SINTEF Teknologi og samfunn
Sikkerhet og pålitelighet

SINTEF IKT
Anvendt kybernetikk

Postadresse: 7465 Trondheim
Besøksadresse: S P Andersensvei 5
Telefon/faks: 73 59 27 56/73 59 28 96

Foretaksregisteret: NO 948 007 029 MVA

SINTEF RAPPORT

TITTEL

Uavhengighet av sikkerhetssystemer offshore – status og utfordringer

FORFATTER(E)

Stein Hauge, Tor Onshus, Knut Øien, Tor Olav Grøtan, Sture Holmstrøm, Mary Ann Lundteigen

OPPDRAGSGIVER(E)

Petroleumstilsynet, Ptil

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS JFR.	
STF50 A06011	Åpen	Torleif Husebø	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	82-14-03884-7	504042.01	32
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
T/504042.01/STF50 A06011 Uavhengighet av Sikringssystemer - endelig.doc		Tor Onshus	Erik Jersin
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
	2006-01-23	Lars Bodsberg, Forskningssjef	

SAMMENDRAG

Sikkerhetssystemene offshore blir stadig mer ”koblede”, for eksempel ved at samme produsent leverer kontroll og sikkerhetssystemer, bruk av felles software og brukergrensesnitt i ulike systemer, felles hardware, økt signaloverføring mellom systemer, innføring av integrerte operasjoner, osv.

Med dette som bakgrunn har SINTEF gjennomført et prosjekt hvor målsettingene har vært å:

1. Definere begrepet ”uavhengighet” (funksjonelt/geografisk, etc.), og deretter si noe om hvorfor dette prinsippet er så viktig rent sikkerhetsmessig;
2. Gi en kort statusbeskrivelse av hvordan Ptils krav til uavhengighet mellom tekniske barrierer er implementert på norsk sokkel og gi eksempler på tilfeller der avhengigheter eksisterer;
3. Beskrive kvalitativt mulige konsekvenser og effekter av disse avhengighetene;
4. Belyse hvordan økt bruk av integrerte operasjoner / eDrift kan påvirke mulige koblinger mellom systemer / barrierer;
5. Beskrive utfordringer og videre arbeid innenfor dette området.

Denne rapporten dokumenterer resultatene fra dette arbeidet.

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Sikkerhet	Safety
GRUPPE 2	Offshore	Offshore
EGENVALGTE	Uavhengighet	Independence
	Tekniske sikkerhetssystemer	Technical safety systems
	Integrerte operasjoner	Integrated operations

INNHOLDSFORTEGNELSE

1. Sammendrag og konklusjoner

Sikkerhetssystemene offshore blir stadig mer "koblede", for eksempel ved at samme produsent leverer kontroll og sikkerhetssystemer, bruk av felles software og brukergrensesnitt i ulike systemer, felles hardware, økt signaloverføring mellom systemer, innføring av integrerte operasjoner, osv.

Med dette som bakgrunn har SINTEF gjennomført et prosjekt hvor målsettingene har vært å:

1. Definere begrepet "uavhengighet" (funksjonelt/geografisk, etc.), og deretter si noe om hvorfor dette prinsippet er så viktig rent sikkerhetsmessig, *jfr. kapittel 3;*
2. Gi en kort statusbeskrivelse av hvordan Ptils krav til uavhengighet mellom tekniske barrierer er implementert på norsk sokkel. Gi eksempler på tilfeller der avhengigheter eksisterer, *jfr. avsnitt 4.1 og 4.2;*
3. Beskrive kvalitativt mulige konsekvenser og effekter av disse avhengighetene *jfr. avsnitt 4.3;*
4. Belyse hvordan økt bruk av integrerte operasjoner / eDrift kan påvirke mulige koblinger mellom systemer / barrierer, *jfr. kapittel 5;*
5. Beskrive utfordringer og videre arbeid innenfor dette området, *jfr. avsnitt 1.4.*

I dette kapittelet oppsummerer vi hovedresultater, anbefalinger og konklusjoner fra arbeidet.

1.1 Dagens status

Som en del av prosjektet ble det gjennomført telefonintervjuer med utvalgt fagpersonell. Basert på disse intervjuene samt SINTEFs egne erfaringer, er det i kapittel 4 gitt en rekke eksempler på koblinger og avhengigheter mellom systemer som i dag er mer eller mindre vanlige. Dette innbefatter blant annet:

- ulike koblinger og avhengigheter mellom prosesskontroll- og prosessavstengningssystemet
- tilsvarende mellom prosessavstengnings- og nødavstengningssystemet
- koblinger mellom andre sikkerhetskritiske systemer og funksjoner, slik som for eksempel mellom sjøvanns- og brannvannsystemet, mellom ballastkontroll og nødballastering og mellom HVAC og brann- & gassystemet;
- avhengigheter som en følge av økt standardisering i prosjektene;
- bruk av felles operatørstasjoner og felles kommunikasjonskanaler for kontrollsystemet og sikkerhetssystemene;
- avhengigheter som innføres i forbindelse med oppgraderinger av programvare.

Fagfolkene opplever selv å ha bra kontroll med de kjente avhengighetene og mener at løsningene stort sett er gjennomtenkt og at konsekvensene er grundig vurdert i prosjektene.

På spørsmål om hva som gjøres for å påvise "tilstrekkelig" uavhengighet mellom systemer viser fagfolkene til erfaringene fra tidligere prosjekter, samt analyser av pålitelighet (blant annet SIL beregninger). Utover dette er det SINTEFs inntrykk at det er noe begrenset hva som gjøres for å påvise og dokumentere uavhengighet mellom systemer og funksjoner. Mangel på gode verktøy og metoder antas å være hovedgrunnen til dette.

1.2 Er konsekvensene av de innførte avhengighetene akseptable?

Det er vanskelig å svare et entydig ja eller nei på dette spørsmålet. Generelt kan en imidlertid si at den økte kompleksiteten både i anleggene og i Safety and Automation System (SAS) medfører at nye avhengigheter introduseres, og at systemene derfor blir tettere koblet. Dette kan medføre at anleggene blir vanskeligere å forstå, operere og ikke minst å vedlikeholde, og at det i nødssituasjoner kan være vanskeligere for operatøren å skaffe seg oversikt over situasjonen.

Mangel på systematiske analyser av eksisterende avhengigheter, og analyser hvor en søker å identifisere hittil ukjente avhengigheter, gjør det derfor nærliggende å konkludere med at myndighetenes krav til "tilstrekkelig" uavhengighet mellom systemene (jfr. avsnitt 3.1) ikke er godt nok dokumentert.

1.3 Hvilken vei går utviklingen? – Integrerte operasjoner

Mange av de identifiserte koblingene og avhengighetene som er beskrevet i denne rapporten vil være av en slik karakter at feil i det ene systemet vil medføre en stopp eller nedstengning av andre systemer. Dette betinger imidlertid at systemene går til sikker tilstand ved nedstengning, dvs. at de er "fail-safe". For eksempel skal sikkerhetssystemene gå til sikker tilstand hvis de oppdager meldingsstorm på nettet eller at en oppdatering via nettet blir forsinket.

En har i den seinere tid sett en tendens til at enkle robuste "fail-safe" løsninger har blitt erstattet med mer komplekse, "aktive" systemer, hvor sikker tilstand ikke er like entydig definert som før. Eksempler på slike løsninger kan være sekvensiell nedblåsning av prosessanlegget, områdebasert branndeteksjon, HIPPS som erstatning for PSV, og flytende produksjonsløsninger (som FPSO) hvor en er avhengig av å holde en del systemer i gang ved en nedstengning.

Et enda mer sentralt utviklingstrekk er overgangen til eDrift / integrerte operasjoner. Denne utviklingen sees av mange på som en forutsetning for at norsk petroleumsindustri skal kunne holde seg konkurransedyktig i årene framover, ref. /11/. I forbindelse med overgangen til integrerte operasjoner er blant annet følgende problemstillinger diskutert (jfr. kapittel 5):

- Det bør ligge en implisitt forutsetning og målsetning om at de tekniske sikkerhetssystemene i hvert fall ikke skal bli dårligere når en flytter deler av styring og kontroll inn til land (eller til en annen installasjon);
- Overgangen til integrerte operasjoner vil medføre et ytterligere påtrykk mot standardisering av systemene på plattformen og mot en enda høyere grad av integrasjon mellom disse, ref. /11/. At det derfor kan oppstå motsetningsforhold mellom det å beholde størst mulig grad av uavhengighet mellom systemene og det å videreutvikle ulike eDriftsformer, synes åpenbart;
- Flere komponenter vil måtte omfattes av uavhengighetsprinsippet, noe som medfører at det vil bli en enda større utfordring å holde systemene atskilte;
- Når en går fra en situasjon med fysisk nærhet til systemene og prosessen, til en situasjon hvor personell på land "styrer" driften, blir det svært viktig at operatørene på land blir presentert informasjon på en ryddig og informativ måte, slik at de har grunnlag for en god og oppdatert virkelighetsforståelse.

1.4 ”Tar du den så tar du den” – utfordringer og videre arbeid

Når en forsøker å analysere nye ”innovative” løsninger, vil disse enkeltvis svært ofte være akseptable. Det er flere årsaker til dette; dersom en bruker risikoanalyse (QRA) som verktøy, vil en slik analyse være såpass ”grov” at eventuelle avhengigheter i liten grad modelleres inn. Dessuten er det gjerne slik at risikobidraget fra én enkelt endring (slik som å erstatte PSV med HIPPS) er for liten til at dette i seg selv ”velter” akseptkriteriet. Ved bruk av pålitelighetsanalyse har en noe av det samme problemet; tilnærmingen er forholdsvis grov og faktorer knyttet til kompleksitet og avhengighet - både designmessig og operasjonelt - reflekteres i begrenset grad.

Nedenfor er satt opp en del forslag til videre arbeid og fokusområder innenfor temaene avhengighet, kompleksitet og integrerte operasjoner:

- Det kan være aktuelt at også petroleumsindustrien vurderer å ta i bruk noen av metodene som er tilgjengelig fra andre industrier for å analysere avhengighet (jfr. avsnitt 3.5 og kapittel 6).
- Én mulighet vil være å ta for seg to eller flere konkrete systemer, for eksempel knyttet til boring eller brønnhodekontroll, og utføre en avhengighetsanalyse etter tilsvarende ”mal” som det som gjøres innenfor andre industrier. Dette vil kunne avklare hvorvidt det kan være fornuftig å kreve slike analyser offshore også.
- Ofte er det slik at avhengighetene ligger på et svært ”lavt nivå” og derfor ikke avdekkes i tradisjonelle risiko- og pålitelighetsanalyser. En tilnærming kan derfor være å ta for seg et par konkrete installasjoner, gjerne med eDrift, og gå gjennom signalgangen i detalj for å fastslå hvilke koblinger som egentlig finnes.
- En annen tilnærming vil være å gå gjennom noen viktige ulykkesscenarier for en installasjon og forsøke å vurdere hvor viktig/kritisk det faktisk er at barrierene og sikkerhetsfunksjonene er uavhengige.
- Når en setter SIL krav til ulike systemer, stiller en også konkrete krav til konfigurasjon og utviklingsprosess. Det er imidlertid slik at avhengigheter på tvers av systemer ikke nødvendigvis fanges opp i slike SIL analyser, som for eksempel potensielle avhengigheter og sårbarheter i brukergrensesnittet og nettverk. Dette er derfor et område der en bør skaffe seg mer innsikt.
- Kravene som regelverket i dag setter til uavhengighet er på et forholdsvis overordnet nivå (ref. avsnitt 3.1). I forbindelse med nye utbyggingsløsninger, ikke minst knyttet til eDrift / integrerte operasjoner, kan det være behov for å konkretisere og operasjonalisere disse uavhengighetskravene. Videre arbeid med å utarbeide fornuftige funksjonelle krav innen dette området vil derfor være hensiktsmessig.
- Innenfor integrerte operasjoner er det viktig å spesifisere hvilke komponenter som skal omfattes av uavhengighetskravet, og hvorvidt det er behov for å sette eventuelle SIL (eller tilsvarende) krav til nye systemer og funksjoner. Det kan i denne sammenheng nevnes et prosjekt innenfor Petromaks programmet – ”Secure Safety” – der man tar sikte på å etablere en metodikk og praktiske løsninger (tilsvarende SIL) for å kunne identifisere og etablere tillit til funksjoner og komponenter som kan beskytte integriteten til SIS mot security-relaterte trusler.

2. Innledning

2.1 Bakgrunn

Sikkerhetssystemene offshore blir stadig mer ”koblede”, for eksempel ved at samme produsent leverer kontroll og sikkerhetssystemer, bruk av felles software og brukergrensesnitt i ulike systemer, bruk av felles hardware slik som felles nettverk, økt signaloverføring mellom systemer, økt bruk av integrerte operasjoner, osv.

Med andre ord vet vi at det eksisterer en rekke avhengigheter og koblinger mellom sikkerhets-systemene i petroleumsindustrien. Den teknologiske utviklingen har ført til en gradvis aksept av dette, uten at vi fullt ut klarer å beskrive de mulige konsekvensene av den avhengigheten som er innført.

Petroleumstilsynet har derfor bedt SINTEF om å beskrive status på dette området og se nærmere på hvorvidt de koblinger som er innført er akseptable. Spesielt ønsker en å fokusere på effekten av integrerte operasjoner i forhold til om dette medfører ytterligere avhengigheter og/eller forsterker eksisterende forhold.

2.2 Målsettinger

Målsettingene med dette prosjektet er følgende:

- Definere begrepet ”uavhengighet” (funksjonelt/geografisk, etc.), og deretter si noe om hvorfor dette prinsippet er så viktig rent sikkerhetsmessig.
- Gi en kort statusbeskrivelse av hvordan Ptils krav til uavhengighet mellom tekniske barrierer er implementert på norsk sokkel. Gi eksempler på tilfeller der avhengigheter eksisterer.
- Forsøke å beskrive kvalitativt mulige konsekvenser og effekter av disse avhengighetene.
- Belyse hvordan økt bruk av integrerte operasjoner /eDrift kan påvirke mulige koblinger mellom systemer / barrierer.
- Beskrive utfordringer og videre arbeid innenfor dette området.

2.3 Rapportens innhold

Kapittel 1 gir et sammendrag av hovedkonklusjonene fra arbeidet og beskriver utfordringer og mulig videre arbeid innenfor området.

I kapittel 3 har vi diskutert uavhengighetsbegrepet og en del andre beslektede begreper. Det er videre angitt et mulig skjema for å klassifisere ulike typer avhengighet. Det er dessuten gitt eksempler på hvordan en tenker rundt uavhengighet innenfor andre industrier.

Som en del av prosjektet har det blitt gjennomført telefonintervjuer med en del utvalgt fagpersonell. Kapittel 4 oppsummerer resultatene fra disse intervjuene, hvor det spesielt ble fokusert på å gi eksempler på ulike avhengigheter og koblinger mellom systemer. Mulige konsekvenser og effekter av disse avhengighetene er dessuten diskutert.

I kapittel 5 er det sett nærmere på hvorvidt økt bruk av integrerte operasjoner / eDrift kan endre dagens bilde, ellers sagt på en annen måte: vil potensialet for avhengigheter bli større, uendret eller mindre?

I kapittel 6 er det diskutert ulike analytiske tilnærminger for å vurdere uavhengighet.

2.4 Forkortelser

B&G	-	Brann og gass
BOP	-	BlowOut Preventor
CCTV	-	Close Circuit Television
FPSO	-	Floating Production, Storage and Offloading
IP	-	Internett Protokoll
LAN	-	Local Area Network
NAS	-	Nødavstengningssystem
NDE	-	Normally de-energised (normalt spenningløst)
NE	-	Normally energised (normalt spenningssatt)
OPC	-	Object linking and embedding for Process Control
OS	-	Operatørstasjon
PALL	-	Prosess Alarm Lav Lav
PAS	-	Prosessavstengningsystem
PRA	-	Probabilistic Risk Assessment (brukes blant annet innenfor kjernekraft)
PROSS	-	Prosess kontrollsystemet
QRA	-	Quantitative Risk Assessment (brukes blant annet innenfor offshore)
SAS	-	Safety and Automation System
SIS	-	Safety Instrumented System
VLAN	-	Virtual Local Area Network
VNC	-	Virtual Network Computing
WLAN	-	Wireless Local Area Network

3. Begrepsavklaringer og definisjoner

3.1 Hva mener vi med uavhengighet?

I Ptils styringsforskrift, § 1, er det stilt krav om "tilstrekkelig" uavhengighet mellom sikkerhets-barrierer. I veiledningen til § 1 utdypes dette som følger:

> *Kravet til uavhengighet som nevnt i tredje ledd, innebærer at flere viktige barrierer ikke skal kunne svekkes eller settes ut av funksjon samtidig, blant annet som følge av en enkelt feil eller en enkelt hendelse*.

I innretningsforskriftens § 31-33 brukes det følgende formulering om krav til uavhengighet (gjelder for B&G, NAS og PAS):

> *Systemet skal utføre tiltenkte funksjoner uavhengig av andre systemer*.

I veiledningen blir dette utdypet med at

> *Systemet kommer i tillegg til systemer for styring og kontroll og andre sikkerhetssystemer*

og:

> *Systemet kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket som følge av systemsvikt, feil eller enkelthendelser i disse systemene.*

Også IEC 61508-1(§ 7.5.2.4, punkt d) og ISO 10418 (§ 6.2.5 og 6.2.9) har krav om at sikkerhetssystemene skal være separat og uavhengig fra prosesskontrollsystemet.

I internasjonale standarder er det vanligvis avhengighet som defineres. Eksempelvis benytter IEC 61508 følgende definisjon av avhengige feil:

> *Failure whose probability cannot be expressed as the simple product of unconditional probabilities of the individual events which caused it. (Note – two events A and B are dependent, where P(z) is the probability of event z, only if: P(A and B) > P(A) · P(B)).*[1]

Dersom vi skal overføre definisjonene ovenfor til et generelt krav til uavhengighet for sikkerhets-systemer, foreslås følgende formulering:

> *Med uavhengighet mellom systemer menes at funksjonaliteten i et system ikke påvirkes (negativt) av feil eller svikt i ett eller flere andre system*

Eller som det står i veiledningen til § 1 i styringsforskriften; en enkelt feil eller hendelse skal ikke kunne påvirke flere barrierer samtidig. Dersom flere barrierer kan påvirkes samtidig er ikke barrierene lenger uavhengige.

---

[1] Normalt vil sammenhengen være slik, dvs. at det er en "positiv avhengighet", men i prinsippet kan man også ha en "negativ avhengighet". Den generelle betingelsen for *avhengighet* er derfor P(A og B) ≠ P(A) · P(B).
Matematisk kan vi da si at *uavhengighet* mellom to hendelser A og B krever at P(A|B) = P(A) og P(B|A) = P(B), noe som betyr at hendelse A ikke påvirker sannsynligheten for at hendelse B skal inntreffe og motsatt.

3.2 Klassifisering av avhengighet

Hvordan kan vi vite om kravet til uavhengighet er oppfylt? Eneste måte er å påvise at det ikke finnes avhengigheter mellom systemene, eller at de som finnes er identifisert og vurdert som akseptable.

Det er altså behov for systematisk identifikasjon av mulige avhengigheter, noe som er lettere å få til dersom vi vet hva vi skal lete etter. Til dette har vi behov for og nytte av å kunne klassifisere avhengighet.

En mulig slik klassifisering av avhengighet (tilpasset fra en retningslinje for risikoanalyse av kjernekraftanlegg, /4/) er følgende:

1. *Funksjonell avhengighet*, dvs. et system er avhengig av et annet system for å fungere, eller et system behøves kun dersom et annet system feiler.
2. *Fysisk avhengighet*, dvs. at feil i ett system oppstår pga. feil i et annet system (også betegnet som kaskadefeil).
3. *Utstyrsavhengighet*, dvs. at samme komponent eller modul inngår i flere systemer.
4. *Felles lokalisering* som gjør at systemene kan utsettes for felles påvirkning fra enten omgivelser (ytre påvirkning) eller operativt personell (menneskelig påvirkning).

Disse kategoriene er ikke gjensidig utelukkende, men kan være til hjelp ved identifisering av mulige avhengigheter mellom systemer.

Funksjonelle avhengigheter mellom systemer (1) er ofte både åpenbare og nødvendige, mens fysiske avhengigheter (2), utstyrsavhengighet (3) og avhengighet pga felles lokalisering (4) – for eksempel felles kabelgate eller samme prosessbetingelser - ofte kan være vanskelig å avdekke. Dessuten er de i høyeste grad uønsket fra et sikkerhetssynspunkt (selv om det riktignok kan være designmessige, økonomiske og/eller andre fordeler med slike løsninger).

3.3 Hvorfor er uavhengighet så viktig?

3.3.1 Forsvar i dybden

Det har opp gjennom tiden blitt benyttet ulike sikkerhetsstrategier for å oppnå en akseptabel risiko knyttet til farlige virksomheter. En av disse strategiene er ”avstand”, dvs. å legge risikofylte virksomheter langt fra befolkningssentra, som for eksempel å legge produksjon av kjernefysiske våpen til ørkenområder. En annen strategi er å benytte ”fail safe” prinsippet dersom teknologien ikke er for kompleks. En slik strategi forutsetter at man kan identifisere alle feil som inntreffer, og innrette seg slik at prosessen går til sikker tilstand ved feil.

I noen tilfeller kan man verken benytte seg av ”avstand” eller ”fail safe” prinsippet, og et mye brukt alternativ er da å benytte multiple sikkerhetsbarrierer, også kalt ”*forsvar i dybden*”. Dette ble bl.a. innført i kjernekraftindustrien da man gikk over fra produksjon av kjernefysiske våpen til også å produsere kjernekraft.

Filosofien bak ”forsvar i dybden” er at enkeltbarrierer kan svikte, men dersom man har mange lag med barrierer vil sannsynligheten for at disse skal svikte samtidig være svært liten *dersom barrierene er uavhengige*. Uavhengighet er med andre ord en forutsetning for at denne sikkerhetsstrategien skal virke. I ytterste konsekvens – ved fullstendig avhengighet mellom barrierene – er systemet med multiple barrierer ikke sikrere enn én enkelt barriere.

3.3.2 Diagnostiserbarhet og styrbarhet

Perrow /5/ har undersøkt en rekke store ulykker som har skjedd i forskjellige typer industrier. Utgangspunktet var å finne ut hva som skiller teknologier som har stort risikopotensial, og hvorfor noen teknologier er mer ulykkesutsatt enn andre. Perrow mener at det er to dimensjoner som kan brukes for å avgjøre hvor utsatt en teknologi eller et system er for ulykker. Den ene dimensjonen, som Perrow kaller "interaction", har med systemets *diagnostiserbarhet* å gjøre. I korte trekk kan dette knyttes til operatørens (og de tekniske systemers) evne til å kunne diagnostisere situasjonen både ved normale driftsforstyrrelser og ved feiltilstander i systemet.

Det vil være en mengde faktorer som spiller inn på operatørenes evne til å stille en riktig diagnose av systemets tilstand, slik som utdannelse, erfaring, opplæring, tekniske hjelpemidler, osv. Perrow mener imidlertid at graden av kompleksitet i vekselvirkningene mellom ulike deler av totalsystemet (både prosess og tekniske systemer), vil være den viktigste begrensende faktor for hvorvidt en operatør innenfor rimelig tid er i stand til å diagnostisere en feil. Skjulte koblinger og ikke-intuitive tilbakekoblinger er altså faktorer som reduserer diagnostiserbarheten av tekniske systemer og derfor virker ulykkesfremmende.

Den andre dimensjonen i Perrows klassifisering av ulykkesfremmende systemer er "coupling", som blant annet sier noe om operatørens mulighet til å styre systemet i en ønsket retning i tilfelle en feilsituasjon. Dersom en operatør er i stand til å diagnostisere hva som er feil i et system, er det ikke dermed gitt at han er i stand til å styre systemet dit han vil (for eksempel til sikker tilstand), dersom det er sterke koblinger mellom systemer. Slike koblinger virker med andre ord inn på systemets *styrbarhet*.

Diagnostiserbarhet og styrbarhet[2] er dermed sikkerhetsmessig viktige egenskaper ved et system, egenskaper som svekkes ved å innarbeide koblinger mellom de ulike (del)systemene. Uavhengighet medfører ingen eller et lite antall koblinger mellom systemer og gjør det derfor enklere å diagnostisere systemene og styre dem til en ønsket tilstand.

3.4 Andre beslektede begreper

Vi vil i dette avsnittet diskutere en del relaterte begreper og se nærmere på forholdet mellom disse begrepene og uavhengighet.

Fellesfeil

"Fellesfeil" (eng.: common cause failure) ble i /7/ definert som følger:

- *Feil på to eller flere (redundante) komponenter som har samme årsak, og som skjer innenfor et begrenset tidsintervall.*

IEC 61508, /2/, benytter følgende definisjon av "common cause failure":

- *Failure, which can result in one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure.*

Dersom vi holder disse definisjonene opp mot definisjonen av avhengighet, ser vi at avhengighet er et mer generelt begrep enn fellesfeil. Vi kan med andre ord ha avhengighet uten at det nødvendigvis er fellesfeil involvert.

[2] Diagnostiserbarhet og styrbarhet er begge begreper med en matematisk stringent definisjon innen Kybernetikken /6/. Teorier om disse krever imidlertid at en har en (lineær) dynamisk matematisk modell som beskriver systemet.

Funksjonell og fysisk avhengighet er eksempler på typer av avhengighet som kan gi avhengige feil (for eksempel kaskadefeil), men hvor disse ikke har samme feilårsak (feil i komponent A gir feil i system B, som så gir feil i system C. Det er altså system B som er årsak til feil i system C, ikke komponent A).

Utstyrsavhengighet og avhengighet pga. felles lokalisering er eksempler på avhengighet som leder til fellesfeil (for eksempel vil feil i felles komponent A kunne resultere i fellesfeil i system B og C.) Dette er imidlertid en noe ”rund” fortolkning av begrepet fellesfeil.

Redundans og diversitet

Redundans og diversitet er gitt følgende definisjoner i IEC 61508:

- ***Redundancy.*** *Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information.* *(Note 1 – Redundancy is used primarily to improve reliability or availability. Note 2 – The definition in IEV 191-15-01 is less complete.)*

- ***Diversity.*** *Different means of performing a required function.*

Diversitet kan ses på som ett (av flere) tiltak for å forhindre uønsket avhengighet og påfølgende muligheter for fellesfeil. I begrepet *diversitet* legger vi at redundante komponenter er funksjonelt ulike, for eksempel ved at prosessen stenges ned via to ulike systemer, eller ved at to ulike måleprinsipper benyttes for å lese av nivået i en væsketank. Dette etterstrebes også for multiple barrierer ved ”forsvar i dybden”. De bør helst være forskjellig av natur. Internt i en og samme barriere kan det imidlertid også benyttes redundans med enten identiske komponenter eller komponenter med diversitet. Eksempel på det siste kan være kombinert bruk av røyk- og flammedetektorer for å få bedre branndeteksjon.

3.5 Hvordan tenker man innenfor andre industrier?

3.5.1 Kjernekraftindustrien

Innenfor kjernekraftindustrien er sikkerhetsprinsippet med ”forsvar i dybden” svært sentralt, og det er en kjent sak at for at dette skal kunne fungere etter hensikten betinger det ”tilstrekkelig” uavhengighet mellom de enkelte barrierene. Det legges derfor stor vekt på grundige analyser av avhengige feil i kjernekraftindustrien. En slik analyse består grovt sett av følgende hoved-elementer:

- *Identifisering*
- *Kvantifisering*
- *Reduksjon*

Analyse av avhengige feil som en separat og sentral del av en risikoanalyse av kjernekraftanlegg ble innført allerede ved etableringen av dagens risikoanalysemetodikk (PRA – Probabilistic Risk Assessment), i forbindelse med The Reactor Safety Study i 1975, ref. /8/. Siden en PRA er tilstrekkelig detaljert til å inkludere alle sikkerhetssystemer/barrierer eksplisitt, kan også (i teorien) ”alle” avhengigheter avdekkes, modelleres og kvantifiseres. Det er imidlertid en stor utfordring å identifisere alle disse avhengighetene.

I en PRA for kjernekraftindustrien er en separat analyse av avhengige feil like sentral som konsekvensmodelleringen er i en QRA for prosess- eller offshoreindustrien.

Tross dette har noen av de alvorligste hendelsene i kjernekraftindustrien i den vestlige del av verden (vi ser bort fra Chernobyl) oppstått som følge av avhengige feil. Dette gjelder bl.a. (ref. /4/):

1. Feil i alle de tre redundante fødevannspumpene ved Three Mile Island kjernekraftverk, pga. at innløpsventilene ikke ble åpnet etter vedlikehold (fellesfeil type 4, jfr. kap. 3.2);
2. Feil påføring av isolasjonsmateriale førte til overoppheting og samtidig feil i tre trykkavlastningsventiler ved Vermont Yankee kjernekraftverk (fellesfeil type 4, jfr. kap. 3.1);
3. Pakningsbrudd i hjelpevannsystemet førte til vannspray som resulterte i feil i trykkbryter ved Brunswick kjernekraftverk (avhengig feil type 2 – kaskadefeil, jfr. kap. 3.1).

Disse og andre erfarte fellesfeil/avhengige feil, har bl.a. ført til designendringer, som for eksempel krav om at ikke alle sentrale kabler til et viktig sikkerhetssystem/barriere ligger i samme kabelgate.

3.5.2 Romfartsindustrien

Innen romfart har man arvet mye av tenkningen fra kjernekraftindustrien, i alle fall hva angår risikomessig håndtering av avhengigheter.

Også her er det erfart alvorlige hendelser som følge av fellesfeil, for eksempel (ref. /9/):

1. Hydrazinlekkasje som førte til brann i to APU (Auxiliary Power Unit) enheter i området ved innfestingen av haleroret i romfergen Columbia;
2. Feil i to O-ringer som førte til gjennomblåsing av varm gass i en faststoffsrakett til romfergeflyvning 51L;
3. Feil i to redundante kretskort pga. elektrostatisk sjokk fra vedlikeholdspersonell under utskifting av en tilliggende enhet.

En systematisk identifisering av sårbarhet for fellesfeil anbefales gjennomført som del av en PRA, basert på bruk av såkalte ”koplingsfaktorer” /9/. Koplingsfaktorer antas å eksistere når to eller flere komponenter har tilsvarende karakteristika mht. feilårsak og feilmekanisme. Det letes da systematisk etter komponenter som deler en eller flere av følgende forhold:

- Samme design/type/leverandør
- Samme hardware
- Samme funksjon/bruk/initiell driftstilstand (normalt lukket, normalt åpen, ”energized”, etc.)
- Samme installasjons-, vedlikeholds- eller operativt personell
- Samme prosedyrer (testprosedyrer, effekt av test på systemoperasjon, testkonfigurasjon)
- Samme system-/komponentgrensesnitt
- Samme lokalisering (lokaliseringsnavn, lokaliseringskode)
- Samme miljø/betingelser (temperatur, strømningsrate, vibrasjon, etc)

Basert på sjekklister over koplingsfaktorer kan komponenter som er sårbare for avhengige feil identifiseres.

3.5.3 Flyindustrien

Flyindustrien har i likhet med romfart og kjernekraft problemer med å benytte "fail safe" som sikkerhetsstrategi (et fly i lufta kan ikke bare "stenge ned"). Heller ikke et kjernekraftanlegg har momentan nedstengning som "sikker tilstand" – det må kjøres gradvis og kontrollert ned.

Forsvar i dybden og utstrakt bruk av redundans er derfor også svært sentralt innen luftfart. Likevel har en også her erfart flere ulykker som følge av fellesfeil, for eksempel:

1. Multippel motorfeil i en Fokker F27 i 1997
2. Multippel motorfeil i en Boeing 747 i 1992
3. Feil i tre hydraulikksystem i en DC10 i 1989 som følge av feil i motor nr. 2

I et såkalt "Advisory Circular" (AC 23.1309-1C, 1999) fra Federal Aviation Administration (FAA) står det følgende om analyse av fellesfeil (fritt oversatt):

> ***Fellesfeilanalyse:*** Aksept av tilfredsstillende sannsynlighet for feiltilstander er ofte basert på vurderinger av multiple systemer under forutsetning av at feilene er uavhengige. Det er derfor nødvendig å erkjenne at slik uavhengighet ikke behøver å eksistere i virkeligheten, og at spesifikke studier må gjennomføres for å sikre at uavhengigheten enten kan garanteres eller anses som akseptabel. "Fellesfeilanalysen" består i 3 typer av undersøkelse/analyse:
>
> ***Områdesikkerhetsanalyse (Zonal Safety Analysis):*** Denne analysen har til hensikt å sikre at utstyr som installeres innenfor hver sone i flyet har en fullgod sikkerhetsstandard mht. design og installasjonsstandarder, forstyrrelse (interference) mellom systemer, og vedlikeholdsfeil.
>
> ***Særskilt risikoanalyse (Particular Risk Analysis):*** Særskilt risiko er definert som de hendelser eller påvirkninger utenfor systemene som betraktes (for eksempel brann, lekkasjer, kollisjon med fugl, dekkeksplosjon, lyn, etc.) Hver risiko bør studeres for å avdekke og dokumentere simultane effekter, kaskadeeffekter, eller andre påvirkninger som kan forhindre uavhengighet.
>
> ***Analyse av felles feilmode (Common Mode Analysis):*** Denne analysen gjennomføres for å underbygge/bekrefte antakelsen om uavhengighet mellom hendelser som i kombinasjon leder til en gitt feiltilstand. Effekten av spesifikasjon, design, implementering, installasjon, vedlikeholdsfeil, produksjonsfeil, miljøfaktorer utover de som ble betraktet i den særskilte risikoanalysen, og feil i systemkomponenter bør vurderes.

Det må altså gjennomføres systematiske analyser av avhengighet for å kunne bedømme om systemene er "tilstrekkelig" uavhengige. Dette er relevant for spørsmålet om hvorvidt regelverkskravene til uavhengighet er oppfylt (jf. Styringsforskriften § 1 og Innretningsforskriften § 31-33). Det er vanskelig å se at det er mulig å besvare dette spørsmålet uten at det gjennomføres systematiske og grundige analyser av avhengighet.

4. Statusbeskrivelse

Vi vil i dette kapittelet forsøke å gi en beskrivelse av hvordan regelverkets krav til uavhengighet er implementert innenfor petroleumsindustrien. Som en del av dette gis det en rekke eksempler på avhengigheter som eksisterer per i dag. På slutten av kapitlet er dessuten mulig konsekvenser og effekter av de ulike avhengighetene nærmere diskutert. Kapittelet er primært basert på følgende input:

- Intervjuer med fagfolk hos leverandører, operatører, engineeringselskap og konsulenter;
- SINTEFs egne erfaringer fra ulike prosjekter.

4.1 Oppsummering fra intervjuer med fagfolk

Telefonintervjuer har blitt gjennomført med utvalgt fagpersonell, 9 i tallet. I dette avsnittet oppsummeres hovedinntrykkene fra disse intervjuene.

Intervjuene ble primært brukt til å diskutere eksempler på avhengigheter eller koblinger mellom systemer som fagfolkene kjente til. Det ble også diskutert mulige konsekvenser av disse avhengighetene, samt hvorvidt myndighetskravene til uavhengighet oppfattes som klare nok.

Synspunkter på integrerte operasjoner / eDrift og tilhørende tekniske løsninger som kom fram under intervjuene, er innarbeidet i kapittel 5.

4.1.1 Eksempler på avhengigheter og koblinger

I løpet av intervjuene kom det frem flere eksempler på avhengigheter og koblinger mellom systemer. Noen eksempler gikk igjen i flere intervjuer, og dette er forsøkt påpekt i de tilfeller det gjelder.

Koblinger – PROSS og PAS

Flere av fagfolkene satte fokus på avhengigheter mellom kontroll- og prosessnedstengnings-systemene. Det ble hevdet at PAS ses på som en forlengelse av kontrollsystemet (PROSS) og at holdningene til PAS som en egen barriere til en viss grad er noe ”frynsete”.

På den annen side ble det også trukket fram at disse to systemene er nært sammenknyttet rent funksjonelt - dersom prosesstyringen svikter skal PAS-systemet aktiveres. Hvis for eksempel kontrollventilene inn til en separator feiler i åpen tilstand, skal PAS-systemet stenge inne separatoren på høyt nivå (eller trykk). Denne tette koblingen medfører også at PAS-funksjoner kan komme i konflikt med PROSS-funksjoner, spesielt i oppstartssituasjoner.

Konkrete avhengigheter mellom de systemene som ble nevnt, var:

- *Tillatelse til å midlertidig koble ut PAS funksjoner (som PALL) fra kontrollsystemet*:
  Dette gjelder for eksempel i forbindelse med oppstart av pumper og kompressorer;
- *Bruk av samme type hardware/software*:
  Topside PAS implementeres med egen logikk, men ofte med samme software som PROSS og kjøres på samme nett. Det er også utstrakt busskommunikasjon mellom PAS og PROSS;
- *Implementering av alle PAS funksjoner i PROSS*:
  For undervannsapplikasjoner er det standard design at PAS er implementert i

kontrollsystemet (uten egen logikkboks). PAS er dermed en del av PROSS og håndteres deretter, selv om den kan ha PAS-funksjoner implementert;

- *Delvis implementering av PAS funksjoner i PROSS*:
  Det finnes eksempler på sammenblanding av prosessikrings- og kontrollfunksjoner ved kompressorstyring. Her er det en del uklarhet rundt hva som er utstyrbeskyttelse og hva som er PAS-funksjoner og hvordan dette er implementert fra leverandørene. Dette er også tilfelle for brønnhodekontroll.

Koblinger – PAS og NAS
Flere eksempler på koblinger mellom disse to systemene ble nevnt, blant annet følgende:

- *Felles komponenter i felt:*
  Felles NAS- og PAS-ventiler er en velkjent og lite kontroversiell praksis. Dette kan imidlertid medføre andre, mer skjulte avhengigheter mellom komponenter i ventilkontrollpanelet. En har sett designløsninger som er slik at komponenter i PAS-funksjonen må fungere for at NAS-funksjonen skal fungere (og motsatt). Solenoider / piloter satt i serie er et typisk eksempel på dette;
- *NAS funksjoner i PAS*:
  På flere plattformer hvor en kjører med slukket fakkel er systemet for tenning av denne ifm. blowdown) lagt i PAS-systemet. En har dermed lagt en del av en NAS-funksjon (blowdown) i PAS;
- *Tilbakemeldinger for NAS funksjoner lagt i PAS*:
  Det er vanlig at signaler fra endebrytere i NAS går via PAS (eller PROSS). I en nødsituasjon hvor en har mistet kraft (for eksempel til et lokalt utstyrsrom som inneholder en PAS-node), vil operatørene miste kontroll over status/ posisjon til NAS-ventilene;
- *PAS aktiverer NAS-funksjoner*:
  Det finnes en del eksempler på at funksjoner i NAS aktiveres fra signal i PAS. Et eksempel er ved svikt / lekkasje i tetningsgass for kompressor, hvor PAS kan aktivere blowdown.

Koblinger mellom andre sikkerhetskritiske systemer og funksjoner
Flere eksempler på koblinger mellom andre systemer ble også nevnt, blant annet følgende:

- *Sjøvann versus brannvann:*
  På flere installasjoner bruker en sjøvannspumpene også som brannvannspumper. Dette medfører nødvendigvis koblinger mellom B&G-systemet og prosesskontrollsystemet;
- *Ballaststyring versus ballastsikring:*
  Når det gjelder marine systemer, ble ballastsystemet spesielt nevnt fordi dette fungerer både som kontroll- og sikkerhetssystem. Vanlig ballastering er en kontrollfunksjon mens nødballastering er en sikkerhetsfunksjon, men en bruker likevel de samme systemene og komponentene (for eksempel samme ventil). Dette er dermed et eksempel på sammenblanding av en kontrollfunksjon og en sikkerhetskritisk funksjon;
- *PROSS versus NAS:*
  I forbindelse med oppstart av kompressorer kan en få behov for å overbroe NAS-signaler ved at en bruker blowdown ventiler til å kontrollere trykket under oppkjøring (både åpne og tvinge til stengt);
- *Brannvann versus stabilitetskontroll*:
  På flytende installasjoner har en identifisert at operasjon av brannvannspumpene i en nødsituasjon kan utgjøre en risiko i forhold til stabilitet. I en nødsituasjon skal brannpumpene fortsette å kjøre så lenge som mulig. I tilfelle en skade og større lekkasje på hovedbrannledningen kan en imidlertid pumpe så mye vann ut i skroget at dette kan

medføre vannfylling og i verste fall tap av stabilitet. En har derfor installert en egen måling som skal detektere slik vannfylling og som stopper brannvannspumpene. En innfører dermed en kobling som medfører at en feil i målingen i verste fall kan stoppe brannvannspumpene;

- *HVAC versus B&G*:
  En har også sett koblinger mellom B&G og HVAC-systemene, for eksempel i forbindelse med aktiv røykkontroll;
- *Plattformsystemer versus boresystemer*:
  En annen "gråsone" er boring og grensesnittet mellom boresystemer og andre plattformsystemer. Som eksempel ble nevnt wireline/workover BOP hvor alt "henger" på samme hydraulikk og strøm, og hvor systemene er normally de-energized. Videre er det slik at en under en boreoperasjon har mulighet til å hindre at NAS kan ta spenningen (en må slå manuelt over).

Det kan bemerkes at når en har slike koblinger som beskrevet over, er det svært vanskelig å designe de ulike deler av SAS som uavhengige enheter.

Operatørstasjoner (OS) og kommunikasjon – integrerte systemer

Mange av de intervjuede fagfolkene trakk fram felles operatørstasjoner (OS) for kontroll og sikkerhetssystemer som en gråsone. En relatert problemstilling som også ble nevnt, var bruk av storskjermer for alarm- og statuspresentasjon. Felles OS for kontroll- og sikkerhetssystemer er i ferd med å bli standard, og fra en og samme OS kan man gå inn og modifisere settpunkter og andre parametere, også i sikkerhetssystemene. De samme operatørstasjonene brukes dessuten gjerne til alarmpresentasjon. Storskjermer kan se ut til å ta over for direkte koblede ("hardwired") statussignaler som tidligere ble presentert i matriser og mimikk. Det at disse operastørstasjonene og storskjermene som skal erstatte matriser og mimikk gjerne er basert på Windows teknologi, utgjør en ekstra usikkerhet.

Det ble også påpekt økt bruk av felles nett og felles feltbuss for kontroll- og sikkerhetsfunksjoner. Dette gjelder statusinformasjon, men også aksjoner som går over buss. Det ble framhevet at det generelt er verre å holde oversikt over signaler som overføres via buss enn direkte koblede signaler ("hardwired"), da det ofte ikke er like klare I/O lister for signaler som går via kommunikasjon.

Denne typen integrasjon av kontroll- og sikkerhetsfunksjoner, gjør at systemene får flere felles "komponenter" slik som programvare og drivere. I denne forbindelse er det viktig at disse felles komponentene ikke på noen måte kan påvirke sikkerhetsfunksjonene negativt. SINTEF mener at det er to krav som må tilfredsstilles for at forskjellige funksjoner som implementeres i disse systemene kan behandles som uavhengige:

- Operatørstasjonen må ikke utilsiktet kunne endre funksjoner i de enhetene (prosesstasjonene) der sikkerhetsfunksjonene er implementert;
- En slik prosesstasjon må ikke utilsiktet kunne endre funksjonen i en annen.

For SIL-sertifiserte systemer som installeres i dag, finnes det som regel et tilhørende utsagn om "non-interference", dvs. at feil i det ene systemet ikke påvirker det andre systemet negativt.

Den Windows-baserte OPC-protokollen brukes for å hente informasjon ut av systemene og for å utveksle informasjon mellom forskjellige systemer. I utgangspunktet skal dette være et rent administrativt system, og enkelte uttrykte bekymring over at denne tunge kommunikasjons-protokollen også brukes for å realisere enkelte sikkerhetsfunksjoner (for eksempel PAS aksjoner) i tillegg til at det er et rent administrativt system.

Standardisering i prosjektene
Ønsket om størst mulig grad av standardisering og gjenbruk i prosjektene, samt ønsket om å begrense antallet leverandører, ble av flere trukket fram som en faktor som medfører økte avhengigheter. Sikkerhetssystemleverandørene leverer for eksempel ofte komplette SAS-systemer som inkluderer alle SIS samt prosesskontrollsystemet. Hvert system er typisk implementert med egne noder, men er basert på identisk type software og hardware.

Ønsket om standardisering og best mulig funksjonalitet går dermed på bekostning av ønsket om å innføre diversitet mellom systemer og funksjoner (og dermed på bekostning av uavhengighet).

Oppgraderinger av programvare
Feil i programvare kan skape utilsiktede avhengigheter. Flere av fagfolkene nevnte oppgraderinger av programvare som et område hvor en i liten grad føler en har kontroll. Konkrete momenter som ble trukket fram var:

- Engineering og operatører føler seg til en viss grad ”prisgitt” leverandørene i og med at disse partene i liten grad har mulighet til å gå inn og sjekke selve programkoden;
- Ved oppgraderinger av programvare, ”nullstilles” på en måte systemet i og med at installasjonsspesifikke endringer og tilpasninger som tidligere er gjort ikke nødvendigvis kommer med i de nye versjonene. Noe av problemet her skyldes at slike endringer som gjøres under drift ikke blir skikkelig dokumentert og kommunisert tilbake til leverandørene;
- Det samme gjelder ved innføring av nye Windows versjoner;
- Det ble av enkelte stilt spørsmålstegn ved QA i forbindelse med modifikasjoner og endringer av software hos SAS-leverandørene.

4.1.2 Har en kontroll med avhengighetene?

Basert på samtalene med fagfolkene er det klart at det eksisterer avhengigheter mellom kontroll- og sikkerhetsfunksjoner. De avhengigheter som er nevnt, er også de som er kjent, og fagfolkene opplever selv å ha bra kontroll med de kjente avhengighetene. De gangene en for eksempel har I/O signaler som går ”gal vei” (for eksempel fra PAS til NAS), mener fagfolkene at disse løsningene er gjennomtenkt og konsekvensene er nøye vurdert.

Fagfolkene ble også spurt om hva som gjøres for å vise at systemene er ”tilstrekkelig” uavhengige:

- En bruker erfaringene fra tidligere prosjekter og kopierer det som er gjort og som har fungert før (og står dermed i fare for også å kopiere gamle, ukjente ”synder”);
- Det gjøres analyser for å vise at påliteligheten er god nok (blant annet SIL-beregninger). Disse analysene skal inkludere fellesfeilvurderinger;
- Når avhengigheter ”dukker opp” blir disse grundig behandlet i prosjektene.

Ellers er SINTEFs inntrykk at det er noe begrenset hva som gjøres for å påvise og dokumentere uavhengighet mellom systemer og funksjoner. Mangel på gode verktøy og metoder ble trukket fram som en av grunnene til dette.

4.1.3 Andre kommentarer og synspunkter fra intervjuene

Nedenfor oppsummeres en del andre kommentarer og synspunkter som kom fram under intervjuene:

- De fleste fagfolkene mente at myndighetenes krav til uavhengighet stort sett var klare nok;

- Noen etterlyste mer konkrete retningslinjer i forhold til hva som ligger i ”tilstrekkelig” uavhengighet og hva som kreves for å påvise dette;
- Noen kommenterte at det viktigste var å ha en høy pålitelighet, og at uavhengighet for en hver pris ikke nødvendigvis er et mål i seg selv. Uavhengighet må ses på som et praktisk middel for å oppnå høy pålitelighet;
- Dokumentasjon av pålitelighet blir dermed sentralt og inkludering av fellesfeil på en skikkelig måte blir en forutsetning for at regnestykkene kan brukes. Videre blir det viktig å påvise at systemer som antas uavhengige, virkelig er det;
- Dagens QRA modeller tar i liten grad inn avhengigheter mellom systemer;
- Det ble av enkelte fagfolk uttrykt en generell ”bekymring” vedrørende utviklingen som i økende grad må sies å gå på tvers av diversitetsprinsippet; samme type software, samme programmeringsmetode og språk, samme type hardware og felles kommunikasjon.

4.2 Noen flere eksempler på avhengigheter

Som nevnt innledningsvis, eksisterer det ulike avhengigheter mellom sikkerhetssystemene. Noen av disse avhengighetene vil være ”kjente” og kan derfor tas hensyn til i pålitelighets- og risikoanalyser. SINTEFs inntrykk er at slike ”kjente” avhengigheter stort sett kommer opp i prosjektene som en følge av tidligere prosjekterfaringer eller ved at de identifiseres mer ”tilfeldig”. Systematiske vurderinger av nye avhengigheter gjøres i mindre grad.

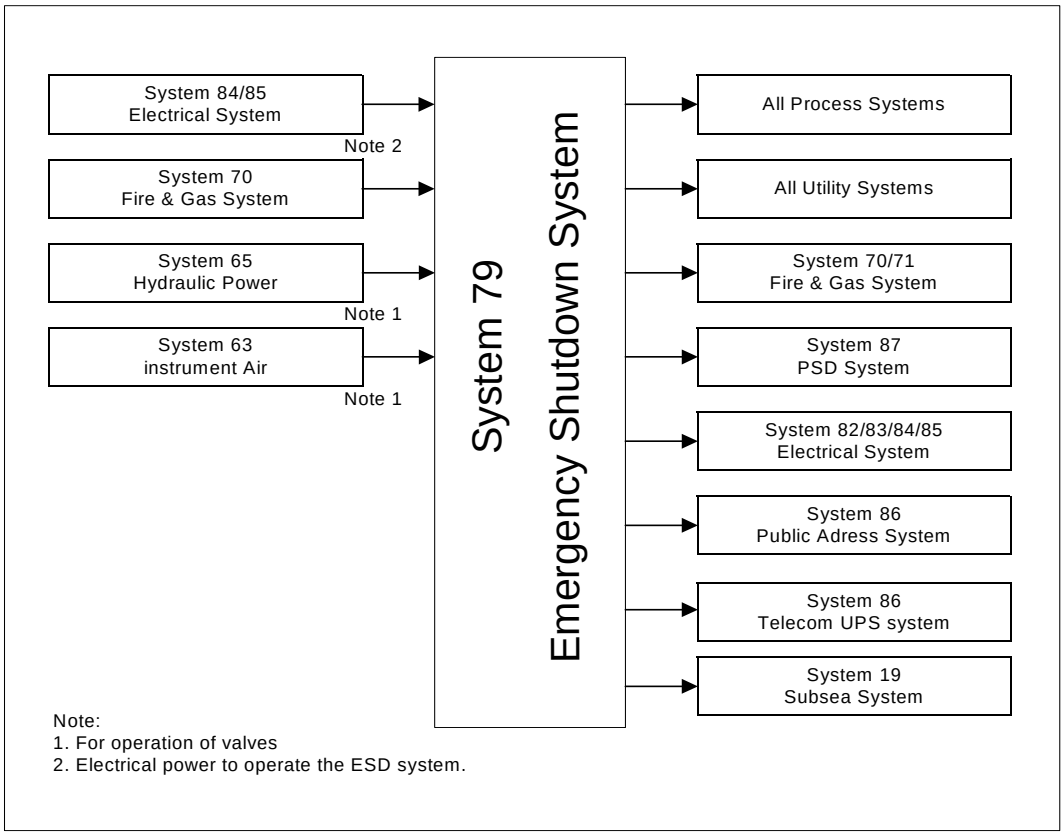
Uten slike systematisk vurderinger, er det sannsynlig at det eksisterer ”skjulte” avhengigheter (det vil si ”ikke kjente”). Det kan være flere årsaker til at avhengigheter ikke er kjent. Avhengighetene kan ligge dypt nede i systemene, for eksempel i en programkode der det kan oppstå avhengigheter i grensesnittet mellom system og operatør, som er vanskelig å få øye på. Det kan også være skulte avhengigheter på et høyere nivå i systemene, enten som funksjonelle avhengigheter eller som avhengigheter innført gjennom måten funksjonene er realisert i design. Årsaker til at avhengighetene er ”skulte” er enten at de ikke er forsøkt identifisert eller at de kan være vanskelige å oppdage selv ved detaljerte gjennomganger.

Vi vil i dette avsnittet ta for oss noen få eksempler på slike avhengigheter.

4.2.1 Eksempler på “kjente” avhengigheter

NAS-systemet

NAS-systemet aktiverer ofte ulike sikkerhetsfunksjoner, slik som segmentering av prosessen, blowdown, start av brannvannspumper, PAS, isolering av tennkilder, osv. Dette betyr at NAS-systemet inngår i flere definerte sikkerhetsbarrierer. Dette er illustrert på figuren under, som er hentet fra NAS spesifikasjonen for et nyere offshore utbygningsprosjekt.



Figur 1 Interaksjon mellom NAS-systemet og andre systemer

I QRA analyser regnes ofte denne typen sikkerhetsbarrierer som uavhengige, eksempelvis NAS seksjonering, aktivering av brannvann og isolering av tennkilder. At NAS-systemet i form av sin logikk og hardware er felles for flere sikkerhetsbarrierer, skaper en avhengighet mellom disse barrierene som sjelden er medregnet i risikoanalysen.

”Bevisst” svekkelse av sikkerhetsfunksjoner

I forbindelse med en del nye konsepter offshore og større anlegg på land, har en sett flere eksempler på at myndighetene har tillatt lempelser i forhold til krav om totalkapasitet for systemer som branndeteksjon, brannvann og blowdown. For eksempel tillates det brannvannsystemer som ikke har tilstrekkelig totalkapasitet til å dekke alle områder, og man løser dette med å tillate områdebasert branndeteksjon og brannvannsutløsning. Et annet eksempel er sekvensiell avlastning av et prosessanlegg fordi en ikke har fakkelkapasitet til å blåse ned alle områdene samtidig.

SINTEF mener at denne typen svekkelser av sikkerhetsfunksjoner kan ha en del betenkelige sider:

- Branndeteksjon har i utgangspunktet en begrenset pålitelighet, blant annet pga. eksponeringssannsynligheten. Områdebasert deteksjon er komplisert, blant annet fordi en må forhindre at branndetektorer oppdager brann i naboområdet. Dette kan derfor medføre en ytterligere svekkelse av denne funksjonen;
- Oppsplitting og sekvensering av funksjoner medfører generelt mer komplisert logikk, som både kan skape tvil om hva som er sikreste tilstand og som kan være en kilde til nye ”ukjente” avhengigheter i og mellom systemer;
- Der sikkerhetsfunksjoner ikke har tilstrekkelig kapasitet, blir man ofte mer ”bekymret” for feilaktig aktivering enn for å sikre aktivering ”on demand”. Dette medfører at man i flere tilfeller forlater tradisjonelle løsninger med ”normally energised” som standard og går

over til systemer der energi må tilføres (”normally de-energised”). Dette medfører en ny type sikkerhetsfilosofi som krever nye vurderinger;
- Det kan stilles spørsmål ved hvorvidt de analysene som benyttes for å påvise at reduksjonene i ytelse er akseptable, er detaljerte nok til å fange opp alle mulige konsekvenser.

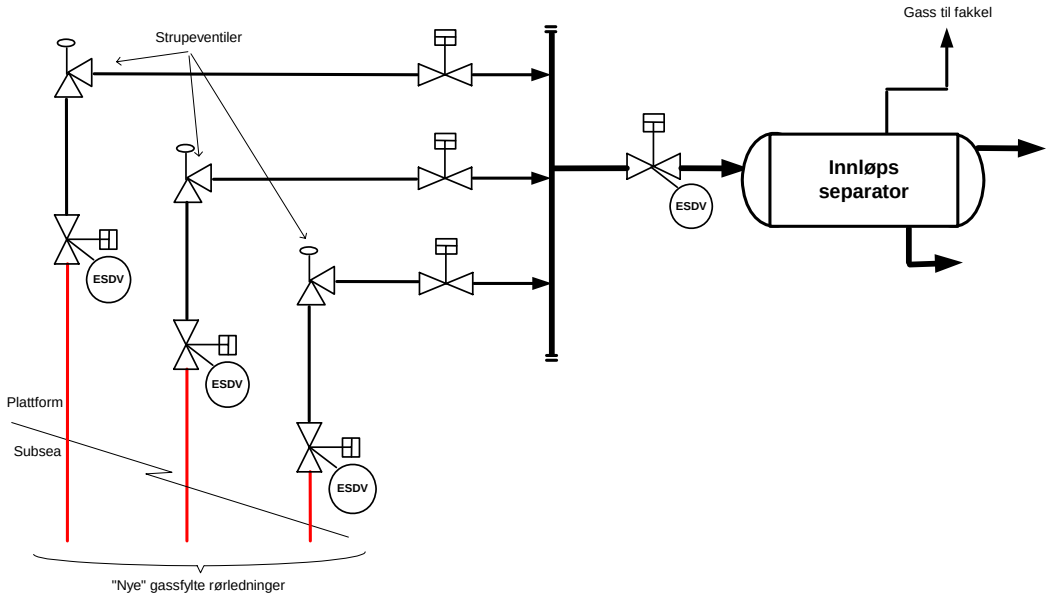
Det er ofte vanskelig å vurdere i hvor stor grad slike løsninger som diskutert over, påvirker graden av uavhengighet, men en innfører uansett ny logikk og nye koblinger som øker kompleksiteten og som reduserer diagnostiserbarheten og styrbarheten til systemene (jfr. avsnitt 3.3.2).

4.2.2 Eksempel på “skjulte” avhengigheter

I det følgende er noen eksempler på skulte avhengigheter diskutert. At de defineres som skjulte begrunnes ut fra at de krever en relativ detaljert analyse for å kunne oppdages.

Tilknytning av satellittfelter

Tilknytning av nye satellittfelter til eksisterende installasjoner er en trend på norsk sokkel. Her kobles nye rørledninger, ofte med høyt trykk og høyt gassinnhold, opp mot gamle plattformsystemer. Et eksempel på en slik situasjon er illustrert på figuren under.



Figur 2 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 slippes 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.

For eksemplet vi her ser på, er det to hovedbarrierer til stede for å unngå overtrykking:

- *Oppstartsprosedyrer,* som i detalj beskriver hvilke prosessbetingelser som skal være tilstede og i hvilken rekkefølge ventiler skal åpnes. Prosessbetingelser skal leses fra sensorer tilknyttet installasjonens kontrollsystem og PAS;
- *Et instrumentert sikringssystem* (i form av "forriglinger"), som ved hjelp av dedikerte sensorer og egen logikk skal hindre operatørene i å feilåpne ventiler.

I forbindelse med en sikkerhetsstudie av dette arrangementet ble det avdekket at når operatørene startet opp ved hjelp av prosedyrer, var det vanlig å bruke statussignaler fra de instrumenterte forriglingene til å verifisere at åpning av en gitt ventil var "tillatt". Resultatet var at det ble innført nærmest full avhengighet mellom de to barrierene som i utgangspunktet var tenkt å være uavhengige (dvs. prosedyrene og det instrumenterte sikkerhetssystemet).

Dette eksemplet illustrerer det faktum at avhengigheter mellom ulike systemer (eller barrierer) ofte er svært godt skjulte. Det var først når de ulike oppstartsskjermbildene ble analysert i detalj, at en fant ut at det var en betydelig avhengighet mellom det instrumenterte sikkerhetssystemet og oppstartsprosedyrene.

4.3 Konsekvenser og effekter

Vi vil i dette avsnittet diskutere mulige konsekvenser og effekter av de avhengighetene og koblingene som er nevnt i avsnitt 4.1 og 4.2. Det vil spesielt fokuseres på hvorvidt feil i ett system kan medføre feil eller påvirke sannsynligheten for (en kritisk) feil i et annet system. For enkelte av aspektene som ble diskutert i avsnitt 4.1.1, slik som for eksempel oppdatering av programvare, er det dessuten viktig å se på hvorvidt en feil kun medfører svikt i enkeltsystemer eller om en også har potensial til å slå ut flere systemer.

4.3.1 Generell diskusjon

Det er vanskelig å si noe generelt om konsekvenser og effekter av de ulike avhengighetene. Et stikkord som imidlertid vil være sentralt, er at avhengigheter medfører økt kompleksitet. Uheldige aspekter ved økt kompleksitet kan være blant annet:

- Det kan (ubevisst) innføres sikkerhetskritiske avhengigheter;
- Under normal drift vil anlegget bli vanskeligere å forstå, operere og ikke minst å vedlikeholde;
- I en nødssituasjon vil det være vanskeligere for operatøren å skaffe seg oversikt over situasjonen og ikke minst oversikt over mulige konsekvenser av ulike aksjoner;
- Ved design, implementering, uttesting og idriftsettelse vil det være vanskelig å identifisere og skille ut de typene feil som har potensial til å forplante seg til andre systemer eller trigge svikt av andre systemer. Under testing er det stort sett fokus på enkeltfunksjoner (eksempelvis sløyfe/loop) og oppretting av enkeltfeil.

Økt kompleksitet vil generelt kreve et godt gjennomtenkt design, der en systematisk vurderer konsekvenser og kompenserende tiltak for avhengigheter. I motsatt fall kan "feilkoblinger" innføres, og disse vil gjerne være vanskelig å identifisere. Ta for eksempel praksisen med felles (dobbeltvirkende) NAS- og PAS-ventiler. En har her sett tilfeller hvor de to solenoidventilene har vært designet slik at NAS-solenoiden må fungere for å få stengt ventilen på en PAS aksjon[3]. Dette vil opplagt ikke være i tråd med regelverkskravet om uavhengighet.

[3] Grunnen til feilen var at en ny type pilot hadde tilbakeslagsventil på forsyningsporten slik at alt så ut som før, selv om endringen kunne være kritisk. Også når en regner på slike løsninger tar en sjelden med feilmoden at piloten låser seg i midtstilling og blokkerer for den andre piloten.

Mange av de koblingene og avhengighetene som er beskrevet i foregående avsnitt, vil være av en slik karakter at feil i det ene systemet trolig vil medføre en stopp eller nedstengning av (det) andre system(et). Dette betinger imidlertid at systemene går til sikker tilstand ved nedstengning, dvs. at de er "fail-safe". For eksempel skal sikkerhetssystemene gå til sikker tilstand hvis de oppdager meldingsstorm på nettet eller en oppdatering via nettet blir forsinket.

For systemer hvor sikker tilstand er å "holde maskineriet i gang", slik som et flytende produksjonsskip (eller et fly), kan imidlertid koblinger og avhengigheter mellom systemer være mer kritisk fordi det ikke bare er å stenge ned ved en feil i det ene systemet. En kan da ende opp i situasjoner der en mister oversikt over hva som er status på enkelte systemer og hvilken tilstand en faktisk er i. For eksempel på en FPSO vil det være slik at prosessanlegget skal stenges ned i tilfelle en nødsituasjon, mens en samtidig er avhengig av å holde i gang andre deler av installasjonen. Dette aspektet er litt nærmere diskutert i avsnitt 4.3.3.

4.3.2 Mulige konsekvenser av spesifikke koblinger

Vi vil i dette avnittet diskutere mulige konsekvenser knyttet til noen av de spesifikke koblingene og avhengighetene fra avsnitt 4.1.1 (det er for oversiktens skyld stort sett brukt de samme overskriftene som i dette avsnittet). Diskusjonen knytter seg først og fremst til "fail-safe" løsninger, der det er tilstrekkelig å stenge ned /skru av for å komme til sikker tilstand.

Mulige konsekvenser av koblinger mellom PROSS og PAS

- Ved at PROSS og PAS implementeres med samme type software og hardware, innføres en avhengighet som (i hvert fall i teorien) kan gi en samtidig kritisk feil av de to systemene, for eksempel som følge av en programmeringsfeil. Slike feil kan imidlertid til en viss grad "tas høyde for" ved at en i pålitelighets- og SIL-vurderinger tar begrenset eller null høyde for risikoreduksjon fra kontrollsystemet, og/eller ved at en modellerer inn en høy fellesfeilrate mellom PROSS og PAS;
- Enkelte metoder som brukes for å fastsette SIL tar høyde for funksjoner implementert i PROSS, slik at SIL kan være lavere enn hvis all risikoreduksjonen skal implementeres i sikkerhetssystemet. Det er ikke kjent om slike metoder stiller strengere krav til uavhengighet enn ellers i industrien.
- At undervannsapplikasjoner er implementert med felles PROSS og PAS node vil tilsynelatende kunne øke sannsynligheten for en kritisk prosesshendelse;
- Midlertidig utkobling av PAS funksjoner fra PROSS ved oppstart av pumper og kompressorer er også en kobling som kan være farlig, dersom en svikt i PROSS fører til at PAS utkoblingen blir liggende inne. Her er det godheten av selve designen (for eksempel hvor en plasserer "timer" funksjonen) som i stor grad bestemmer hvor kritisk en slik kobling er. Utover dette bør nevnes at det i OLF-GL, app. G.4.2.1, beskrives som uakseptabelt å koble ut PAS aksjon fra PROSS.

Mulige konsekvenser av koblinger mellom NAS og PAS

- Som diskutert over, vil løsninger hvor feil i ESD solenoiden kan føre til at en kombinert NAS/PAS-ventil ikke lukker på for eksempel høyt trykk, være uakseptable;
- I de tilfeller hvor posisjonstilbakemelding fra NAS går via en PAS node, vil en svikt i PAS kunne medføre at operatøren ikke får tilbakemelding på NAS ventil posisjoner. Siden slik informasjon i gitte tilfeller kan være kritisk, kan en spørre seg om dette er en akseptabel kobling;
- På installasjoner med slukket fakkel hvor tenning av fakkel ligger i PAS-systemet, bør en kunne foreta en nedblåsning uten at fakkel tennes. En må med andre kunne "leve med" at

PAS-systemet feiler, ellers har en innført en kritisk avhengighet mellom PAS- og NAS-systemet.

Mulige konsekvenser av koblinger mellom andre systemer

- Koblinger på grunn av at samme komponent brukes både i regulering/styring og som del av en sikkerhetsfunksjon (for eksempel i ballastsystemet), kan i verste fall medføre at PROSS hindrer sikkerhetsfunksjonen;
- For flere av de andre avhengighetene, slik som mellom sjøvann- og brannvannsystemet og mellom B&G og HVAC systemet, vil den tekniske implementeringen av koblingene være avgjørende for kritikaliteten.

Mulige konsekvenser av felles operatørstasjoner / Windows

- En feil i Windows kan stoppe hele brukergrensesnittet, inkludert storskjermer. Hvis dette skjer i forbindelse med eller som følge av en kritisk hendelse, kan oversikt og krisehåndtering bli svært vanskelig.

Mulige konsekvenser av felles kommunikasjonskanaler

- En av de mest sannsynlige hendelsene på et felles nett er at en enhet belaster nettet så mye at de andre ikke får sendt sine meldinger. Så lenge en kan gå til sikker tilstand ved å skru av, er ikke det nødvendigvis kritisk for sikkerheten, men snarere for produksjons-regulariteten;
- Det blir svært viktig at sikkerhetssystemene ikke kan påvirkes negativt av feil eller andre hendelser på nettet. De fleste leverandører har implementert en eller annen form for beskyttelse mot dette, men det er lite informasjon tilgjengelig og lite åpenhet rundt temaet.

Mulige konsekvenser av standardisering i prosjektene

- Kravene, løsningene og det som implementeres, blir mer og mer likt, fordi tidligere løsninger vanligvis kopieres og gjenbrukes uten at bakgrunnen og implementeringen vurderes på nytt. Dette kan føre til at en ubevisst feil begått på et prosjekt, kan spre seg til andre deler av bransjen.

Mulige konsekvenser av oppgradering av programvare

- En har sett mange eksempler på at oppgradering av software har ført til samtidig feil av flere komponenter. Dette har skyldes feil i den nye programvaren, men har også vært resultat av at feil program har blitt lastet slik at for eksempel tripp punktet på flere sensorer har blitt satt feil;
- Dersom samme programvare benyttes i flere systemer (for eksempel NAS og PAS), kan dette medføre kritiske avhengigheter;
- I utgangspunktet skal modifikasjoner og oppgraderinger holde samme høye nivå som den opprinnelige implementeringen. Erfaring tilsier at dette ikke alltid er tilfelle. Ofte er det annet personell enn de som opprinnelig designet systemene som er involvert i oppgraderingene, og det er dessuten gjerne et press for å komme i gang med produksjonen så fort som mulig;
- Av konfidensialitetsgrunner er det vanskelig å få innsyn i systemleverandørenes rutiner og prosedyrer knyttet til oppgradering av programvare, og hvordan disse rutinene blir fulgt opp.

4.3.3 Funksjoner med annen sikker tilstand enn stopp

En del konsepter og løsninger innenfor petroleumsindustrien er slik at sikker tilstand ikke vil være å foreta en ”normal nedstengningsprosedyre (stenge ned, kutte strøm, trykkavlaste, osv.). Noen typiske slike anvendelser er:

- Fakkelsystemer som krever at prosessen trykkavlastes i sekvens, og hvor samtidig nedblåsning fra hele anlegget kan være en farlig hendelse i seg selv;
- Systemer som ikke er konstruert slik at de automatisk går til sikker tilstand ved svikt (for eksempel NDE utganger på B&G, hvor en må tilføre spenning for å utføre aksjoner);
- Dynamisk posisjonerte og andre fartøy (som FPSO) vil ha dette problemet for den maritime delen av anlegget.

For systemer der sikker tilstand ikke er å stoppe, vil problematikken som er diskutert i forrige avsnitt selvsagt fortsatt gjelde, men i tillegg får en noen nye problemstillinger. For eksempel vil det som har med energitilførsel å gjøre, ofte bli et problem. En kan selvsagt kompensere med bruk av redundans, slik at en har forsyning fra flere steder, men ett sted må alt gå sammen for å kontrollere en bestemt enhet. Selv på skip, der slike krav og løsninger har eksistert i årevis, får en av og til full blackout på grunn av en enkelt feil.

Problemet blir at flere av de feilene som ovenfor ble betraktet som ukritiske fordi en stenger ned, nå *kan* bli farlige feil, og de vil som sådan kunne påvirke de aktive barrierene.

En kan generelt si at dette problemet ikke er så omfattende så lenge regelverk og standarder sørger for at de fleste funksjoner går til sikker tilstand når energitilførselen fjernes. Som diskutert i avsnitt 4.2.1, ser en imidlertid en tendens til at tradisjonelle ”fail-safe” løsninger blir utfordret for å spare kostnader.

5. Uavhengighet mellom sikkerhetssystemer ved integrerte operasjoner

I dette kapitlet vil vi belyse hvordan økt bruk av integrerte operasjoner (eller eDrift) kan påvirke mulige koblinger mellom systemer / barrierer.

5.1 Hva legger vi i integrerte operasjoner / eDrift?

Vi vil i denne rapporten ikke gi oss inn på eksakte definisjoner av begrepene "integrerte operasjoner" og eDrift, men bare konstatere at dette dreier seg om nye driftskonsepter der IKT og sanntidsdata utnyttes til å optimalisere operasjonene på sokkelen. Noen konkrete eksempler på slike løsninger kan være den normalt ubemannede plattformen Huldra, som fjernstyres fra Veslefrikk, de planlagte havbunnsinstallasjonene på Ormen Lange, som skal fjernopereres fra et prosessanlegg på Nyhamna i Møre- og Romsdal, eller BPs landbaserte støttesenter på Forus som blant annet skal effektivisere boreoperasjoner.

I forbindelse med integrerte operasjoner har det vært mye fokus på "security-relaterte" utfordringer knyttet til kommunikasjon, informasjonssikkerhet og sikker og kontrollert fjernaksess til anleggene på sokkelen. På HMS-siden har det i enkelte rapporter, ref. /11/, blitt konkludert med at integrerte operasjoner totalt sett vil kunne ha en positiv effekt på sikkerheten for installasjonen. Dette primært fordi personell flyttes bort fra farekildene, og fordi det totale omfanget av helikoptertransport til og fra installasjonene reduseres[4].

Det har i noe mindre grad vært fokus på de tekniske sikkerhetssystemene, men det bør ligge en implisitt forutsetning og målsetning om at systemene i hvert fall ikke skal bli dårligere når en flytter deler av styring og kontroll inn til land (eller til en annen installasjon). Dette betyr igjen at kritiske avhengigheter mellom de ulike systemene ikke bør øke signifikant ved overgang til integrerte operasjoner.

5.2 Tekniske løsninger knyttet til integrerte operasjoner

Det kan i forbindelse med integrerte operasjoner være nyttig å se litt på de muligheter og de tekniske løsninger som er implementert for å beskytte seg mot negativ påvirkning. Vi vil i dette avsnittet derfor kort diskutere noen slike løsninger.

5.2.1 Dagens løsninger

I de løsninger som i dag benyttes for installasjoner i Norge, er det som regel implementert tiltak for å:

- Hindre at SIS blir negativt påvirket fra nettet;
- Hindre at nettet blir påvirket fra omverdenen.

Systemene er som oftest basert på et felles nettverk for både sikkerhetsfunksjoner og andre funksjoner. For de fleste løsninger har en bare ett brukergrensesnitt, der informasjon fra forskjellige systemer kan vises sammen i felles bilder. Slike løsninger betinger at sikkerhetssystemene har mekanismer for å hindre at sikkerhetsfunksjonen blir negativt påvirket fra nettet eller operatørstasjonen.

[4] Konklusjonen fra /11/ relaterer seg nok først og fremst til grupperisiko. Dersom en ser på individrisikoen til det personellet som blir igjen på en installasjon, eller som av og til må transporteres ut, kan risikoen for disse godt bli høyere enn den er i dag. Dette må vurderes i hvert enkelt tilfelle.

I OLF-070 (se /10/, App. G), er det beskrevet en del flere krav som må oppfylles for den type løsninger som er diskutert foran.

5.2.2 Datasikkerhet

Når en ser på datasikkerhet i forbindelse med integrerte operasjoner, er det naturlig å tenke seg tre hovedmoduser i forhold til hvordan en installasjon kan kommunisere med omverdenen:

1. Ingen tilgang fra eksterne maskiner til systemene på installasjonen;
2. Kun lesetilgang; informasjon kun fra installasjonen til land (eller en annen installasjon). Ingen aksjoner eller kommandoer motsatt vei;
3. Skrive- og lesetilgang: Mulighet til å sende kommandoer og aksjoner og drive aktiv styring fra land (eller fra annen installasjon).

Under vil vi kommentere hver av disse for seg.

1. Ingen tilgang

Selv om en har løsninger der eksterne ikke har adgang til systemene på installasjonen, må en beskytte seg mot uønsket påvirkning ved at ekstern program- og maskinvare bringes inn og kobles opp mot de interne systemene. Dette er imidlertid ikke forskjellig fra situasjonen slik den er i dag.

2. Bare lesetilgang

Et viktig skille går mellom det å bare kunne lese informasjon og det og kunne skrive til systemer på en installasjon. Selv om en bare har lesetilgang, er det imidlertid svært viktig hvordan denne adgangen gis, da det for de fleste løsninger fører til sending av meldinger til enheter på innsiden. Alternativer løsninger kan være:

- Fjerne muligheten i maskinvare til å sende på det interne nettet. Ved dette alternativet blir det fysisk umulig og ikke avhengig av programvare og konfigurasjon om en kan sende på det interne nettet;
- Ved hjelp av programvare på enheten som kobler mellom utvendig og innvendig nett: hindre at det sendes meldinger ut på nettet.

3. Skrive- og lesetilgang

Hvis en i tillegg til å lese skal kunne skrive inn i de interne systemene, er det også da flere trinn og muligheter:

- Hindre skriving til sikkerhetssystemene (NAS, B&G, PAS). I en slik løsning er en helt avhengig av at de interne mekanismene i SAS er tilstrekkelige for å unngå negativ påvirkning;
- Ved mulighet for skriving inn i sikkerhetssystemene, blir en også avhengig av tilsvarende mekanismer som de en har i dag for å hindre at operatørstasjonene skal kunne introdusere feil i sikkerhetssystemene.

5.3 Innspill fra fagfolkene vedrørende integrerte operasjoner

I forbindelse med telefonintervjuene ble fagfolkene også spurt om hvordan de trodde integrerte operasjoner kunne påvirke graden av avhengighet mellom systemene. Det ble dessuten diskutert en del rundt tekniske løsninger i forbindelse med fjerndrift.

5.3.1 Hvordan kan integrerte operasjoner påvirke avhengighet?

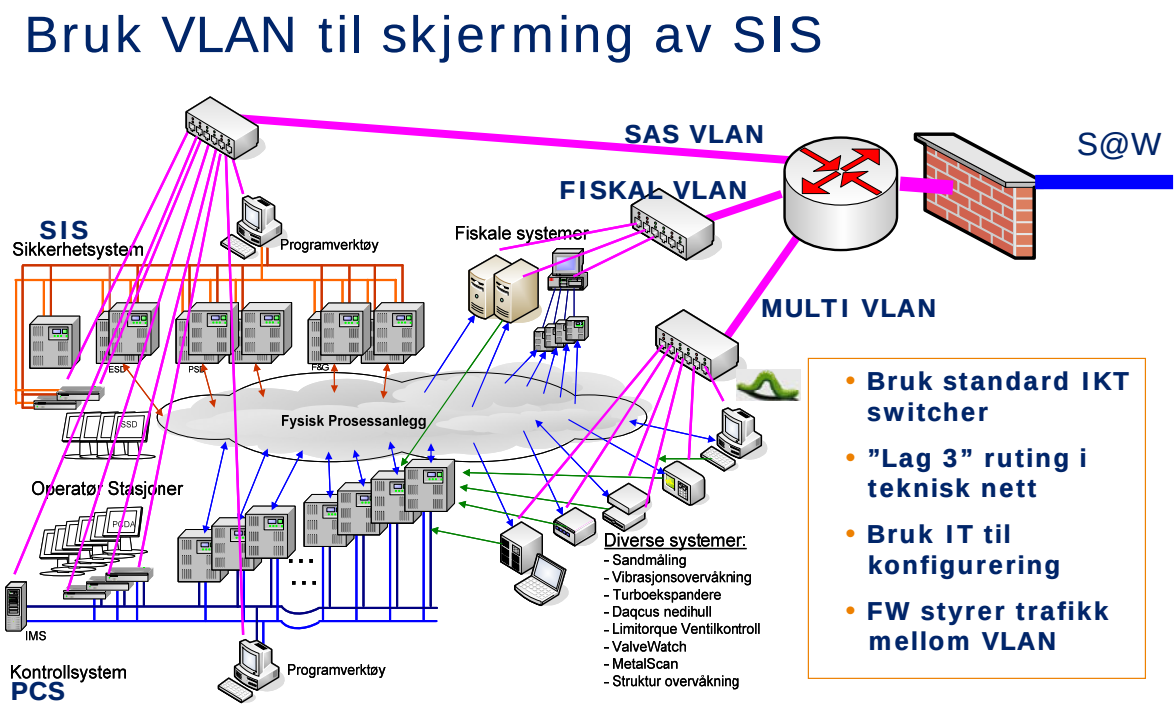
Det var noe begrenset med synspunkter vi fikk på dette spørsmålet, men noen punkter kom opp:

- Det ble fremhevet at fjernstyring generelt bør medføre enda strengere krav til ”disiplin og klare linjer” i forhold til hva som må være uavhengig, hvem som skal ha tilgang til hva, hva som er sikkerhetskritiske funksjoner og ikke, osv.
- Fjernstyring vil medføre flere komponenter som skal dekkes av uavhengighetsprinsippet, og det vil dermed være vanskeligere å oppnå uavhengighet (for eksempel pga. felles kabler);
- Det vil være en utfordring å ”overføre privilegiet” til å kunne operere systemene mellom ansvarlige på land og hav (og motsatt). Som en følge av brudd i kommunikasjonene kan en dessuten miste ting (slik som å tilbakestille overbroinger) i disse prosessene. Det kan også være problematisk med re-synkronisering etter kommunikasjonsbrudd, for eksempel av utkoblinger;
- Oppdatering av informasjon gjort fra land bør *i prinsippet* ikke være så forskjellig fra om noen sitter i et rom 100 meter unna logikken på selve plattformen og gjør det samme;
- Det ble i denne sammenheng trukket fram at flytting til land kan være positivt ved at en faktisk kan få bedre kontroll med enkelte ting, slik som oppdateringer, logginger, osv.

5.3.2 Innspill fra fagfolkene angående tekniske løsninger

Det kom også opp en del synspunkter på tekniske løsninger knyttet til integrerte operasjoner:

- Det absolutt viktigste før en åpner opp for fjerndrift, er å rydde opp og lage en struktur som segregerer de forskjellige som ønsker tilgang, slik at ikke alle har tilgang til alt, men at det er basert på ”need to know”. Følgelig må en gå fra en situasjon der alle har tilgang til alt i et flatt teknisk nett, til en situasjon hvor det brukes en eller annen form for datafiltreringsfunksjon for å styre tilgangen til ulike systemer. Én mulig[5] teknisk løsning på dette er vist i *figur 3*, hvor en bruker VLAN til skjerming av de instrumenterte sikkerhetssystemene (se også Appendiks G.3 i OLF-070, ref. /10/):



Figur 3 Eksempel på bruk av VLAN til skjerming av SIS, ref. /14/

[5] Denne løsningen er én mulighet av flere. Blant annet kan en se for seg at kryptering / sterk autentisiering kan være et annet, mer ”transparent” alternativ.

- Når en ved svak skjerming (”låst kontor”) kun gir lesetilgang fra land, ble det gjort et poeng av at en på land bør benytte ”CCTV” overføring av kontrollromsbilder. Det vil si at en hardware ”grabber” skjermsignalene i kontrollrommet og overfører disse til land. En bør unngå kopiering til land basert på systemer som benytter seg av Windows sikkerhetsmodell (slik som NetOP/ VNC/ PcAnyWhere) siden slike systemer inneholder sikkerhetshull som gir en mulig ”bakdør" til kritiske systemer og sterk eksponering av teknisk nett;
- Dersom en skal tillate skrivetilgang, må dette kreve et velutstyrt supportsenter på land med systemer og rutiner som garanterer en tilsvarende kontroll (mht. adgang, rettigheter, kompetanse, osv) på landdelen som en i dag har på plattformene.

5.4 Effekten av integrerte operasjoner – SINTEFs synspunkter

5.4.1 Generelt

Hvilken effekt integrerte operasjoner vil få for avhengigheter mellom sikkerhetssystemer, henger sammen med hvilke endringer som gjøres på den enkelte installasjon ved overgang til integrerte operasjoner. Normalt vil dette være noe mer enn bare å strekke en fiberkabel til land. Endringene kan variere fra installasjon til installasjon, og enkelte av dem behøver ikke nødvendigvis å være påkrevd for å oppnå ”fjernstyring”, men kan gjøres for å redusere eventuelle negative konsekvenser ved fjerndrift. For eksempel kan det være tale om innføring av overvåkingskameraer som erstatning for uteoperatører, eller endringer for å bedre økonomien i prosjektet (for eksempel automatisering av manuelle operasjoner for å kunne redusere antallet operatører).

Det er vanskelig å si noe generelt om hvilken effekt slike endringer kan få for avhengigheter mellom sikkerhetssystemer, fordi virkningen vil henge sammen med de tekniske løsningene som velges. For eksempel kan en se for seg at nye overvåkingssystemer integreres med eksisterende sikkerhetssystemer, noe som *kan* medføre at det innføres nye avhengigheter. Det har tidligere blitt advart mot at slike nye overvåkings- og IT-systemer integreres med sikkerhetssystemene, ref. /13/.

Aktuelle tekniske endringer i forbindelse med overgang til integrerte operasjoner kan bl.a. være:

- Innføring av nye overvåkings- og IT-systemer
- Automatisering av manuelle operasjoner
- Utskifting av hele eller deler av eksisterende SIS
- Innføring av ekstern kraftforsyning
- Utskifting av utstyr med lav pålitelighet

Disse endringene må analyseres nærmere for å kunne si noe om effekten i forhold til mulig økt avhengighet mellom sikkerhetssystemer. Dette gjelder kanskje spesielt ved utskifting av hele eller deler av SIS, hvor man jo nettopp modifiserer PROSS, PAS og NAS.

5.4.2 Hva med spesifikke koblinger og avhengigheter?

I kapittel 4 ble en del konkrete koblinger og avhengigheter mellom ulike systemer nevnt, og mulige effekter av de ulike koblingene ble diskutert. Ser vi for oss at disse effektene kan endres ved innføring av integrerte operasjoner?

I avsnitt 4.1.1 diskuterte vi blant annet en del problemstillinger knyttet til standardisering av systemer. Det er grunn til å tro at innføring av integrerte operasjoner vil være en ytterligere pådriver for en slik utvikling.

En må blant annet forvente at standardiserte kommunikasjonsløsninger mellom land og offshore og mellom ulike aktører (som operatør og serviseselskapene), vil tvinge seg fram, og at disse trolig vil være IP[6] baserte. Slike løsninger må igjen forventes å kunne medføre et ytterligere påtrykk for standardisering av systemene på plattformen.

Vi må forutsette at felles kommunikasjonskanaler (nett) vil øke i omfang på bekostning av "trådbundne" løsninger. Dette medfører en vesentlig sårbarhet (for eksempel for "blackout"), men det er mulig å bygge også slike nett robuste og feiltolerante. Dette krever imidlertid en felles strategi/arkitektur. Med økt bruk av IP-baserte tjenester og standardiserte løsninger kommer også en økende security-problematikk. Alt i alt tilsier dette en betydelig innsats i å drifte og administrere kompliserte nettverk.

De nye kommunikasjonsløsningene mellom land og installasjonene vil kreve at en holder kontinuerlig fokus på oppdatering av systemene og nettet i form av nye "patcher" for antivirussystemer, brannmurer, osv. En slik fokus vil "komme av seg selv" i en tidlig fase hvor eDrift anses som noe "nytt", men etter hvert som teknologien alminneliggjøres vil dette kunne bli en utfordring.

En kan også se for seg at ved overgang til fjerndrift vil det tvinge seg fram en enda høyere grad av integrasjon mellom systemene, ref. /11/, noe som igjen medfører flere koblinger, blant annet fordi fravær av personell vil medføre økte krav til funksjonalitet, og fordi det vil bli enda viktigere å unngå tripper / problemer (for eksempel under oppstart). Behovet for økt innsikt i, tilgang til og deling av data vil dessuten kunne forsterke denne effekten. At det derfor kan oppstå motsetningsforhold mellom det å beholde en størst mulig grad av uavhengighet mellom systemene og det å videreutvikle ulike eDriftsformer, synes derfor åpenbart.

Mye av diskusjonen i tidligere avsnitt har dreid seg om at kompleksiteten totalt sett øker når vi innfører ulike koblinger mellom systemer. Når en går fra en situasjon med fysisk nærhet til systemene og prosessen, til en situasjon hvor personell på land "styrer" driften, er det naturlig å spørre seg om ikke oversikten og systemforståelsen vil forringes, og at det derfor blir enda viktigere å holde systemene enkle og atskilte. Med andre ord; vil det over tid være mulig å opprettholde en like god "realitetsorientering" - spesielt i krisesituasjoner? I et slikt perspektiv vil det bli svært viktig at operatørene på land blir presentert informasjon på en ryddig og informativ måte, slik at de har grunnlag for en god og oppdatert virkelighetsforståelse. Nødsituasjonen og barrierene må derfor fortone seg som like "virkelige" på land som ute på installasjonen. At systemene er mest mulig uavhengige og atskilte, må forventes å kunne forenkle en slik presentasjon.

[6] Internet Protocol

6. Hvordan påvise tilstrekkelig uavhengighet? – Analysemetoder

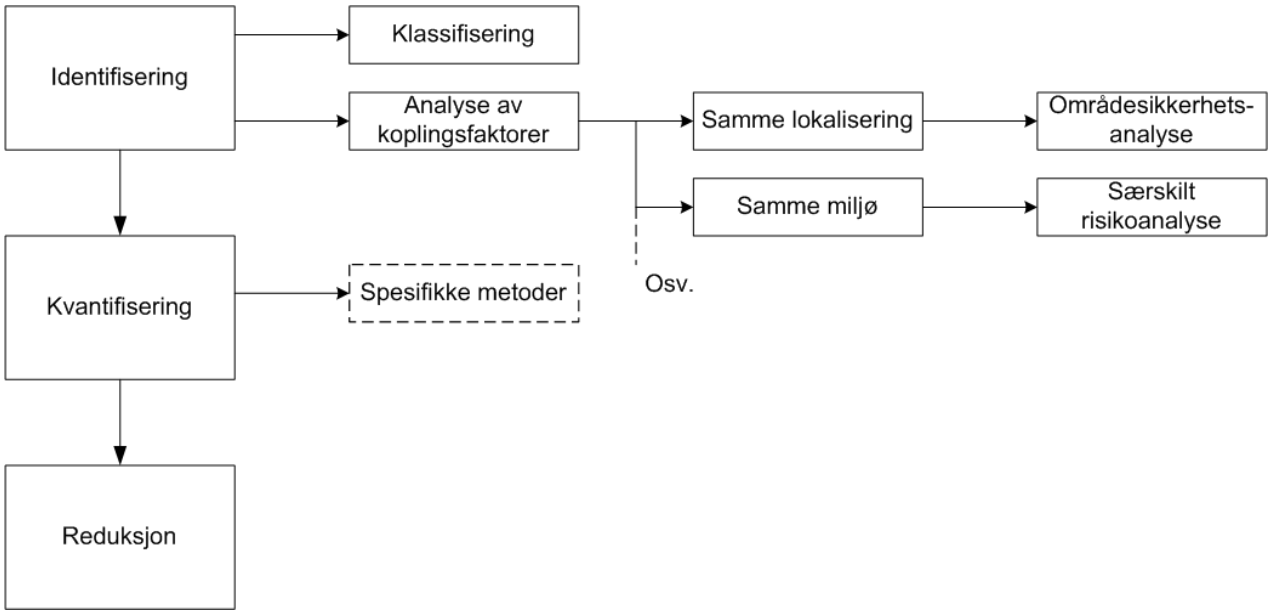
Vi kan skille mellom tre prinsipielt forskjellige innfallsvinkler ved en vurdering av hvorvidt uavhengigheten er tilstrekkelig:

1. Enkeltvis vurdering av hver avhengighet (”avviksbehandling”). Hver enkelt kjente/ identifiserte avhengighet vurderes for seg og gis aksept eller ikke-aksept (med eller uten krav om tilpasninger/endringer).
2. Helhetlig vurdering gjennom å analysere hver enkelt komponent/delsystem/system, med en underliggende antakelse om at ”helheten er lik summen av delene”. En risikoanalytisk tilnærming er et eksempel på en slik helhetlig vurdering.
3. Helhetlig vurdering av gitte karakteristikker av et system uten å betrakte hver enkelt komponent/delsystem/system, med en underliggende antakelse om at helheten er for kompleks til at det lar seg gjøre å benytte innfallsvinkel 2.

Litt forenklet kan en si at situasjonen offshore er slik at en for de kjente avhengighetene for en stor del har benyttet innfallsvinkel 1, og for visse sikkerhetssystemer også innfallsvinkel 2 (bl.a. gjennom eksplisitt modellering i hendelsestrær og feiltrær, samt bruk av parametriske metoder som beta-faktor-metoden i pålitelighetsanalyser).

Noe av problemet innen petroleumsindustrien er at en i liten grad har kontroll med helheten, dvs. hvorvidt totalen av de avhengigheter som finnes mellom sikkerhetssystemene er akseptabel. Dette skyldes at de kjente avhengighetene i for stor grad har blitt vurdert isolert, samt at det ikke har blitt lagt tilstrekkelig vekt på systematisk identifisering av andre mulige (ukjente) avhengigheter.

Innenfor andre industrier (kjernekraft-, romfarts-, og flyindustrien, jfr. avsnitt 3.5) har en lagt større vekt på analyse av avhengige feil som bl.a. inkluderer en systematisk identifisering av mulige ukjente avhengigheter, samt modellering og kvantifisering av betydningen av disse. En oppsummering av tilnærmingene nevnt i avsnitt 3.5, er vist i *Figur 4*.



Figur 4 Tilnærminger ved analyse av avhengige feil

Når det gjelder spesifikke metoder for analyse av avhengige feil, henviser en innen kjernekraft bl.a. til følgende metoder, ref. /4/:

- Eksplisitte metoder
  - Hendelsesspesifikke modeller (initierende hendelser som gir fellesfeil)
  - Hendelsestreanalyse
  - Feiltrekopling
  - Feiltre årsakstabell
  - Menneskelig pålitelighetsanalyse (modellering av avhengigheter i oppgavetrinn)
- Parametriske metoder
  - Beta-faktor metoden
  - Binomial feilrate modell
- Datamaskinbaserte metoder (søkeprosedyrer for identifisering av viktige avhengigheter), slik som GO, WAMCOM, BACKFIRE og COMCAN

Vi vil ikke her gå nærmere inn på hver av disse metodene – det ville føre for langt.

Tilnærmingen til analyse av avhengige feil innen kjernekraft-, romfarts-, og luftfartsindustrien følger innfallsvinkel 2 nevnt foran, og bygger på en antakelse om at helheten består av summen av delene, og at de systemene som inngår er ”analyserbare”. Helheten ivaretas gjennom en overbyggende risikoanalyse (Probabilistic Risk Assessment – PRA).

Når kompleksiteten øker, kan det selvsagt stilles spørsmål ved om den form for modellering som gjøres i en PRA gjenspeiler virkeligheten på en god nok måte – om systemet i det hele tatt er ”analyserbart” (i hvert fall uten bruk av ekstremt store ressurser). Det er dette Perrow, /5/, er kritisk til (se også avsnitt 3.3.2), og hvor han i stedet benytter innfallsvinkel 3, der en betrakter systemer ut fra visse karakteristika uten å analysere hver enkelt bestanddel. Viktige karakteristika er systemenes kompleksitet og hvorvidt delene er ”tett koplet” eller ”løst koplet” (som bl.a. sier noe om hvor mye tid man har til rådighet dersom en initierende ulykkeshendelse inntreffer).

For offshorenæringen er det problemer forbundet både med innfallsvinkel 2 og 3. Innfallsvinkel 2 er problematisk fordi en offshore risikoanalyse er langt grovere enn en kjernekraft PRA, og det er derfor lite trolig at de nødvendige komponenter og systemer er godt nok modellert. Innfallsvinkel 3 kan bidra til en økt bevissthet rundt behovet for enkle (”rene”) systemer (begrense kompleksiteten), samt en bevissthet rundt begrensningene til en ren risikoanalytisk tilnærming. Denne innfallsvinkelen gir imidlertid ingen hjelp til å vurdere avhengigheter og hvorvidt uavhengigheten mellom sikkerhetssystemer er tilstrekkelig.

Et forslag til videre tilnærming til analyse av avhengige feil i ulike sikkerhetssystemer, er å benytte noen av de samme metodene som bl.a. anvendes innen kjernekraftindustrien. I så fall bør dette gjøres som en form for utvidete pålitelighetsanalyser, der en ser på flere eller alle viktige sikkerhetssystemer under ett, men uten at disse inngår i en totalrisikoanalyse. I tillegg vil det også være nyttig å benytte systematiske analyser for å identifisere avhengigheter *innen* et sikkerhetssystem.

En vurdering av hvorvidt uavhengigheten er tilstrekkelig, må baseres på at alle avhengigheter er identifisert (med rimelig stor grad av konfidens). Dessuten må uavhengighetene være kvantifisert, slik at en i hvert fall kan vurdere det relative bidraget fra avhengige feil i forhold til totalbidraget til upålitelighet/utilgjengelighet. Dersom en er i stand til å fastsette krav til pålitelighet/ tilgjengelighet til flere sikkerhetssystemer under ett, kan dette benyttes som kriterium for å

avgjøre hvorvidt en har tilstrekkelig uavhengighet. Mest sannsynlig vil nok dette være så vidt komplisert at den endelige vurderingen hovedsakelig vil være kvalitativ, i hvert fall inntil videre.

7. Referanser

/1/ Petroleumstilsynets regelverk med veiledninger.

/2/ IEC 61508, versjon 1.0, del 1 – 7 (forskjellige datoer).

/3/ EN ISO 10418, " Petroleum and natural gas industries - Offshore production installations - Basic surface process safety systems", 2003.

/4/ PRA Procedures Guide -A Guide to the Performance of PRAs for Nuclear Power Plants, NUREG/CR-2300, January 1983.

/5/ Perrow, C., "Normal accidents. Living with high-risk Technologies", Princeton University Press 1999.

/6/ Balchen, Andresen og Foss: Reguleringsteknikk, Teknisk kybernetikk, NTNU, januar 2002.

/7/ PDS Memo: "The Impact of Common Cause Failures in Safety Systems", dated 22.04.2004.

/8/ US Nuclear Regulatory Commission: Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, report WASH-1400 (NUREG-75/014), October 1975.

/9/ NASA: Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC, August 2002.

/10/ OLF 070: "Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry", rev. 02, oktober 2004.

/11/ OLF rapport: eDrift på norsk sokkel – det tredje effektiviseringsspranget, 2003

/12/ OLF rapport: Integrated Work Processes: Future work processes on the NCS, 2005

/13/ Øien, K., Guttormsen, G., Hauge, S., Sklet, S., Steiro, T., 2002. Morgendagens HMS-analyser for vurdering av tekniske og organisatoriske endringer. Prosjektrapport 2002. SINTEF Teknologi og samfunn, rapport STF38 A02423

/14/ Presentasjon fra Ken Møller: "Barrierebygging i teknisk nett", Statoil, 2005