med tanke på den informasjon disse trenger for i det daglige å vite hvordan man skal forholde seg for eksempelvis å bedre sikkerheten på egen arbeidsplass. En liste med ulike formål/nytteeffekter gjengis nedenfor og er hentet fra [1].

- Underlag for å prioritere mellom alternative løsninger og tiltak.
- Underlag for å vurdere om pålitelighet og risiko er akseptabel.
- Underlag for å vurdere lønnsomheten til et prosjekt.
- Grunnlag for utvikling av sikre og effektive prosedyrer for operasjon eller overvåking av prosess eller utstyr.
- Systematisk beskrivelse av uønskede hendelser, og de følger slike hendelser kan få.
- Kompetanse og motivasjon for systematisk sikkerhetsoppfølging.

Kvalitet og nytteeffekt avhenger av hvordan analysene gjennomføres. For kompliserte systemer er det sjelden en person som alene har kompetanse for å gjøre alle nødvendige vurderinger. Å forestille seg det uventede blir dessuten enklere i en gruppe hvor personer

gjensidig inspirerer hverandre, enn for en person som kanskje låser seg i spesielle tankerekker.

En analyses troverdighet vil som regel vinne på at personell som i det daglige arbeider med systemet, bringes inn i analysearbeidet. Dette personell blir vanligvis gjennom deltagelsen også mer motivert for siden å yte aktive bidrag i sikkerhetsarbeidet. Motsatt er beste oppskrift på å sikre at en analyse nedstøves i skuff, å gi en "ekspert" et oppdrag og siden passivt avvente oversendelsen av rapport.

Erfaringen til personell som arbeider i et produksjonssystem, kan imidlertid være begrenset. Tyve års tjeneste er ikke det samme som tyve års erfaring. Det optimale blir derfor å føre sammen eget personell of konsulenter til felles innsats.

Som illustrasjon av hva som bør inkluderes av kompetanse ved en større risikoanalyse kan det vises til [1].

- Kunnskap om tekniske og operasjonelle sidene ved det aktuelle system.
- Kunnskap om tekniske og operasjonelle forhold som kan lede til svikt.
- Kunnskap om analysemetoder og -teknikker samt nødvendig matematisk/statistisk begrepsapparat.
- Innsikt i adferd og organisasjon.
- Kunnskap om økonomiske beregninger.
- Kjennskap til relevante pålitelighetsdata (ulykkesdata).

Det kan ellers nevnes at det i Sverige for noen år tilbake ble gjennomført en undersøkelse av risikoanalytikeres evne til å fokusere uøskede hendelser ved et kjemisk anlegg. Innledningsvis gjorde man en teoretisk analyse. Deretter sammenholdt man resultatet av denne med relevant internasjonal skadestatisikk. Det viste seg da at den teoretiske analysen fikk med seg 50-60 % av de hendelser statistikkene dokumenterte. Hvorvidt de ikke avdekkede hendelser var av høy kritikalitet, vet derimot undertegnede intet om.

6. Sannsynlighet for uønsket hendelse.

Begrepet sannsynlighet omtales i kapittel 3. Forhold gjeldende dette blir ofte illustrert med myntkast, terningkast eller spillkort. Tenker en seg at en skal kaste "mynt og krone", vet en at det er 50 % mulighet for mynt og 50 % mulighet for krone. Dette betyr likevel ikke at man ved to kast får en gang mynt og en gang krone. Skal man sammenligne gitt sannsynlighet med kastresult og få overenstemmelse, forutsetter dette et stor antall kast.

Spesielt for myntkastet er imidlertid at det alltid, forutsatt skikkelig utført kast, blir samme sannsynlighet for mynt og krone uansett hvor mange kast det er gjort med penge-

stykket. For en teknisk komponent vil derimot muligheten for uønsket hendelse kunne variere over komponentens levetid. I denne forbindelse blir 5 ulike begrep særdeles sentrale.

$F_T(t)$: Sannsynlighet for at en komponents funksjon feiler innenfor intervallet 0 - t. T blir tidspunktet for feil. Uttrykket angir egentlig fordelingsfunksjonen for T.

$f_T(t)$: Sannsynlighetstetthet. I praksis blir denne lik den deriverte av $F_T(t)$.
$f_T(t) = d / dt \cdot (F_T(t))$

$R_T(t)$: Funksjonssannsynlighet (overlevelsessannsynlighet). Sannsynligheten for at en komponents funksjon er tilstede i intervallet 0 -t. $R_T(t) = 1 - F_T(t)$

$z_T(t)$: Sviktintensitet. Denne er tilnærmet lik forholdet mellom sannsynligheten for at en komponent skal feile i et lite tidsintervall, og det aktulle tidsintervall. Det forutsettes samtidig at komponenten fungerer ved tidsintervallets begynnelse.
$z_T(t) = d / dt \cdot (\ln R_T(t))$

MTTF : Midlere levetid til feil, kan også kalles forventet levetid.

$$MTTF = \int_0^\infty t \cdot f_T(t) \cdot dt$$

For praktiske tilfeller kan det være ulike funksjoner for $F_T(t)$. To viktige funksjonstyper bør fremheves: Den eksponensielle T-fordeling og Weibulls fordeling.

Ved førstnevnte blir: $R_T(t) = e^{-\lambda t}$, $z_T(t) = \lambda$ og $MTTF = 1 / \lambda$. Her er λ en konstant. Dette innebærer at det ved denne feilfordeling også blir konstant mulighet for feil innenfor et tidsintervall Δt uavhengig av når dette forekommer i tid. Sagt på annen måte betyr dette at nye og gamle komponenter som i nyutgave har samme sviktintensitet λ, vil være like gode. Et system med slike komponenter forbedres derfor ikke ved at gamle fortsatt fungerende deler byttes med nye.

Med Weibulls fordeling blir: $R_T(t) = e^{-(\lambda t)^\alpha}$ og $z_T(t) = \alpha \cdot \lambda \cdot (\lambda \cdot t)^{\alpha-1}$. For $\alpha = 1$ tilsvarer Weibulls fordeling den eksponesielle fordeling. Er $\alpha > 1$, får man økende sviktintensitet som funksjon av tiden t. I praksis viser det seg at $2 < \alpha < 4$ passer for komponenter som er utsatt for utmatting. Har man $\alpha < 1$, avtar derimot sviktintensiteten med tiden t. Dette kan være situasjonen for utstyr og komponenter hvor "barnesykdommer" dominerer sviktbildet.

Ofte forutsettes det imidlertid at komponeter og utstyr oppfører seg iht. den eksponesielle feilfordeling. Undertegnede tror dessuten at denne feilfordelingen gjelder for det meste av utstyret i en kraftverksvannvei, forutsatt at dette ved vedlikehold holdes i hevd og ikke til-

lates å forfalle. Det ses da også bort fra de første årer i utstyrets levetid slik at "barnesykdommer" kan forutsettes kurert.

Er man ute etter påliteligheten for et system bestående av mange enkeltkomponenter, har man likeledes regler for hvordan systempåliteligheten kan beregnes ut fra enkeltkomponentenes pålitelighet. Som eksempel vil en se på sannsynligheten for å få åpnet en kraftverksluke ved plutselig opptreden av stor flom. Det forutsettes at tilfredsstillende sluttresultat avhenger av samtidig funksjon for fire ulike elementer. Disse sammen med antatt sannsynlighet for funksjonsevne settes til:

- Åpning initieres og overføres ($\lambda_1 = 0{,}96$).
- Strømtilførsel til spill fungerer ($\lambda_2 = 0{,}95$).
- Spill med opptrekk fungerer ($\lambda_3 = 0{,}99$).
- Luke går fritt i føringer ($\lambda_4 = 0{,}98$).

Iht. produktsetningen for pålitelighet blir systemets pålitelighet:

$$\text{Systempålitelighet} = \lambda_1 \cdot \lambda_2 \cdot \lambda_3 \cdot \lambda_4 = 0{,}96 \cdot 0{,}95 \cdot 0{,}99 \cdot 0{,}98 = 0{,}885$$

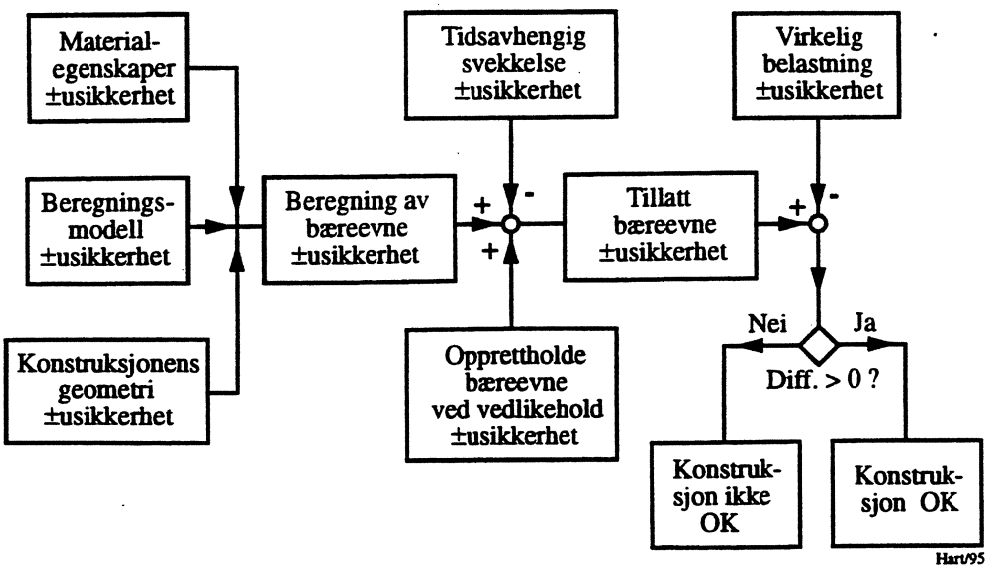
Antas det at spillets sannsynlighet for å fungere i hovedsak blir bestemt av spillmotorens pålitelighet, kan man tenke seg å la spillet utføre med to motorer. Er det etter dette fortsatt motorpåliteligheten som er bestemmende for spillet, kan ny spillpålitelighet beregnes til: $\lambda_3' = 1 - (1 - \lambda_3)^2$. Ny systempålitelighet blir med produktsetningen nå 0,894.

7. Sikkerhet og sikkerhetsfaktor.

Innen sikkerhets- og pålitelighetsteknikk er sikerhet et sammensatt begrep. Referanse [4] splitter eksempelvis sikkerheten opp i gruppene: Akseptabel, aktiv, forebyggende, innebygget og passiv sikkerhet.

Slik [4] definerer forannevnte begrep, kan det hevdes at en konstruksjon har både forebyggende, innebygget og passiv sikkerhet. Men "sikkerheten" for konstruksjonen må også vurderes ut fra de usikkerheter som eksisterer. Sikkerhetsfaktoren som benyttes ved dimensjonering, kan derfor like gjerne omtales som en usikkerhetsfaktor. Forholdet illustreres med blokkskjemaet i figur 7.1.

Det ønskelige blir selvsagt at belastningen alltid er mindre enn bæreevnen. Dog er konstruksjoner ikke til enhver tid helt sikre. Norske bygningsforskrifter utdyper dette for de konstruksjoner disse forskrifter omfatter, og gjeldende stålkonstruksjonsstandard NS 3472 baseres på de samme forutsetninger. Det kan dessuten hevdes at man ved konstruksjon har ulike "bruddsikkerhetsprinsipper".



Figur 7.1: Elementer som påvirker en konstruksjons sikkerhet mot brudd.

- Uendelig levetid.
  Sikkerheten mot brudd skal være 100% uten tidsbegrensning. (Ingen konstruksjon tilfredsstiller i praksis dette krav.)

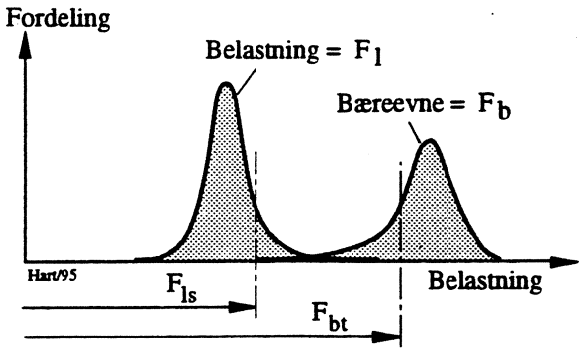
- Sikker levetid.
  Konstruksjonens levetid spesifiseres. Uforutsette belastninger og "tidens tann" skal ikke innenfor levetiden medføre brudd i konstruksjonen. (Prinsippet legges offisielt til grunn for vannkraft-installasjoner, men sjelden ser man at ideen trenger helt inn i det konkrete arbeid med å utforme konstruksjonene.)

- "Fail safe".
  Innenfor konstruksjonens fastsatte levetid tillates det at brudd oppstår. Det er imidlertid et krav at de krefter (funksjoner) som eventuelt får sine "veier" brutt, skal ledes via andre "baner" slik at bruddets konsekvenser minimaliseres og konstruksjonen unngår det totale havari. (Prinsippet benyttes i noen grad for vannkraftutstyr, men er i de fleste tilfeller begrenset til enkelte av konstruksjonens underordnede elementer.)

- Statistisk akseptabel sikkerhet mot brudd.
  Innenfor konstruksjonens fastsatte levetid tillates det brudd med alvorligere konsekvens enn ved "fail safe".

Sistnevnte bruddsikkerhetsprinsipp er nok uoffisielt det som gjelder konstruksjonene i kraftverks vannveier. Forklaringen på hvordan dette kan forenes med dagligtalens krav om at vannkraftkonstruksjoner skal være sikre, er for det første at man ikke setter likhetstegn mellom sikker konstruksjon og ingen mulighet for brudd. Dertil kommer det faktum at man med tanke på en konstruksjons pålitelighet må forholde seg til usikkerhet.

I de senere år har det eksempelvis blitt vanlig å vurdere belastninger og bæreevne som sannsynlighetsfordelte størrelser. Dette er søkt belyst i figur 7.2.



Figur 7.2: Sannsynlighetsfordeling av belastning og bæreevne for en tenkt konstruksjon.

Ut fra figur 7.2 kan man tenke seg spesifisert belastning gitt ved F_{ls} og at beregnet bæreevne skal være minst lik den tillatte, F_{bt}. Nødvendig sikkerhetsfaktor blir i dette tilfellet forholdet mellom F_{bt} og F_{ls}. Man ser imidlertid at det likevel er en viss, men liten, mulighet for at F_l kan bli større enn F_b. Dette kan i så tilfelle medføre brudd.

8. Akseptkriterier.

Når en risikoanalyse kartlegger uønskede hendelser og konsekvensene ved disse, blir det som regel også spørsmål om akseptkriterier før avgjørelse om større tiltak kan tas.

Smisveiste kraftverksrør vil her kunne tjene som eksempel. I utgangspunktet hadde man for smisveiste kraftverksrør et forholdsvis høyt antall rørbrudd. Eiere av rørtypen påviste at rørbruddene for størstedelen hadde sammenheng med turbinregulatorfeil og menneskelig svikt og at sannsynligheten for rørbrudd kunne reduseres vesentlig ved innsats på nevnte områder. Tilsynsmyndigheten NVE mente på sin side at målt skårslagseighet for smisveiste rør var utilstrekkelig når man sammenlignet med materialkrav i aktuelle dimensjoneringsstandarder.

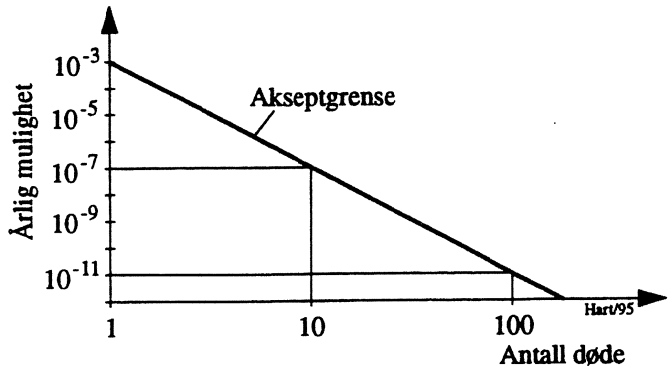
Konklusjonen fra NVE ble at alle smisveise rør skulle tas ut av drift innen år 2005 og at aktuelle tiltak for å hindre regulatorfeil og menneskelig svikt måtte iverksettes umiddelbart. Som det fremgår var akseptkriteriet ikke koplet mot risiko, dvs. muligheten for uønsket hendelse og konsekvenser ved denne. Derimot la NVE til grunn et generelt materialkrav. Dette ble underbygget av at dimensjoneringsstandarden som materialkravet var hentet fra, ga et akseptert og nødvendig sikkerhetsnivå og at betydelige avvik fra materialkravet følgelig også ville gi uakseptable avvik fra sikkerhetsnivået.

Mer vanlig er det imidlertid at akseptkriteriene koples til sannsynlighet for gitt ulykke, risiko. Forholdsvis tidlig begynte diskusjonen om aktuelle akseptkrav vedr. maksimal muligheten for dødsulykke. I dag er det dels tale om individuell risiko, dels samfunnsrisiko.

Kjent er ellers de akseptkriterier Norsk Hydro har satt for egen virkomhet. Som individuell risiko refereres:

- Mulighet for død for Hydro-ansatt: 10^{-3}
- Mulighet for stor skade på annenpersons eiendom: 10^{-4}
- Mulighet for død for annenperson: 10^{-5}

Når det gjelder samfunnsrisiko kan det bli tale om hvor mange som blir berørt av en ulykke. Dette angis ved FC- eller FN-diagram. I det siste tilfellet blir konsekvensen som antall døde, se figur 8.1. I FC-diagrammet byttes antall døde ut med det økonomiske tap som kan følge av en ulykke.



Figur 8.1: Eksempel på FN-diagram med akseptkriterium for samfunnsrisiko.

Ifm. de antydede akseptgrenser for individuell risiko, kan det til sammenligning nevnes at det i Norge er størrelsesorden 2000 personer som hvert år dør i ulykke. Med 4 mill. nordmenn, blir den enkeltes årlige mulighet for slik død: $0{,}5 \cdot 10^{-3}$.

Når det gjelder tap av menneskeliv, blir det til tider stillt spørsmålet om dette kan omregnes til omkostning. Slik omregning har vanskelige etiske sider. I utgangspunktet tas det avstand fra selv ideen om at omregningen skal kunne gjøres. Det må likevel kunne hevdes at analogisering skjer indirekte.

For noen år siden refererte media en undersøkelse utført av Transportøkonomisk institutt hvor instituttet hadde sett på ulike veiprosjekter. Ved å sammenligne kalkylene for forslag hvor bevilgende myndigheter hadde sagt henholdsvis ja og nei, med tilhørende trafikksikkerhetsberegninger, kunne det hevdes at "prisen" for et menneskeliv var i overkant av 10 mill. kroner. I tillegg registrerte man i høsten 1995 et forlag fra Fiskeridepartementet som gikk ut på at det skulle bevilges 20 mill. kroner for over 4 år å spare 50 menneskeliv. Dette er 50 % av de dødsulykker som ellers innen samme periode kunne påregnes innen fiskeflåten. Tallene gir i gjennomsnitt 400 tusen kroner pr. menneskeliv Til sammenligning har det regionale kraftselskapet i British Colombia i data for risikoaksept analogiserer et menneskeliv med et økonomisk tap på 10 mill. kanadiske dollar.

9. Gjennomføring av pålitelighets-/risikoanalyse.

Er det aktuelt å gjennomføre en analyse, bør man først fastslå eget behov for analyse. Spørsmålet blir: Hva skal analysen være underlag for og hvilke nytteeffekter ønsker en. Det som her kan påregnes, er omtalt i kapittel 3 i dette manuskript. Ved fastleggelsen av behovet blir det imidlertid viktig å være nøktern og spesifikk. Velges alt fra "alle hyller", har man vært for raus.

Med formulert behov kan planleggingsfasen innledes. Denne består i at det for analysen bestemmes mål og omfang. Målet følger som regel av behovet. Omfanget bør drøftes med noen som har erfaring fra lignende oppgaver. Det samme gjelder to andre elementer som hører hjemme i planleggingsfasen: Tempoplan og organisering.

Førstnevnte gis imidlertid også ofte av behovet. Trenger man analyseresultetet som underlag ved budsjettarbeid, må selvsagt resultatet foreligge iht. de tider dette krever.

For organiseringen er det hvis man tenker å involvere eget personell i analysearbeidet, viktig å også bringe disse inn i planleggingen. Det bør dessuten ovenfor ens egne i denne fase gis prioritet til oppgavepresentasjon og innsatsmotivering. Sentrale stikkord blir: Hva ønsker man å oppnå, og hva skal gjøres. Erfaringer viser at det er vel så viktig å overbevise eget deltagerpersonell som å "selge" oppgavegjennomføringen til den som bevilger penger.

Etter planleggingsfasen kommer gjennomføringen. Denne kan inneholde ulike elementer avhengig av hva som er bestemt ved planleggingen. Stikkord kan være: Systembeskrivelse, systemfeil, forutsetninger, årsaksanalyse, datainnsamling, dataanalyse og presentasjon.

Bruken av resultatene markerer avslutningen for oppgaven, alternativt den egentlige begynnelse. Dette blir alt etter som man ser det. Skal resultatene benyttes ifm. valg mellom to ulike tilbud, kan det være nærliggende å tenke på førstnevnte måte. Er det derimot ønskelig at analysen gir grunnlag for videre sikkerhetsarbeid, har en kanskje de største utfordringene foran seg når rapporten ligger på bordet.

10. Analyseteknikk.

Ulike analyseteknikker er listet i kapittel 3. I det følgende vil man kort si hva de viktigste går ut på.

Grovanalyse benyttes for kartlegging av farer, vanligvis hvilke faremomenter som knyttes til bestemte aktiviteter. Ved analysen avdekker man uønskede hendelser og

analyserer disse med tanke på årsak og konsekvens. Forbedringer og forebyggende tiltak drøftes. Grovanalyse gjøres ofte som innledende kartlegging ved en større risikoanalyse.

Konsekvensanalyse skal beskrive hendelser som følger etter en spesifisert uønsket hendelse. Målet for analysen blir å angi virkningene som hendelsene får for den uønskede hendelses system, andre systemer, mennesker og miljø. Umiddelbare effekter av hendelsene kan være bestemt ved grovanalyse eller FMEA.

FMEA (Failure Modes and Effect Analysis) gjennomgår et system komponent for komponent og spør hvordan den aktuelle komponet kan feile og hvilke konsekvenser dette vil gi. Metoden anses å være enkel i bruk, men det at den tar for seg enkeltkomponentene og under dette forutsetter at alle andre komponenter fungerer tilfredsstillende, gjør den ikke i stand til å avdekke hva som skjer når ulike komponeter svikter samtidig. Metoden er bl.a. benyttet av Norsk Hydro ved sikkerhetsgjennomgang av Hydros kraftverker. Dokumentasjonen fra FMEA kan føres i egnet skjema. Norsk Hydro har ved sine undersøkelser anvendt skjemaer med kolonnene: Anleggsdel - uønske hendelse - årsak - hyppighet - konsekvens - konsekvensklasse - tiltak/kommentar. Dette er stort sett i overenstemmelse med tilsvarende skjema gitt i [1].

FMECA (Failure Modes, Effects and Criticality Analysis) er FMEA hvor kritikaliteten ved feil rangeres. Kritikalitet sier i denne sammenheng noe om graden av uønskethet ved feilenes konsekvenser. En type FMECA ligger til grunn når Statkraft ved egne kraftverk utarbeider kritikalitetsstyrte vedlikeholdssystemer.

HTA (hendelsestreanalyse), se GFUA.

FTA (feiltreanalyse) blir ansett som den mest anvendte analyseteknikk ved påliteilghets- og risikoanalyser. Feiltreet tegnes med grafiske symboler og har øverst en uønsket "topphendelsen". I vannvei kan en topphendelse være at man ikke får åpnet en luke. Under topphendelsen har feiltreet en "port". Denne angir om topphendelsen avhenger av en eller flere inngangshendelser. Kan luken i eksemplet manøvreres av to uavhengig motorer, er topphendelsen avhengig av at begge motorer svikter. For den enkelte motor avhenger svikten enten av feil ved motoren eller at stømtilførselen er borte. Slik feiltreet tegnes kan det således ha mange nivå. Det anses mest riktig at feiltreanalyser gjennomføres av grupper på 2-4 personer. Disse bør utfylle hverandre slik at "gruppen" har inngående kunnskap om anvendt analyseteknikk og det system som skal analyseres. Fastleggelse av topphendelser og opptegningen av feiltre kan imidlertid kun bli en del av feiltreanalysen. I tillegg er det ofte aktuelt å bestemme minimale kuttmender, nødvendig ved fastleggelse av funksjonssannsynlighet, samt å analysere feiltreet såvel kvalitativt som kvantitativt. Det siste krever tilgang til pålitelighetsdata. Når det gjelder systemet, kan det ved FTA være aktuelt å ha dette dokumentert ved FMEA.

GFUA (grafisk feilutviklingsanalyse) benyttes ved analyse av systemer og situasjoner hvor rekkefølger og tidspunkt for hendelser har betydning. GUFA blir vanligvis en kombinasjon av feiltreanalyse og konsekvensanalyse, som regel inngår også HTA.

HAZOP (Hazard and Operability) anses velegnet for påvisning av faremomenter i større anlegg. Ved gjennomføringen ser en på prosessen og vurderer hvordan avvik fra forutsatte betingelser kan oppstå og medføre konsekvens. Analysen gjennomføres ved bruk av stikkord. Tenker en seg en vannoverføring, blir det her aktuelt å spørre hva som kan gi redusert, henholdsvis økt vannstrøm og hva konsekvensene ved dette blir.

SMORT (Safety Management and Organization Review Technique) benyttes for vurdering av virksomhet og kommer bl.a. til anvendelse ved granskning etter ulykker. SMORT fokuserer i særlig grad tre forhold: Uoverenstemmelse mellom faktiske forhold og spesifiserte krav. Forhold som kan føre til ulykke. Risikoforhold som ved beslutninger er vurdert og akseptert. SMORT kan dessuten fungere på inntil fire nivå. Det laveste knyttes til konkret ulykkessituasjon. Det øverste gjelder risikoforhold som kan knyttes til overordnet ledelse.

11. Litteratur.

En liste over litteratur som kan være nyttig for den som ønsker å utdype sin kunnskap ifm. forhold presentert i dette dokument, er gitt nedenfor. Etter listen følger en kort omtale av de enkelte publikasjoner. Referansenummereringen overenstemmelser med referansene som er angitt tidligere i dette dokument.

Forfatter/redaktør.	Tittel	Utgiver	Referanse
Aven, Terje.	Pålitelighets- og risikoanalyse.	Universitetsforlaget.	[1]
Høyland & Rausand.	System Reliability Theory.	John Wiley & Sons.	[2]
Rausand, Marvin.	Risikoanalyse.	Tapir.	[3]
RTT.	Ordbok sikkerhet og risikoan.	Universitetsforlaget.	[4]

[1] Boken gir en grei oversikt ifm. ulike analyseteknikker, og er velegnet for den som ønsker å studere faget sikkerhets- og pålitelighetsteknikk uten at dette skal forutsette særlige matematiske forkunnskaper. Utgivelsesår for 2. utgave er 1994.

[2] Boken benyttes som lærebok ved NTH. Den er skrevet på engelsk og krever gode matematiske forkunnskaper hos den som ved selvstudium skal trenge inn i stoffet. På den annen side er boken den eneste av de i dette kapittel angitte referanser som i særlig grad belyser teoretiske sider ved sikkerhets- og pålitelighetsteknikk. Utgivelsesår er 1994.

[3] Boken er skrevet som veiledning til NS 5814, "Krav til risikoanalyser" og rettes mot personer som ønsker en enkel innføring i vanlig benyttede metoder. Boken er lettlest og presenterer fyldige referanselister i tilknytning til de enkelte kapitler. Utgivelsesår er 1991.

[4] Heftet på 30 sider er utgitt av Rådet for teknisk terminologi (RTT). Fullstendig tittel: "Ordbok for sikkerhet og risikoanalyse". Vanlige norske ord og uttrykk benyttet innen sikkerhets- og pålitelighetsteknikk, blir definert. Tilhørende engelske termer angis. Heftet ble utgitt i 1983, og er i dag for enkelte uttrykks vedkommende noe foreldet.