22. juli-kommisjonen

NOTAT: 10/12

EN MODELL FOR SAMFUNNSSIKKERHET

Professor Per Morten Schiefloe, Dr. Philos

Institutt for sosiologi og statsvitenskap
NTNU Samfunnsforskning AS

November 2011

www.22julikommisjonen.no

En modell for samfunnssikkerhet

Per Morten Schiefloe, Dr. Philos.

professor
Institutt for sosiologi og statsvitenskap
NTNU

forskningssjef
NTNU Samfunnsforskning AS

Samfunnssikkerhet

Samfunnssikkerhet har å gjøre med samfunnets evne til opprettholde viktige samfunnsfunksjoner og ivareta liv og helse under ulike former for kritiske hendelser. Hendelsene kan være naturskapte, som storm og ekstremnedbør. De kan skyldes teknisk svikt, for eksempel i strømforsyning eller datanett, de kan skyldes ulykker, for eksempel i transportsektoren, og de kan skyldes intenderte handlinger, som terror og sabotasje.

Samfunnssikkerhet har i det siste tiåret fått en tydeligere plass på den politiske agendaen, noe som f.eks. kom til syne i Stortingsmelding 17 (2001-2002) – *Samfunnssikkerhet* – som i stor grad tok utgangspunktet i innstillingen fra *Sårbarhetsutvalget* (Willoch-utvalget), som ble fremlagt i 2000. Administrativt sorteres temaet primært under *Direktoratet for samfunnssikkerhet og beredskap* (DSB) som er lokalisert i Tønsberg og ble opprettet i 2003. DSB har overtatt oppgavene fra de tidligere direktoratene for sivilt beredskap og for brann- og elsikkerhet. DSB's samfunnsoppdrag, slik de selv formulerer det, er som følger:

> Med god oversikt over risiko og sårbarhet i samfunnet skal DSB arbeide for at det drives et godt forebyggende arbeid, at vi har fullgod beredskap for å møte uønskede hendelser og en god evne til å håndtere slike (www.dsb.no).

Etter terroraksjonen 22.juli er også det politiske ansvaret synliggjort, ved at Justisdepartementet har endret navn til *Justis- og beredskapsdepartementet*.

Selv om samfunnssikkerhet er erkjent som en sentral og viktig problemstilling, og selv om det, i følge DSB, er nødvendig å ha «et helhetsperspektiv på sikkerhetsutfordringene i et komplekst samfunn i

rask endringstakt» (www.dsb.no), har forskningsinnsatsen på området til nå vært relativt begrenset. Unntaket er forskningsprogrammet «Samfunnssikkerhet og risiko – Samrisk», som ble gjennomført i årene 2006-2011 (www.forskningsradet.no/samrisk). Ut over dette har forskningsinnsatsen i Norge vært relativt fragmentert og i stor grad styrt av individuelle forskerinitiativ.

Sikkerhetsforskning

Både nasjonalt og internasjonalt har sikkerhetsforskning i overveiende grad vært innrettet mot å kartlegge og analysere risiko og sikkerhet innenfor spesielle sektorer med stort farepotensial og/eller mange ulykker; industri, energiproduksjon, forsvar og transport. Dette er etter hvert blitt et ganske omfattende forskningsfelt, det arrangeres store internasjonale konferanser (ESREL, WOS, PSAM, SRA m.fl.) og det publiseres årlig en stor mengde vitenskapelige arbeider i tidsskrift og bøker.

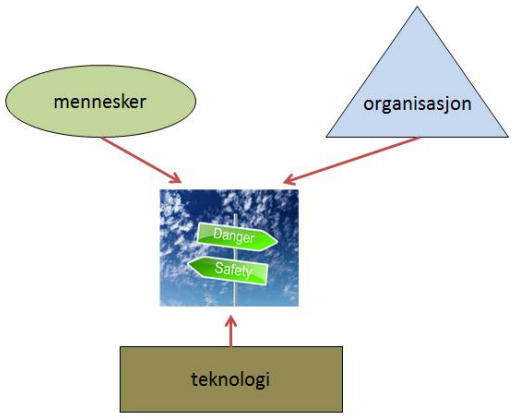
Forskningsbidrag, granskninger, årsaksanalyser og praksis har tydelig dokumentert at sikkerhet er et sammensatt felt, der årsaker, virkemidler og tiltak spenner over mange fagområder. Hale og Hovden (1998) skiller mellom tre generasjoner i sikkerhetsforskningen. Den første betegnes som *den tekniske epoken*. Sikkerhet ble betraktet primært som et teknisk problem og fokus var rettet mot utvikling av maskiner, utstyr og infrastruktur. Den andre generasjonen sikkerhetsforskning trekker også inn *den menneskelige faktoren* og retter oppmerksomheten mot atferd som viktig element sikkerhet. Menneske-maskin problematikk og feilhandlinger settes i fokus, med utgangspunkt i fag som ergonomi, fysiologi og persepsjons- og atferdspsykologi. Den tredje generasjonen omtales som *ledelse og kultur*, etter hvert som forskningen avdekker betydningen av *organisatoriske kvaliteter og prosesser*. Erik Hollnagel (2006) fremhever at en i tillegg til disse tilnærmingene kan legge til en fjerde, som han omtaler som basert på *ikke-lineære og systemiske modeller*. Det sentrale argumentet for slike tilnærminger er at ulykker kan inntreffe i komplekse systemer og på uforutsette måter, fordi de er utsatt både for interne (endogene) og ytre (eksogene) påkjenninger og variasjoner.

MTO – Mennesker, teknologi og organisasjon

Praktisk sikkerhetstilnærming i risikoutsatt virksomhet styres dag i de fleste tilfeller ut fra en tilnærming som bygger på en erkjennelse av at sikkerhet skapes i et samspill mellom teknologiske, menneskelige og organisatoriske faktorer, oftest omtalt som MTO. I Norge er dette særlig tydelig uttalt i olje- og gassindustrien. Det gjelder både i selskapene og som grunnlag for tilsynsmyndighetenes arbeid. Dette uttrykkes blant annet I Stortingsmelding 12 (2005-2006) «Helse, miljø og sikkerhet i petroleumsvirksomheten»:

MTO-forhold som myndighetene har lagt særlig vekt på i sin oppfølging og som også blir er viktig å følge opp i årene framover er bl.a. knyttet til:

- *Psykososiale og organisatoriske forhold*
- *MTO i sikkerhetskritiske systemer*
- *Alarmsystemer i drift*
- *Kompetanse, opplæring*



Figur 1: MTO

Ut fra denne typen erkjennelse fremstår dagens avanserte sikkerhetsforskning som et utpreget flerfaglig felt, som trekker på bidrag fra teknologi, matematikk/statistikk, organisasjons-/samfunnsfag og psykologi. Ut av dette er det utkrystallisert en del sentrale begreper, modeller og teorier som er av relativt generisk karakter, og som i større eller mindre grad også kan overføres til problematikken omkring samfunnssikkerhet.

Teknologi og mennesker

Teknologi må i sikkerhetssammenheng forstås ut fra to dimensjoner. Den første har å gjøre med teknologiens pålitelighet i seg selv, både i forhold til operasjoner og som mulig barriere. Avgjørende for sikre operasjoner er at teknologien som benyttes ikke svikter, at det er tilstrekkelig kapasitet, og at det for kritiske funksjoner er etablert tilstrekkelig redundans i form av reservesystemer. Den andre dimensjonen har å gjøre med teknologien som redskap for mennesker og som noe de benytter seg av eller forholder seg til. Teknologien kan være mer eller mindre trygg i forhold til arbeidsulykker, mer eller mindre lett å operere, mer og mindre sikret mot feilhandlinger, og mer eller mindre lett å tolke.

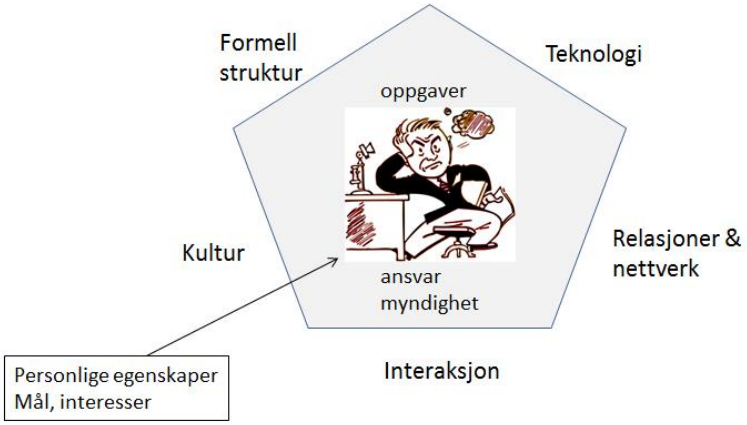
Vi kan definere sikkerhetskritisk atferd som: *Atferd der utfallet av atferden kan ha direkte eller indirekte konsekvenser for sikkerheten i en operasjon eller aktivitet*. Det vil si at dette ikke bare omfatter de som arbeider i den «skarpe enden», men også alle andre aktiviteter som kan ha betydning for hva slags avveininger som foretas, hvilke beslutninger som fattes og hvordan operasjoner utføres. Et hovedpoeng hos den danske sikkerhetsforskeren Jens Rasmussen (1997) er eksempelvis påvisningen av at press mot lønnsomhet, som utøves fra ledelse eller eiere, kan medføre reduserte sikkerhetsmarginer og at risikoen for ulykker øker.

Menneskelig handling er en sentral kilde til ulykker, ved at forhold oversees, glemmes eller misforstås, eller ved at operasjoner utføres feilaktig eller i strid med vedtatte prosedyrer eller regelverk. Granskninger av hendelser ender ofte med at ulike former for «menneskelig svikt» er direkte årsak eller utløsende faktor. Generelt kan en skille mellom fire hovedtyper av slik svikt:

- Feilvurderinger, forårsaket av manglende kunnskap eller feiltolkninger
- Feilhandlinger/operatørfeil
    - slurv, uoppmerksomhet, forglemmelser
    - kompetansesvikt - manglende opplæring
    - sabotasje
- Utelatelser – regelbrudd

    - bevisst
    - ubevisst
- Koordineringsfeil (misforståelser, feilleveranser, manglende kommunikasjon)

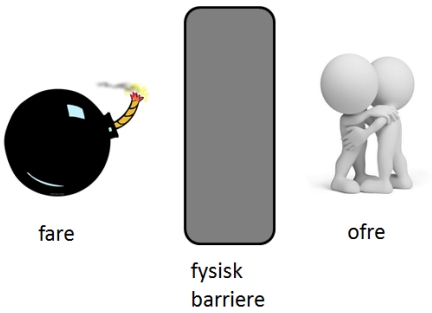
Noen ganger stopper forklaringen der, men ofte vil nærmere analyser avdekke at svikten har bakenforliggende årsaker av organisatorisk eller arbeidsmessig karakter. Det kan for eksempel dreie seg om høyt arbeidspress, uhensiktsmessig utstyr, uklare rutiner, dårlig ledelse, manglende opplæring og trening, eller trekk ved organisasjonskulturen. Både for å forklare uønskede hendelser og for å avdekke mulig risiko, er det derfor oftest nødvendig med mer omfattende analyser, der en fokuserer på hva slags kontekst sikkerhetskritisk atferd finner sted innenfor. I en slik analyse kan det være nødvendig å rette oppmerksomheten mot et bredt sett av organisatoriske faktorer. Et mulig utgangspunkt er å benytte en «pentagonanalyse», der en ser sikkerhetskritisk atferd og personlige egenskaper og arbeidsoppgaver i en kontekst som konstitueres av formell struktur, teknologi, organisasjonskultur, interaksjon (samhandling, kommunikasjon mm) og sosiale relasjoner og nettverk Schiefloe m.fl. 2005, Schiefloe 2011, 2012).



Figur 2: Pentagonanalyse av konteksten for sikkerhetskritisk atferd.

Barrieremodeller

Ulykker kan oftest føres tilbake til situasjoner der mennesker, materiell eller miljø påføres skade som følge av ukontrollert overføring av energi (trykk, varme) eller farlige substanser (kjemikalier, gift, stråling). Beskyttelse mot slik ukontrollert overføring kan skje i form av fysiske barrierer. Slike barrierer kan være av ulik type. De kan være knyttet til kilden for energi eller substanser. Eksempel er overrislingsanlegg og utblåsningsventiler. De kan ha form av ulike former for å beskytte omgivelsene mot konsekvenser av hendelser. Eksempel er brannvegger og splintsikkert glass. Beskyttelsen kan også være knyttet direkte til personer, f.eks. påbud om bruk av verneutstyr. En kan skille mellom *preventive barrierer*, som har til hensikt å forhindre at ulykker skjer, og *beskyttende barrierer*, som har til formål å redusere konsekvensene av en hendelse.



Figur 3: Energi-barrieremodell

Mennesker kan også fungere som en form for fysiske barrierer. Det viktigste eksemplet er vakthold som forhindrer kontakt mellom farekilde og mulige ofre.

Barrieretenkningen er utviklet for å forhindre skader som følge av uhell; som brann, eksplosjoner og fallulykker. Den er naturligvis også relevant i forhold til intenderte handlinger, som sabotasje, kriminalitet og terror. Eksempler er skuddsikkert glass og adgangskontroll.

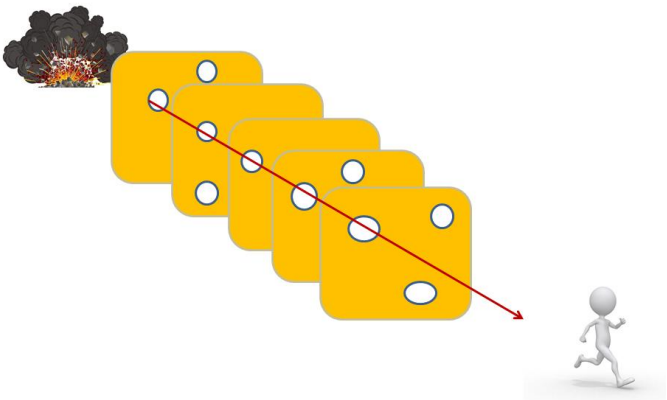
Barrieretenkning er ikke begrenset til fysiske barrierer. Vi kan også snakke om organisatoriske og menneskelige barrierer – «myke barrierer». Vi kan dele disse i to hovedgrupper. Noen barrierer dreier seg om å sikre at ting gjøres riktig, mens andre omfatter ulike former for kvalitetskontroll. Noen av disse barrierene er formelle, i den forstand at de er vedtatt og formulert skriftlig. I en organisasjon kan en for eksempel ha regler som sier hvordan ulike arbeidsoppgaver skal utføres, og hva slags sikrings- og kontrolltiltak som skal benyttes i ulike sammenhenger. Eksempler er styrende dokumentasjon, krav til sertifisering, sjekklister, sikker jobb analyse (SJA) og prosedyrer for håndtering av farlige stoffer. I mange sammenhenger er det også slik at potensielt farlige operasjoner skal godkjennes av overordnede eller ansvarshavende før de iverksettes.

Noen sikkerhetsbarrierer er av uformell karakter, i den forstand at de ikke er vedtatt eller har formell status. På individnivå sikres sikker arbeidsutførelse dels ved at de som gjør jobben har tilstrekkelig kompetanse, dels ved at de tar oppgaven alvorlig, unngår personlige feil, og har «gode holdninger» til sikkerhet. I mange sammenhenger er det også relevant å snakke om uformelle sikkerhetsbarrierer av sosial karakter. Det kan for eksempel dreie seg om at kolleger bidrar med råd og erfaringer, eller ved at de passer på hverandre og griper inn dersom noe er i ferd med å gå galt, eller dersom arbeidsoperasjoner utføres på en uforsvarlig eller ureglementert måte.

	Formelle mekanismer	Uformelle mekanismer individuelle	Uformelle mekanismer sosiale
Gjøre tingene riktig	prosedyrer/ sjekklister	kompetanse holdninger praksis	råd fra kolleger
Kvalitets-kontroll	godkjenning/ arbeidstillatelse		«passe på hverandre/ si fra»

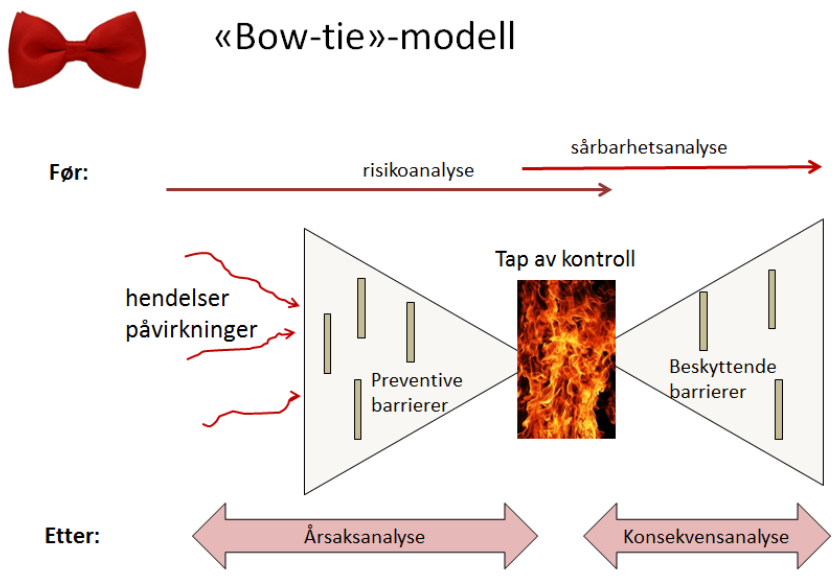
Figur 4: Organisatoriske og menneskelige sikkerhetsbarrierer

James Reason (1990) har pekt på at ulykker ofte skjer når flere barrierer svikter samtidig. Dette er kjent som «sveitserostmodellen», fordi tankegangen kan illustreres som en rekke barrierer som hver inneholder potensielle «hull». Disse barrierene kan være materielle/fysiske, menneskelige og organisatoriske. Ulykker skjer når alle hullene slumpmessig ligger på rekke, slik at energi eller farlige substanser (eller en person som planlegger terror) slipper gjennom alle planlagte hindringer.



Figur 5: «Sveitserost-modellen»

«Bow-tie» er det engelske uttrykket for en sløyfe som knyttes rundt halsen. En slik stilisert sløyfe kan benyttes for å illustrere forholdet mellom preventive og beskyttende barrierer. Dette kalles ofte for en «Bow-tie-modell». Bow-tie-modellen illustrerer også forholdet mellom ulike former for analyser. For å forhindre, eller forberede seg, på en mulig hendelse, kan en skille mellom en risikoanalyse, som sier noe om hvor sannsynlig det er at noe kan skje, og at det i så fall ikke fanges opp av de preventive barrierene, mens en sårbarhetsanalyse omfatter de beskyttende barrierenes styrke og relevans, og hva slags konsekvenser en ulykke kan tenkes å føre med seg. Etter at en hendelse har inntruffet, kan en skille mellom en årsaksanalyse og en konsekvensanalyse.



Figur 6: Bow-tie-modell

Hendelsesforløp

Forskning om makrohendelser i industrielle systemer viser at store ulykker sjelden kommer som «lyn fra klar himmel». I ettertid viser det ofte at det forut for hendelsen har skjedd en gradvis svekkelse av materielle eller organisatoriske sikkerhetsbarrierer, og at det har vært ulike tilløp og nestenhendelser (Perrow 1999). Et kjent eksempel er eksplosjonen som fant sted i et gassprosesseringsanlegg i Longford i Australia i 1998. Her sies det i en påfølgende studie at:

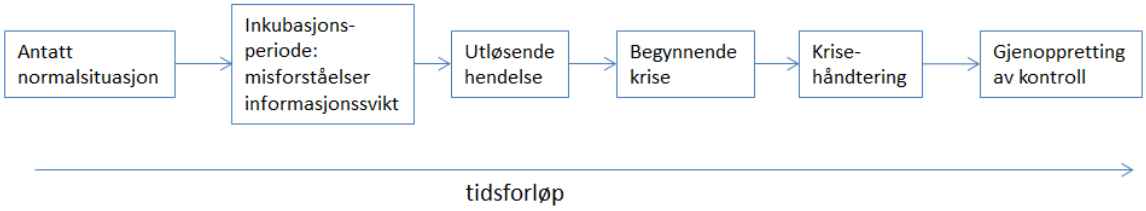
> *«The accident was quite preventable. It was caused by a series of organizational failures: the failure to respond to clear warning signs, superficial auditing, and, as much as anything, a failure to learn from previous experience."* (Hopkins 2000)

I årsaksanalysen etter gassutblåsningen på Snorre A-plattformen i 2004 viste også den påfølgende årsaksanalysen at sikkerhetsmarginene i organisasjonen over tid var blitt gradvis svekket (Schiefloe m fl 2005).

Turner (1978) introduserte begrepet *menneskeskapte katastrofer* (Man-made disasters) for å betegne ulykker som utvikler seg over tid gjennom kjeder av hendelser, og som potensielt kunne vært forhindret med tilstrekkelig oppmerksomhet og adekvat informasjonsflyt. Et hovedpoeng hos Turner er at årsakskjedene som leder frem til katastrofen blir muliggjort som følge av en kultur preget av feiltolkninger av signaler, overflatiskhet og utvikling av uformelle normer og væremåter som også kan være i strid med formelle regler og godkjente prosedyrer. På dette grunnlaget formuleres følgende definisjon av denne typen hendelser:

> *«an event, concentrated in time and space, which threatens a society or a relatively self-sufficient subdivision of society with major unwanted consequences as a result of the collapse of precautions which had hitherto been culturally accepted as adequate." (Turner & Pidgeon 1997:70)*

Turner oppsummerer sine funn vedrørende utviklingen av ulykker i en stadiemodell:



Figur 7: Stadier i utvikling av ulykker.

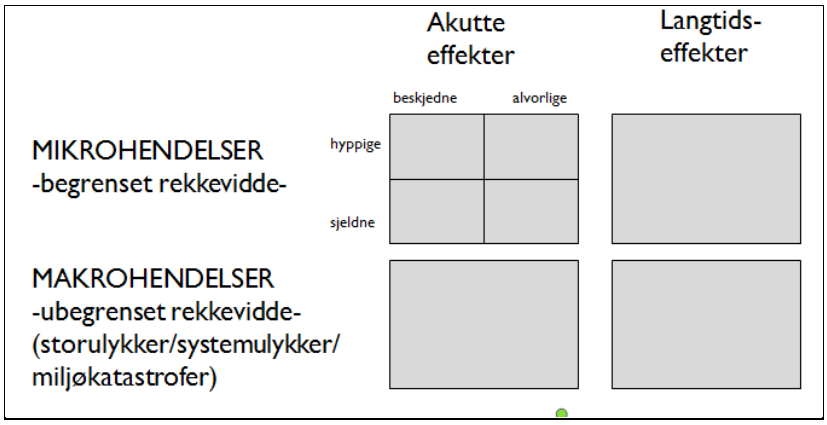
Systemulykker og hendelser med begrenset rekkevidde

Perrow (1999) bruker uttrykket *systemulykke* for å betegne en hendelse som rammer et større system, der en utløsende teknisk svikt, uventet ytre påvirkning eller feilhandling fører til systemsammenbrudd eller katastrofe. Perrow sier at slikt er «normal accidents». Et hovedpoeng hos Perrow er at slike ulykker er noe en må regne med vil forekomme i systemer som er komplekse og tett koblet. Et relevant eksempel på en systemulykke er utblåsningen og gasseksplosjonen på boreriggen Deepwater Horizon i Mexicogulfen i 2010. På norsk sokkel har en også eksempler på hendelser som kunne utviklet seg til systemulykker, men som ble avverget (Snorre A i 2004, Gullfaks C i 2010). Systemulykker kan også inntreffe på samfunnsnivå, f.eks. i form av sammenbrudd i strømforsyningen eller i tele- og datanettet.

Andre typer hendelser kan en si har begrenset rekkevidde. Det vil si at de når de inntreffer rammer begrenset, og ikke fører til forsterkende viderekoblinger. Slike hendelser kan også være alvorlige. Eksempler er dødsulykker i arbeidslivet eller trafikkulykker. Hvis de rammer en eller et fåtall personer, eller har begrensede materielle konsekvenser, kan vi omtale dette som *mikrohendelser*. Hvis de rammer mange, eller har omfattende materielle eller miljømessige konsekvenser, kan vi omtale det som *makrohendelser*.

Noen hendelser er akutte, i den forstand at de oppstår plutselig og uventet, og med umiddelbare konsekvenser. Eksempler er arbeidsulykker og eksplosjoner. Andre hendelser utvikles langsomt og med konsekvenser som kanskje blir merkbare først etter lang tid. Eksempler er helseskader som skyldes langvarig eksponering for giftige substanser eller miljøødeleggelser som følger av skadelige utslipp over lang tid.

En utfordring i arbeidet med sikkerhet er å holde disse ulike typene hendelser fra hverandre, fordi de oftest har ulike årsaker og må møtes med ulike typer virkemidler. I ulike systemer for avviksregistrering og avviksbehandling ser en imidlertid ofte at de ulike kategoriene ikke holdes tilstrekkelig atskilt. Særlig når det gjelder mikrohendelser, kan det også være nødvendig å skille mellom det som skjer hyppig og det som skjer sjeldent, og mellom hendelser som har beskjedne og alvorlige konsekvenser.



Figur 8: Mikro- og makrohendelser

Høypålitelige organisasjoner (high-reliability organizations – HRO)

Mens Perrows teori om normale ulykker (Normal Accident Theory – Nat) fremhever at komplekse og tett koblete systemer i praksis vil være umulige fullt ut å kontrollere og overskue, og at det derfor innimellom nødvendigvis vil skje ulykker, peker andre forskere på at praksis viser det motsatte. LaPorte & Consolini (1991) fremhever dette i en artikkel som de har gitt den talende overskriften *Working in Practice but Not in Theory: Theoretical Challenges of «High-Reliability Organizations»* . Deres poeng er at noen særdeles komplekse og potensielt ulykkesutsatte organisasjoner viser seg å operere over lang tid uten at noe alvorlig skjer. Eksempler som trekkes frem er hangarskip og systemer for kontroll av flytrafikk. Slike organisasjoner betegnes som *høypålitelige organisasjoner*, på engelsk forkortet til *HRO*. LaPorte & Consolini trekker frem *organisatorisk redundans* som sentral forklaring. Det vil si at når det gjøres feil, eller noe svikter, så korrigeres dette umiddelbart og før det får negative konsekvenser. Overlappende kompetanse, årvåkenhet og en kultur der sikkerhet har høyeste prioritet er viktige faktorer i denne sammenhengen.

Weick & Sutcliffe (2007) sier at høypålitelige organisasjoner kjennetegnes av det de omtaler som «mindfulness», og som kan oversettes med *oppmerksomhetsfokus*. Dette innebærer at aktørene (de som jobber i organisasjonen) er kontinuerlig fokusert på helhet og sammenhenger og er oppmerksomme på mulige avvik som kan indikere risiko. De peker videre på at dette er en form for dynamisk kompetanse som stadig er i utvikling, og som innrullerer nye erfaringer.

Weick & Sutcliffe fremhever fem sentrale egenskaper ved HRO:

(1) Preoccupation with failure . Det vil si at en kontinuerlig ser etter og rapporterer alle mulige feil eller forsømmelser, fordi dette sees som symptomer på noe som kan gi opphav til hendelser med stort negativt potensial. Knyttet til dette er også evnen til å lære av erfaringer.

(2) Reluctance to simplify. Med dette menes at en motstår tilbøyeligheten til å operere med forenklede og overflatiske bilder av virkeligheten, fordi mer komplette og nyanserte bilder gir bedre forståelse av det som er komplekst og uforutsigbart. I sikkerhetsstyring innebærer det at en ikke faller for fristelsen til å benytte for få eller for enkle indikatorer på tilstanden.

(3) Sensitivity to operations. I følge Weick & Sutcliffe er høypålitelige organisasjoner primært opptatt av det som skjer i «den skarpe enden»: «The 'big picture' in HROs is less strategic and more situational than in most other organizations» (2007:12).

(4) *Commitment to resilience*, som innebærer at organisasjonen er i stand til å håndtere og korrigere uventede hendelser og tilløp til hendelser uten at dette får avgjørende konsekvenser for virksomheten. Høypålitelige organisasjoner er ikke feilfrie, men de håndterer de feilene som oppstår før situasjonen utvikler seg eller kommer ut av kontroll.

(5) Deference to Expertise. Med dette pekes på at myndigheten til å fatte avgjørelser i kritiske situasjoner er delegert til de som står oppe i situasjonen og forstår hva som foregår, uavhengig av godkjenning i et hierarkisk system: «Decisions are made on the front line, and authority migrates to the people with the most expertise, regardless of their rank» (2007:16).

Resilience – robusthet

Resilience kan forstås som motstandskraft eller evne til å opprettholde eller gjenopprette en normaltilstand. Hollnagel (2006:16) sier at kjernen i resilience-begrepet dreier seg om en organisasjons iboende evne til å opprettholde en stabil tilstand og fortsette sin virksomhet tilnærmet upåvirket etter en større hendelse/uhell eller i en situasjon preget av kontinuerlig stress.

Et system som er resilient har fire sentrale kjennetegn (Hollnagel m.fl. 2010):

- De vet hva de skal gjøre, det vil si hvordan en skal håndtere forstyrrelser, uventede hendelser og tilløp.
- De vet hva de skal se etter. Det vil si at en har kapasitet til å overvåke det som skjer, både innenfor systemet og i omgivelsene.
- De vet hva som kan forventes. Det vil si at en har evne til å tolke signaler og forutse mulige forstyrrelser, påkjenninger og trusler.
- De har evnen til å analysere og forstå hendelser, slik at en kan lære.

I fagterminologien omtales denne forskningsretningen oftest som *Resilience Engineering*, begrunnet med at det gjennom bevisste analyser og tiltak er mulig å utvikle organisasjoner slik at de utvikler denne formen for robusthet og motstandskraft mot påkjenninger og ulykker.

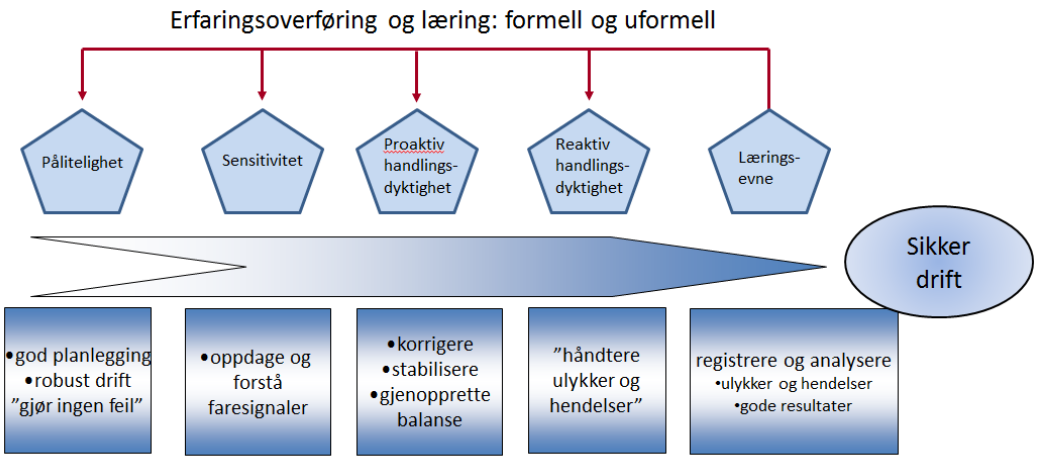
Det meste av den etablerte sikkerhetsforskningen tar utgangspunkt i ting som gikk galt og søker forklaringer og virkemidler ut fra dette. Det som særpreger Resilience Engineering er at en legger hovedvekt på det som går bra og å hente erfaringer og læring ut fra dette. Det vil si at en definerer målsettingen primært til forsikre seg om at ting går som de skal, og ikke bare til å forhindre ulykker. Hollnagel sier det slik:

> "Safety is the sum of accidents that do not occur. While accident research has focused on accidents that occurred and tried to understand why, safety research should focus on the accidents that do not occur and try to understand why."(2006:10)

Organisatorisk sikkerhet

Med utgangspunkt i de modellene og teoriene som er presentert ovenfor, kan vi utlede en enkel modell for organisatorisk sikkerhet, som viser at en organisasjon som skal operere sikkert over tid, må utvikle fem ulike sett av organisatoriske egenskaper:

- Organisasjonen må være **pålitelig**. Det vil si at virksomheten er godt planlagt og styrt, med gode rutiner og tydelige ansvars- og myndighetsforhold. Organisasjonene re også robust og opererer med tilstrekkelig redundans. Medarbeiderne har kompetanse for å håndtere arbeidsoppgavene, og kompetansen utvikles etter behov, gjennom opplæring og trening. Slike organisasjoner «gjør ingen feil».
- Organisasjonen må være **sensitiv**. Det vil si at en har prosedyrer, rutiner, praksis og kultur som gjør at en oppdager og forstår mulige faresignaler innenfor eller utenfor virksomheten, også når dette forutsetter at en kombinerer informasjon på nye og ikke-planlagte måter, bruker nye tolkingsmodeller, eller at informasjonene fanges opp av noen som ikke har det aktuelle feltet som definert ansvarsområde.
- Organisasjonen må utvikle **proaktiv handlingsdyktighet**. Det vil si at en har kompetanse, rutiner og reaksjonsevne, slik at tilløp stoppes før de utvikles til mer omfattende og alvorlige hendelser. I mange situasjoner innebærer det at organisasjonen må ha evne til **improvisasjon**, fordi det kan oppstå situasjoner som en ikke har forestilt seg eller har forberedt seg på.
- Organisasjonen må ha **reaktiv handlingsdyktighet**. Det vil si at en må være i stand til å håndtere hendelser og ulykker som uansett måtte inntreffe, slik som tekniske sammenbrudd, brann, utblåsninger, kollisjoner eller terrorhandlinger.
- Organisasjonen må ha **evne til læring**. Det vil si at en må være i stand til å registrere og analysere ulykker og hendelser og bruke dette som grunnlag for både formell og uformell erfaringsoverføring og læring. Som understreket av Hollnagel (2006), er det også viktig at en er i stand til å trekke lærdom ut av det som går som det skal.



Figur 9: Modell for organisatorisk sikkerhet.

Et sentralt poeng her er at de ulike kapabilitetene forutsetter ulike organisatoriske og egenskaper, fordi det ikke er noen nødvendig sammenheng mellom disse. En veldrevet byråkratisk organisasjon kan operere pålitelig og «uten feil», men være dårlig rustet til å oppdage tilløp som ikke er definert

inn som noens bestemte ansvarsområde, eller som fordrer at en kombinerer informasjon fra ulike kilder på måter som det ikke finnes prosedyrer eller rutiner for. En tilsynelatende robust organisasjon kan også vise seg å være ute av stand til å håndtere uventede hendelser dersom disse forutsetter evne til improvisasjon. Eller det kan være omvendt. Årsaksanalysen etter gassutblåsningen på Snorre A i 2004 viste at organisasjonen ikke var så pålitelig som den burde, og at en heller ikke var i stand til å oppdage at en alvorlig hendelse var i ferd med å utvikle seg, før gassen strømmet ut. Da utblåsningen først var et faktum, viste det seg imidlertid at organisasjonen hadde en særdeles velutviklet evne til improvisasjon og til å finne løsninger som gjorde at situasjonen etter hvert kom under kontroll (Schiefloe m fl 2005).

I organisasjonsutvikling for sikkerhet impliserer dette at en må rette oppmerksomheten mot alle disse kapabilitetene og stille spørsmål ved i hvilken grad organisasjonen har de kvalitetene som er nødvendige; for tilstrekkelig pålitelighet, sensitivitet, proaktiv handlingsdyktighet, reaktiv handlingsdyktighet og læring.

Samfunnssikkerhet og sikkerhet mot terror

Mens det etter hvert er utviklet mange modeller og teorier om sikkerhet i organisasjoner og industriell sikkerhet, er samfunnssikkerhet et mindre utviklet forskningsområde. Dette gjelder også internasjonalt. Det er mange årsaker til det. En viktig forklaring er at dette er et svært komplekst felt, og at det rommer mange og ulike typer årsaker og hendelser; som naturkatastrofer, pandemier og teknologiske sammenbrudd som rammer kritisk infrastruktur. Samfunnssikkerhet omfatter også beskyttelse mot viljeshandlinger som opprør, opptøyer, datakriminalitet og terror.

Ansvaret for samfunnssikkerhet er også fragmentert og fordelt på ulike organisasjoner og myndighetsorganer som opererer ut fra ulike lovverk og reguleringer. Beredskapshåndtering ivaretas også av ulike organisasjoner. Med utgangspunkt i etablert kunnskap om sikkerhet i industriell og annen virksomhet har en imidlertid grunnlag for å formulere en overordnet og holistisk modell av forutsetninger for samfunnssikkerhet som kan anvendes både i forhold til intenderte og ikke-intenderte trusler og hendelser. Primære utgangspunkt er Reason's barrieremodell, Turner's stadiemodell og teorien om resilience. I denne sammenhengen illustreres med intenderte hendelser, slik som terroraksjonen 22.07.2011. Følgende elementer inngår da i modellen:

Forebygge. Det vil si at sikkerhet mot intenderte handlinger fremmes ved virkemidler som reduserer eller eliminerer rekrutteringspotensialet for terrorisme. For noen typer potensiell terror kan mulige tiltak være bedre integrering av minoriteter, fattigdomsbekjempelse, utdanningstilbud og bedre tilgang til arbeidsmarkedet. For andre typer kan det dreie seg om tidlig inngripen i forhold til utviklingen av høyreekstreme ungdomsmiljøer.

Vanskeliggjøre, ved bruk av barrierer. Barrierene kan være passive, i form av fysiske stengsler o.a. som gjør at terrorhandlinger gjøres vanskelig eller umulig. Eksempler er beskyttelsestiltak som hindrer adgang til potensielle terrormål. Barrierene kan også være aktive. Sikkerhetskontrollen og bagasjekontrollen på flyplasser, med kombinasjon av menneskelige og teknologiske sjekkpunkter, er et eksempel. Byråkratiske rutiner, godkjenningsprosedyrer m.m. kan også virke på lignende måte. Dersom en skal få adgang til visse militære eller andre særlig utsatte installasjoner, kan det for eksempel være krav om søknad, anbefalinger og godkjenning i forkant.

Oppdage. Dette elementet svarer til det som ovenfor er omtalt som sensitivitet. D.v.s. at en er i stand til å fange opp, kombinere og tolke informasjon eller signaler som indikerer at noe er under utvikling. Vi kan også omtale dette som overvåkning, som kan foregå ved bruk av teknologi, manuelt eller i kombinasjon. Eksempler på organer som driver aktiv overvåkning er Politiets sikkerhetstjeneste og militær etterretning, som har dette som primæroppgave. Andre organer eller enkeltpersoner kan ha dette som formelt tillagt arbeidsoppgave, men det kan også fungere som varsling på mer uformelt grunnlag. Kombinasjonsovervåkning skjer ved bruk av videokameraer og avlytting.

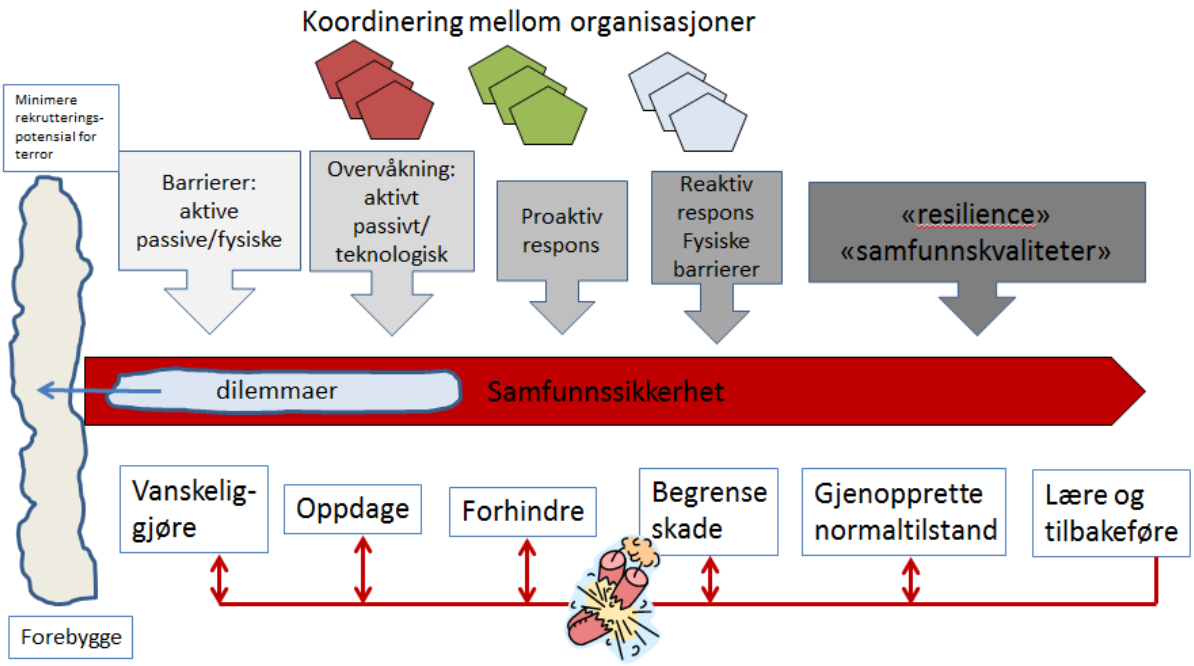
Overvåkning kan også foregå bare ved bruk av teknologi. Eksempler er ulike former for dataroboter og systemer for kunstig intelligens som overvåker nettrafikk. Det foregår også utviklingsarbeid med sikte på dataanalyse av bilder fra overvåkningskameraer basert på atferdsmønstre eller ansiktsgjenkjenning.

Overvåkning av ordinær aktivitet og dagligliv, for eksempel ved bruk av videokamera, representerer et dilemma i forhold til personvern og alminnelige krav til beskyttelse av privatlivet. Ved overvåkning av spesielle grupper, for eksempel unge menn med muslimsk bakgrunn, risikerer en også at dette oppfattes som trakassering og mistenkeliggjøring, og at dette igjen øker tilbøyeligheten til å bli rekruttert til terrorgrupper.

Forhindre innebærer at relevante aktører/myndigheter reagerer når noe oppdages. Eksempel er når terrorplaner avsløres og potensielle terrorister arresteres, før planene er satt ut i livet. Vi kan omtale dette som evnen til proaktiv respons.

Å **begrense skade** dreier seg om evnen til å redusere virkningene av en hendelse som en ikke har lykkes i å forhindre. Begrensning kan skje ved etablering av fysiske barrierer. Terrorutsatte bygninger kan eksempelvis utstyres med splintsikkert glass, sprinkleranlegg og effektive brannvegger. De kan også konstrueres slik at de ikke raser sammen dersom de utsettes for bombeangrep. Brannvesen, politi og redningsetater har også som oppgave å begrense effektene av hendelser. Vi kan si at begrensing av skade dreier seg om et systems evne til **reaktiv respons**.

Etter at en hendelse har funnet sted, er neste steg å **gjenopprette normaltilstand**. Dette kan omfatte både fysiske, medisinske, sosiale og psykiske dimensjoner. På grunnlag av **erfaringsinnhenting** og analyser, kan en så **lære** av det som har skjedd og benytte kunnskapen på en slik måte at en er bedre i stand til å forhindre og eventuelt håndtere nye hendelser. Når det er snakk om hendelser som omfatter eller berører større deler av et samfunn, kan vi si at dette har å gjøre med samfunnets iboende robusthet og kvaliteter. Vi kan også omtale dette som «resilience» på samfunnsnivå.



Figur 10: Modell for samfunnssikkerhet

Utfordringer i arbeid med samfunnssikkerhet

Koordinering kan enkelt defineres som *håndtering av avhengigheter mellom aktiviteter* (Malone & Crowston (1994: 90).

Sikker drift av en ulykkesutsatt organisasjon fordrer at ulike deler av organisasjonen kommuniserer koordinerer ansvar og aktiviteter på en hensiktsmessig måte. Koordinering forutsetter igjen sammenfall i mål- og middeloppfatning, kommunikasjon og samarbeid. I en kompleks organisasjon krever god koordinering en kombinasjon av (1) sentral ledelse som setter retning og stiller krav og (2) lokal beslutningsmyndighet og ansvarliggjorte medarbeidere som har nødvendig frihet til å gjøre de tilpasningene som er nødvendige i forhold til ansvarsområde og arbeidssituasjon.

Et forhold som gjør at sikkerhetsmodellen på samfunnsnivå blir mer komplisert enn tilsvarende modell på organisasjonsnivå, er at de fleste elementene i modellen forutsetter koordinering mellom ulike offentlige etater og organisasjoner, og at slik koordinering alltid er vanskelig å få til.

I de fleste industrielle organisasjoner som er potensielt ulykkesutsatte, har både ledelse og ansatte sikkerhet og risikohåndtering kontinuerlig på agendaen. Det investeres i teknologiske løsninger som skal forhindre og begrense ulykker, og det gjennomføres jevnlige beredskapsøvelser. En sentral drivkraft for aktivt sikkerhetsarbeid er at de involverte i den skarpe enden selv kan bli ofre dersom ulykker inntreffer. For ledelse og eiere, som kanskje ikke er personlig utsatt for fare, er også potensielle økonomiske konsekvenser en faktor som tas inn i vurderingene. Eksplosjonen og utblåsningen på Deepwater Horizon kostet ikke bare 11 mennesker livet, det var også en økonomisk katastrofe for BP. Slike erfaringer er gode argumenter for investeringer i økt sikkerhet. I sikkerhetsforskningen sier en det gjerne på denne måten: «Hvis du synes investeringer i sikkerhet er dyrt, så prøv en ulykke».

På samfunnsnivå er det vanskeligere å få gjennomslag for at investeringer i sikkerhet er nødvendige og «lønnsomme». Sikkerhet krever investeringer og driftsutgifter, og de fleste typer sikkerhetstiltak vil oppleves som plunder og heft i dagliglivet. Et eksempel er sikkerhetskontrollen på flyplassene. I en politisk hverdag der en hele tiden må foreta avveiinger mellom ulike interesser og mange gode formål, kan det være særlig vanskelig å prioritere formål som «ikke vises». Et aktuelt eksempel: Dersom en hadde hatt fysiske barrierer som hadde gjort det umulig å bombe regjeringskvartalet 22.juli, slik at ingen ting hadde skjedd der, ville det vært en «ikke-hendelse», som ingen hadde lagt merke til, eller fått anerkjennelse for at en hadde forhindret.

I forhold til samfunnsmessig kriseberedskap peker McDonnel & Drennan (2006) på fire sentrale utfordringer:

- Kriser og ulykker skjer sjelden (low-probability events), men forberedelse krever store ressurser og konkurrerer mot andre «gode formål»
- Det er vanskelig å forberede seg på en systematisk måte mot hendelser som en ikke har erfaring med, eller kan forutsi
- Krisehåndtering krever integrasjon og synergi mellom ulike aktører, mens samfunnsutviklingen går mot større fragmentering (f.eks. ved outsourcing, privatisering og oppsplitting)
- Katastrofeøvelser og andre former for trening er svært kostbare og blir ofte mer av symbolsk enn av praktisk verdi, fordi eventuelle svakheter som avdekkes, ikke følges opp i praksis og gjennom bevilgninger.

Referanser

Hale, Andrew & Jan Hovden, (1998). “Management and culture: The third age of safety. A review of approaches to organizational aspects of safety, health and environment”, in Williamson, A., Feyer, A.M., (eds) *Occupational injury: a selection of papers presented at the Occupational Injury Symposium*, Sydney, Australia, February 1996, Exeter: Pergamon (129-165).

Hollnagel, Erik, Woods, David D. & Nancy Leveson (eds) (2006) *Resilience Engineering. Concepts and Precepts*. Aldershot: Ashgate

Hollnagel, Erik, Tveiten, Camilla K., & Eirik Albrechtsen (2010) *Resilient Engineering and Integrated Operations in the Petroleum Industry.* Trondheim: Sintef report A16331

Hopkins, Andrew (2000) *Lessons from Longford. The Esso Gas Plant Explosion*. Sydney: CCH Australia

LaPorte, Todd R. & Paula M. Consolini (1991) Working in Practice but Not in Theory: Theoretical Challenges of «High-Reliability Organizations». Journal of Public Administration Research and Theory, 1 (19-48)

Malone, Thomas W. & Kevin Crowston (1994) “The Interdisciplinary Study of Coordination”. *ACM Computer Studies* 26:1 (87-119)

McConnell, Allan & Lynn Drennan (2006)“Mission Impossible? Planning and Preparing for Crisis”, *Journal of Contingencies and Crisis Management*, 14 (59-70)

Perrow, Charles (1999) *Normal Accidents. Living with High-Risk Technologies*. Princeton: Princeton University Press

Rasmussen, J. (1997) "Risk Management in a Dynamic Society". *Safety Science*, 27 (183-213)

Reason, James (1990) *Human Error*. Cambridge: Cambridge University Press

Schiefloe, Per Morten m.fl. (2005) *Årsaksanalyse etter Snorre A hendelsen 24.11.04*. Stavanger: Statoil

Schiefloe, Per Morten (2011) *Mennesker og samfunn. Innføring i sosiologisk forståelse*. Bergen: Fagbokforlaget

Schiefloe, Per Morten (2012) *Analyzing and developing organizations: The Pentagon approach*. Trondheim: NTNU Samfunnsforskning (forthcoming)

Turner, B.A. (1978) *Man-made Disasters*. London: Wykeham Science Press

Turner, B.A. & Pidgeon, N.F. (1997) *Man-made Disasters* (2nd ed). London: Butterworth-Heinemann