SINTEF Teknologiledelse
Sikkerhet og pålitelighet

Postadresse: 7465 Trondheim
Besøksadresse: S P Andersens veg 5
Telefon: 73 59 27 56
Telefaks: 73 59 28 96

Foretaksregisteret: NO 948 007 029 MVA

SINTEF RAPPORT

TITTEL

Feiltoleranse, barrierer og sårbarhet

(Tema 2 innen HMS Petroleum K2: Endring – organisasjon – teknologi)

FORFATTER(E)

R. Rosness, A.B.M. Skjerve, B. Alteren, Ø. Berg, A. Bye, S. Hauge, L.Å. Seim, S. Sklet, C.K. Tveiten, K. Aase

OPPDRAGSGIVER(E)

Norges forskningsråd

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS REF.	
STF38 A03404	Åpen	Prosjektnr. 153537/210 HMS Petroleumsforskning: Endring – organisasjon - teknologi	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	82-14-02714-4	38 45 14.12	68
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
C:\WINNT\Profiles\rosnes.000\Application Data\eRoom\eRoom Client\V6\EditingFiles\Rapport		Ragnar Rosness (sign.)	Jan Hovden (sign.)
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
	2002-12-10	Lars Bodsberg, forskningssjef (sign.)	

SAMMENDRAG

Denne rapporten oppsummerer arbeid utført i Fase 1 under Tema 2 ”Feiltoleranse – barrierer – sårbarhet” i prosjektet ”HMS petroleum: Endring – organisasjon – teknologi”.

Gjennom denne rapporten ønsker vi å synliggjøre menneskelige og organisatoriske aspekter ved barrierer og feiltoleranse. Vi har videre identifisert temaer for empirisk forskning.

Rapporten av skrevet av forskere ved IFE, SINTEF og Høgskolen i Stavanger.

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Sikkerhet	Safety
GRUPPE 2	Pålitelighet	Reliability
EGENVALGTE	Feiltoleranse	Fault Tolerance
	Barriere	Barrier
	Sikkerhetsfunksjon	Safety Function

INNHOLDSFORTEGNELSE

Sammendrag

Denne rapporten oppsummerer arbeid utført i Fase 1 under Tema 2 ”Feiltoleranse – barrierer – sårbarhet” i prosjektet ”HMS petroleum: Endring – organisasjon – teknologi”. Gjennom denne rapporten ønsker vi å synliggjøre menneskelige og organisatoriske aspekter ved barrierer og feiltoleranse. Videre har vi identifisert temaer for empirisk forskning.

Petroleumsvirksomhet på norsk sokkel står overfor en rekke farekilder med storulykkespotensial. I mange tilfelle er produksjonssystemene tett koblede. Dette innebærer at forstyrrelser (f eks en gasslekkasje og en gnist) raskt kan eskalere til en storulykke. Under slik forhold kan et lavt risikonivå bare oppnås gjennom en høy grad av *feiltoleranse*.

I petroleumsvirksomheten designes feiltoleranse inn i innretningene ved at en etablerer en rekke tekniske og fysiske barrierer (forsvar i dybden). I tillegg etableres administrative systemer som bl.a. skal opprettholde sikkerhetsnivået dersom en eller flere tekniske barrierer ikke er tilgjengelige.

I system hvor risikokontroll er basert på forsvar i dybden, vil større ulykker ofte ha sammenheng med avhengigheter mellom barrierer. Sannsynligheten for at fire eller fem barrierer skal svikte uavhengig av hverandre på samme tidspunkt, er som regel forsvinnende liten sammenlignet med sannsynligheten for at flere barrierer skal svikte samtidig på grunn av én eller to felles årsaker eller bakenforliggende faktorer.

I analyser som fokuserer ensidig på fysiske og tekniske barrierer, vil en ofte undervurdere avhengigheter mellom barrierer. Fordi mennesker vedlikeholder og overvåker barrierer, og kan sette disse ut av funksjon, kan organisatoriske faktorer skape betydelige avhengigheter.

Organisatorisk redundans innebærer at en organisasjon har etablert samhandlingsmønstre som setter organisasjonen i stand til å utføre oppgaver mer pålitelig enn enkeltpersoner. Organisatorisk redundans skapes ved at personer rådfører seg med hverandre, sjekker hverandre og korrigerer hverandre. Dette kan oppnås gjennom formelle og uformelle mekanismer.

Vi mangler i dag gode metoder for å vurdere i hvilken grad personer kan fungere som uavhengige barrierer i forhold til tekniske barrierer eller i forhold til hverandre. Eksempelvis kan sterke avhengigheter oppstå dersom flere operatører deler samme feilaktige mentale modell av en systemtilstand, eller hvis en teknisk barriere og en operatør benytter seg av samme feilaktige informasjonskilde.

I videreføringen av Tema 2 ønsker vi å ta utgangspunkt i hovedspørsmålet ”Hvordan skape økt feiltoleranse i petroleumsvirksomheten” med særlig fokus på bidrag fra menneskelige og organisatoriske faktorer. Innenfor denne rammen har vi identifisert følgende problemstillinger:

1. Hvordan vurdere hvilken redundans som finnes i en organisasjon når en inkluderer menneskelige og organisatoriske bidrag til redundans i vurderingen?
2. Hvilken betydning har menneskelige og organisatoriske bidrag til feiltoleranse for risikonivået?
3. Hvordan kan en organisasjon utvikle det menneskelige og organisatoriske bidrag til feiltoleranse?

4. Hvordan kan tekniske og organisatoriske endringer påvirke menneskelige og organisatoriske bidrag til feiltoleranse?

Forkortelser

ALARP	As Low As Reasonably Practicable
CPU	Central processing unit
CRIOP	Crisis Intervention in Offshore Production
DFU	Definert fare- og ulykkessituasjon
DTS	Det tekniske sikkerhetssystemet
ESD	Emergency Shut Down
FGD	Fire & Gas Detection
HMS	Helse, miljø og sikkerhet
HRO	High Reliability Organisation
MTO	Menneske – teknologi – organisasjon
NAC	Normal Accidents
NAS	Nødavstengning
OD	Oljedirektoratet
OLF	Oljeindustriens landsforening
PAS	Prosessavstengning
PC	Process Control
PDS	Pålitelighet av datamaskinbasert sikkerhetssystemer
PFD	Probability of failure on demand
PSD	Process Shut Down
RNNS	Risikonivå på norsk sokkel
SEPA	Safety and emergency perparedness analysis
SIL	Safety Integrity level
SJA	Sikker jobb-analyse

1 Innledning

1.1 Bakgrunn

Stortingsmelding nr. 7 (2002-2002) legger til grunn at petroleumssektoren skal være en foregangsnæring som skaper verdier for samfunnet gjennom bevisst satsing på kvalitet, kunnskap og kreativitet, og som driver virksomheten basert på målsettingene om ”kontinuerlig forbedring” og ”føre-var” som grunnleggende prinsipper. Stortingsmeldingen fastslår at risikonivået i petroleumsvirksomheten er økende, og at én av årsakene til dette er de omfattende endringsprosessene som ble gjennomført på 90-tallet. Endringene involverte at teknologiske, operasjonelle og organisatoriske effektiviseringstiltak ble iverksatt uten at det ble satt tilstrekkelig fokus på konsekvensene for helse, miljø og sikkerhet. Regjeringen oppfordrer derfor i stortingsmeldingen alle aktører til å foreta en kritisk gjennomgang av egen virksomhet og prioriteringer, og til å sette i verk tiltak som er nødvendige for å redusere risikonivået.

Forskningsprogrammet HMS Petroleum ble satt i gang som ledd i oppfølgingen av stortingsmeldingen. Programmet omfatter blant annet de fire kompetanseprosjektene

K1. HMS-kultur

K2. Endring – organisasjon – teknologi

K3. Beslutningsstøtteverktøy

K4. Fysisk arbeidsmiljø og helse.

Det overordnede målet med prosjektet ”Endring – organisasjon – teknologi” er å utvikle ny kunnskap som kan sette aktørene i norsk petroleumsvirksomhet bedre i stand til å ivareta HMS ved organisatoriske og teknologiske endringer, og å få HMS-området til å fungere som premissleverandør i forhold til endringer. Prosjektet er i første fase delt inn i fire temaer (delprosjekter):

1. Overvåke og vurdere teknologiutviklingen
2. Feiltoleranse – barrierer – sårbarhet
3. HMS-aspekter ved endringsprosesser
4. HMS-arbeid under endring.

Denne rapporten oppsummerer arbeid utført i Fase 1 under Tema 2, ”Feiltoleranse – barrierer – sårbarhet”.

1.2 Fire fortellinger om feiltoleranse, barrierer og sårbarhet

Feiltoleranse vil si at et system fortsetter å fungere selv om feil forekommer, eller at systemet i det minste har egenskaper eller mekanismer som effektivt begrenser skadevirkningene av feil. Denne rapporten dreier seg om feiltoleranse i systemer hvor mennesker og teknologi spiller sammen. Vi vil illustrere feiltoleranse og fravær av feiltoleranse med fire eksempler.

1.2.1 Manglende feiltoleranse på Piper Alpha

Storulykken på Piper Alpha skjedde om kvelden, 6. Juli 1988 (se Reason, 1997 for kort beskrivelse av hendelsesforløp). 165 av 226 mennesker som var ombord på olje- og gassplattformen døde, samt to av mannskapet på et redningsfartøy som lå ved installasjonen. Årsaken til eksplosjonen var lekkasje av kondensat som følge av at arbeiderne på nattskiftet prøvde å starte opp en pumpe som var nedstengt for vedlikehold. De visste ikke at vesentlig vedlikehold som medførte at pumpen var ute av normal funksjon, var utført under dagskiftet. Årsaken til at de ikke visste dette, var at kommunikasjonen under skiftbytte tidligere den kvelden ikke hadde vært som den skulle og at arbeidstillatelsessystemet knyttet til vedlikehold på ventilen hadde sviktet.

Forut for ulykken var det tre inspeksjoner på Piper Alpha. Den første var en rutine inspeksjon som ikke ga noen pålegg om oppfølging, den andre en inspeksjon etter en dødsulykke som identifiserte svakhet i skiftbytte-rutiner og i arbeidstillatelsessystemet. Ti dager før ulykken var det en tredje inspeksjon som konsentrerte seg om områder der det foregikk konstruksjonsarbeid. Denne tredje inspeksjonen er beskrevet som mangelfull, da den ikke avdekket mange av de faktorene som førte til ulykken fem dager senere. Blant annet mente inspektøren at svakheten i arbeidstillatelsessystemet var utbedret uten at han gjorde forsøk på å undersøke dette ved for eksempel å benytte eksisterende sjekkliste for evaluering av arbeidstillatelsessystemer, eller å se på prosedyremanualen i sammenheng med arbeidstillatelsessystemet – noe han mente han ikke hadde tid til.

Skal man stole på feiltoleranse slik vi definerer det innledningsvis, som en måte å unngå større hendelser og ulykker, er det vesentlig at organisasjonen klarer å skille mellom grad av fare og alvorlighet i funn som blir gjort i inspeksjoner og rapportering. Dette gjelder både for operatør og tilsynsmyndighet. Det er organisasjonens evne til andre ordens læring[1] som blir vesentlig for om forskjellige former for inspeksjon og rapportering vil ha positiv effekt på sikkerheten. I forbindelse med Piper Alpha forsto man ikke hvor viktig arbeidstillatelsessystemet er for nettopp å sikre tilstrekkelig feiltoleranse, ei heller forsto man viktigheten av kommunikasjon i forbindelse med skiftbytte.

Lord Cullen, som ledet granskningskommisjonen etter ulykken, peker også på inspektørens rolle og Energidepartementets svakhet i evne til å følge opp sikkerheten ombord, som vesentlige bidragsytere til at ulykken inntraff. (Lord Cullen, 1990).

1.2.2 Multiple svikt på utstyr, styresystemer og ledelse ved Milford Haven

Den 24 juli 1994 inntraff det en eksplosjon etterfulgt av flere branner ved Texacos raffineri i Pembroke i England. Den direkte årsaken til eksplosjonen var en kombinasjon av flere feil innen ledelse, utstyr og styresystemer under en forstyrrelse på anlegget. 26 personer ble skadet, men ingen alvorlig. 5 timer før eksplosjonen var det en storm som førte til uregelmessigheter i elektrisitetsforsyningen og forstyrrelse i produksjonsprosessen. Selve hendelsen startet ved at en pumpet brennbar hydrokarbon væske inn i en tank med stengt utgang. Trykkavlastningssystemet sviktet, og et utslipp på 20 tonn væske og gass eksploderte.

Følgende kombinasjon av hendelser ble identifisert:

[1] ”Andre ordens læring” vil si at vi ”lærer å lære”, dvs at en organisasjon lærer seg nye måter å løse problemer på.

- en styreventil ble stengt, mens styresystemet indikerte at den var åpen;
- en modifikasjon hadde blitt utført i anlegget uten at konsekvensene var vurdert;
- styrepanelgrafikken viste ikke nødvendig prosessoversikt; og
- driftspersonellet forsøkte å holde anlegget i drift når det burde vært kjørt ned.

I sitt forsøk på å gjenopprette normal drift ved anlegget etter den forutgående driftsforstyrrelsen, feilet ledelsen i å ta et overordnet perspektiv på situasjonen for å finne den underliggende årsaken til problemet. I stedet konsentrerte de seg om lokale symptom. Det ble også oppdaget mangler i HMS ledelsen ved anlegget, slik som feil ved:

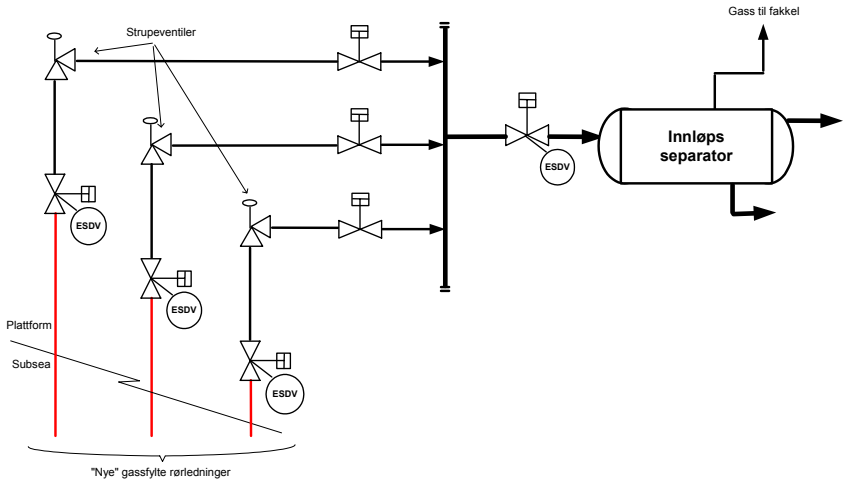
- vurdering av risiko ved modifikasjoner i anlegget og prosedyrer;
- bruk av programmerbare elektroniske systemer; og
- ledelse av inspeksjoner og vedlikehold.

Erfaringer og anbefalinger fra ulykken (HSE) (utvalgte):

- Systemer for sikkerhetsledelse bør ha mulighet for å lagre informasjon fra hendelser på tilsvarende anlegg (incident reports);
- Trening av stab bør også inkludere en vurdering av deres kunnskap og kompetanse relatert til deres aktuelle driftsrolle under høyt stress nivå;
- Klare retningslinjer for når operatørene skal initiere enten kontrollert nedkjøring eller foreta nødavstengning;
- Hvordan håndtere ikke-planlagte hendeleser og arbeide effektivt under stress;
- Alarmsystem: Sikkerhetskritiske alarmer bør skilles fra driftsalarmer og antall alarmer bør begrenses til hva en operatør effektivt kan håndtere. Dessuten bør ikke sikkerheten for et anlegg i for stor grad avhenge av en operatørs respons på en alarm fra styresystemet;
- Sikkerhetssystemer skal spesifiseres og designes basert på Hazard- og risikoanalyser. Sikkerhetsfunksjoner og plassering i sikkerhetsintegritetsnivå (SIL) skal bestemmes på en systematisk måte;
- Det bør innføres en formell og kontrollerbar prosedyre for å utføre Hazard identifikasjon og driftsanalyse ved modifikasjoner på anlegget. Dette skal sikre at alle sikkerhetsaspekter identifiseres under design og inkorporeres i gjennomføringen av modifikasjonene.
- Alle sikkerhetskritiske deler av anlegget bør inkluderes i det totale inspeksjonsprogrammet ved bedriften.

1.2.3 Økt kompleksitet og tettere koblinger i forbindelse med modifikasjoner på en norsk produksjonsplattform

Tilknytning av nye satellittfelter til eksisterende installasjoner er en trend på norsk sokkel. Her kobles nye rørledninger, ofte med høyt gassinnhold, opp mot gamle plattformsystemer. Hva skjer når det eksisterende fakkelsystemet ikke er i stand til å håndtere de nye gassmengdene? Et eksempel på en slik situasjon er illustrert nedenfor.



Figur 1 Typisk innløpsarrangement på en produksjonsplattform

Her er tre nye rørledninger med høyt gassinnhold koblet opp mot eksisterende innløpsseparator. Ved en nedstengning på plattformen vil trykket i rørledningene øke, og en kan dermed bli stående med fullt brønninnstengningstrykk helt opp til plattformens innløpsventil. Når en da skal starte opp igjen, er det viktig at den trykksatte gassen sleppes inn til separatoren på en kontrollert måte, fordi fakkelsystemet opprinnelig ikke var designet for å tåle de nye gassratene som kan oppstå. I praksis betyr dette at strupeventiler må åpnes gradvis som siste ventil på hvert løp. Dersom en annen ventil åpnes som siste ventil, kan dette medføre overtrykking av prosessutstyr og i verste fall en lekkasje.

En opplagt løsning på dette problemet vil være å oppgradere fakkelsystemet på plattformen til å kunne håndtere de mulige gassratene (”inherent safe design”), noe som imidlertid ofte er uaktuelt både av økonomiske og praktiske årsaker. Dette ”oppstartscenariet” blir derfor håndtert ved hjelp av alternative tekniske og/eller administrative barrierer. Dette kan være:

- *prosedyrer* som i detalj beskriver hvilke prosessbetingelser som skal være tilstede og i hvilken rekkefølge ventiler skal åpnes;
- *instrumenterte sikringssystemer* (såkalte forriglinger) som ved hjelp av logikk skal hindre operatørene i å feilåpne ventiler;
- *oppsplitting av strømningsrør* i flere små løp med hver sin strupeventil, slik at gassmengdene gjennom hvert enkelt løp ikke blir kritisk i tilfelle feilåpning;

Problemet ovenfor, med for liten fakkelkapasitet i forbindelse med oppstart av gassfylte rørledninger, finnes på flere norske produksjonsplattformer, både modifiserte plattformer så vel som nybygg. Eksempler på sikkerhetsmessige utfordringer som er knyttet til dette:

- Hvordan være sikker på at barrierene er uavhengige? I forbindelse med et prosjekt ble det for eksempel avdekket at når operatørene startet opp ved hjelp av prosedyrer, var det vanlig å bruke statussignaler fra de instrumenterte forriglingene som en aktiv ”støtte” under oppstart. Det ble dermed innført en høy grad av avhengighet mellom de to barrierene (den teknisk og den administrative).
- Hvordan innføre og vedlikeholde en (noen steder ny) kultur som tilsier at skriftlige prosedyrer må brukes og følges hver gang?
- Hvordan designe skjermbilder slik at muligheten for feiloperasjon minimaliseres?

- Hvordan unngå unødig fokus på at oppstart er noe som skal skje så raskt som mulig, for eksempel ved at en person fra land ringer og spør hvorfor en ikke er kommet i gang?

1.2.4 Feiltoleranse gjennom organisatorisk redundans på et hangarskip

En høyere amerikansk offiser ga følgende oppsummering av risikoforholdene i forbindelse med hangarskip-operasjoner (Rochlin m.fl. 1987, vår oversettelse):

> Så du vil gjerne forstå et hangarskip? Vel, bare forestill deg at det er en travel dag, og du skrumper San Francisco Airport til bare én kort rullebane og én rampe og oppstillingsplass. La flyene ta av og lande samtidig, med halvparten av dagens tidsintervall, vugg rullebanen fra side til side, og krev at alle som tar av om morgenen, returnerer samme dag. Sørg for at utstyret er så tett innpå de operative grensene at det er sårbart. Så slår du av radaren for å unngå å bli oppdaget, legger strenge begrensninger på bruk av radio, tanker flyene på stedet med motorene i gang, plasserer en fiende i luften, og sprer skarpe bomber og raketter rundt omkring. Endelig fukter du det hele med salt vann og olje, og bemanner det med 20-åringer, hvorav halvparten aldri har sett et fly på kort hold. Eh - og forresten – forsøk å ikke drepe noen.

All sunn fornuft tilsier at det er umulig å operere et slikt system uten mange dødsulykker hver dag. Imidlertid kan de amerikanske hangarskipene vise til langt bedre ulykkesstatistikk enn sunn fornuft skulle tilsi. Forskere som har studert slike *høy-pålitelige organisasjoner*, hevder at enkelte organisasjoner oppnår ekstremt pålitelige operasjoner ved at personell som utfører kritiske oppgaver, overvåker hverandres oppgaveutførelse og om nødvendig korrigerer feil. På samme måte som en kan oppnå høy teknisk pålitelighet ved å duplisere kritiske delsystem eller komponenter.

Dette reiser flere spørsmål:

- Er det mulig å organisere aktiviteter på en slik måte at organisasjonen som helhet blir mer pålitelig enn enkeltpersonene?
- Er det mulig å oppnå tilsvarende grad av pålitelighet innenfor norsk petroleumsvirksomhet? Kan det tenkes at enkelte aktiviteter innenfor norsk petroleumsvirksomhet allerede fungerer som høy-pålitelige organisasjoner?
- Hvordan kan vi legge til rette for høy organisatorisk pålitelighet ved design av installasjoner og ved utvikling av organisasjoner?

1.3 Formål med rapporten

For å minimere ulykkesrisikoen i komplekse systemer med storulykkespotensial er det nødvendig å kombinere strategier for å forebygge at feil inntreffer med strategier for å hindre at feil fører til uønskede konsekvenser. Petroleumslovgivningen legger til grunn at fare- og ulykkessituasjoner skal unngås, og setter i tillegg krav om etablering av tiltak for å hindre eller redusere skadevirkningene av fare- og ulykkessituasjoner (Stortingsmelding nr. 7, §4.15.1). Kontroll av storulykkesrisiko i petroleumsvirksomheten er i høy grad basert på barrierer eller sikkerhetsfunksjoner. Disse spenner fra passive fysiske tiltak (f.eks. brannvegger) via aktive

tekniske systemer (f.eks. nødavstengning) til administrative systemer (f.eks. arbeidstillatelses-system). Barrierer og sikkerhetsfunksjoner bidrar til å skape feiltoleranse – de reduserer sannsynligheten for at en alvorlig ulykke skal inntreffe, dersom det oppstår en enkeltfeil, f.eks. en gasslekkasje. I senere tid har selskapene lagt økende vekt på å overvåke tilstanden til fysiske og tekniske barrierer, bl.a. gjennom systematiske tilstandsvurderinger og utvikling av risikoindikatorer. Mennesker inngår som element i mange av barrierene som implementeres for å forebygge storulykker. Brannvegger bygges og vedlikeholdes av mennesker, nødavstengning kan aktiveres men også kobles ut av mennesker, administrative systemer utvikles og styres av mennesker. Det betydelige element av menneskelig bidrag til tross, har en neppe kommet like langt i å kvalitetssikre dette bidraget til barrierene som i å vurdere tekniske forhold. De operative barrierene, f.eks. arbeidstillatelsessystemet, har tradisjonelt fått mindre oppmerksomhet enn fysiske og tekniske barrierer som brannvegger og nødavstengnings-system, til tross for at arbeidstillatelsessystemet i enkelte situasjoner påvirker godheten av flere tekniske barrierer samtidig. Den senere tid har det skjedd en rekke alvorlige hendelser som har synliggjort problemer i tilknytning til menneske-maskin grensesnittet, manglende etterlevelse av prosedyrer, mangler ved opplæring, og svakheter ved organiseringen av arbeidet (Stortingsmelding nr. 7, § 4.9.2). Disse hendelsene understreker viktigheten av å sette fokus på menneskets rolle i relasjon til opprettholdelse av sikkerheten på norsk sokkel.

Oppgaven med å planlegge og vedlikeholde feiltoleranse spenner over mange fagdisipliner. Dette kan føre til at kunnskapen om feiltoleranse blir tilsvarende fragmentert. Både blant forskere og praktikere er det en utfordring å se de ulike bidrag til feiltoleranse i sammenheng, slik at en blir oppmerksom på mulige avhengigheter, og dermed blir i stand til å forestille seg hvordan flere barrierer kan svikte samtidig. For praktikere er dette problemet særdeles kritisk. Dette skyldes at bestemmelsene i OD's forskrifter (regelverket) i stor grad er utformet som funksjonskrav, der det overlates til den 'ansvarlige' å fastlegge hvordan kravene konkret skal møtes ut fra en vurdering av risikoforholdene i de enkelte virksomheter (Stortingsmelding nr. 7, §3.3.1). En slik oppgave er vanskelig å gjennomføre på en tilfredsstillende måte når kunnskapen som skal legges til grunn er fragmentert. Gjennom denne rapporten og videre arbeid innen temaet "Feiltoleranse – barrierer – sårbarhet" ønsker vi å bidra til et slikt helhetlig syn på feiltoleranse.

Denne rapporten er den første dokumentasjonen fra Tema 2, "Feiltoleranse – barrierer – sårbarhet" innen prosjektet "Endring – organisasjon – teknologi". Gjennom Tema 2 ønsker vi å

- synliggjøre menneskelige og organisatoriske aspekter ved barrierer og feiltoleranse;
- bidra til å skape et mer helhetlig bilde av de mekanismene som bidrar til feiltoleranse;
- oppsummere eksisterende kunnskap innen utvalgte problemstillinger knyttet til feiltoleranse;
- fremskaffe ny kunnskap knyttet til utvalgte problemstillinger knyttet til feiltoleranse.

Denne rapporten har to hovedfunksjoner. For det første ønsker vi å formidle et grovt omriss eller helhetsbilde av området. For det andre vil vi identifisere prioriterte temaer for empirisk forskning.

1.4 Avgrensninger

Rapporten er avgrenset ved i all hovedsak å fokusere på de i Stortingsmelding nr. 7 nevnte problemstillingene i relasjon til samspillet i organisasjonen, forstått i bred forstand. Vi vil sette fokus på samspillet mellom mennesker, samt på samspillet mellom mennesker og teknikk. Vi vil unnlate å sette fokus på områder der industrien allerede har kommet langt, som f.eks. systematikk for tilstandsovervåkning av fysiske og tekniske barrierer.

Tid og ressurser har ikke gitt rom for å diskutere *strategier og metoder for å utvikle, overvåke og vedlikeholde feiltoleranse* i denne første delprosjektrapporten. Vi ser imidlertid på dette som et sentralt tema i det videre arbeidet.

Når det gjelder teknologitrender og feiltoleranse, henvises til rapporten for Tema 1. Vi har imidlertid tatt med noen foreløpige tanker om dette i Vedlegg 1.

1.5 Leserveiledning

I Kapittel 2 presenterer vi ulike perspektiver på feiltoleranse. Poenget er å åpne opp for ulike betraktningsmåter og å introdusere teorier som vi kan bruke i diskusjoner senere i rapporten.

Det har vært foreslått en rekke ulike definisjoner på barrierer, feiltoleranse og beslektede begreper. Vi presenterer noen av disse i kapittel 3.

Kapittel 4 gir en oppsummering av sentrale krav til barrierer i regelverket til OD. Vi gir også en kort oppsummering av krav til sikkerhetsfunksjoner i standarden IEC 61508, ettersom denne har blitt sentral i norsk petroleumsvirksomhet.

I kapittel 5 forsøker vi å konkretisere hvordan en skaper feiltoleranse med utgangspunkt i en typisk produksjonsinnretning. Vi tar utgangspunkt i fare- og ulykkessituasjoner identifisert gjennom risikoanalysen. Vi ser noe nærmere på prosesskontroll, prosessavstengning og nødavstengning, som er tekniske systemer med mulighet for avgjørende operatørinngrep. Til slutt diskuterer vi hvordan de ansatte kan skape feiltoleranse gjennom måten de samhandler på i utførelse av arbeidet.

I kapittel 6 tar vi opp en del problemstillinger omkring feiltoleranse. Hvor harde er egentlig harde barrierer (tekniske og fysiske tiltak)? Hvor realistisk er det å forutsette at barrierer er uavhengige? Kan det tenkes at den risikoreduksjonen en teknisk barriere skal skape, blir spist opp fordi barrieren gir en falsk følelse av trygghet?

Kapittel 7 fungerer både som oppsummering og foreløpig ramme for videre arbeid. Vi har formulert noen overordnede problemstillinger og et teoretisk rammeverk – dvs. et sett antakelser vi vil arbeide ut fra. Vi drøfter videre aktuelle tilnærmingsmåter og datakilder.

2 Feiltoleranse, barrierer og sårbarhet i perspektiv

Dagens dynamiske samfunn medfører generelt betydelige endringer innen industriell risikoledelse. Det skjer i dag hurtige endringer i teknologi, det er en stadig høyere grad av integrering og sammenkobling av systemer, samtidig som omgivelsene er mer aggressivt konkurrerende (Rasmussen og Svedung, 2001:10). Dette medfører at organisasjonene får et større behov for å bygge opp motstandskraft mot store ulykker.

Slike større ulykker omtales også som organisatoriske ulykker. Med organisatoriske ulykker menes relativt sjeldne, men ofte katastrofale, hendelser som kan inntreffe innen komplekse moderne teknologiske miljø, så som atomkraftverk, luftfart, petrokjemisk industri, kjemiske prosessanlegg m.m. (Reason, 1997). Organisatoriske ulykker har sammensatte årsaksforhold og involverer mange mennesker på ulike nivå i organisasjonen – og i noen tilfelle fra ulike organisasjoner. De kan i tillegg ha en ødeleggende effekt på ikke-involverte parter, eiendom og miljø.

I dette kapitlet beskrives noen perspektiver som kan bidra til å gi innsikt i hvorfor noen organisasjoner blir rammet av storulykker, mens enkelt andre organisasjoner kan vise til oppsiktsvekkende lave ulykkestall. For ikke å gjøre kapitlet for omfattende, har det vært nødvendig å konsentrere seg om å gi en kort beskrivelse av et utvalg av de mest sentrale teorier knyttet til større ulykker. For en mer utfyllende presentasjon, kan den interesserte leser se bl.a. Rosness m.fl. (2002).

Perspektivene som presenteres, er gitt betegnelsene:

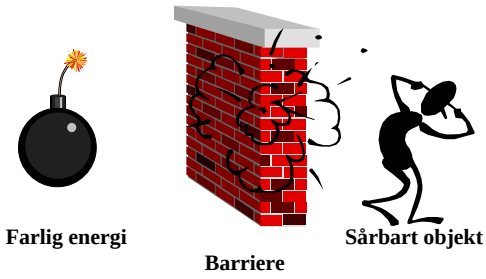
- energi og barriere-perspektivet
- interaktive og tett koblede teknologier – Perrows teori om normalulykker
- teorien om høy-pålitelige organisasjoner (High Reliability Organisations)
- Turners teori om menneskeskapte katastrofer pga svikt i informasjonsbehandlingen
- Beslutningsperspektivet – målkonflikter

Perspektivene er sammenstilt som typer av ulykkesmodeller i kapittel 2.6. Noen av perspektivene bygger på en kausalmodell, der eksplisitte sammenhenger mellom årsak og virkning er forutsatt.

2.1 Energi og barriere-perspektivet

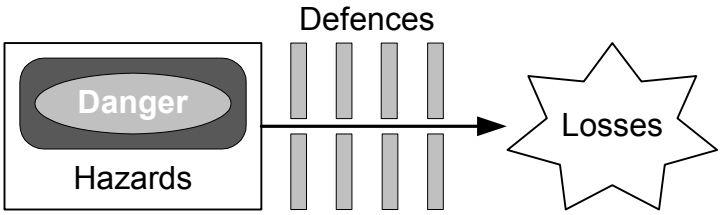
Ifølge energi og barriere-perspektivet kan ulykker forstås som en hendelse som skjer som en følge av ukontrollert overføring av skadelig energi til et sårbart mål. Ut fra denne teorien kan ulykker forhindres ved å fokusere på strategier for 1) å unngå / redusere oppbygging av farlige energier, 2) ved å innføre fysiske, tekniske eller administrative midler (barrierer) som kan hindre slike energier i å gjøre skade på sårbare objekter eller 3) ved å øke offerets motstandskraft (Gibson, 1961; Haddon 1970; 1980).

Begrepet barriere kan lett gi assosiasjoner til konkrete og fysiske stengsler. I sin mest direkte form kan energimodellen fremstilles som i figur X1. Det kan imidlertid være mer nyttig å forstå begrepet barriere fra et funksjonelt synspunkt, der barrierer kan ses som enhver sikkerhetsfunksjon som har som mål å forhindre ulykker (inklusive prosedyrer, opplæring etc.). Et system som mangler tilstrekkelige barrierer vil lett kunne bli utsatt for ulykker.



Figur 2. Energi- og barrieremodellen (etter Haddon, 1980).

Reason (1997) påpeker at alle organisatoriske ulykker innebærer brudd på barrierer og sikkerhetsordninger som skiller farer fra sårbart personell eller eiendeler (kalt tap).



Figur 3. Sammenhengen mellom farer, forsvar (barrierer) og tap (Reason, 1997).

I forskningslitteraturen, regelverk og standarder finnes en rekke ulike definisjoner av begrep som ”barriere” og ”defence”. Vi kommer tilbake til dette i kapittel 3.

2.1.1 Forsvar i dybden

Kravet om redundans er hovedhjørnesteinen innen moderne sikkerhetstenkning. Tidligere tiders tillit til at feil og svikt kan unngås om bare teknologien som anvendes er tilstrekkelig pålitelig og medarbeiderne som utfører den operasjonelle aktiviteten er tilstrekkelig velutdannet og disiplinert, er borte. Den har veket plassen for erkjennelsen av at feil og svikt alltid vil kunne forekomme. Kravet om redundans er etablert som konsekvens av denne erkjennelsen. Redundans betraktes som nødvendig for å sikre at feil og svikt kompenseres. Dette innebærer at begrepet redundans innen moderne sikkerhetstenkning snarere blir anvendt i betydningen *'avløsnings- (back-up) funksjon som er nødvendig for å kunne opprettholde sikkerheten i tilfeller av feil og svikt,*' enn i sin opprinnelige betydning: '*overflødig repetisjon.*'[2]

Konkret utmynter kravet om redundans seg i krav om implementering av *barrierer*. Barriereretenkning baserer seg på den antagelsen at enhver ulykke kan assosieres med en eller flere hendelser som kan sette i gang en uønsket prosess. Disse hendelsene kalles *faresituasjoner*[3] (”hazards”; DOE Workbook, 1999). En faresituasjon kan f.eks. være et utslipp av hydrokarboner eller radioaktiv stråling. En faresituasjon kan lede direkte til en ulykke eller etablere en tilstand

[2] Denne definisjonen finnes f.eks. Merriam-Webster.
[3] Alternative oversettelser av “hazard” kan være fare, faresituasjon, farekilde, hasard. Vi vil fortrinnsvis bruke ‘fare’ eller ‘faresituasjon’om en *hendelse* som kan sette i gang en uønsket prosess, og ‘farekilde’ om en energikilde e.l., altså et mer statisk forhold, som kan forårsake skade.

der sannsynligheten for at en ulykke kan inntreffe øker. Kun om farekilden kommer i direkte kontakt med et *mål* vil ulykken bli en realitet. Et *mål* kan være en person eller et objekt som farekilden kan beskadige, såre, eller ødelegge. Begrepet *barriere* brukes som betegnelse på 'hindringer' som bygges inn i produksjonssystemet og/eller i arbeidsprosessen med det formål å få kontroll over farene (Neogy, Hanson, Davis & Fenstermacher, 1996). I tekniske termer er formålet med barrierer således å hindre at en fare skal nå et gitt mål.

'*Forsvar-i-dybden*' er en velkjent strategi for organisering av barrierer innen høyteknologiske produksjonssystemer med stort risikopotensiale, som f.eks. kjernekraftverk. Den grunnleggende filosofien bak forsvar-i-dybden er at ingen enkelt feil, det være seg menneskelig eller teknisk, må kunne lede til ulykker (enkeltfeilsprinsippet). Forsvar-i-dybden har to formål, 1) å forebygge ulykker, og 2) å begrense konsekvensene dersom en ulykke inntreffer (INSAG-10, 1996). Ulykkesforebyggelse er den aktiviteten som blir prioritert høyest. Dette skyldes at inngrep som tar utgangspunkt i velkjente operasjonelle tilstander generelt vurderes som mer effektive enn tiltak som tar sikte på å lindre konsekvensene av avvikende operasjonelle betingelser.[4]

Forsvar-i-dybden innebærer at en etablerer suksessive lag av uavhengige barrierer i det sosiotekniske systemet, slik at enhver sikkerhetskritisk aktivitet blir assosiert med kontrollmuligheter som sikrer at kritiske hendelser vil bli oppdaget og kompensert (IAEA, 2000, 5). Strategien fordrer således etablering av *redundans*, dvs. implementering av flere lag av barrierer, samt *diversitet*, dvs. sikring av at barrierene er uavhengige av hverandre slik at ikke flere barrierer vil feile samtidig om et gitt hendelse inntreffer (f.eks. strømsvikt). Tankegangen bak forsvar-i-dybden er at risikoen for uhell og ulykker reduseres for hver barriere som implementeres mot den spesifikke faresituasjonen. Denne tankegangen illustreres på eksellent måte av Bendor:

> "Suppose an automobile had dual breaking (sic) circuits: each circuit can stop the car, *and* the circuits operate independently so that if one malfunctions it does not impair the other. If the probability of either one failing is 1/10, the probability of both failing simultaneously is $(1/10)^2$, or 1/100. Add a third independent circuit and the probability of the catastrophic failure of no brakes at all drops to $(1/10)^3$, or 1/1000." (Bendor, sitert i Sagan, 1993, 20)

Innen kjernekraftindustrien anvendes en forsvar-i-dybden strategi, som impliserer fem lag av barrierer (INSAG-10, 1996, 6):

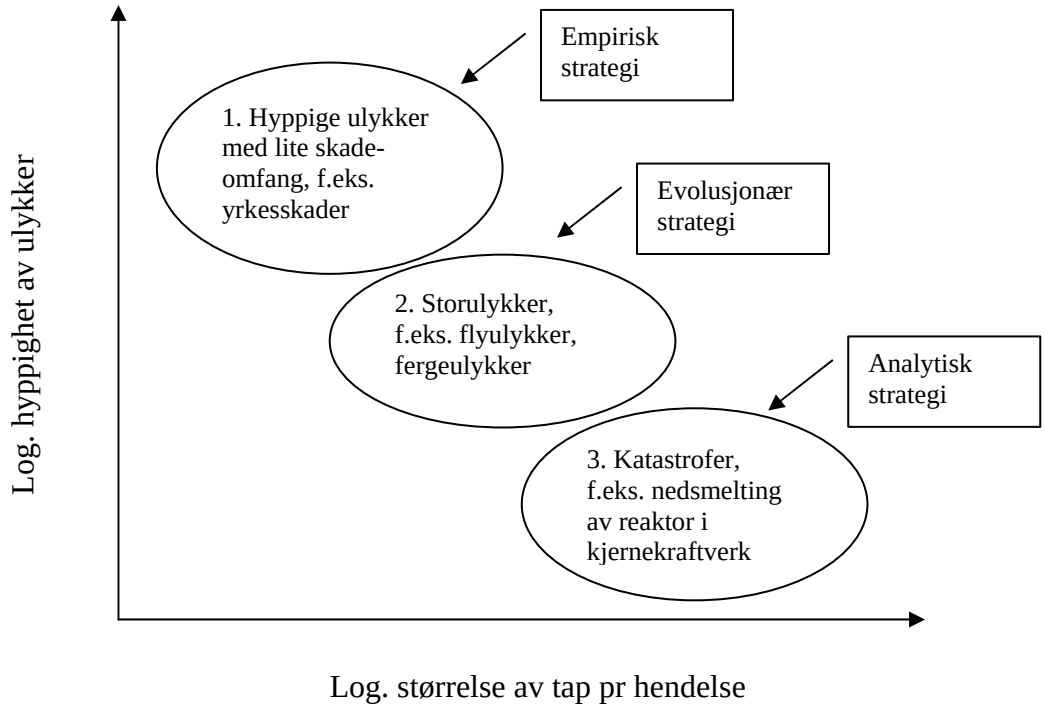
Levels of defense in depth	**Objective**	**Essential means**
Level 1	Prevention of abnormal operation and failures.	Conservative design and high quality in construction and operation.
Level 2	Control of abnormal operation and detection of failures.	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis.	Engineered safety features and accident procedures.
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents.	Engineered safety features and accident management.
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response.

[4] Innen f.eks. kjernekraftverk er det slikt at tilstanden i verket generelt forverres i takt med at avvikene fra normal situasjonen økes.

Implementering av barrierer skjer som regel med referanse til anerkjente standarder og til funksjonsbaserte krav fastsatt av tilsynsførende myndighet. Kravene angir typisk hvilke spesifikke sikkerhetsfunksjoner som skal være ivaretatt i produksjons- og/eller i arbeidsprosessen.

2.1.2 Forsvar i dybden som ledd i en analytisk strategi for risikokontroll

Forsvar-i-dybden kan forståes som ledd i en analytisk strategi for risiko-kontroll (Rasmussen, 1997). For å vise hva dette innebærer, tar vi utgangspunkt i Rasmussens inndeling av ulykker i tre klasser som krever ulike strategier for risikokontroll (
Figur 4).



Figur 4. Tre hovedklasser av ulykkesrisiko; basert på Rasmussen (1997).

1. Den første gruppen omfatter typiske mindre ulykker med forholdsvis enkle årsaksmønstre, f.eks. fallskader eller fremmedlegeme i øyet. Her kan det forebyggende arbeidet i stor utstrekning bygge på *statistisk bearbeidelse av erfaringsdata*, f.eks. typiske skademønstre, opphopning av skader i forbindelse med spesielle arbeidsoperasjoner (black spots). Rasmussen kaller dette en *empirisk* strategi for risikokontroll. Denne ulykkeskategorien faller utenfor rammen for dette prosjektet.
2. Den andre gruppen hendelser omfatter storulykker med flere dødsfall og/eller omfattende materielle skader, f.eks. flyulykker og fergeulykker. Her må det forebyggende arbeid bygge dels på at en lærer av *enkeltulykker*, og dels av at en tolker *symptomer* på storulykkesrisiko, f.eks. uønskede hendelser av mindre omgang. Rasmussen kaller dette en *evolusjonær* strategi

for risikokontroll. Dette innebærer at sikrere systemer utvikles gjennom designforbedringer basert på enkelthendelser, f.eks. siste store flyulykke eller fergeulykke.

3. Den tredje gruppen omfatter hendelser som er så omfattende og uakseptable at en ikke kan tillate seg å lære av ulykker. Design og drift må bygge på risikoanalyser, dvs. troverdige *prediktive modeller* av mulige ulykkesforløp og deres hyppighet. Under konstruksjon og drift må en sørge for at forutsetningene som ligger til grunn for risikoanalysene, til enhver tid er oppfylt. Erfaringsdata kan være relevante som middel til å overvåke barrierer og sikkerhets-funksjoner som er forutsatt i risikoanalysen. Rasmussen kaller dette en *analytisk* strategi for risikokontroll.

2.2 Interaktive og tett koblede teknologier – Perrows teori om normalulykker

Perrow (1984) mener at egenskapene ved noen større ulykker er fundamentalt ulike egenskapene ved mindre ulykker. Mindre ulykker skyldes typisk en eller annen forutsigbar svikt i en eller to komponenter i et system. I motsetning til dette finnes systemulykker, som skyldes overraskende og uheldige sammentreff av flere latente og aktive feil i et komplekst system. Systemulykker kommer ofte overraskende på dem som befinner seg i systemet. Perrows hevder at noen systemer har egenskaper som gjør ulykker nærmest uunngåelige. Han kaller disser systemulykkene ”normalulykker”.
Perrow karakteriserer samspillet mellom de tekniske/fysiske komponenter eller enheter i et produksjonssystem ved bruk av to nøkkelbegreper: interaktivitet og kopling. Han definerer ikke de to begrepene entydig - hvilket gjør dem vanskelige å operasjonalisere - men diskuterer begrepenes sentrale attributter, og tilhørende implikasjoner for operatøren av produksjonssystemet.

2.2.1 Interaktivitet

Begrepet interaktivitet henviser til graden av kompleksitet som kjennetegner interaksjonene mellom komponentene/enhetene i produksjonssystemet. Lav kompleksitet involverer linære interaksjoner, mens høy kompleksitet involverer komplekse interaksjoner. Desto høyere graden av interaktiv kompleksitet er, desto større er risikoen for at systemoperatøren vil ha vanskelig for å skjønne hva som skjer i produksjonsprosessen (Perrow, 1984, 72).

Linære interaksjoner er interaksjoner som systemdesigneren har planlagt, og som gjennomføres en-for-en i en klart definert sekvens. I produksjonssystemer med en høy grad av lineær interaktivitet er det enkelt å observere avvik: Frem til operasjonssekvensen, hvor avviket har oppstått, forløper produksjonen korrekt, etter dette punktet forløper produksjonen ikke korrekt. Sett fra perspektivet til systemoperatøren er linære interaksjoner forventede produksjonssekvenser - herunder velkjente operasjons- og vedlikeholdssekvenser, samt interaksjoner som er synlige, skjønt ikke direkte forventede (ibid., 78). Det typiske eksempel på et system med en høy grad av lineær interaksjon er samlebåndsproduksjon.

Komplekse interaksjoner er i reglen ikke planlagte av systemdesigneren (ibid., 77). En kompleks interaksjon oppstår f.eks. når en komponent/enhet som tjener to eller flere formål feiler, slik at systemet samtidig mister to eller flere funksjoner med derav følgende konsekvenser. Komplekse interaksjoner kan også oppstå ved at to komponenter/enheter, som tilfeldigvis har blitt plassert nær hverandre i produksjonssystemet, uventet kommer i forbindelse med hverandre, slikt at tilstanden i produksjonssystemet forandres på uforutsette og overraskende måter. Et væskeutslipp i et lagerrom kan f.eks. uventet trenge igjennom et bortglemt rør til et tilstøtende rom og utløse en eksplosjon. Sett fra perspektivet til systemoperatøren er komplekse interaksjoner lite kjente,

ukjente eller ikke planlagte og uventede operasjonssekvenser, som enten ikke er synlige eller som ikke er umiddelbart forståelige (ibid., 77). Et typisk eksempel på et system med potensiale for komplekse interaksjoner er et kjernekraftverk.

Hovedparten av interaksjonene i alle produksjonssystemer er linære. Dette gjelder også i komplekse produksjonssystemer. Perrow foreslår at rundt 1% av komponentene/enhetene i et lineært system er i stand til å produsere komplekse interaksjoner, mens rundt 10% av elementene i et komplekst system er i stand til å gjøre det samme (ibid., 75).

2.2.2 Kopling

Begrepet kopling henviser til graden av buffere eller slak som finnes i produksjonssystemet. Et produksjonssystem kan være stramt eller løst koplet. Et stramt koplet system har ingen buffere, mens et løst koplet system har mange buffere. Desto strammere koplinger som finnes i et produksjonssystem, desto større er risikoen for at systemoperatøren forhindres i å hurtig gjenopprette oppståtte avvikssituasjoner (Perrow, 1984, 72).

I et produksjonssystem med løse koplinger er det mulig å avbryte eller forsinke produksjonen ved å sette produksjonsprosessen på 'stand-by' uten at dette vil skade de delvis ferdiggjorte produktene. Dette skyldes at produksjonssystemet rommer slakk i form av buffere, f.eks. i form at lagerplass. Produksjonssekvensene i løst koplede systemer kan dessuten legges om. Ofte vil sekvens B kunne utføres før sekvens A - skjønt omkostningene som er forbundet hermed kan være betydelig større enn ved å utføre sekvens A før B. Designet i et løst koplet produksjonssystem tillater ytterligere at produksjonsmetoden endres, f.eks. at roboter kan inkluderes og ekskluderes. Det klassiske eksemplet på produksjons-systemer med løse koplinger er tradisjonelle fremstillingsvirksomheter.

I et produksjonssystem med stramme koplinger vil det som skjer i en operasjonssekvens ha direkte effekt på det som skjer etterfølgende (ibid., 90). Det finnes ikke slakk eller buffere mellom operasjonssekvensene. Et stramt koplet system rommer flere tidsavhengige prosesser (ibid.,93), hvorfor det ikke er mulig å sette produksjonen på 'stand-by' uten at dette vil skade de delvis ferdiggjort produktene. Stanses eller avbrytes produksjonen må hele produksjonsprosessen initieres på ny. Produksjonssekvensene i et stramt koplet system er lite fleksible. Produksjonen må gjennomføres på den fastlagte måten (ibid., 94): Utførelsen av sekvens B må etterfølge utførelsen av sekvens A. Det klassiske eksemplet på produksjons-systemer med stramme koplinger er kontinuerlige produksjonsprosesser.

Perrows teori om normalulykker hevder at noen av de større ulykkene skyldes manglende samsvar mellom teknologien som kontrolleres og strukturen til organisasjonen som kontrollerer den (Perrow, 1984). Perrow mener at systemer med høy interaktiv (gjensidig avhengig) kompleksitet kun kan kontrolleres i en *desentralisert* organisasjon. Samtidig mener han at systemer med tette koblinger og liten grad av ”buffere” krever en *sentralisert* organisasjon for å kunne kontrolleres effektivt. Dette innebærer et organisatorisk dilemma for tekniske systemer som er både interaktive og tett koblede, så som f.eks. atomkraftverk. Perrow konkluderer ut fra dette med at dersom et system kommer i dette organisatoriske dilemmaet, og aktiviteten samtidig har stort katastrofepotensial, bør virksomheten legges ned. Perrow fremmer således idéen om at noen teknologier burde forbys, fordi de ikke kan kontrolleres godt nok av noen tenkelig organisasjon. Dette standpunktet har framprovosert atskillig fruktbar strid, og har bl.a. bidratt til utarbeidelse av teorien om høy-pålitelige organisasjoner.

2.3 Teorien om høy-pålitelige organisasjoner (High Reliability Organisations)

Teorien om høy-pålitelige organisasjoner ble utviklet delvis som en reaksjon på utfordringen gitt i normalulykkesteorien (Rochlin m.fl., 1987; LaPorte og Consolini, 1991). Teorien om høy-pålitelige organisasjoner er fundert på studier av organisasjoner som har vist evne til å håndtere komplekse og krevende teknologier uten å forårsake store ulykker. Viktige resultater fra denne forskningen er kunnskapen om organisatorisk redundans[5] og organisasjoners evne til spontan strukturendring som tilpasning til kriser og plutselige belastningstopper.

Ingeniører vil i noen tilfeller bygge inn ekstra komponenter og utstyr for å unngå fatale hendelser i tilfelle en kritisk komponent skulle svikte. Et eksempel på dette er bilers bremsesystem, som er bygd med to hydrauliske kretser, selv om én hadde vært tilstrekkelig. Slike løsninger gir mulighet for feil i systemet uten at det får katastrofale følger. Tilsvarende vil organisasjoner med innebygd duplisering kunne oppnå en bedre toleranse for feil. Dette tilstrebes ofte i høypålitelige organisasjoner f.eks. ved at personell overlapper hverandre med hensyn til kompetanse og arbeidsoppgaver. Slik overlapping legges inn ut fra troen på at mennesker før eller siden alltid vil gjøre feil. Med overlapping er det større sannsynlighet for at disse feilene vil kunne bli oppdaget og korrigert øyeblikkelig, før de eventuelt medfører større ulykker. Rosness m. fl. (2000) kalte denne feilrettingsmuligheten for *organisatorisk redundans*, og beskrev forholdet som *samhandlingsmønstre som tillater organisasjonen som et hele å opptre mer pålitelig enn operatørene hver for seg*. For å oppnå organisatorisk redundans må både de strukturelle (f.eks. bemanning, arbeidsoppgaver) og kulturelle forhold i organisasjonen ligge til rette for slik gjensidig feilretting.

LaPorte og Consolini (1991) påviste også at mange høypålitelige organisasjoner har evnen til spontant å omstrukturere seg i spesielle situasjoner. De brukte som eksempel et hangarskip, hvor man under normale driftsbetingelser hadde en hierarkisk struktur med klart definerte kommandolinjer. I kriser eller andre spesielt krevende situasjoner omstilte de seg imidlertid øyeblikkelig til en mer fleksibel organisasjon, der autoriteten ble bestemt av aktuell kompetanse og ikke av hvilken rang man hadde i hierarkiet. Tilsvarende kan en f.eks. innen flykontroll se hvordan flygelederne trer støttende til overfor hverandre dersom noen i en periode har ekstra krevende arbeidsoppgaver.

Begrepet 'mindfulness'[6] ble utviklet for å fange karakteristika ved samhandlingsmønstre i høypålitelige organisasjoner (Weick og Roberts, 1993). Mindfulness innebærer at sikkerhet og pålitelighet betraktes som dynamiske ikke-hendelser der håndtering av det uventede blir vesentlig. Sikkerhet og pålitelighet er ikke en statisk størrelse som kan bygges inn i organisasjonen, men oppnås gjennom interaksjon, oppmerksomhet, kommunikasjon og kompetanse. Disse mekanismene inngår i begrepet 'mindfulness'. I følge Weich & Sutcliffe (2001) består begrepet nærmere bestemt av følgende dimensjoner:

1. **Fokus på feil ('Preoccupation with failure')**
   Betrakter feil som viktige symptomer. Fokus på læring av feil og nesten-ulykker. Hendelsesgjennomganger og -analyser, rapporteringskultur, åpenhet. Stor grad av trening for kontinuerlig oppdatering av kunnskap om tekniske systemer.

[5] Etymologisk betyr "redundans" noe som er overflødig. I pålitelighetsteori snakker en om redundans dersom det finnes flere enn ett middel til å utføre en oppgave (dvs. ivareta en funksjon).
[6] Vi har ikke funnet noen dekkende norsk overssettelse av begrepet 'mindfulness'. Begrepet spiller på en rekke assosiasjoner, herunder "åndsnærvær", det å bry seg, det å vise hensyn, kanskje også det å være bekymret.

2. **Motstand mot å forenkle ('Reluctance to simplify')**
   Fokus på et fullstendig og nyansert bilde for å håndtere det usikre og uventede. Kontekst, differensiering og konstant interaksjon gir et rikere, variert bilde av potensielle konsekvenser. Heterogene grupper gir ulike perspektiver. Troverdighet, tillit, mellommenneskelige relasjoner.

3. **Fokus på drift ('Sensitivity to operations')**
   Stor grad av oppmerksomhet og åpenhet vedrørende symptomer og latente feil. Velutviklet situasjonsbilde. Redusert forskjell mellom operativt, taktisk og strategisk nivå med dreining mot operativt nivå. Hyppige driftsmøter, direkte kontakt/ interaksjon, spredning av operasjonelle ytelsesmål.

4. **Satsing på robusthet ('Commitment to resilience')**
   Unngå at feil blir lammende. Intelligente reaksjoner og improvisasjon. Kunnskap, erfaring, kombinasjon, trening, simulering av 'worst case' scenarier. Divergens i analytiske perspektiv (konseptuell slakk), uformelle nettverk.

5. **Respekt for ekspertise ('Deference to expertise')**
   Kultivering av diversitet. Beslutningsmigrasjon fra makt/ politikk til ekspertise. Skifte av lederskap i krise- og problemsituasjoner i henhold til grad av ekspertise. Empowerment, hybridisering mellom hierarki og spesialisering.

Karakteristikkene er utarbeidet på bakgrunn av forskning innen typiske høyrisiko organisasjoner som kjernekraftverk, hangarskip, brannredning, etc. Høy grad av 'mindfulness' gjør disse komplekse organisasjonene høypålitelige, og dermed i stand til å utføre sin virksomhet med bortimot fravær av alvorlige ulykker.

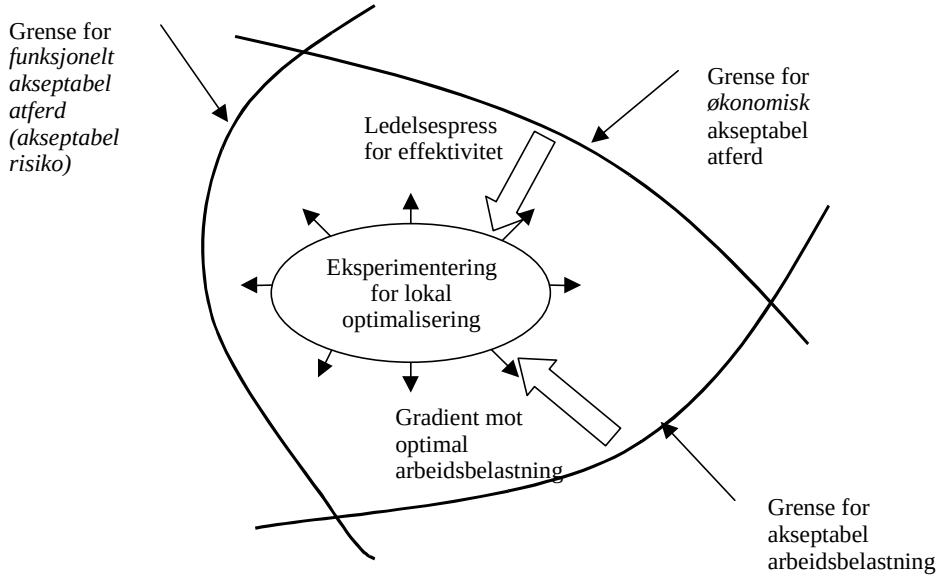
2.4 Turners teori om menneskeskapte katastrofer pga svikt i informasjonsbehandlingen

Informasjonsbehandlings-perspektivet tar utgangspunkt i Turner's teori om menneskeskapte katastrofer (Turner, 1978; Turner og Pidgeon, 1997). Turner hevder at ulykker og katastrofer utvikler seg gjennom en lang kjede av hendelser, som leder tilbake til grunnleggende årsaker som mangel på flyt i informasjon og individuelle feiltolkninger av informasjon. Turner kaller tidsrommet hvor informasjonssvikt og feiltolkninger utvikler seg, for inkubasjonstiden. Inkubasjonstiden representerer en prosess hvor en kjede av avvikende hendelser får utvikle seg og akkumuleres uten at det oppdages. Og dersom noen faktisk foretar seg noe som et resultat av slike avvik, viser det seg gjerne i ettertid at man har misforstått signalene, slik at tiltaket bare har bidratt til å lede oppmerksomheten ytterligere bort fra det virkelige problemet. Katastrofer vil ut fra dette perspektivet nesten alltid være assosiert med sammenbrudd av den eksisterende forståelse av risiko i systemet. Modellen inkluderer også trinnene etter katastrofen, dvs. redningsoperasjoner og deretter full tilpasning av systemet i forhold til de nye erkjennelser.

2.5 Beslutningsperspektivet – målkonflikter

Innen beslutningsperspektivet fokuseres spesielt hvordan målkonflikter behandles. I hvor stor grad velger man aktivt å ta en sjanse, og i hvor stor grad løper man risikoen uten å være klar over det? Noen ganger kan bedrifters ledelse prioritere kortsiktige økonomiske besparelser eller gevinster, selv om det går på bekostning av sikkerheten for de ansatte og eventuelt også kundegrupper. Rasmussens (1996; 1997) migrasjonsmodell om aktiviteter i bevegelse mot grensene for akseptabel utførelse, introduseres innen dette temaet (se Figur 5). Modellen beskriver hvordan individer og grupper streber mot å holde arbeidsbelastningen på et overkommelig nivå, å

ha intellektuelle utfordringer i arbeidet og mot å unngå feil. Arbeidsgiveren vil samtidig operere med visse grenser for hva som er økonomisk akseptabelt.



Figur 5. I presset fra målkonflikter har aktivitetene en tendens til å bevege seg mot grensen for akseptabel risiko (etter Rasmussen, 1996).

I en arbeidssituasjon kan man ha frihet til å bevege seg innenfor disse grensene, men grensene vil i enkelte tilfeller også bli utfordret. Ulykker kan skje idet man passerer grensen for hva som er funksjonelt akseptabel opptreden (akseptabel risiko). Innen beslutningsperspektivet fokuseres således spesielt spørsmål og valg omkring denne grensen. Spørsmål omkring beslutningsprosessene og hvordan ulike målkonflikter påvirker valgene, inngår dermed i denne modellen.
Dersom en innfører tekniske eller fysiske sikkerhetstiltak, kan dette føre til at aktørene endrer sin arbeidspraksis, fordi de opplever at grensen for funksjonelt akseptabel adferd har flyttet seg (risikokompensasjon). I et system med multiple barrierer er det dessuten en utfordring at en tilnærming til eller overskridelse av én barriere ikke nødvendigvis har noen umiddelbar synlig effekt og dermed ikke nødvendigvis blir oppdaget. Dette henger blant annet sammen med at sikkerhetsbarrierer ofte er ”sovende” i sin natur, dvs de kan kuttes helt bort uten at dette får noen synlig effekt bortsett fra i en ulykkessituasjon (for eksempel manglende passiv brannbeskyttelse).

2.6 Kausale og systemiske ulykkesmodeller

I de foregående avsnittene er noen forskjellige perspektiver på ulykker gitt. Hollnagel (2002) klassifiserer ulykkesmodeller i tre kategorier, der skillene mellom kategoriene spesielt kan sees i henhold til hvilken grad av kausalitetstenkning som preger dem. Kategoriene betegnes som sekvensielle, epidemiologiske og systemiske ulykkesmodeller.

Sekvensielle ulykkesmodeller forutsetter at det er en spesifikk årsak til en spesifikk virkning (ulykken). Målet med en analyse med denne type modell er å eliminere eller innkapsle årsaken. Et konkret eksempel av en slik ulykkesmodell er dominomodellen (Heinrich, 1930), der en brikke som faller er årsak til en sekvens av hendelser, og velter alle dominobrikkene. Forebygging kan gjøres ved å fjerne en brikke, som å fjerne en kjede i hendelsestreet. *Epidemiologiske* ulykkesmodeller er også bygget på kausalsammenhenger mellom årsak og virkning, men ser mer

på kompleksiteten i systemet, og representerer gjerne årsakene med et kausalt nettverk. Identifikasjon av barrierer, energibærere og latente betingelser, samt styrking av barrierer og forsvar er viktige momenter i analysemålene til denne modellen. Både sekvensielle og epidemiologiske modeller er det vi kan kalle kausale modeller, med klare relasjoner mellom årsak og virkning. Energi-barriere perspektivet i kap. 2.1 bygger på en kausal modell, så vel som Turners modell, kap. 2.4. Sveitserostmodellen til Reason (1997) er også et klassisk eksempel på en kausal modell. Hendelsestrær (event trees) og feiltrær (fault trees) er mye brukt innen risikoanalyser og pålitelighetsanalyser innen både petroleumsvirksomhet og kjernekraftindustrien. Menneskelige handlinger har begrenset plass i risikoanalyser for innretninger, men de tillegges betydelig vekt i pålitelighetsanalyser av sikkerhetssystem (Bodsberg m.fl., 1994).

Systemiske ulykkesmodeller unngår å gi en beskrivelse av relasjonene mellom årsak og virkning ved ulykker. Modellene setter fokus på uvanlige avhengigheter i systemet samt på betingelser som erfaringsmessig assosieres med uønskete situasjoner. Målet med analyse av systemisk karakter er å overvåke og kontrollere variabiliteten i prestasjon og oppførsel av systemet. Kriteriene for hva som er god og dårlig prestasjon må fastsettes. Men ved bruk av kun systemiske modeller kan det være et problem at man ikke har relasjonen til virkning eller til risikonivået, og det kan være vanskelig å si hvor mye risikonivået forbedres ved å forbedre prestasjonen innen et område. En modell av normal prestasjon er nødvendig for å kunne relatere avvik til sikkerhetsnivå, en slik modell finnes i følge det vi vet ikke på det nåværende tidspunkt. Perrows teori om normalulykker legger opp til bruk av en systemisk ulykkesmodell. Et annet eksempel er Rasmussens migrasjonsmodell, som er vist ovenfor.

Kausaltenkningen har vært gjennomgående i ulykkesanalyser. Men dette gjør oss gode til å finne årsaker, og dermed å forhindre denne årsaken neste gang. Vi blir gode til å ”forhindre den forrige ulykken”. Men i forebygging av ulykker er det viktig å kunne analysere et bredere sett av muligheter for ulykker. Det er heller ingen motsetning mellom kausalitetstenkning og systemtenkning. F.eks må en kunne se på barrierer samtidig som en prøver å analysere en større variabilitet i systemet.

Ved prediksjon som en del av forebygging bør en imidlertid være oppmerksom på at ensidig kausaltenkning kan være for enkel for å fange opp den type komplekse, organisatoriske ulykker som vi diskuterer her. En annen følge av en ensidig kausalitetstenkning, kan også være at det i analyse av ulykker blir et sterkt fokus på å søke syndebukker og fokusere på “menneskelige feil”.

3 Barrierer, feiltoleranse og sårbarhet – en diskusjon om sentrale begrep

"Halvparten av problemene innenfor HMS skyldes at personer bruker samme ord i forskjellige betydninger.

Den andre halvparten skyldes at personer bruker forskjellige ord for samme betydning"

Stan Kaplan

I dette kapitlet vil vi presentere og kommentere noen av definisjonene vi har kommet over på begrep som 'barriere', 'sikkerhetsfunksjon' og 'feiltoleranse'. I denne omgang avstår vi imidlertid fra å ta standpunkt i forhold til de mange definisjonene som er i bruk. På slutten av kapitlet introduserer vi begrepet 'organisatorisk redundans', som er sentralt i denne rapporten.

3.1 Definisjoner og diskusjon av begrep

I tabellen nedenfor har vi samlet en oversikt over relevante definisjoner av begrepet barrierer og relaterte begrep. Noen begrep er definert i forskjellige dokumenter, og vi har da listet dem her for å få et bilde av mangfoldet i litteraturen og i definisjonene vi må forholde oss til.

Tabell 1. Oversikt over definisjoner.

Begrep	Definisjon	Kilde
Barrier	Measure which reduces the probability of realizing a hazards's potential for harm and which reduces its consequence Note: Barriers may be physical (materials, protective devices, shields, segregation, etc.) or non-physical (procedures, inspection, training, drills, etc.)	ISO 17776: 2000
Barriere	Tiltak som reduserer sannsynligheten for å utløse en fares potensial for skade eller reduserer skadepotensialet	ISO 17776/ RNNS
Barrier	Barrier is anything used to control, prevent, or impede energy flows. Common types of barriers include equipment, administrative procedures and processes, supervision/ management, warning devices, knowledge and skills, and physical. Barriers may be either control of safety.	DOE, 1997
(Well) Barrier	A well barrier is an item that, by itself, prevents flow of the well reservoir fluids from the reservoir to the atmosphere	Holand/ Tallby
Barriere	Tiltak som minsker sannsynligheten for at en fare med stort skadepotensiale skal realiseres, og som dersom den virker, minsker de potensielle konsekvensene av skaden. Barrierer kan være fysiske (materialer, beskyttelsesinnretninger, atskillelse og lignende) og ikke-fysiske (prosedyrer, inspeksjon, opplæring, øvelser)	NORSOK S-001
Barriers	The physical and procedural measures to direct energy in wanted channels and control unwanted release.	Johnson, 1980
Barriers	We will use the term 'barriers' rather than 'strategies' to denote the physical counter-measures that intervene in the accident process to eliminate or reduce the harmful outcome	Kjelén, 2000
Beredskapstiltak og barrierer	Beredskapstiltak er barrierer som skal rettes mot tilløp til ulykker, inntrådte ulykker og andre uønskede tilstander som kan føre til skade. Barrierene kan være av både teknisk, operasjonell og organisatorisk art.	St.meld. nr. 7, §4.15.1
Control	Stay on course, adhere to a standard, prevent unwanted change.	Johnson, 1980

Defence	Various means by which the goals of ensuring the safety of people and assets can be achieved. Defence-in-depth means successive layers of protection	Reason, 1997
Defence in depth	Principle: To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.	INSAG-12
Null-filosofi	Null-filosofi kan oppsummeres som at ulykker ikke skjer, men forårsakes. Alle ulykker kan derfor forebygges, slik at målet vil være null skader og ulykker.	St.meld. nr. 7, §3.2.4
Protection layer	Any independent mechanism that reduces risk by control, prevention or mitigation Note: It could be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical engineering mechanism such as a relief valve, a safety instrumented system or an administrative procedures such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions.	IEC 61511-1
Protection layer	Protection layers typically involve special process designs, process equipment, administrative procedures, the basic process control system (BCPS) and/or planned responses to imminent adverse process conditions; and these responses may be either automated or initiated by human actions.	CCPS, 1993
Sikkerhets-funksjoner	Fysiske tiltak som reduserer sannsynligheten for at en fare- og ulykkessituasjon oppstår, eller som begrenser konsekvensene ved en ulykke	OD, 2001b
Safety function	Function to be implemented by a SIS, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event	IEC 61511-1 Tilsvarende def. i IEC 61508-4:1998
Sikkerhets-kritisk funksjon	Systemfunksjon, teknisk og/eller operasjonell aktivitet og/eller handling i jernbanevirksomheten som ved feil, uteblivelse, endret operasjonskarakteristikk inklusiv utilsiktet og/eller uautorisert aktivering kan forårsake tap av menneskeliv eller alvorlig personskade. Primære SKF vil være knyttet til de tekniske systemene på rullende materiell, kjøreveien og trafikkstyringen. Sekundære SKF vil være aktiviteter som gjøres for å vedlikeholde de SKF, f.eks. inspeksjonsprogram for hjulaksler, visitas av spor, ultralydmålinger med målevogn osv. Tertiære SKF vil være ulike styringssystemer for sikkerhet, vedlikehold, kostnadsoppfølging, mm.	Jernbane-tilsynets forskrift av 23. des 1999
Sikkerhets-system	Et system som realiserer én eller flere aktive sikkerhetsfunksjoner	OD, 2001b
Essential safety system	Any system which has a major role in the control and mitigation of fires and explosions and in any subsequent EER activities	EN ISO 13702:1999
Redundancy	Use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy)	IEC 61511-1
Redundancy	Existence of a means, in addition to the means which would be sufficient, for a functional unit to perform a required function of for data to represent information	IEC 61508-4 1998
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors	IEC 61508-4 1998 Også I IEC 61511-1

Sårbarhet	Sårbarhet ("vulnerability") er manglende evne til å tåle påkjenninger og avvik som kan føre til stor skade eller stort verditap. Sårbarhet sier noe om hvor lett noe kan skades eller settes ut av funksjon. Begrepet brukes blant annet om menneskets "sårbarhet" overfor visse fysiske og psykiske påkjenninger, og sikkerhetssystemets manglende evne til å motstå ulykkesbelastninger (som ikke alltid er fanget opp i pålitelighetsbegrepet). Sårbarhet i økonomisk forstand uttrykker manglende evne til å motstå hendelser som i verste fall kan medføre nedleggelse av virksomheten (langsiktig overlevelsesevne).	ROS

Barrierer er et sentralt begrep i offshoreindustrien når en snakker om sikkerhet, og mange ulykkesmodeller bruker dette begrepet. Samtidig illustrerer tabellen at det ikke finnes noen presis, samlende definisjon innen fagområdet. Det synes å være et fellestrekk at definisjonene refererer til en farekilde, og i de fleste tilfelle synes et energi- og barriere-perspektiv å være underforstått (jfr kapittel 2). Ulikhetene dreier seg bl.a. om hvorvidt barriere-begrepet er begrenset til fysiske tiltak (f.eks. Kjellén, 2000), eller om det også omfatter f.eks. administrative tiltak eller muligheten for menneskelig intervensjon. Vi ser også at en rekke begrep er gitt betydninger som ligger tett opp til barrierebegrepet, f.eks. protection layer og sikkerhetsfunksjon/safety function.

I mange tilfelle inngår begrepene ”barriere” eller ”sikkerhetsfunksjon” i en sammenheng hvor det forutsettes at tiltakene er gjenstand for ulike former for kvalitetssikring eller oppfølgingstiltak.

I det følgende utbroderes dette litt spesielt i forhold til Reason’s modell, se kap. 2.1 (Reason, 1997). Det er allikevel ikke dermed sagt at vi velger å kun bruke hans modell i det videre arbeid, men vi kommer til å bruke deler av denne type modell.

Barrierefunksjoner

Reason påpeker at alle ‘defences’ er designet for å oppfylle en eller flere av de følgende funksjonene:

1. To create understanding and awareness of the local hazards.
2. To give clear guidance on how to operate safely.
3. To provide alarms and warnings when danger is imminent.
4. To restore the system to a safe state in an off-normal situation.
5. To interpose safety barriers between the hazards and the potential losses.
6. To contain and eliminate the hazards should they escape this barrier.
7. To provide the means of escape and rescue should hazard containment fail.

Vi ser av punkt 5 at Reason bruker begrepet ”safety barrier” i en snevrere betydning enn begrepet ”defence”. Barrierer synes å være spesifikt knyttet til det å skape fysisk atskillelse mellom farekilder og sårbare objekter.

Kategorisering av barrierer

Reason (1997) skiller mellom soft vs hard defences:

> Hard defences include such technical devices as automated engineered safety features, physical barriers, alarms and annunciators, interlocks, keys, personal protective equipment, non-destructive testing, designed-in structural weaknesses (for example, fuse pins on aircraft engine pylons) and improved system design. Soft defences rely heavily upon a combination of paper and people: legislation, regulatory surveillance, rules and procedures, training, drills and briefings, administrative controls (for example, permit-to-work systems and shift handovers), licensing, certification, supervisory oversight and – most critically – front-line operators, particularly in highly automated control systems.

Kjellén (2000) skiller mellom *aktive og passive barrierer*. Passive barrierer en innebygd i design av arbeidsplassen og er uavhengig av operasjonelle kontroll- og styresystemer. Aktive barrierer er avhengig av aksjon fra operatør eller et teknisk kontroll- og styresystem for å funksjonere som planlagt. Kjelléns definisjon bidrar til bedre forståelse av barrierebegrepet, sett sammen med Reasons definisjon.

CCPS (1993) skiller også mellom *passive and active protection layers*:

> A passive protection layer mitigates potential hazards by virtue of design decisions (equipment selection, plant layout, etc.). An active protection layer initiates specific action when a hazardous event is likely (instrumentation is often part of an active protection layer).

Her brukes "protection layer" på samme måte som Kjellén bruker barrierer.

Hollnagel (1999) foreslår at barrierer klassifiseres i fire kategorier: fysiske, funksjonelle, symbolske og immaterielle barrierer:

- Fysiske barrierer
  Hindrer hendelser fysisk, f.eks. vegger, gjerder, bygninger, mennesker.
- Funksjonelle barrierer
  Hindrer hendelser ved menneskelige eller automatiske inngrep, f.eks. f.eks. nødavstengningssysem (NAS).
- Symbolske barrierer
  Avbryter/forebygger en hendelsessekvens hvis de tolkes riktig av mennesker, f.eks. skilter og signaler.
- Immaterielle barrierer
  Avbryter/forebygger en hendelsessekvens ved å påvirke menneskets tenkning og kunnskap, f.eks. et innlært samhandlingsmønster.

Feiltoleranse – fault tolerance

Feiltoleranse-begrepet brukes hyppig i forbindelse med software-utvikling, som ett av flere hjelpemidler/prinsipper for å produsere sikre og pålitelige programmer. Andre prinsipper som benyttes er for eksempel *feilunngåelse (fault avoidance)* og *feil-deteksjon og korrigering (fault detection and correction).* Tradisjonelt, har feiltoleranse henvist til å bygge sub-systemer av redundante komponener som plasseres i parallell (Marciniak, 1994).

I erkjennelse av at kompleks software "alltid" vil inneholde feil, må en designe systemer som tolerer feil. Feiltoleranse (i software) oppnås på ulike måter:

- *Redundans*; dvs at flere *like* systemer utfører det samme, med avstemningslogikk (votering)
- *Passiv 'stand-by'*; dvs at en annen (sovende) enhet overtar dersom en enhet feiler (for eksempel 2x100% pumper)
- *Diversifisering*; dvs at flere *ulike* systemer (basert på ulike fysiske prinsipper, ulik leverandør, forskjellige programmerere, osv.) utfører det samme, med avstemningslogikk
- *'Recovery blocks'*; dvs at resultatet fra en 'modul'/ et 'trinn' må aksepteres før det brukes videre. Dersom resultatet ikke aksepteres utløses i stedet en *alternativ modul*, osv.
- *'Exception handling'*; dvs at systemet inneholder rutiner som håndterer situasjonen dersom det oppstår en unormal systemtilstand.

Slik 'redundans' ofte brukes i dagligspråket dekker det de fleste av begrepene ovenfor.

3.2 Kommentarer

Det finnes ingen enhetlig og allmenngyldig definisjon av barriere, med andre ord så mangler vi et felles begrepsapparat.

De ulike barrieredefinisjonene har til dels forskjellige perspektiver på begrepet, som kan ses i sammenheng med kategoriene og egenskapene diskutert over. Kategoriseringen er viktig i den forstand å velge fra hvilket synspunkt en vil analysere barrierer, og ut fra problemstillingene en vil ta opp. Siden vi er opptatt av en MTO-vinkling, av menneskets og organisasjonenes rolle i analysene, og at arbeidet skal ha diagnostisk verdi, foreslår vi å velge Reasons myke og harde klassifikasjon som en bakgrunn for den videre behandling av barrierer. Men mennesket kan gå inn i både aktive og passive barrierer, og Hollnagels klassifikasjon i fire nivåer er trolig også velegnet til å karakterisere menneskers rolle i barrierer. I kapittel 6 vil vi diskutere hvor "harde" tekniske og fysiske barrierer er, dersom de er avhengig av mennesker.

Mens tekniske barrierer i stor grad er identifisert og beskrevet gjennom ODs regelverk samt prosjektet 'Risikonivå på norsk sokkel' (OD-RNNS, 2002), mangler det en taksonomi for andre typer barrierer.

OD definerer ikke barriere-begrepet eksplisitt, men synes å tolke begrepet tilsvarende som definisjonene gitt av ISO 17776 og NORSOK S-001 (ref. tabell 1), dvs at en barriere kan være både et fysisk og ikke fysisk tiltak. Mht sikkerhetsfunksjoner, tolker OD dette som en rent fysisk innretning, mens andre forskrifter/standarder har en utvidet tolkning av begrepet.

Begrep som feiltoleranse og robusthet kan brukes på ulike nivåer – både som egenskaper ved det totale systemet og ved en enkelt barriere eller sikkerhetsfunksjon. OD knytter robusthetsbegrepet til ytelse av en barriere, altså en egenskap ved en barriere. Feiltoleranse slik det defineres i forbindelse med softwareutvikling kan tolkes å være en egenskap ved systemet som helhet, men kan også tolkes å vare en egenskap ved en barriere dersom software-komponenten for eksempel inngår som en del av et instrumentert sikkerhetssystem.

4 Krav til barrierer og sikkerhetsfunksjoner i regelverket og sentrale standarder

Dette kapitlet diskuterer krav til barrierer, løsninger og sikkerhetsfunksjoner i regelverket til OD, samt gir en kort presentasjon av standarden IEC 61508.

4.1 **Krav til barrierer i regelverket til OD**

I St.meld. nr. 7 (AAD, 2001) påpekes det at ODs nye regelverk inneholder en innskjerping på områdene styring og operasjon, økt fokus på bruken av barrierebegrepet og kravet til barrierer.

I ODs Styringsforskrift §1 hetter det at den 'ansvarlige' skal "...velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår feil og fare- og ulykkessituasjoner." (OD, 2001a, 2, vår fremhevning). Det hedder videre:

"I tillegg skal det etableres barrierer som

a) reduserer sannsynligheten for at slike feil og fare- og ulykkessitasjoner utvikler seg,

b) begrenser mulige skader og ulemper.

Der det er nødvendig med flere barrierer, skal det være tilstrekkelig uavhengighet mellom barrierene." **(**ibid**.)**

Begrepet *uavhengighet* defineres i Veiledning til Styringsforskriften som innebærende "... at flere barrierer ikke skal kunne svekkes eller settes ut av funksjon samtidig, blant annet som følge av en enkelt feil eller en enkelt hendelse." (OD, 2002a, 2). Veiledningen til Styringsforskriften viser slikt hen til enkeltfeilsprinsippet.[7]

I Styringsforskriftens §2 (OD, 2001a, 2) blir det presisert at det er den 'ansvarlige', dvs. den som har ansvar for driften, som skal fastsette strategiene og prinsippene som legges til grunn for utformning, bruk og vedlikehold av barrierer. Det spesifiseres dessuten at den ansvarlige må sikre at fire forhold er kjente:

1) hvilke barrierer som er etablert

2) hvilken funksjon de enkelte barrierer skal ivareta

3) hvilke krav til ytelse som er satt til de tekniske, operasjonelle eller organisatoriske elementer som er nødvendige for at den enkelte barrieren skal være effektiv.[8]

4) hvilke barrierer som er ute av funksjon eller svekket

- samt at den ansvarlige skal sette i verk tiltak for å rette opp eller kompensere for manglende eller svekkede barrierer.

I forhold til prioritering av barrierer angis det i Styringsforskriftens §1 at løsninger som har størst risikoreduserende effekt skal velges,[9] samt at kollektive vernetiltak skal foretrekkes framfor

[7] Enkeltfeilsprinsippet tolkes tradisjonelt som at ingen enkelt feil - verken en enkelt teknisk eller en enkelt menneskelig feil - må kunne føre til tap av menneskeliv eller til alvorlig personskade (se f.eks. Jernbanetilsynets forskrift av 23. desember 1999 nr. 1402 §6.)

[8] Det presiseres i Veiledning til Styringsforskriften (OD, 2002a, 2) at ytelse bl.a. kan være kapasitet, pålitelighet, tilgjengelighet, effektivitet, evne til å motstå laster, integritet og robusthet.

vernetiltak som er rettet mot enkeltpersoner." (OD, 2001a, 2). I rammeforskriften (OD, 2001b, 15) angies at begrepet risiko generelt viser hen til en kombinasjon av sannsynlighet og konsekvens, mer presist at risiko er lik produktet av sannsynlighet og konsekvens.

Det har ikke vært mulig for oss å finne en eksplisitt definisjon av begrepet barriere i ODs forskrifter. Styringsforskriftens §1 fastsetter imidlertid som ovenfor nevnt at en barriere må oppfylle minst et av to funksjonelle krav: Barrieren må redusere sannsynligheten for at fare- og ulykkessitasjoner utvikler seg og/eller begrense mulige skader og ulemper. Denne presisering indikerer at OD anvender begrepet barriere i betydningen *konsekvensreduserende barrierer*, dvs. med referanse til tiltak som har til formål å begrense konsekvensene av en allerede inntruffet fare- eller ulykkessituasjon.

I Innretningsforskriften definerer OD videre en rekke krav til barrierer - alle teknisk/fysiske barrierer - som skal beskytte mot *spesifikke* forhold. Dette inkluderer f.eks. krav til brannskiller, brann- og gassdeteksjonssystem, krav til nødavstengningssystem (OD, 2001c, 12-14) - samt krav til brønnbarrierer (ibid., 16). Kravene som stilles er ganske spesifikke. I forhold til brannskiller hetter det bl.a.:

> "Hovedområdene på innretningene skal atskilles med brannskiller som kan motstå de *dimensjonerende brann- og eksplosjonslastene* og minst oppfylle *brannklasse H-0*. Rom som har viktige funksjoner og viktig utstyr, samt rom med høy brannrisiko skal være *atskilt fra omgivelsene* ved brannskiller. Brann skillene skal utformes for å motstå *dimensjonerende brann- og eksplosjonslaster* slik at hovedsikkerhetsfunksjoner opprettholdes i tilstrekkelig tid, men alltid *minst én time*." (OD, 2001c, 12; våre fremhevninger)

Det finnes ingen tilsvarende spesifikke krav til ustyret som skal sikre at medarbeiderne vil være i stand til å utføre *spesifikke* sikkerhetskritiske arbeidsoppgaver. Kravene det stilles til medarbeidernes utstyr av mer *generell* natur. Det hetter f.eks. i §20 som berører menneske-maskin grensesnitt og informasjonspresentasjon:

> "Skjermbasert utstyr [...] skal utformes slik at *faren for feilhandlinger som kan ha betydning for sikkerheten reduseres*. [...] Informasjonsgivere og betjeningsinnretninger skal utformes, plasseres og grupperes, slik at det *enkelt og hurtig kan mottas nødvendig informasjon og utføres nødvendige aksjoner*." (Innretningsforskriften, 2001c, 11; våre fremhevninger)

Ovenstående indikerer at OD ikke betrakter medarbeiderne som eksplisitt del av organisasjonenes barrierer - og således at OD følger den tradisjonelle bruk av barrierebegrepet som innebærer at barrierer betraktes som fysiske/tekniske tiltak. Dette betyr *ikke* at OD underkjenner medarbeidernes bidrag til sikkerheten. OD påpeker eksplisitt at operasjonelle og organisatoriske *løsninger* skal anvendes til å redusere sannsynligheten for at feil og fare- og ulykkessituasjoner vil oppstå (Styringsforskriften §1). Skillet mellom *løsninger* rettet mot forebyggelse av faresituasjoner, og *barrierer* rettet mot bekjempelse av allerede inntrufne faresituasjoner kan imidlertid bety at oppgavene som allokeres til medarbeiderne - herunder arbeidsredskapene som kreves for å kunne gjennomføre de allokerte oppgavene - kvalitetssikres på mer generelt måte enn tilfellet er i forhold til de tekniske/fysiske barrierer (jf. avsnitt 3.1).

Det forhold at medarbeidere spiller en avgjørende rolle for sikkerheten, presiseres generelt i ODs forskrifter. Aktivitetsforskriften §21 understreker f.eks. at den 'ansvarlige' skal sikre :

[9] Bemerk: I Veiledning til styringsforskriften (OD, 2002a) §6, vises til Norsok Z-013 kapittel 4. Her henvises igjen til kapittel 5.1.4. der det står at tiltak som har til hensikt å redusere sannsynligheten skal prioriteres fremfor tiltak som har som formål å begrense konsekvensene.

”...at det utføres nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner på en effektiv måte.” (OD, 2001d, 8)

I Veiledning til Styringsforskriften (OD, 2002a) settes også en rekke krav til kompetansen hos medarbeidere som jobber med SIS (Safety Instrumented Systems). Kravene er sammenfattet i ”OLF 070, Recommended guideline for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian continental shelf” (OLF, 2001). Kravene som stilles inkluderer krav til organisatoriske elementer, f.eks. i forhold til tilretteleggelse og gjennomføring av operatørtrening:

“All activities that affect the safety life cycle of the SIS shall be managed and performed by personnel who are competent to do so in accordance with the relevant requirements in the NPD regulations and in IEC 61508 and IEC 61511. As a minimum, the following items should be addressed when considering the competence issue:

- engineering knowledge, training and experience appropriate to the:
- process application;
- technology used (e.g., electrical, electronic or programmable electronic);
- sensors and final elements.
- safety engineering knowledge (e.g., process safety analysis);
- knowledge of the legal and safety regulatory requirements,
- adequate management and leadership skills appropriate to their role in safety lifecycle activities;
- understanding of the potential consequences of undesirable events;
- the safety integrity level of the safety instrumented functions;
- the novelty and complexity of the application and the technology.

Furthermore, both operators and contractors working with such systems must have formal employee appraisal and training programs to ensure the above.”
(OLF, 2001, 18)

4.2 Krav til sikkerhetsfunksjoner i regelverket til OD

Innretningsforskriften anvender ytterligere et begrep som har direkte relasjon til opprettholdelse av sikkerheten. Dette er begrepet *sikkerhetsfunksjon*. Sikkerhetsfunksjoner defineres som:

”Fysiske tiltak som reduserer sannsynligheten for at en fare- og ulykkessituasjon oppstår, eller som begrenser konsekvensene av en ulykke.” (OD, 2001c, 6).

Kravet om at sikkerhetsfunksjoner skal begrense konsekvensene av en ulykke, motsvarer kravet som stilles til organisasjonens barrierer. Kravet om å *redusere sannsynligheten* for at fare- og ulykkessituasjoner oppstår går imidlertid videre. Dette kravet korresponderer med den tradisjonelle definisjonen av begrepet *frekvensreduserende barriere*, dvs. barrierer som har til formål å redusere frekvensen av kritiske hendelser.

I § 7 står det at innretninger skal være utstyrt med nødvendige sikkerhetsfunksjoner som til enhver tid kan

a) oppdage unormale tilstander,
b) hindre at unormale tilstander utvikler seg til fare- og ulykkessituasjoner,
c) begrense skadene ved ulykker.

Det presiseres ytterligere at det skal fastsettes krav til ytelsen for sikkerhetsfunksjoner, samt at status for sikkerhetsfunksjoner skal være tilgjengelig i det sentrale kontrollrommet. I veiledningen til styringsforskriften er ytelsesbegrepet forklart på følgende måte:

> Ytelse [...] kan blant annet være kapasitet, pålitelighet, tilgjengelighet, effektivitet, evne til å motstå laster, integritet og robusthet.

I RNNS (2002) er ytelsesbegrepet utdypet videre. Der står det at ytelse oppfattes å ha følgende 3 komponenter:

1. Funksjonalitet/effektivitet, dvs. den effekt barrieren har på ulykkesforløpet, gitt at den er til stede (funksjonerer) som forutsatt i design
2. Tilgjengelighet/pålitelighet, dvs. barrierens evne til å være til stede ved behov (on demand)
3. Robusthet (invers av sårbarhet), dvs. barrierenes evne til å funksjonere under relevante (spesifiserte) ulykkesforløp og –laster.

4.3 Krav til sikkerhetsfunksjoner i IEC 61508

IEC 61508, ”Functional safety of electrical/electronic/programmable electronic safety-related systems”, er en relativt ny standard (fra 1998) som allerede er tatt i bruk innenfor offshore industrien både nasjonalt og internasjonalt. Hovedformålet med standarden er å beskrive en risikobasert metodikk for å spesifisere og realisere instrumenterte sikkerhetssystemer slik at et akseptabelt nivå av sikkerhet oppnås.

Standarden begrenser seg til å omhandle instrumenterte sikkerhetssystemer (slik som nødavstengning- og brann og gass systemer), men forutsetter at det stilles krav til andre typer sikkerhetssystemer og/eller risikoreduserende tiltak dersom dette er nødvendig. Standarden er generisk i den forstand at den i prinsippet skal kunne anvendes av alle bransjer hvor slike systemer anvendes.

ODs nye regelverk krever at prinsipper fra IEC 61058 skal ligge til grunn ved spesifikasjon og design av instrumenterte sikkerhetssystemer. Standarden er imidlertid omfattende og forholdsvis tung, så for å forenkle bruken gikk industrien sammen om å utvikle en egen retningslinje; ”OLF 070, Recommended guideline for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian continental shelf”.

IEC 61508 behandler ikke barrierebegrepet eksplisitt, men opererer med ”sikkerhetsfunksjon” som et sentralt begrep. En sikkerhetsfunksjon kan tolkes som et påkrevd tiltak for å sikre at risikoen knyttet til en spesifikk fare er akseptabel. En sikkerhetsfunksjon kan være realisert enten i form av

- et instrumentert sikkerhetssystem (SIS),
- sikkerhetssystemer basert på annen teknologi, eller
- andre risikoreduserende tiltak.

For en identifisert risiko, slik som for eksempel hydrokarbon lekkasje, og et gitt akseptkriterium, kan en definere et tilhørende krav til risikoreduksjon (ΔR). For å oppnå denne risikoreduksjon må en eller flere sikkerhetsfunksjoner realiseres. En nøyaktig spesifikasjon av hver

sikkerhetsfunksjon i forhold til funksjonalitet og integritet er en grunnpilar i IEC 61508, og skal sikre at sikkerhetsfunksjonen oppfylles med en viss pålitelighet.

Når det gjelder kravet til integritet, opererer IEC 61508 med fire såkalte SIL (Safety Integrity Level) klasser. For systemer som opererer ved behov (i motsetning til kontinuerlig), slik som for eksempel et nødavstengningssystem, er disse fire SIL klassene definert ved:

Safety Integrity Level (SIL)	Krav til PFD (probability of failure on deman)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Selv om IEC 61508 er en risikobasert standard, er det viktig å understreke at standarden i tillegg til de kvantitative SIL kravene ovenfor, også setter krav til robusthet i design av sikkerhetssystemene. Disse mer kvalitative kravene, er i hovedsak basert på fire parametere:

- at en skal forebygge og kontrollere systematiske feil
- at en skal bestemme andelen sikre feil
- at en skal bestemme såkalt ”hardware feil toleranse”, dvs hvor mange feil som tolereres før sikkerhetsfunksjonen svikter, og
- at en skal vurdere i hvilken grad utstyret er slik at alle mulige feilmoder kan beskrives på forhånd eller ikke

Kombinasjonen av disse parametrene bestemmer, i tillegg til den tekniske påliteligheten (PFD) til utstyret, hvilket SIL nivå sikkerhetsfunksjonen kan oppnå, og dermed hvilken risikoreduksjon som kan ”kreves”.

5 Barrierer og feiltoleranse i praksis

I dette kapitlet vil vi først se mer konkret på hvilke barrierer som i praksis er etablert på en typisk produksjonsplattform.

5.1 Analytisk risikokontroll i petroleumsvirksomheten

I avsnitt 2.1.2 introduserte vi Rasmussens (1997) skille mellom empiriske, evolusjonære og analytiske strategier for risikokontroll. Tradisjonelt har ulykkesforebyggende arbeid offshore lagt hovedvekten på empiriske og analytiske strategier for risikokontroll. En har arbeidet empirisk med å forebygge skader på enkeltpersoner. Her har *Synergi* hatt betydning både som en erfaringsdatabase og som holdepunkt for å følge opp hver enkelt hendelse.

Når det gjelder de alvorligste hendelsene offshore (dimensjonerende ulykkeshendelser, f.eks. store eksplosjoner), er det ikke akseptabelt å lære gjennom prøving og feiling. En har derfor valgt en *analytisk* strategi rettet mot disse hendelsene. *Konsept-risikoanalysene* (SEPA – Safety and Emergency Preparedness Analysis) er et sentralt verktøy i denne strategien. I designfasen etablerer en de fysiske/tekniske barrierene som er nødvendige for å holde beregnet risiko på et akseptabelt nivå. I praksis innebærer dette at en må etablere flere uavhengige barrierer. Tabell 2 viser hvilke fysiske/tekniske barrierer som normalt brukes for å forebygge og begrense branner og eksplosjoner i prosessanlegget.

Tabell 2. Barrierer for forebyggelse og begrensning av branner og eksplosjoner i prosessanlegg offshore. (Etter Kjellén, 1999).

Independent safety barriers	Strategy according to Haddon , 1970.
Inherent safety through high quality containment (quality of material/equipment, thickness of piping/vessels)	Prevent build-up of energy
Process control system to keep pressure, temperature etc. within acceptable limits	Prevent build-up of energy
Reduce the release of hydrocarbons through leak detection, emergency shut down and depressurisation of process equipment	Limit the amount of energy
Prevent ignition through area classification and isolation of ignition sources and ventilation	Prevent uncontrolled release
Limit the size of the affected area through fire and blast walls	Separation by physical barriers
Passive protective measures to limit the consequences through fire insulation of process equipment	Improve target's ability to endure energy flow
Fire protection of building structures and explosion ventilation of building	Improve target's ability to endure energy flow
Active fire protective measures such as fire detection and fire fighting equipment (sprinkler/deluge systems, fire hydrants)	Limit the development of damage
Escape and evacuation emergency preparedness	Limit the development of injury/damage

I praksis vil en analytisk strategi legge hovedvekten på fysiske og tekniske barrierer, fordi det er problematisk å forutsi sannsynligheten for at operatørinngrep blir utført korrekt. Operatørinngripen, manuell deteksjon av lekkasjer, osv, er til en viss grad 'bakt inn' i de erfaringsdata som brukes i analysene, men er ikke uttrykt eksplisitt. Menneskets rolle i storulykker er derfor lite synlig i en konseptrisikoanalyse, jfr. Tabell 2. I driftsfasen må en imidlertid *overvåke og vedlikeholde* de tekniske sikkerhetsbarrierene, f.eks. gjennom regelmessig testing av gassdetektorer. Dersom én eller flere barrierer settes ut av funksjon under drift, må disse i prinsippet erstattes med en likeverdige barrierer (*kompenserende tiltak*). I praksis kan det oppstå situasjoner hvor en kortvarig *opphever en barriere for å unngå driftsstans*. En kontrollromsoperatør kan f.eks. endre et settpunkt for å hindre automatisk nedstengning ved en kortvarig trykkoppbygning.

En viktig utfordring ved analytisk risikokontroll er å sørge for at en *ikke taper flere sikkerhets-funksjoner samtidig*. Dette kan inntreffe gjennom *fellesfeil*, f.eks. koordineringssvikt ved et inngrep under drift, hvor flere tekniske barrierer er satt ut av funksjon samtidig. Det kan også inntreffe dersom en eller flere sikkerhetsfunksjoner er utilgjengelige pga. *latente feil* (f.eks. at en utkobling ikke er opphevet etter et tidligere inngrep, eller at brannbeskyttende belegg ikke er tilstrekkelig vedlikeholdt) og det i tillegg inntreffer en aktiv feil. Alvorlige problemer i en organisasjon kan føre til en opphopning av latente feil, f.eks. dersom det ikke er ressurser til å teste og vedlikeholde barrierer tilfredsstillende eller dersom systemet for å rapportere og korrigere avvik ikke fungerer tilfredsstillende.

Analytisk risikokontroll forutsetter i følge Rasmussen at storulykkesrisikoen kan beskrives gjennom noen *få, velavgrensede hendelsesforløp*, jfr. ulykkeshendelsene som modelleres i en SEPA. Videre forutsettes at en kan oppnå akseptabel risiko ved å etablere barrierer og sikkerhetsfunksjoner som stanser hendelseskjeden *etter at en farekilde er utløst* (f.eks. etter en gasslekkasje). Dette fordi en mangler troverdige modeller for å forutsi og kontrollere alle mulige hendelsesforløp som kan utløse en farekilde.

En finner også klare eksempler på at offshore-næringen søker å redusere storulykkesrisikoen ved å lære av alvorlige enkeltulykker, f.eks. britiske og norske myndigheters oppfølging av Piper-Alpha-katastrofen. Den evolusjonære strategien for kontroll av storulykkesrisiko har likevel ikke vært like sentral innen oljevirksomheten i Nordsjøen som innen luftfart. Et tradisjonelt plattformkonsept gir muligheter for analytisk risikokontroll fordi det er teknisk mulig å føre prosessen automatisk over i en sikker tilstand (PAS / NAS) og å etablere passive fysiske barrierer mot forventede brann- og eksplosjonslaster. Tilsvarende muligheter er ikke til stede når et fly er i luften. Her er hovedoppgaven i en kritisk situasjon å fortsette å fly. Kontroll av storulykkesrisiko innen luftfart er derfor i sterkere grad fokusert på å *forebygge at kritiske situasjoner inntreffer* og at en *bevarer de viktigste operative funksjonene* i en kritiske situasjon. Dette avspeiles bl.a. i høye krav til opplæring og vedlikeholdstrening av piloter, omfattende bruk av prosedyrer og menneskelig redundans, f.eks. at pilotene på et fly overvåker hverandre og retter hverandres feilhandlinger.

Overgang til nye konsepter (f.eks. flytende produksjonsplattformer, produksjonsskip) kan føre til at en blir mer avhengig av aktive menneskelig inngrep for å håndtere kritiske situasjoner. I så fall vil forutsetningene for analytisk risikokontroll svekkes. En må i større grad begrense storulykkes-risikoen gjennom årsaksfjernende tiltak og ved å sikre operatørenes forutsetninger for å håndtere kritiske situasjoner som ikke ivaretas av tekniske sikkerhetsfunksjoner alene.

5.2 Definerte fare- og ulykkessituasjoner, barrierer og sikkerhetsfunksjoner

Styringsforskriften (§ 15) krever at risikoanalysene skal identifisere fare- og ulykkessituasjoner. De definerte fare- og ulykkessituasjonene (DFUene) vil være utgangspunkt for risikomodellering. Dette medfører at barrierene som inngår i risikoanalysen, blir relatert til DFUene.

I prosjektet Risikonivå på norsk sokkel (OD-RNNS, 2002) er det etablert et sett med risikoindikatorer for å kunne vurdere trender for utviklingen i storulykkesrisiko. I 2001 ble det samlet inn data fra selskapene om DFU'er gitt i tabellen nedenfor.

Tabell 3. DFUer for storulykker i prosjektet Risikonivå på norsk sokkel.

DFU	Beskrivelse
1	Ikke-antent hydrokarbonlekkasje
2	Antent hydrokarbonlekkasje
3	Brønnspark/tap av brønnkontroll
4	Brann/eksplosjon i andre områder, antennbar væske, ikke HC
5	Skip på kollisjonskurs (mot innretning)
6	Drivende gjenstand (på kurs mot innretning)
7	Kollisjon med feltrelatert fartøy/innretning/skytteltanker (mot innretning)
8	Skade på innretningskonstruksjon/stabilitets-/forankrings-/posisjoneringsfeil
9	Lekkasje fra undervanns produksjonsanlegg/rørledning/stigerør/ brønnstrøms-rørledning/lastebøye/lasteslange
10	Skade på undervanns produksjonsutstyr/rørledningssystemer/dykkerutstyr forårsaket av fiskeredskaper
11	Evakuering /føre var/nød evakuering)
12	Helikopterstyrt/nødlanding på/ved innretning

Av disse er DFU nr. 1-2, 3, 5 og 12 vurdert til å ha høyest risikobidrag. Følgende tekniske barrierer/barriereelementer er identifisert som de høyest prioriterte:

DFU 1-2

- Integritet av prosessanlegg
- Gassdeteksjon
- Tennkildekontroll
- Nødavstengning
- Prosesskontroll
- Trykkavlastning
- Branndeteksjon
- Mønstring og evakuering

DFU3

- Deteksjon av brønnspark
- BOP m/trykkontrollutstyr
- Ventiler for nedstengning av brønn
- Mønstring og evakuering

DFU5

- Deteksjon av skip på kollisjonskurs
- Tiltak for å varsle skip om behov for kursendring
- Mønstring og evakuering

DFU12

- Diskuteres med myndigheter og helikopteroperatører

I 2002 skal selskapene også rapportere overordnet vurdering av status og utvikling av barrierenes ytelse og pålitelighetsdata for barrierer.

Veiledningen til innretningsforskriften (§ 1) (OD, 2001b) lister eksempler på sikkerhetsfunksjoner, se tabellen nedenfor.[10] Det er stor grad av overlapping mellom denne listen og barrierene som ble identifisert i RNNS (2002).

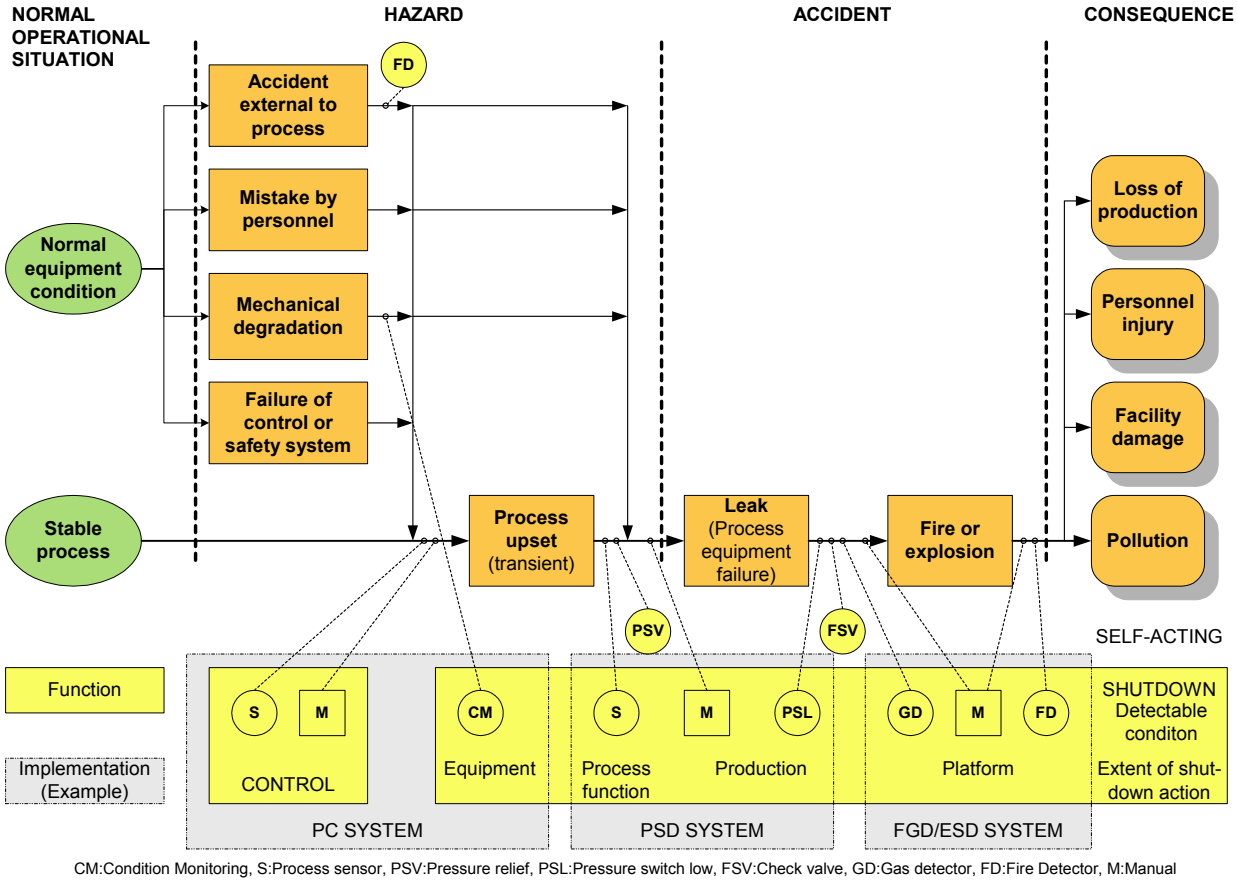
Tabell 4. Eksempler på sikkerhetsfunksjoner listet i Innretningsforskriften

a) seksjonering av prosessen	b) deteksjon av brann
c) deteksjon av gass	d) tennkildeutkopling
e) opprettholdelse av overtrykk i uklassifiserte rom	f) start og stopp av brannpumper, både manuelt og automatisk
g) aktiv brannbekjempelse	h) aktiv røykkontroll
i) prosessikring	j) brønnsikring
k) trykkavlastning	l) generell alarm og evakueringsalarm
m) produksjon og fordeling av nødkraft	n) nødbelysning
o) nødlensing	p) ballastering for flytende innretninger
q) opprettholdelse av riktig trykk, fuktighet, temperatur og gassammensetning i dykkeranlegg	

5.3 Prosesskontroll, prosessavstengning og nødavstengning – PDS prosjektet

I prosjektet *Pålitelighet av datamaskinbaserte sikkerhetssystemer (PDS)* ble det utviklet en modell for kvantifisering av påliteligheten til kontroll- og sikkerhetssystemene ved prosessanlegg på produksjonsplattformer[11]. Vi vil vise den kvalitative modellen her, fordi den illustrerer funksjonene til sikkerhetssystemene og hvordan de kan svikte.

[10] Med brønnsikring som nevnt i bokstav j, menes utblåsingssikring, strupe- og trykkontrollsystem, avledningssystem, brønnsikringsventiler og hurtig-frakoplings-system.
[11] Det skal nevnes at det i år er det gjort et arbeid for å gjøre regnemodellen i PDS 'kompatibel' med IEC 61508.



Figur 6. Funksjonene til kontroll- og sikkerhetssystem

På produksjonsinnretninger vil det være implementert to *hovedfunksjoner* (Bodsberg et al., 1994):

- Prosesskontroll: Opprettholde produksjon med minst mulig avvik fra spesifikasjonene.
- Prosess-sikkerhet: Forebygge og minimere skader ved tap av kontroll.

Disse funksjonene er implementert gjennom tre system:

1. Prosesskontrollsystemet (Process Control – PC)
2. Prosessnedstengningssystemet (Process Shut Down – PSD)
3. System for brann- og gassdeteksjon og nødavstengning (Fire & Gas Detection – FGD; Emergency Shutdown – ESD)

Virkemåten til disse tre systemene er vanligvis definert gjennom årsak-virknings-matriser, som angir hvilke aksjoner som utløses ved ulike tilstander. Sikringssystemene kan utløse ulike tiltak, avhengig av hvilke forstyrrelser som er detektert. Mindre forstyrrelser (f eks unormalt høyt trykk) vil i første omgang bli korrigert av prosesskontrollsystemet. Dersom dette ikke lykkes, vil prosessnedstengningssystemet bli aktivert. Dersom kontrolltapet fører til en hydrokarbonlekkasje, utløses en nødavstengning.

De instrumenterte systemene ovenfor omfatter prinsipielt tre hoveddeler

- en *deteksjonsdel*, i form av automatiske sensorer, trykkmålere, gassdetektorer etc., eller manuell inngang fra en uteoperatør som trykker på brannalarmknappen;

- en *beslutningsdel*, i form av for eksempel en sentral logikkenhet (CPU), et relé, eller en operatør som manuelt trykker på nødavstengningsknappen; og
- en *aksjons-/handlingsdel*, i form av for eksempel en automatisk ventil som isolerer prosessen, en bryter som stopper en kompressor, eller et menneske som manuelt stenger en ventil

I tillegg kommer informasjonsgivere slik som storskjermer og arbeidsstasjoner i kontrollrommet, som ikke minst er viktige i forhold til muligheten for manuell inngripen.

Som en ser inngår mennesker på flere måter i funksjonen til sikringssystemene. Ytelsene til sikringssystemene overvåkes gjennom vedlikehold og testing, men feil i forbindelse med vedlikehold kan også føre til svikt i prosess-sikkerhetsfunksjonen. En operatør kan utløse en nedstengning manuelt. En operatør kan også gjøre inngrep som hindrer eller utsetter en nedstengning, eksempelvis ved å endre et setpunkt. Her er det tett samspill mellom egenskaper ved prosessen og operatørens forutsetninger for å finne en god balanse mellom sikkerhet og produksjon. En uhensiktsmessig innstilt reguleringssløyfe kan eksempelvis føre til at operatøren får unødvendig kort tid til å håndtere forstyrrelser før automatisk prosessavstengning blir aktivert.

5.4 Barrierer i arbeidsprosesser

I OD's regelverk (Aktivitetsforskriften av 3. september 2001) stilles det krav til planlegging og utførelse av arbeid (kapittel VII). De forskjellige selskapene ivaretar disse kravene ved å ha administrative system for arbeidstillatelser og for overlevering av informasjon mellom f. eks. skift (handover). Disse systemene fungerer som *ikke-fysiske* barrierer i den forstand at de skal hindre at parallelt pågående aktiviteter eller manglende kunnskap om det tekniske systemets tilstand skal bidra til dårligere sikkerhet. De er *aktive*, ikke-fysiske barrierer i den forstand at de må brukes riktig kvalitativt sett for å fungere som barrierer. Like fullt er de kritiske barrierer fordi de ofte kan tilsidesette passive, fysiske barrierer dersom de ikke benyttes tilfredsstillende. De kan dermed virke som det svakeste leddet i kjeden av sikkerhetsbarrierer. Tydelige bevis på dette finner vi i flere ulykker og uønskede hendelser, f.eks. Piper Alpha, der hendelsene var direkte relatert til mangelfull handover mellom skift (se innledningskapitelet). I forbindelse med dødsulykken på Byford Dolphin 17.04.02, hvor en person ble truffet av en rørstubb i boreområdet, ble det i OD sin rapport etter ulykken blant annet pekt på følgende årsaksfaktorer:

- mangelfull planlegging og arbeidsforberedelser
- mangelfull bruk av sikkerhetsmessige analyser
- mangelfull kjennskap til og brudd på gjeldende prosedyrer
- mangelfull kommunikasjon og praksis for utføring av samtidige operasjoner og arbeid på ulike nivå
- mangelfull tildekning av åpninger i dekk mellom arbeidsområder.

5.5 Organisatorisk redundans på en oljeplattform

I et arbeidstillatelsessystem er det definert hvilke personer som skal vurdere, gjennomføre og verifisere sikkerhetstiltak i forbindelse med en arbeidsoperasjon. Her legges det som regel opp til en betydelig grad av dobbeltsjekking av at riktige sikkerhetstiltak er foreskrevet, at disse blir gjennomført korrekt, og at jobben blir avsluttet på en forsvarlig måte. Et velfungerende

arbeidstillatelsessystem kan derfor være et effektivt formelt virkemiddel for å bygge opp organisatorisk redundans (jfr avsnitt 2.3, side 23) i forbindelse med kritiske arbeidsoperasjoner.

I en studie av en norsk produksjonsplattform ble det undersøkt om det er grunn til å tro at organisatorisk redundans bidrar til å redusere risikoen og øke driftspåliteligheten (Rosness m.fl. 2000). De fant mange holdepunkter for at det forekom organisatorisk redundans på plattformen vi besøkte. Her er noen eksempler:

- Mekanikere sa at de ofte stilte kritiske spørsmål til uteoperatøren som klargjorde for et inngrep i prosessanlegget, spesielt dersom uteoperatøren hadde lite erfaring. Dette var for å sikre seg mot misforståelser og forglemmelser.
- Driftssjefen på skiftet som ble intervjuet, ba ofte om en Sikker Jobb-Analyse (SJA)[12]. Under SJA-møtene tok han ofte rollen som djevelens advokat, og forsøkte å få frem alt som kunne gå galt. På den måten bidro han til å etterprøve antakelser eller beslutninger, og skapte en mulighet for å korrigere feilvurderinger.
- Det var to kontrollromsoperatører på plattformen. Disse brukte hverandre bl.a. til å vurdere trender[13], og spørre hverandre om forhold i prosessen. Driftssjefen deltok ikke i det kontinuerlige arbeidet i kontrollrommet, men satt med utsyn til kontrollrommet. Han ble ofte kalt inn til kontrollrommet for rådspørring. På den måten utnyttet operatørene driftssjefens kompetanse for å skape organisatorisk redundans.
- En erfaren mekaniker på plattformen fulgte med på alt som foregikk, og blandet seg inn hver gang han observerte noe som kunne true sikkerheten. Ved én anledning grep han inn idet to jobber kom i konflikt med hverandre. Han fikk da stanset et ukontrollert gassutslipp i siste øyeblikk, før den førte til eksplosjonsfare og automatisk nedstengning av produksjonen.

Eksemplene tyder på at organisatorisk redundans ikke bare skapes gjennom formelle systemer, men også gjennom uformelle rutiner som utvikler seg på arbeidsplassen. Den daglige driften ute på plattformen var preget av tette bånd, åpen kommunikasjon og rask tilgang til rådføring med ledelsen. Dette ble oppfattet som viktige forutsetninger for organisatorisk redundans.

[12] En SJA er en enkel, men systematisk gjennomgang av farlige forhold i en arbeidsoppgave. En SJA utføres like før jobben starter, av personene som er involvert i oppgaven.
[13] Med "trender" mener vi gradvise endringer i en eller flere parametre i prosessanlegget – f eks en økning i trykket i en separator. Slike trender kan være signaler om at en unormal situasjon er under utvikling. En operatør som er dyktig til å tolke trender, kan ligge i forkant av utviklingen i prosessen og forebygge driftsforstyrrelser.

6 Barrieretenkning – en kritisk diskusjon

I dette kapitlet vil vi diskutere menneskets rolle som bidragsyter i forhold til tekniske og fysiske barrierer. Diskusjonen vil trekke på erfaringer fra kjernekraftindustrien. Vi vil ta opp spørsmål om uavhengighet mellom barrierer, og pålitelighet til barrierer. Dessuten vil vi sette fokus på to typer redundans: teknisk og organisatorisk redundans.

6.1 Mennesket som del av en organisasjons sikkerhetsbarrierer

Innen industrien blir begrepet barriere tradisjonelt anvendt med eksplisitt henvisning til tekniske barrierer. Man kan imidlertid argumentere for at medarbeiderne i praksis ofte fungerer som barrierer, og derfor på avgjørende måte bidrar til å opprettholde sikkerheten. Dette gjelder innen petroleumsvirksomheten så vel som innen andre industrier. Kjernekraftinspektoratet i USA[14] understreker den kritiske rollen til medarbeiderne ved å presisere at "Human factors plays a significant role in supporting plant safety and providing defense in depth. (NUREG-0711, 2002, 1).[15] Det forhold at medarbeiderne - og dermed de administrative rammene[16] som de opererer under - har avgjørende betydning for opprettholdelse av sikkerheten innen petroleumsvirksomheten, avspeiler seg f.eks. i arbeidsoppgavene rettet mot vedlikehold og operasjon av de tekniske/fysiske sikkerhetsbarrierene.

Medarbeiderne utfører vedlikehold/testing for å opprettholde de tekniske/fysiske barrierenes funksjon. Aktivitetene her er i varierende grad prosedyrestyrt med mer fokus på noen systemer enn på andre. Det er f.eks. generelt meget høy fokus på nødavstengningssystem (NAS), prosessavstengningssystem (PAS) brann- og gassdeteksjonssystem (B&G), brannvann og nødkraft. I relasjon til disse oppgavene er det store variasjoner i den konkrete utførelse mellom innretningene, som det fremgår ved ODs inspeksjoner (Eskedal, Ellingsen & Seim, 2002). Dette kan ha sammenheng med forskjellige organisatoriske karakteristika så som kvaliteten på prosedyrene som anvendes,[17] intensiteten på oppfølging av om arbeidet utføres i henhold til prosedyrene (om ikke innsatsen følges tett opp sklir ting ut), krav til kompetansen hos medarbeiderne, herunder til medarbeidernes forståelse av konsekvensene som vil følge om arbeidet ikke utføres riktig.[18]

I forhold til daglig drift er operatørenes intervensjon med de tekniske sikkerhetssystemene i vesentlig grad knyttet til inn/utkobling av enkeltfunksjoner Det er observert store forskjeller i kvaliteten på de retningslinjene/prosedyrene som legges til grunn for disse aktivitetene på de forskjellige installasjonene (Eskedal, Ellingsen & Seim, 2002; Seim, 2002), og det er tilsvarende

[14] US Nuclear Regulatory Commission.
[15] Mennesket rolle for opprettholdelse av sikkerheten avspeiler seg også innen nyere barriereklassifikasjonssystemer som inkludere mennesket som mulig barriere. Svenson (1991, 501) opererer således med 'human factors-organizational systems' som en spesifikk type barrierefunksjon, mens Hollnagel (1999) understreker at mennesket er i stand til å ivareta samtlige av fire barrieretypene han har definert: fysiske, funksjonelle, symbolske og immaterielle.
[16] F.eks. rutiner for prosedyreutforming, prosedyrebruk, oppfølgning, design og implementering av verktøy, opplæring, etc.
[17] Eksempel på kvalitet av prosedyrene: Medarbeiderne skal teste brannvannsystemets kapasitet f. eks hver uke. Oppgaven utføres ved å starte pumpene, og pumpe vannet til sjøs via en dumpeventil. En sjekker om kapasiteten er OK, men oppgaveløsningsprosessen inneholder ingen krav til regulær inspeksjon av ledningsnettet forøvrig. På en OD inspeksjon viste det seg at deler av ledningsnettet var helt tett (Seim, 2002).
[18] Dette problemet kan synes å bli større alt ettersom bruken av out-sourcing økes.

stor variasjon i praksis for hvordan dette registreres og følges opp. På noen installasjoner føres en egen loggbok som daglig gjennomgås av driftsledelsen. På andre installasjoner gjøres ingen registreringer overhodet. Prosedyrene sier generelt at en funksjon ikke skal utkobles før kompenserende tiltak er iverksatt. Men kvaliteten på de kompenserende tiltak som i praksis kreves kan variere (Eskedal, Husebø, Heber & Seim, 2001). Hvis f.eks. en kontrollromsoperator kobler ut en sensor for høyt væskenivå, kan det kompenserende tiltaket være at operatøren skal følge ekstra nøye med på nivået uten at det angis hvordan operatøren skal takle situasjonen i fall han eller hun blir avbrutt av en alarm, en telefon, et oppkall på radio, etc. (Seim, 2002).

For å sikre at vedlikeholds- og modifikasjonsarbeider blir gjennomført på en sikkerhetsmessig forsvarlig måte er det utarbeidet et arbeidstillatelsessystem.[19] Dette innebærer at en arbeidstillatelse (”Permit To Work”) må fylles ut og godkjennes før sikkerhetskritisk arbeide påbegynnes. I arbeidstillatelsen skal det bl.a. spesifiseres hvilke sikkerhetsfunksjoner som må utkobles og hvilke kompenserende tiltak som skal settes inn. Det er typisk overlatt til den enkelte arbeidsleder å vurdere hvilke kompenserende tiltak som er nødvendige. En arbeidstillatelse vil også gi anvisning om hvilke prosedyrer som gjelder for arbeidet. Sikker-Jobb-Analyse (SJA) er en slik prosedyre som skal følges dersom man finner det nødvendig. Det heter generelt at dersom bare én person mener det er nødvendig, så skal en ikke påbegynne arbeidet før en SJA er utført. Da det imidlertid ikke rutinemessig utføres SJA kan behovene undertrykkes i forhold til arbeidspress. En slik situasjon kan f.eks. ha være medvirkende årsak til en hendelse som resulterte i at en sveiser brann hull i et luftsignalrør slik at deluge ventilen ble utløst og man fikk en utilsiktet nødavstengning (Seim, 2002). Her spurte sveiseren sin arbeidsleder om de burde forta en SJA, men arbeidsleder mente ikke at det var nødvendig, og fant forøvrig at det heller ikke var tid da arbeidet måtte være ferdig i løpet av dagen (ibid).

En sentral funksjon på en plattform innehas av kranoperatøren. Løfteoperasjoner blir betraktet som en av de mest kritiske operasjonene på en installasjon, da hvert løft representerer en potensiell risiko både med hensyn til skade på personell og utstyr. Dette ble f.eks. tydelig ved den meget omtalte dødsulykken som inntraff på Oseberg Øst julaften 2000, samt ulykken som nylig inntraff på Gyda feltet. Også her har mennesket en sentral rolle som sikkerhetsbarriere. Kranoperatør må kommunisere med flaggmann visuelt og via radio der han ikke kan se hivet. Hjelpemidlene som medarbeiderne har til rådighet kan også være av redusert verdi, som f.eks. et krankart som ikke viser på hvilke områder av plattformen det er høyde- og vekt-begrensninger (Seim, 2002).

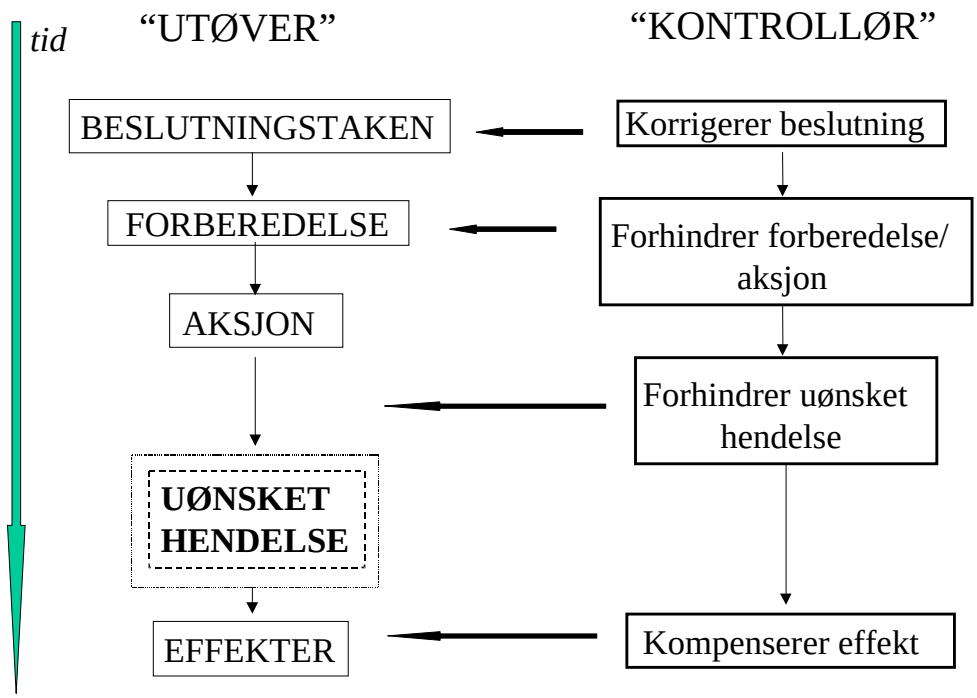
6.2 Menneskets rolle som ”kontrollør/barriere”

En barriere kan betraktes som en 'kontrollør' som etterprøver kvaliteten til en 'utøvers' aktivitet med referanse til et gitt mål for sikkerhet, og som om nødvendig setter inn med korrigerende eller kompenserende tiltak. "Kontrolløren" kan operere i minst fire modi: 1) korrigere 'utøvers' beslutning om å gjennomføre en aktivitet, 2) forhindre 'utøvers' forberedelse av en aktivitet, 3) forhindre ’utøver’ i å gjennomføre en aktivitet, og 4) kompensere de negative effektene som følger av ’utøvers’ aktivitet. Samspillet mellom 'utøver' og 'kontrollør' er illustrert i Figur 7..

En medarbeider kan inngå i rollen som 'kontrollør'/barriere på tre måter (Skjerve *et al.*, 2003): 1. Medarbeideren kan ivareta rollene som 'utøver' og 'kontrollør' samtidig. Dette er f.eks. tilfellet når en kontrollromsoperatør kobler ut en kritisk sensor for væskenivå og samtidig kompenserer for den økte risikoen ved å følge væskenivået ekstra nøye (jfr. forrige avsnitt). 2. Medarbeideren kan etterprøve aktiviteten til det tekniske system, dvs. ivareta rollen som 'kontrollør' mens det tekniske system har rollen som 'utøver.' 3. Medarbeideren kan etterprøve aktiviteten til sine kolleger, dvs. ivareta rollen som 'kontrollør' mens et eller flere andre mennesker har rollen som 'utøver.' Det er

[19] Arbeidstillatelsessysetmet gjelder imidlertid ikke for alle aspekter av arbeid, kun de som har blitt definert i ordren.

sistnevnte type aktivitet det refereres til med begrepet *organisatorisk redundans*, og som vi primært vil sette fokus på i dette prosjektet.



Figur 7. Modell av samspillet mellom en 'utøver og en 'kontrollør'/barriere.

6.3 Sentrale problemstillinger

Det forhold at medarbeidere tradisjonelt ikke har blitt definert som en del av organisasjonenes sikkerhetsbarrierer, er trolig en viktig årsak til at vi har mangelfull kunnskap om hvordan medarbeidere mest hensiktsmessig kan anvendes som del av en organisasjons barrierer. I det følgende vil vi særlig sette fokus på to problemstillinger: 1) Når fungerer medarbeideren selvstendig som uavhengig barriere - og når fungerer han som del av en uavhengig barriere? 2) Hvordan skal arbeidsforholdene legges til rette for å sikre at medarbeideren kan ivareta de spesifikke barrierefunksjonene som er allokert til ham eller henne på en pålitelig måte?

6.3.1 Avhengighet

I utgangspunktet er det uklart når en medarbeider skal betraktes som en uavhengig barriere. Er det rimelig å betrakte en medarbeider som uavhengig av det tekniske sikkerhetssystem (DTS) - et system som det typisk vil være mulig for medarbeideren å 'koble ut' eller å 'overkjøre'? Og omvendt, når er det rimelig å betrakte DTS som en uavhengig barriere i forhold til medarbeideren? Tilsvarende er det uklart når en medarbeider skal betraktes som uavhengig

barriere i forhold til sine kolleger. *En praktisk konsekvens av ovenstående er at det kan være vanskelig å eksplisitt bestemme hvilken redundans/diversitet som faktisk finnes i en organisasjons sikkerhetssystemer.* Hvor mange barrierer finnes f.eks. i en situasjon hvor to medarbeidere og DTS skal beskytte mot en gitt fare?

– 1 barriere: (medarbeider 1 + medarbeider 2 + DTS)?
– 2 barrierer: (medarbeider 1 + medarbeider 2) + (DTS)?
– 3 barrierer: (medarbeider 1) + (medarbeider 2) + (DTS)?

Begrepet uavhengighet har tradisjonelt blitt definert med tanke på tekniske/fysiske systemer. En klassisk definisjon av begrepet lyder f.eks.: "Et system er uavhengig av andre systemer hvis systemet utfører tiltenkt funksjon uansett hva som skjer med andre systemer." (Onshus, Hansen, Hauge, Holmstrøm, Lone, Nybø & Aarø, 1998, 14). Basalt sikter ovenstående definisjon mot å bestemme når et teknisk sikkerhetssystem kan betraktes som uavhengig av andre tekniske sikkerhetssystemer.

6.3.2 Avhengighet mellom medarbeidere

Dette fører oss videre til behovet for å bestemme *når* en medarbeider i en aktuell situasjon kan sies å (kunne) *fungere* uavhengig av andre medarbeidere. For å kunne fungere uavhengig må medarbeideren være i stand til å utføre sin rolle som sikkerhetsbarriere uansett hva som skjer med hans eller hennes kolleger. En mulig definisjon på når en medarbeider fungerer uavhengig av sine kolleger kunne tentativt formuleres som følger (Skjerve *et al.*, 2003):

> En medarbeider er uavhengig av andre medarbeidere hvis han eller hun selvstendig:
>
> a) observerer sikkerhetskritiske parametere
> b) vurderer sikkerhetskritiske parametere
> c) planlegger tiltak
> d) gjennomfører tiltak.

Ovenstående forsøk på å definere begrepet uavhengighet med referanse til medarbeiderne innen en industriell kontekst viser seg imidlertid ganske hurtig å være noe forenklet (ibid.).

Et menneske utvikler et sett av forventninger til den situasjonen han eller hun aktuelt befinner seg i, f.eks. en gitt operasjonell situasjon, med utgangspunkt i sine erfaringer. Disse forventningene impliserer et sett av antagelser om hvordan situasjonen vil utvikle seg over tid (se f.eks., Schank, 1982; Schank & Abelson, 1977). Personens forventninger influerer hvilke deler av omgivelsene han eller hun velger å fokusere på. Generelt har mennesket en tendens til å søke bekreftelse på egne antagelser fremfor å søke å avkrefte disse (se f.eks. Wason & Shapiro, 1971). Denne tendensen vil ytterligere forsterke personens tilbøyelighet til å fokusere på visse aspekter i situasjonen og overse andre. Dette innebærer en risiko for at personen ikke vil observere forhold som potensielt kunne korrigere hans eller hennes aktuelle forståelse av situasjonen. Ovenstående tendenser har gjort seg gjeldende i en rekke større ulykker. I forbindelse med ulykkene på kjernekraftverkene Three Mile Island, enhet 2, den 28.03.1979 (Perrow, 1984) og Tsjernobyl, enhet 4, den 26.04.1986 (Reason, 1987), jobbet operatørene i lengre perioder ut fra ett misforstått bilde av tilstanden i prosessanlegget. Operatørene var pålagt i gitte situasjoner å implementere en rekke barrierer, men ettersom de ikke oppfattet faresituasjonene korrekt, ble barrierene ikke implementert etter intensjonen.

Erfaringer fra større ulykker indikerer at en medarbeider kanskje kun bør oppfattes som én (1) sikkerhetsbarriere, uansett om han eller hun selvstendig gjennomfører operasjonene a) - d) (se ovenfor) flere ganger i løpet av samme hendelsesforløp. Årsaken er at hvis medarbeiderens forventninger til situasjonen på avgjørende måte er feil, da vil det være en risiko for at han eller hun igjen og igjen kommer frem til samme feilaktige konklusjon, og dermed kan bidra til å redusere snarere enn til å øke sikkerheten. Ovennevnte hendelser setter tilsvarende spørsmålstegn ved hvorvidt en veletablert arbeidsgruppe - f.eks. en gruppe av kontrollromsoperatører - generelt kan betraktes som mer enn en (1) barriere? På begge kjernekraftverkene bygde operatørene opp en mer eller mindre kollektiv forståelse av situasjonen - en forståelse som tilsynelatende først ble korrigert da henholdsvis et nytt skiftelag møtte frem (Three Mile Island), og eksplosjonen inntraff (Tsjernobyl).

Innebærer dette at en ekstra person ikke under noen omstendigheter kan tilføre systemet reell redundans? Dette spørsmålet vil vi komme tilbake til i avsnitt 6.4.3.

6.3.3 Avhengigheter mellom medarbeidere og tekniske sikkerhetssystem

Til nå har begrepet 'uavhengighet' blitt diskutert eksklusivt med referanse til spørsmålet om uavhengighet *mellom medarbeiderne*. Samspillet *mellom medarbeiderne og de tekniske sikkerhetssystemene* er imidlertid også svært kritisk. Flere ulykker har demonstrert at medarbeideren og det tekniske systemet - herunder det tekniske sikkerhetssystemet - *ikke* alltid fungerer uavhengig av hverandre;

Da ulykken ved Tsjernobyl verket inntraff, hadde operatørene koblet ut nødavkjølingssystemet på ordre fra verkets ledelse. Årsaken var at det skulle utføres en rekke tester som forutsatte at nødavkjølingssystemet ikke var aktivt (Reason, 1987). Nødavkjølingssystemet skal sikre at det automatisk bringes kjølevann til reaktoren når det trenges, og utgjør en særdeles viktig sikkerhetsbarriere. Å koble ut nødavkjølingssystemet svekker på en helt åpenbar måte de tekniske sikkerhetsbarrierer. Det er imidlertid grunn til å anta at handlingen også svekker medarbeiderens evne til å fungere som sikkerhetsbarriere. Når nødavkjølingssystemet kobles ut, forandres arbeidskonteksten til operatøren umiddelbart. Operatøren må fra dette tidspunktet utføre sine oppgaver i forhold til en annen operasjonell kontekst (den kontekst som resulterer av at nødavkjølingssystemet er utkoblet) enn den operatøren normalt opererer med referanse til. Dette innebærer at konsekvensene av operatørens inngrep - herunder konsekvensene av rene rutine-inngrep - *potensielt* kan bli annerledes enn de ville ha vært i den normale situasjon. Slikt kan – særlig i kombinasjon med andre inngrep som ytterligere endrer den operasjonelle tilstand - gjøre det vanskeligere for operatøren å forstå hendelsene i prosessen korrekt, og dermed vanskeligere å oppfylle sin funksjon som sikkerhetsbarriere.

I forbindelse med dødsulykken som inntraff på *Byford Dolphin* den 17. april 2002 bad boreren via sin radio medarbeiderne som gikk på dekket under om fjerne seg innen han påbegynte en løfteoperasjon. Boreren mottok ingen tilbakemelding fra disse medarbeidere. Han antok imidlertid at medarbeiderne hadde etterlevd anmodningen. Dels kunne han ikke lenger se medarbeiderne, og dels var det ikke uvanlig at det ikke ble gitt bekreftende tilbakemeldinger på radiobeskjeder (Andreassen *et al*., 18). Problemet var imidlertid at medarbeiderne ikke hadde hørt meldingen, fordi de lyttet på en annen radiokanal. Denne hendelse viser hvordan ledelsens aksept av en praksis som innebar at medarbeiderne ikke nødvendigvis måtte gi tilbakemelding på radiobeskjeder, på avgjørende måte bidro til å svekke borerens mulighet til å fungere som sikkerhetsbarriere.

Kontrollromsdesign har likeledes innflytelse på medarbeidernes evne til å fungere effektivt som sikkerhetsbarriere. På Three Mile Island viste indikatorer på kontrollromsoperatørenes panel at fødevannspumpene var aktivert. Operatørene noterte seg dette, og var derfor trygge på at fødevann fra sekundærsystemet kjølte ned reaktoren. Imidlertid var ventilene som sitter mellom

fødevannstankene og fødevannspumpene, lukket. Selv om pumpene kjørte som de skulle, kom det likevel ikke kjølevann til reaktoren (Perrow, 1984). Om representasjonen på operatørenes panel hadde vist status på disse ventilene så hadde operatørene antagelig hurtigere oppnådd en korrekt forståelse av situasjonen, og derved mer effektivt kunnet agere i funksjonen som sikkerhetsbarriere.

Ovenstående eksempler understreker behovet for å utvikle metoder som kan understøtte realistiske vurderinger av hvilken redundans/diversitet som finnes i en organisasjons sikkerhetssystemer. Bestemmelsen av eksisterende redundans vil øke muligheten for å etablere effektive metoder for risikohåndtering, og dermed bidra til å øke produksjonssystemets toleranse for feil.

6.3.4 Pålitelighet

OD fastsetter i Styringsforskriftens §1 at den 'ansvarlige' skal ha oversikt over hvilke barrierer som er *svekket* (se side 33). Vurderingen av om en barriere er svekket, forutsetter kunnskap om hva som karakteriserer barrieren i normal (usvekket) tilstand. Kravet om evaluering av barrierens tilstand innebærer slikt på generelt nivå en vurdering av hvor pålitelig barrieren er, dvs. i hvilken grad barrieren er i stand til å motstå feil (Neogy, Hanson, Davis & Fenstermacher, 1996).

Ved en vurdering av påliteligheten til mennesket som barriere vil det være helt sentral å fastsette i hvilken grad medarbeideren har fått den påkrevde opplæring, og dermed kompetansen, som setter ham eller henne i stand til å utføre den gitte oppgaven. Det at medarbeideren besitter den nødvendige kompetansen er imidlertid ingen garanti for at han eller hun i praksis alltid utfører oppgaven korrekt. Denne distinksjonen er sentral fordi den impliserer at to eller flere redundante barrierer ikke nødvendigvis vil være mer pålitelige enn én (Dahll, Skjerve & Sivertsen, 2001). To uavhengige medarbeidere som besitter den grunnleggende kompetansen men mangler praktisk erfaring, kan - sett over ett - ha større risiko for å feile, enn en medarbeider som besitter den grunnleggende kompetanse i tillegg til betydelig praktisk erfaring.

Menneskers atferd er dessuten sterkt influert av *kontekstuelle faktorer*. Eksemplene i forrige avsnitt satte således fokus på hvordan design av utstyr og tilretteleggelse av arbeidsrutiner sterkt kan bidra til å svekke påliteligheten til mennesket som en barriere.

Det forhold at medarbeidere ikke eksplisitt blir definert som en del av organisasjonenes sikkerhetsbarrierer er formodentlig den vesentligste årsak til at kravene som stilles til medarbeiderne i forhold til å beskytte mot spesifikke faresituasjoner er *mindre konkrete* enn de som stilles til de tekniske systemene. Dette avspeiles f.eks. i dokumentasjonen av krav til utstyr (se avsnitt 4.1). Et annet forhold er at vår kunnskap om hvordan produksjonssystemer skal konstrueres, grensesnittet designes, og arbeidsoppgavene legges til rette med henblikk på å legge til rette for menneskelig pålitelighet, stadig er mangelfull. Ovennevnte er kritisk sett i forhold til muligheten for å etablere et høyt sikkerhetsnivå som i hovedsak forutsetter høy kvalitet på design, konstruksjon og operasjon av produksjonssystemet:

> "The primary way of preventing accidents is to achieve a high quality in design, construction and operation of the plant, and thereby to ensure that deviations from normal operation are infrequent." (INSAG-10, 1986, 6)

Diskusjonen i dette avsnittet indikerer at det eksisterer et behov for å utvikle metoder som kan understøtte den 'ansvarlige' i å vurdere i hvilken grad eksisterende menneskelige barrierer er pålitelige/svekkede. Slike metoder kan antas å effektivt understøtte muligheten for å gjennomføre

korrekte risikovurderinger, og dermed for å sikre at passende tiltak (barrierer m.v.) blir etablert ved behov.

6.4 Teknisk og organisatorisk redundans

I kapittel 2 introduserte vi to fremtredende perspektiver på spørsmålet om sikkerhet. Begge perspektivene baserer seg på studiet av høyteknologiske produksjonssystemer med et stort risikopotensiale men der uhell og ulykker sjelden forekommer. Det ene kalles 'High-Reliability Organisations' (HRO) perspektivet,[20] det annet 'Normal Accident' (NAC) perspektivet (se avsnitt 2.1.1). Innen såvel HRO som NAC-perspektivet er begrepet redundans sentralt. Betrakter man de to perspektivene eksplisitt med referanse til spørsmålet om redundans, er det imidlertid klart at de fokuserer på forskjellige typer redundans.

HRO-perspektivet setter primært fokus på de sosiale og ledelsesmessige aspektene som knytter seg til en arbeidsprosess. LaPorte og Consolini (1991) skriver f.eks.

> "...little is known systematically about the social or management aspects of such activities or the consequences for the operating organizations of attempting to attain nearly failure-free performance." (ibid., 20),

- og erklærer at de ønsker å studere dette forholdet. Redundanstypen som adresseres innen HRO-relaterte studier vedrører følgelig også de sosiale og ledelsesmessige aspektene som er assosiert med oppgaveløsningen – altså *organisatorisk redundans.* Innen NAC-perspektivet settes det derimot primært fokus på de tekniske aspektene ved produksjonssystemene. Redundanstypen som adresseres er således primært *teknisk redundans,* dvs. teknisk/fysisk redundans som er bygd inn i produksjonssystemene. NAC-relaterte studier søker å avklare hvilke konsekvenser tilføyelsen av teknisk redundans har for medarbeideres mulighet til å operere produksjonssystemene på en sikkerhetsmessig forsvarlig måte - særlig i situasjoner der avvikende operasjonelle tilstander forekommer (Perrow, 1984).

6.4.1 Kritikk av teknisk redundans

Prinsippet om forsvar-i-dybden, som baserer seg på teknisk redundans, har over årene blitt utsatt for vesentlig kritikk, særlig fra forskere som er preget av NAC perspektivet. Kritikken rommer tre sentrale punkter: [21]

1) *Redundante komponenter er ofte mindre uavhengige enn designeren tror*

Tilføyelsen av redundans gjør at antall mulige interaksjoner mellom systemkomponentene økes, og dermed at kompleksiteten i produksjonssystemet økes. Den økte kompleksiteten gjør det vanskeligere for designeren å forestille seg - og dermed å ta høyde for – alle mulige interaksjoner som kan forekomme i produksjonssystemet. Dette innebærer en økt risiko for forekomsten av feil-med-felles-årsak (common cause failures) (Perrow, 1984, 73), dvs. situasjoner der en feil - f.eks. strømsvikt - utilsiktet leder til at en rekke komponenter vil feile samtidig.

[20] I det følgende vil begrepet HRO, som tradisjonelt, bli anvendt med referanse til en enkelt organisasjon. Problemstillinger relatert til samspill mellom HRO'en og andre organisasjoner, dvs. "high reliability systems of organizations" (Roberts, 1998) vil ikke bli inndraget i diskusjonene.
[21] Nedenstående gjennomgang tar utgangspunkt i sammenfatningen hos Sagan (1993).

2) *Tilføyelse av redundans gjør et system mer "ugjennomskinnelig"*

Tilføyelsen av redundans medfører at et i utgangspunktet komplekst produksjonssystem blir enda mer "ugjennomskinnelig". Økt redundans impliserer at enkelte feil og svikt ofte ikke umiddelbart får synlige konsekvenser. Dette skyldes den kompenserende aktiviteten til redundansen. Ofte vil det være nødvendig at flere uavhengige hendelser inntreffer samtidig før et produksjonssystem responderer med en synlig forandring (Rasmussen, 1988, i Reason, 1992, 179-80). Den manglende synlighet på konsekvensene av enkelte feil og svikt kan gjøre det vanskelig for medarbeiderne å bedømme tilstanden i prosessystemet korrekt. Det forhold at feil kan forekomme uten å bli observert av medarbeiderne, gjør at feiltilstander over tid kan hope seg opp i produksjonssystemet som 'latente' feil. Tilstedeværelsen av latente feil bidrar til å redusere sikkerhetsmarginene. Hvis f.eks. et tog har et dobbelt sett bremser og det ene svikter uten at det oppdages vil ikke enkeltfeilprinsippet tilfredsstilles lenger, i og med at svikt i de fungerende bremser ikke lengre vil bli kompensert. En ytterligere effekt av at konsekvensene av feil og svikt ofte ikke er umiddelbart synlige, er at det blir vanskelig for medarbeideren å lære seg hvordan systemet fungerer (Reason, 1992, 179). Opphopningen av latente feil kan f.eks. føre til at en handling som operatøren kanskje har utført mange ganger uten å være klar over at den var feilaktig, plutselig kan resultere i en faresituasjon. Sett fra medarbeiderens synsvinkel vil denne konsekvensen fremstå som fullstendig uforståelig.

3) *Redundans kan gi operatøren en falsk følelse av trygghet*

"Ugjennomskinneligheten" som følger ved introduksjon av redundans, gjør at produksjonssystemet kan fremstå som svært 'sikkert' for medarbeiderne, slikt at en falsk følelse av trygghet kan utvikle seg. NAC perspektivet påpeker at systemene kan fremstå som så sikre at operatørene rett og slett glemmer å være redde. Som konsekvens av den opplevde sikkerheten kan medarbeiderne – og deres ledere – i visse tilfeller søke å dra fordel av dette ved å ytterligere øke produksjonen. Dette innebærer at sikkerhetsmarginene blir redusert, og risikoen for kan derfor øke.

6.4.2 Reduksjon av negative effekter ved teknisk redundans

Det synes generelt å være enighet om at forsvar-i-dybden - forutsatt at de redundante komponentene reelt er uavhengige - er en effektiv strategi med henblikk på å forebygge at uhell og ulykker vil oppstå som følge av enkeltfeil. Reason uttrykker dette synspunktet slik:

> "It is this multiplicity of overlapping and mutually supporting defences that makes complex technological systems, such as nuclear power plants and modern commercial aircraft, largely proof against single failures, either human or technical." (Reason, 1997, 7)

NAC perspektivet antar at sikkerheten som er forbundet med en produksjonsprosess, kan økes hvis *tidsperioden* som de latente feilene befinner seg i et produksjonssystem reduseres (Rasmussen, referert av Reason, 1992:180). Mulige metoder for dette kunne være å re-designe menneske-maskin grensesnittet slik at konsekvensene av feil blir åpenbare,[22] og/eller å bedre rutinene for kontinuerlig vedlikehold og testning.

[22] På amerikanske atomubåter ble det i mange år anvendt en design strategi som prioriterte enkelthet - herunder at konsekvensene av operatørens handlinger skulle være åpenbare. Strategien innebar bl.a. at automatisering ble unngått med mindre den var absolutt nødvendig (Bierly III & Spender, 1995, 653).

6.4.3 Forsvar for organisatorisk redundans

Organisatorisk redundans, som tidligere ble definert som *samhandlingsmønstre som setter en organisasjon i stand til å utføre oppgaver mer pålitelig enn enkeltpersoner* (jf. side 53), er en annen redundanstype som kan bidra til å øke sikkerheten innen høyteknologiske produksjonsprosesser med stort risikopotensiale. Organisatorisk redundans kan inndeles i minst to overordnede, om enn i praksis ikke alltid klart atskilte, kategorier: 1) prosedyrestyrte samhandlingsmønstre, dvs. samhandlingsmønstre som eksplisitt er definert i en organisasjons prosedyrer, og 2) samhandlingsmønstre som oppstår uten å være eksplisitt definert i organisasjonens prosedyrer.

Begrepet *prosedyre* kan defineres som et sett av instruksjoner som beskriver en oppgave eller en prosess. Prosedyren kan bestå i enkeltstående regler og/eller i en samling av sammenhengende regler (Zimmerman & Campbell, 1987). Rochlin, LaPorte & Roberts (1998, 6) fant at prosedyrene som anvendes på amerikanske hangarskip, ofte er usedvanlig robuste, og at prosedyrene vesentlig bidrar til å øke påliteligheten til medarbeidernes innsats. Skjønt Rochlin *et al*. ikke dokumenterer i hvilke grad prosedyrene også definerer samhandlingsmønstre mellom medarbeiderne, er det nærliggende å anta at dette er tilfellet. Bierly III & Spender (1995, 648) rapporterte at standard operasjonsprosedyrer har en helt sentral betydning på amerikanske atomubåter. Formålet med standardprosedyrene er å sikre at reaktoren håndteres på en kontrollert måte, slik at antallet 'overraskelser' reduseres. En standardprosedyre inneholder krav om spesifiserte samhandlingsmønstre. En standard operasjonsprosedyre for operasjon av ventiler krever bl.a. at medarbeideren som mottar en ordre *gjentar ordren ordrett*, slik at medarbeideren som har avgitt ordren kan sjekke at mottakeren har forstått ordren. Eksempler på prosedyrestyrte samhandlingsmønstre som er kjente fra andre domener omfatter f.eks. *fire-øyne prinsippet*, som i utstrakt grad anvendes av pilot - co-pilot innen luftsfartsdomenet, og *to-manns reglen*, som anvendes innen det amerikanske forsvar i relasjon til operasjoner som involverer kjernevåpen (Sagan, 1993, 250).

Gjennom definisjon av medarbeideres ansvarsområde, av arbeidsplassdesign, samt av ledelsesformen som anvendes i en organisasjon, kan det dessuten legges til rette for en annen type organisatorisk redundans. Denne er ikke eksplisitt prosedyrestyrt, men oppstår som konsekvens av en kombinasjon av instrumentelle (fastsettelsen av medarbeidernes ansvarsområder og arbeidsplassens design) samt kulturelle forutsetninger (ledelses- og samarbeidsformer). Det synes å være denne andre typen redundans som er det primære fokus innen HRO perspektivet. Rochlin *et al.* (1998, 8) foreslår at denne redundans typen kalles *beslutnings/ledelses-redundans*. Begrepet henviser til ”... a number of organizational strategies to ensure that critical decisions are timely and correct. ”(ibid.) Med referanse til deres studier av amerikanske hangarskip skillerer Rochlin *et al.* mellom to aspekter av beslutnings/ledelses-redundans: *interne kryssjekk* av beslutninger, og *feil-sikker redundans*.

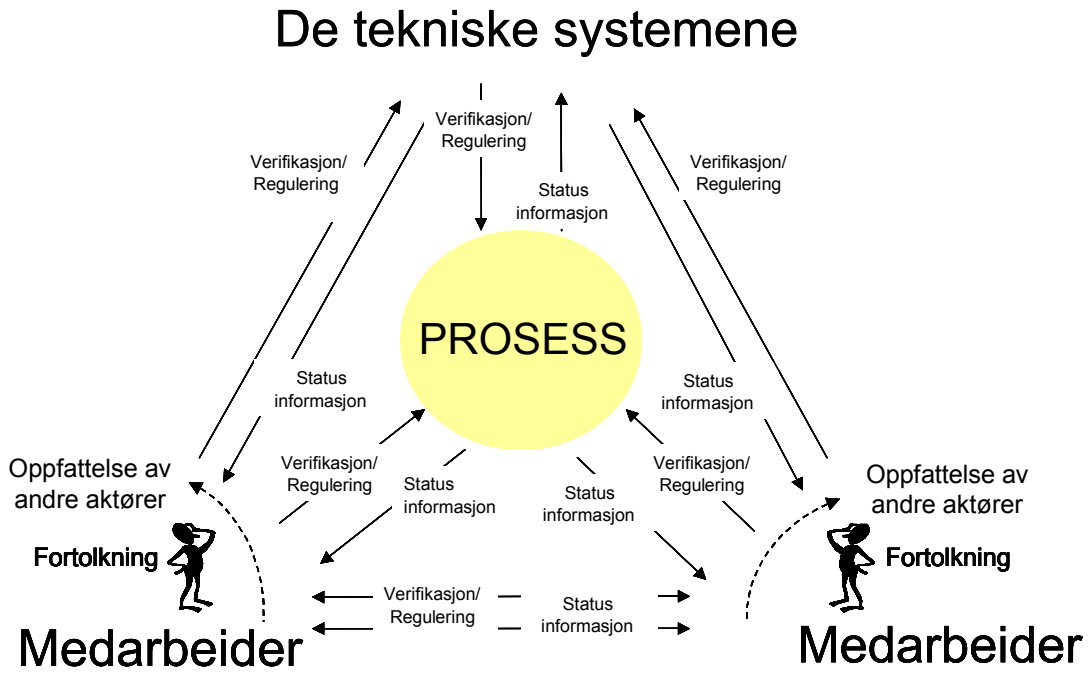
Interne kryssjekk henviser til oppgaverettet kommunikasjon som gjennomføres på kanaler som høres av mange medarbeidere - medarbeidere som ofte har en høy grad av fortrolighet med hverandres jobb. Et eksempel kan være kommunikasjonen som gjennomføres når et fly skal bringes til landing på et hangarskip. Et slikt samhandlingsmønster innebærer at ethvert kritisk element som ikke er på plass med stor sannsynlighet vil bli oppdaget - og påpekt - av *en eller annen* av de involverte personer før det blir årsak til problemer.

Feil-sikker redundans har til formål å sikre at om en ledelsesenhet av en eller annen grunn ikke lengre fungerer korrekt, da vil andre enheter trå til enten ved å understøtte at eventuelle feil blir korrigert og/eller ved å ta over ansvaret for utførelse av enhetens oppgave. Feil-sikker redundans kan etableres på mange forskjellige måter. De vanligste metodene er dublering og overlapp av

oppgaver og kompetanser. *Dublering* innebærer at to forskjellige enheter utfører akkurat samme funksjon. *Overlapp* innebærer at to enheter har oppgaver som er delvis overlappende i forhold til hverandre. I begge tilfeller vil det være mulig for en av enhetene å observere og korrigere feil begått av den andre enheten. "*Stressing-the-survivor"* innebærer at enhver enhet i normalsituasjonen opererer et stykke under sin fulle kapasitet, slikt at om det blir nødvendig vil enheten være i stand til å ta over oppgaven til en annen enhet uten å bli alvorlig overbelastet. "*Mobilizing reserves"* er også en mulig strategi. Den innebærer etableringen av en "skygge-enhet" som er i stand til å utføre oppgaver etter behov. Mobilizing reserves vurderes å være ganske effektiv strategi, men det understrekes samtidig at den er ganske omkostningsfull, fordi den stiller betydelige krav til kompetansen hos de involverte medarbeidere. Bierly III & Spender (1995, 648) rapporterer en strategi som kan kalles *gjensidig utspørring*. Strategien innebærer at to medarbeidere - f.eks. en dekksoffiser og en sonar tekniker kontinuerlig stiller kritiske spørsmål til hverandre med henblikk på å understøtte effektiv respons til eventuelle problemer. Strategien forutsetter en høy grad av felles kunnskap, samt eksistensen av en arbeidskontekst som krever og understøtter en slik arbeidsform.

6.5 Perspektiver

Innen petroleumsvirksomheten utfører medarbeideren sine arbeidsoppgaver i et nært samspill med så vel kolleger som de tekniske systemene - herunder det tekniske sikkerhetssystem (se Figur 8). Av denne grunn blir det avgjørende å se på både tekniske og organisatoriske redundans ved belysning av menneskets rolle som del av organisasjonens sikkerhetsbarrierer. Med henblikk på å øke produksjonssystemets toleranse for feil, blir det sentralt å belyse hvordan teknisk redundans kan designes slikt at den mest mulig effektivt understøtter aktiviteten til medarbeiderne, samt hvordan organisatorisk redundans skal legges til rette for å oppnå størst mulig positiv effekt. Det vil være sentralt å rette oppmerksomheten mot forekomst og korreksjon av så vel enkeltfeil som systemfeil. Det kan f.eks. tenkes at særlige kombinasjoner av teknisk og organisatorisk redundans vil beskytte mest optimalt mot enkeltfeil og systemfeil på oljeplattformer.



Figur 8. En enkel generisk modell av samspillet mellom menneske-menneske og menneske-maskin i et kontrollrom.

7 Hvordan skape økt feiltoleranse i petroleumsvirksomheten - rammeverk for videre arbeid

Vi ønsker i det videre arbeid å skape et felles rammeverk som de ulike deltagende forskningsmiljøene kan inngå i. Utgangspunktet er at vi ikke ønsker å opprette selvstendige delprosjekter, men å samarbeide med referanse til en felles overordnet problemstilling.

7.1 Overordnet målsetning

Formålet med prosjektet er å fremskaffe kunnskap som kan brukes til å utvikle, vedlikeholde, overvåke og vurdere det menneskelige og organisatoriske bidrag til feiltoleranse i petroleumsvirksomheten. Den overordnede målsetning vil være å frembringe og formidle kunnskap om temaet *"Hvordan skape økt feiltoleranse i petroleumsvirksomheten - med særlig fokus på bidrag fra menneskelige og organisatoriske faktorer?"* Fokuset på menneskelige og organisatoriske bidrag innebærer at vi ikke prioriterer problemstillinger som kun dreier seg om tekniske aspekter ved redundans (f eks overvåking av tekniske tilstand). I den grad arbeidet gir oss kunnskap om feiltoleranse i forhold til hendelser som fører til andre former for tap (f eks produksjonstap p.g.a. nedetid), ønsker vi også å dokumentere dette.

Vi ser i dag en trend mot blant annet fjernstyring, kortere gjennomføringstider og ytterligere fokus på å redusere driftskostnadene (ref. tema 1 rapporten). Dette er alle trender som vil påvirke hvordan installasjoner designes og opereres, ikke minst med tanke på organisasjons- og bemanningsaspekter. Det anses derfor som viktig å framskaffe kunnskap om hvordan menneskelige og organisatoriske faktorer påvirker graden av feiltoleranse, for på en bedre måte å kunne forutsi og studere effekten av disse endringene.

7.2 Overordnet rammeverk

I det videre arbeidet vil vi ta utgangspunkt i følgende antagelser:

1. I tett koblede høyrisiko-system kan et akseptabelt risikonivå som regel bare oppnåes gjennom en høy grad av feiltoleranse.

2. I system hvor risikokontroll er basert på forsvar i dybden, vil større ulykker ofte ha sammenheng med avhengigheter mellom barrierer.

3. I analyser som fokuserer ensidig på fysiske og tekniske barrierer, vil en som regel undervurdere avhengigheter mellom barrierer. En kan også komme til å undervurdere operatørenes bidrag til å skape feiltoleranse.

4. Mekanismer som skaper feiltoleranse får ofte liten oppmerksomhet fordi de produserer "ikke-hendelser".

5. Barrierer skaper læringsmuligheter fordi systemet tåler enkeltfeil, men barrierene kan samtidig tildekke tapspotensialet i en uønsket hendelse.

6. Organisatorisk redundans kan skapes gjennom formelle og uformelle mekanismer. Disse mekanismene ligger på samhandlingsnivå, og blir ikke fanget opp gjennom studier av enkeltpersoner.

7. Et hensiktsmessig utgangspunkt for å operasjonalisere menneskelige og organisatoriske bidrag til feiltoleranse kan være begrepet ’mindfulness’ (jfr. avsnitt 2.3).

Feiltoleranse designes inn i innretningene ved at det etableres rekker av *barrierer* ('forsvar i dybden'). I system hvor risikokontroll er basert på forsvar i dybden, vil større ulykker ofte ha sammenheng med ikke-erkjente, uventede eller sjeldent forekommende avhengigheter mellom barrierene. Dette kan dreie seg om avhengigheter mellom tekniske barrierer, mellom menneskelige barrierer og/eller mellom menneskelige og tekniske barrierer.

Innen teorier om høy-pålitelige organisasjoner (se avsnitt 2.3) anvendes begrepet "mindfulness' som kollektiv henvisning til fem karakteristika ved organisasjoner som driver sin virksomhet på en svært pålitelig måte til tross for at produksjonen er forbundet med et stort risikopotensiale. De fem karakteristika er (Weick & Sutcliffe, 2001): ’preoccupation with failure’, ’reluctance to simplify’, ’sensitivity to operations’, ’commitment to resilience’ og ’deference to expertise’. Begrepet ’mindfulness’ kan ved første øyekast virke svært abstrakt. Vi tror imidlertid det er mulig å konkretisere det med utgangspunkt i Weick og Sutcliffes beskrivelser av de fem dimensjonen (se avsnitt 2.3). En slik konkretisering kan forøvrig bidra til å gi begrepet ’sikkerhetskultur’ et klarere innhold.

Et av hovedmålene med dette prosjektet er å belyse sammenhengen mellom sikkerhetsnivå og 'mindfulness' ved å sette fokus på mulige sammenhenger mellom ’mindfulness’ og feiltoleranse. En organisasjons grad av 'mindfulness' kan antas å avspeile seg i kvaliteten til de enkelte barrierer, dvs. hvor effektive og robuste de enkelte barrierer er, samt i kvaliteten til organisasjonens totale barrieresystem. Spørsmålet om barrierers kvalitet har tradisjonelt blitt adressert med referanse til teknisk redundans. Når mennesker trekkes inn som en eksplisitt del av en organisasjons sikkerhetsbarrierer, må disse spørsmålene derfor adresseres på nytt med utgangspunkt i medarbeidernes karakteristika og oppgaver og forutsetningene for samhandling.

Organisatorisk redundans kan inndeles i to overordnede typer (se kapittel 6): formalisert og ikke-formalisert redundans. *Formalisert redundans* er samhandlingsmønstre som er eksplisitt definert, f.eks. i operasjonsprosedyrer eller arbeidsforskrifter. Den formaliserte redundansen er typisk etablert på basis av krav fra myndigheter og selskapenes ledelser, formelle undersøkelser og utredninger, etc. Den har til formål å sikre at *organisasjons eksplisitte kunnskap* om hvordan arbeidsoppgavene kan utføres på en sikker måte blir effektivt formidlet til medarbeiderne. *Ikke-formalisert redundans* er samhandlingsmønstre som oppstår som resultat av den overordnede tilretteleggelsen av arbeidet, herunder utformingen av arbeidskonteksten. Den ikke-formaliserte redundansen er etablert på bakgrunn av de praktiske erfaringene medarbeidergruppen har opparbeidet ved konkret å utføre de gitte oppgavene. Ikke-formalisert redundans kan derfor fange opp lokal og taus kunnskap hos personene som utfører jobben. Prinsipielt vil den formaliserte redundansen sikre at samtlige kjente risikofaktorer blir korrigert, mens den ikke-formaliserte vil sikre at ytterligere faktorer som medarbeiderne har erfart kan være sikkerhetskritiske også blir fanget opp. Begge redundanstypene er vesentlige for etableringen av feiltoleranse, og innflytelsene fra så vel formalisert som ikke-formalisert redundans vil derfor bli adressert i dette prosjektet.

Prosjektet vil adressere konkrete problemstillinger som kan få spesifikke praktiske konsekvenser for hvordan sikkerhetsarbeidet drives offshore. Vi ser for oss at studiet av mulige sammenhenger

mellom 'mindfulness' og feiltoleranse vil fungere som det overordnede rammeverk rundt prosjektet, mens problemstillingene knyttet til organisatorisk redundans vil fungere som konkrete praktiske eksempler som kan bidra til å belyse de mulige sammenhenger. I seg selv vil studiene av formalisert og ikke-formalisert redundans styrke forståelsen av hvordan feiltoleransen i petroleumsvirksomheten kan økes ved hjelp av menneskelige og organisatoriske tiltak, og resultatene fra denne del av prosjektet vil avslutningsvis kunne transformeres til et sett av retningslinjer for bruk av organisatorisk redundans. Overordnet sett vil studiet av sammenhenger mellom 'mindfulness' og feiltoleranse øke forståelsen av hvilke overordnede risikoindikatorer som er kritiske ved vurdering av kvaliteten til menneskelig og organisatorisk redundans.

7.3 Aktuelle problemstillinger for videre arbeid

Med referanse til den overordnede problemstillingen ønsker vi i det videre arbeidet å forholde oss til problemstillingene nedenfor. Det vil neppe være mulig å behandle alle problemstillingene grundig innenfor rammen av HMS petroleum.

1. Hvordan vurdere hvilken redundans som finnes i en organisasjon når en inkluderer menneskelige og organisatoriske bidrag til redundans i vurderingen?
For å kunne utvikle, overvåke og vedlikeholde feiltoleranse må en organisasjon ha en realistisk oppfatning av hvordan mennesker og organisasjon (i samspill med tekniske systemer) bidrar til feiltoleranse. Dette omfatter også negative bidrag – f.eks. muligheten for at en operatør kan hindre en automatisk nedstengning og derigjennom bidra til eskalering av et hendelsesforløp. Et viktig tema er avhengighet mellom barrierer, for eksempel i forhold til hvordan mennesker kan virke som en mulig kilde til fellesfeil. Utfordringen her er å utvikle metoder for å vurdere når mennesket fungerer som uavhengig barriere eller som en del av en uavhengig barriere (jfr. avsn. 6.3). Kunnskap om hvordan begrepet *uavhengig* skal anvendes i relasjon til menneskelige og organisatoriske faktorer kan bidra til å videreutvikle metoder for risikohåndtering, og dermed til å ytterligere øke produksjonssystemets toleranse for feil.

2. Hvilken betydning har menneskelige og organisatoriske bidrag til feiltoleranse for risikonivået?
Utfordringen er her å kunne si noe troverdig om hvor stor effekt de positive og negative bidragene til feiltoleranse har på risikonivået. Her står vi overfor store metodiske utfordringer. Modelleringsteknikker som brukes til å analysere tekniske systemer, kan ikke uten videre overføres til menneskelige og organisatoriske fenomen. Data om uønskede hendelser kan fortelle oss en del om svikt i mekanismer som skulle skape feiltoleranse, mens hendelser hvor disse mekanismene virket, ikke nødvendigvis blir rapportert. Komparative studier – f.eks. sammenligninger mellom bransjer – må forholde seg til at analyseenhetene kan være ulike på en rekke andre dimensjoner, slik at ulike effekter kan være vanskelig å skille fra hverandre.

3. Hvordan kan en organisasjon utvikle det menneskelige og organisatoriske bidrag til feiltoleranse?
Her er utfordringen å finne frem til tiltak og virkemidler for å styrke det menneskelige og organisatoriske bidrag til feiltoleranse. Under denne problemstillingen ligger det også å evaluere tiltak for å styrke feiltoleranse. Et sentralt tema er hvordan organisatorisk læring kan legges til rette med henblikk på å understøtte kvaliteten til menneskelig og organisatorisk redundans? Her bør vi være åpne for både eksplisitt kunnskap (f eks at erfaringer med nestenulykker brukes til å omarbeide arbeidsbeskrivelser) og taus kunnskap (f eks at en arbeidsgruppe justerer sin praksis uten at dette kodifiseres i en ny prosedyre). På denne måten kan vi fange opp både formalisert og

ikke-formalisert redundans. Vi må også ta høyde for at ikke all læring nødvendigvis fører til lavere ulykkesrisiko.

4. Hvordan kan tekniske og organisatoriske endringer påvirke menneskelige og organisatoriske bidrag til feiltoleranse?
Denne problemstillingen ligger i grenseflaten mot Tema 1 (Overvåke og vurdere teknologiutviklingen) og Tema 3 (HMS-aspekter ved endringsprosesser). Eksempler på endringer kan være overgang til fjernstyring av en installasjon eller nedbemanning i forbindelse med haleproduksjon. Her er det også en utfordring å finne frem til metoder som kan brukes til å avgjøre når organisatorisk redundans er svekket (jfr. avsn. 6.3.4). Etablering av slike metoder kan antas å effektivt understøtte den 'ansvarliges' mulighet til å gjennomføre korrekte risikovurderinger.

7.4 Metodisk tilnærming

Hovedspørsmålet ” *Hvordan skape økt feiltoleranse i petroleumsvirksomheten med særlig fokus på bidrag fra menneskelige og organisatoriske faktorer*" danner grunnlaget for utviklingen av det overordnede rammeverket for videre arbeid. Et grunnleggende spørsmål av en slik art krever metodetriangulering, dvs at resultatet må avledes på basis av en kombinasjon av individuelle undersøkelser med ulike metodikk. De ulike problemstillingene som er knyttet til ’mindfulness’ med fokus på organisatorisk redundans vil fordre ulike metodiske tilnærminger.

Mulige data innsamlingsmetoder:
- Spørreskjema
- SYNERGI (hendelsesdatabase)
- Dybde intervjuer
- Offentlige ulykkesrapporter utarbeidet av OD
- Avreisemøter
- Dokumentasjon: prosedyrer, risikoanalyser, etc.
- SJA teknikker fra de forskjellige selskapene
- Feltstudier – 2-3 dagers opphold
- Eksperimentelle studier, f.eks. simulatorstudier

En informasjonskilde kan være diskusjoner med utgangspunkt i konkrete uønskede hendelser. Ved å analysere hvilke tema folk fokuserer på og hvordan de vinkler ting, burde vi kunne få svar på flere av problemstillingene knyttet til ’mindfulness’ og feiltoleranse. Diskusjonene kan i enkelte tilfelles fungere som en arena for enkel hypotesetesting.

Kartlegging av ’*mindfulness*’ kan skje gjennom utvikling av et spørreskjema som også kan omfatte andre norske høyrisiko virksomheter utover petroleumsbransjen. Utvikling og testing av spørreskjemaet vil da foregå i samarbeid med petroleumsbransjen, som også kan fungere som referanse for en eventuell sammenligning av feiltoleranse i ulike høyrisiko bransjer (f.eks kraftforsyning, persontrafikk, transport av farlig gods, komplekse byggeprosjekter). Se vedlegg 1 for nærmere beskrivelse av metode/ utvalg knyttet til en spørreskjema-studie av ’mindfulness’.

Ved kartlegging av *organisatorisk redundans* vil det være nødvendig å anvende flere forskjellige metoder. Hvilke metoder som er mest hensiktsmessige ut fra et praktisk perspektiv må avklares i et samarbeid med petroleumsbransjen. Metodene kunne f.eks. omfatte: felt studium, studium av hendelseslogger, samt dybdeintervjuer. Dessuten vil data fra deler av spørreskjemaet (nevnt i

avsnittet ovenfor) kunne inndras. Se vedlegg 2 for nærmere beskrivelse av metode/utvalg knyttet til studiet av organisatorisk redundans.

7.5 Forslag til konkrete arbeidsoppgaver og koblinger mot bruker-initierte prosjekt

Nedenfor følger skisser til mulige konkrete arbeidsoppgaver i videreføringen av Tema 2. Vi ønsker å konsentrere oss om få oppgaver, men presenterer flere mulige aktiviteter, slik at vi kan prioritere i samråd med brukere. I prioriteringen vil vi bl.a. legge vekt på muligheten for å komme i tett inngrep med sluttbrukere og få tilgang til egnede datakilder.

7.5.1 Retningslinjer for bruk av mennesket som del av en organisasjons sikkerhetsbarrierer

Formålet med prosjektet er å *bidra med økt kunnskap om hvordan mennesker fungerer som del av en organisasjons barrierer med formål om å understøtte organisasjonenes kapasitet for risikohåndtering og risikoevaluering*. Prosjektet vil adressere to forskningsspørsmål: 1) når skal medarbeideren defineres som *en* uavhengig barriere, og når som del av en uavhengig barriere? 2) hvilke krav skal være oppfylte innen mennesket kan antas å kunne fungere som pålitelig sikkerhetsbarriere/del av sikkerhetsbarrierene? Bevarelsen av de to spørsmål vil avslutningsvis fungere som grunnlag for utvikling av *et sett av retningslinjer* for bruk av mennesket som del av en organisasjons barrierer. Prosjektet vil anvende en induktiv metode, og omfatte fire faser:

- *Fase 1: Studier av SJA i relasjon til vedlikeholdsoppgaver.* Med henblikk på å få en bedre forståelse av effekten av organisatorisk redundans foreslås det at å gjennomføre et case-studium. En opplagt case kunne være 'sikker-jobb-analyse" [23] (SJA) i forhold til vedlikehold.[24] SJA gjennomføres på forskjellige måter i de forskjellige selskapene. Studiet av SJA kan derfor antas å gi et mangfold av perspektiver (god bredde i data) på problemstillingene som forskningsspørsmålene rommer. Casestudiet vil omfatte en rekke aktiviteter som sikter mot å belyse problemstillingene rundt SJA i relasjon til vedlikeholdsarbeide på en fyldig måte, som f.eks.: 1) felt studium, 2) studium av hendelseslogger som refererer til utførte SJAer, 3) dybdeintervjuer med vedlikeholdspersonale og arbeidsledere, samt med utviklere/ansvarlige for filosofien bak SJA tilnærmingene i de enkelte selskap.
- *Fase 2: Utforming av teoretisk forståelse.* Med utgangspunkt i data brakt til veie i fase 1 vil en teoretisk ramme for beskrivelse av mennesket som sikkerhetsbarriere bli utviklet. Med referanse til denne rammen vil de to forskningsspørsmål søkes besvart.
- *Fase 3: Etterprøving og justering av teoretisk forståelse.* Validiteten til besvarelsen av de to forskningsspørsmål som ble etablert i fase 2 vil bli testet mot en ny type arbeidsoppgaver - f.eks. kontrollromsaktivitet som involverer at sikkerhetssystemene utkobles. Den teoretiske rammen vil etterfølgende bli justert på basis av utfallet av testen.

[23] SJA er en metode som brukes for å klarlegge faremomentene som er forbundet med å utfører sikkerhetskritisk arbeider. SJA innebærer at arbeidsoppgaven brytes ned i del-opgaver, og at hver del-oppgave analysers. Analysen skal sikre at medarbeideren korrekt har forstått faremomentene som er forbundet med oppgaven han eller hun skal utføre, samt eventuelt forslå tiltak som kan bidra til å eliminere/kontrollere faremomentene.

[24] Reason (1997) finner at menneskelige feil relatert til vedlikehold (og dermed til etablering av latente feil i produksjonssystemet) isolert sett utgjør det største bidra av 'menneskelige feil' innen industrielle produksjonsprosesser.

– *Fase 4: Justering av teoretisk forståelse og dokumentasjon av resultater.* Dokumentasjon av resultatene vil inkludere en spesifikasjon av hvilke retningslinjer for bruk av mennesket som del av en organisasjons barrierer som har blitt avdekket i undersøkelsen.

7.5.2 Arbeid i tilknytning til IEC 61508

Standarden IEC 61508 (se side 36) omhandler instrumenterte sikkerhetssystemer, men poengterer gjentatte ganger at ”human factors”-betraktninger må inngå i forbindelse med spesifikasjon, realisering og drift av de tekniske sikkerhetsfunksjonene. Standarden tilbyr imidlertid minimal rettledning i forhold til hva dette innebærer, og en aktuell og nyttig problemstilling vil derfor være å utdype hvordan ’human factors’ skal innarbeides i forhold til IEC 61508. For eksempel kan det være relevant å se på hvordan mennesker og organisasjon bidrar til å vedlikeholde feiltolerante sikkerhetssystemer. SINTEF har per i dag flere pågående prosjekter (blant annet mot Statoil) hvor en arbeider med å implementere IEC 61508 i forbindelse med både modifikasjoner og nybygg. Muligheten for å knytte en slik gjennomgang opp mot et av disse konkrete prosjektene bør derfor vurderes. Blant annet utføres det en SIL analyse av modifisert innløpsarrangement på en av Gullfaks plattformene (jfr. problemstillingen beskrevet i ’fortelling’ 1.2.3), som kan være en interessant case.

7.5.3 Arbeid knyttet til ”Smartere sammen”

Det bruker-initierte prosjektet ”Smartere sammen” kan gi kompetanseprosjektet ”Endring – organisasjon – teknologi” inngrep med flere industriprosjekter som fokuserer på samhandling og kunnskapsdeling på tvers av organisatoriske skillelinjer. Bedre samhandling og kunnskapsdeling kan være et middel til å skape organisatorisk redundans, men også til å styrke organisasjonens kunnskap om og evne til læring om andre aspekter ved barrierer.

7.5.4 Arbeid knyttet til ”Morgendagens HMS-analyser”

I det bruker-initierte prosjektet ”Morgendagens HMS-analyser” er målsetningen å utvikle analysemetodikk som på en troverdig måte kan underbygge og dokumentere at tekniske, operasjonelle og organisatoriske endringer gjennomføres slik at de ivaretar en sikkerhetsmessig forsvarlig drift av organisasjonene. En hovedoppgave innen ”Morgendagens HMS-analyser” vil bli å *videreutvikle CRIOP-metoden*[25] (Ingstad og Bodsberg, 1990). Dette er en scenario-basert metode for å evaluere et kontroll-senters evne til å håndtere unormale situasjoner. En av utfordringene i en slik evaluering er å fange opp i hvilken grad utforming, bemanning og organisering legger forholdene til rette for å skape organisatorisk redundans i forbindelse med kritiske beslutninger.

Et annet tema i ”Morgendagens HMS-analyser” er *barriereanalyser*, med vekt på organisatoriske og operasjonelle barrier. På dette området er det ennå ikke tatt stilling til eksakt tilnærmingsmåte, men her forventer vi også at det vil bli mulig å oppnå synergi-effekter i forhold til videreføringen av Tema 2.

[25] CRIOP ~ Crisis Intervention in Offshore Production

8 Referanser

Andreassen, J., Eskedal, T. S., Førsund, S., Solheim, R., Stephansen, E. (2002). *Rapport etter dødsulykke på Byford Dolphin 17.04.2002*. OD, prosjektnummer: 0222R11.

Bierly III, P.E. & Spender, J.C. (1995). Culture and High Reliability Organizations: The Case of the Nuclear Submarine. In: *Journal of Management, vol. 21, no. 4.* Pp. 639-656.

Bodsberg, L., Hokstad, P., Berstad, H., Myrland, B. og Onshus, T. (1994): *Reliability Quantification of Control and Safety Systems. The PDS-II method.* Rapport STF75 A93064. Trondheim: SINTEF Teknologiledelse.

CCPS, 1993. Guidelines for Safe Automation of Chemical Processes. ISBN 0-8169-0554-1, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York

Dahll, G., Skjerve, A.B.M. & Sivertsen, T. (2001). *Evalueringskriterier for Jernbaneverkets endring av trafikksikkerhetsbestemmelsene.* IFE/HR/F-2001/1179.

DOE Workbook: Conducting Accident Investigations. Department of Energy, US. Tilgjengelig på: DOE Workbook (1999). *Conducting Accident Investigations.* Rev. 2. U.S. Department of Energy Washington, D.C. 20585, May 1, 1999. Tilgjenglig på: http://www.ic.polyu.edu.hk/posh97/private/AccidentPhenonmenon/investigation-workbook.pdf

DOE, 1997. US Department of Energy (DOE) Implementation Guide for use with DOE Order 225.1A, Accident Investigation, DOE G 225.1A-1, November 26, 1997/Rev. 1, United States of America.

Eskedal, T.S., Ellingsen, A. & Seim, L.Å. (2002). *Rapport etter tilsyn med Ekofisk 2/4J-alarmsystemer*. OD rapport, datert 30.09.2002. Saksnummer: 02/684-AA10.N8

Eskedal, T.S., Husebø, T., Heber, H. & Seim, L.Å. (2001). *Rapport etter tilsyn med Heidrun - alarmsystemer*. Saksnummer: 01/615-AA12.P16.

Gibson, J. J. (1961): The contribution of experimental psychology to the formulation of the problem of safety – a brief for basic research. In *Behavioral Approaches to Accident Research,* New York: Association for the Aid of Crippled Children, pp. 77-89. Reprinted in W. Haddon, E.A. Suchman and D. Klein (1964): *Accident Research: Methods and Approaches.* New York: Harper & Row.

Haddon, W. (1970): On the escape of tigers: An ecological note. *Technological review, 72* (7), Massachusetts Institute of Technology, May 1970.

Haddon, W. (1980): The Basic Strategies for Reducing Damage from Hazards of All Kinds. *Hazard prevention,* Sept./ Oct. 1980.

Holand, P, 199x. Offshore Blowouts.

Hollnagel, E. (1999). *Accident Analysis and Barrier Functions*. IFE/HR/F-99/1121.

Hollnagel, E. (1999). Accidents and barriers. In J.-M. Hoc, P. Millot, E. Hollnagel & P. C. Cacciabue (Eds.), Proceedings of *Lez Valenciennes, 28*, 175-182. (Presses Universitaires de Valenciennes.)

Hollnagel, E. (2002). Understanding Accidents – From Root Causes to Performance Variability, IEEE 7th Human Factors Meeting, Scottsdale, Arizona, 2002

IAEA (2000). Safety of Nuclear Power Plants: Design Requirements. IAEA Safety Standards Series. Vienna, No. NS-R-1.

Ingstad O. og Bodsberg, L. (1990): *CRIOP: A Scenario-method for Evaluation of the Offshore Control Center.* Rapport STF75 A89028. Trondheim: SINTEF Teknologiledelse.

INSAG-10 (1996). *Defense in Depth in Nuclear Safety*, A report by the International Nuclear Safety Advisory Group (INSAG-10), International Atomic Energy Agency, Vienna.

INSAG-12. Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1. IAEA, Vienna, 1999.

Jernbanetilsynet forskrift 23. desember 1999 nr. 1402 om krav til styring og oppfølging av forhold relevant for sikker trafikkavvikling på jernbane herunder sporvei, tunnelbane og forstadsbane m.m.

Kjellén, U. (1999): *Prevention of accidents through experience feedback*. Kompendium. Trondheim: NTNU.

LaPorte, T.R. and Consolini, P.M. (1991): Working in practice but not in theory: Theoretical challenges of “High-Reliability Organisations”. In: *Journal of Public Administration Research and Theory, 1*. Pp. 19-47.

LaPorte, T.R. og Consolini, P.M. (1991): Working in practice but not in theory: Theoretical challenges of ”High-Reliability Organisations”. Journal of Public Administration Research and Theory, 1, s.19-47

Marciniak, J. J. (1994):. Encyclopedia of Software Engineering. John Wiley and Sons,.

Merriam-Webster. Tilgjengelig på: http://www.m-w.com/cgi-bin/dictionary

Neogy, P., Hanson, A.L., Davis, P.R. & Fenstermacher, T.E. (1996). *Hazard and Barrier Analysis Guidance Document*. Office of Operating Experience Analysis and Feedback, Rev. 01, November 1996, EH-33. Department of Energy, US.

NUREG-0711 (2002). *Human Factors Engineering Program Review Model*. Rev. 1. U.S. Nuclear Regulatory Commission. Office of Nuclear Regulatory Research, Washington DC. Prepared by J.M. O'Hara, J. Higgins, J. Persensky, P. Lewis & J. Bongarra.

OD (2001a). *Forskrift om styring i petroleumsvirksomheten (Styringsforskriften)*, 3. september 2001.

OD (2001b). *Forskrift om helse, miljø og sikkerhet i petroleumvirksomheten (Rammeforskriften),* 31. august 2001.

OD (2001c). *Forskrift om utforming og utrustning av innretninger med mer i petroleumsvirksomheten (Innretningsforskriften)*, 3. september 2001

OD (2001d). *Forskrift om utføring av aktiviteter i petroleumsvirksomheten (Aktivitetsforskriften)*, 3. september 2001

OD (2002a) *Veiledning til forskrift om styring i petroleumsvirksomheten (Styringsforskriften)*, 1. januar 2002.

OD (2002b) *Veiledning til forskrift om utføring av aktiviteter i petroleumsvirksomheten (Aktivitetsforskriften)*, 1. januar 2002.

OLF (2001). Recommended Guidelines for the Application of IEC 61508 and IEC 61511 in the Petroleum Activities on the Norwegian Continental Shelf. Rapport nr. 070, datert 1.02.2001, revisjon nr. 1: The Norwegian Oil Industry Association.

Onshus, T. Hansen, G.K., Hauge, S., Holmstrøm, S., Lone, S., Nybø, H.O. & Aarø, R. (1998). *Innspill til tekniske krav til sikkerhetssystemer på faste og flytende installasjoner*. STF72 A98315.

Perrow, C. (1984). *Normal accidents. Living with high-risk technologies*. New York: Basic Books.

Rasmussen, J. (1996): Risk management in a dynamic society. Presentation at the seminar *Safety and Reliability in Industrial Management*, Trondheim 29-30 May 1996. (Viewgraphs)

Rasmussen, J. (1997): Risk management in a Dynamic Society: A Modelling Problem *Safety Science, 27* (2-3), pp. 183-213.

Rasmussen, J. og Svedung, I. (2000): *Proactive Risk Management in a Dynamic Society*, Swedish Rescue Services Agency, Karlstad, Sverige

Reason, J. (1987). The Chernobyl errors. In: *Bulletin f The British Psychological Society, 40.* Pp. 201-206

Reason, J. (1992). *Human Error*. 2. opplag, Cambridge: Cambridge University Press.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate.

Roberts, K.H. (1998). The Cross-Cultural Design and Management of High Reliability Organizations and Systems of Organizations: Conceptual Help From The Triandis Review. In: *Advances in International Comparative Management, vol. 12*. Pp. 67-76.

Rochlin, G. I., LaPorte, T. and Roberts, K. H. (1987): The self-designing high-reliability organization: Aircraft carrier flight operations at sea. *Naval War College Review 40*(4), 76-90. Tilgjengelig på: http://www.nwc.navy.mil/press/reveiw/1998/summer/art7su98.htm

Rosness, R. (2001). *Slank og sårbar? Om verdien av organisatorisk redundans.* STF38 A01413. SINTEF.

Rosness, R., Guttormsen G., Tinmannsvik R.K. og Steiro, T. (2002):*Organisational Accidents and Resilient Organisations: Five Perspectives.* Rapport STF38 A02413. SINTEF Teknologiledelse, Trondheim

Rosness, R., Håkonsen, G., Steiro, T. and Tinmannsvik, R.K. (2000): The vulnerable robustness of High Reliability Organisations: A case study report from an offshore oil production platform. Paper presented at the 18th ESReDA seminar *Risk Management and Human Reliability in Social Context.* Karlstad, Sweden, June 15-16, 2000.

Sagan, S.D. (1993). *The limits of safety: organizations, accidents, and nuclear weapons*. Princeton, N.J.: Princeton University Press.

Schank, R.C. & Abelson, R.P. (1977). *Scripts, plans, goals and understanding: an inquiry into human knowledge structures*. Hillsdale, N.J: John Wiley & Sons,

Schank, R.C. (1982). *Dynamic Memory. A theory of reminding and learning in computers and people*. US: Cambridge University Press.

Seim, L.Å. (2002). Personlig kommunikasjon med Lars Åge Seim, IFE. Lars Åge Seim har i mange år jobbet som konsulent for OD i forbindelse med utførelse av tilsynsoppgaver.

Skjerve, A.B.M., *et al.* (2003) Bidrag til hefte med arbeidstittel "Menneske-teknikk-organisasjon (MTO)." Manuskript under utarbeidelse.

Statoils nettsider:
http://www.statoil.com/STATOILCOM/SVG00990.NSF?opendatabase&lang=no&artid=4125666B007254BD412566C2003D4211. Nyhet 24.11.1998

Svenson, O. (1991). The Accident Evolution and Barrier Function (AEB) Model Applied to Incident Analysis in the Processing Industries. In: *Risk Analysis, vol. 11., no. 3*. Pp. 499-507.

The Hon. Lord Cullen (1990). *Public Inquiry into the Piper Alpha Disaster* (Departement of Energy, London: HMSO)

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

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

Wason, P.C. & Shapiro, D. (1971). Natural and contrived experience in a reasoning problem. In: *Quarterly Journal of Experimental Psychology, 23*. Pp. 63-71.

Weick, K.E. & Sutcliffe, K.M. (2001). *Managing the Unexpected. Assuring High Performance in an Age of Complexity*. University of Michigan Business School Management School. Michigan: Jossey-Bass.

Zimmerman, C.M. & Campbell, J.J. (1987). *Fundamentals of Procedure Writing*. Columbia, USA: GP Courseware.

AAD, 2001. Arbeids- og administrasjonsdepartementet (AAD), Stortingsmelding nr. 7 (2001-2002) Om helse, miljø og sikkerhet i petroleumsvirksomheten.