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

Bruk av HIPPS for utstyrsbeskyttelse

FORFATTER(E)

Per Hokstad, Stein Hauge og Tor Onshus

OPPDRAGSGIVER(E)

Oljedirektoratet

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS REF.	
STF38 A01422	Åpen	Arne J. Thorsen, Torleif Husebø	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	82-14-01683-5	384379	52 / 1
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
S:3840/pro/384379/ Rapport OD-HIPPS åpen.doc		Per Hokstad	Tor Onshus
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
	2001-07-31	Lars Bodsberg, forskningssjef	

SAMMENDRAG

Studien presenterer en gjennomgang av bruk av HIPPS (*High Integrity Pressure Protection System*) i norsk petroleumsindustri. Rapporten skal gi innspill til Oljedirektoratets (OD) videre arbeid med HIPPS- problematikken ved å

- beskrive tekniske og operasjonelle aspekter ved "standard" HIPPS-løsninger;
- redegjøre for ulike bruksområder, eksisterende såvel som framtidige;
- redegjøre for hvordan regelverk og standarder forholder seg til bruk av HIPPS;
- gi en oversikt over eksisterende HIPPS-installasjoner og beskrive de erfaringer en har med bruk av HIPPS så langt;
- diskutere spesielle problemområder/utfordringer som kan oppstå ved bruk av HIPPS, og gi enkelte anbefalinger.

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Instrumentering	Instrumentation
GRUPPE 2	Offshore	Offshore
EGENVALGTE	Sikkerhet	Safety

FORORD

SINTEF er bedt av Oljedirektoratet (OD) om å foreta en gjennomgang av bruk av HIPPS (*High Integrity Pressure Protection System*) i norsk petroleumsindustri.

Som en del av dette prosjektet sendte OD ut et spørreskjema til oljeselskap og utstyrsleverandører. Vi vil takke for informasjon mottatt fra Statoil, Norsk Hydro, TotalFinaElf, Mokveld Norge AS, FMC Kongsberg Offshore AS, SAAS ASA og Boo Instrument AS.

En spesiell takk går til Robert-Dennis Garner i TotalFinaElf Exploration Norge, Jarle Øygarden i SAAS Safety System og Willy Frantzen i Boo Instrument, som har utarbeidet eget materiale for oss; noe som har vært til stor hjelp. Vi takker også Statoil som har stilt selskapsspesifikke data til rådighet.

Studien ble gjennomført i perioden september 2000 - januar 2001, og vi vil takke kontaktene i OD, Arne J. Thorsen og Torleif Husebø for god assistanse.

Denne rapporten finnes også i en fortrolig versjon (med ytterligere noe dataunderlag).

INNHOLDSFORTEGNELSE

1 Innledning

1.1 Formål med studien

Studien skal gi innspill til Oljedirektoratets (OD) videre arbeid med HIPPS- problematikken. HIPPS står for *High Integrity Pressure Protection System*, dvs. "høypålitelig trykkbeskyttelses-system".

Målet er å sette (OD) i bedre stand til å evaluere eksisterende og framtidige HIPPS-løsninger. Dette skal oppnås ved å

- beskrive tekniske og operasjonelle aspekter ved ”standard” HIPPS-løsninger;
- redegjøre for ulike bruksområder, eksisterende såvel som framtidige;
- redegjøre for hvordan regelverk og standarder forholder seg til bruk av HIPPS;
- gi en oversikt over eksisterende HIPPS-installasjoner og beskrive de erfaringer en har med bruk av HIPPS så langt;
- diskutere spesielle problemområder/utfordringer som kan oppstå ved bruk av HIPPS, og gi enkelte anbefalinger.

1.2 Historikk vedrørende bruk av HIPPS

Instrumenterte sikkerhetsfunksjoner slik som HIPPS, blir nå tatt i bruk i prosessindustrien som et kostnadseffektivt alternativ til mekaniske/instrumenterte sikkerhetsfunksjoner i standard design.

HIPPS har vært brukt bl.a. i tysk gassindustri siden 1974 (av Ruhrgass). I Norge er det særlig Statoil som har benyttet HIPPS, først på landanlegg men etterhvert også på offshore installasjoner. Statoil Tyskland introduserte "Overpressure Protection System" på Etzel Gas Lager i 1991, og refererte da til en tysk standard for "High Integrity Protection Shutdown" (HIPS) system. Statoils første HIPPS-anvendelsen i Norge var på Kårstø, der HIPPS har vært i bruk siden 1991. I dag er det i størrelsesorden 100 HIPPS-ventiler på Kårstø. Mens disse er direkte pneumatisk operert, ble elektronisk opererte HIPPS-ventiler installert på Sleipner i 1993. Statoil har også brukt en slags HIPPS eller nærmere bestemt *Pipeline Protection System* (PPS) på rørledninger, bl.a. på Zeepipe II siden 1997.

Ellers benyttet Elf en form for HIPPS kalt OPPS (*Over Pressure Protection System*) på Frigg-feltet allerede fra 1987, og en annen variant på Lille-Frigg fra 1992.

Norsk Hydro skal ha en HIPPS-løsning på Visund og planlegger dessuten å ta i bruk HIPPS når Tune blir tilkoplet Oseberg D. Norsk Hydro har også en del FCS (Flare Control System) som er et system for trykkavlastning med *hurtigåpnende* ventiler. Ellers har Snorre TLP (tidligere Saga) diverse IOPS (*Instrumented Overpressure Protection System*) løsninger, som også er en nær ”slektning” av HIPPS.

Den største leverandøren av HIPPS-ventiler, Mokveld, har i dag installert omtrent 500 HIPPS-ventiler *på verdensbasis.*

Som antydet ovenfor, benytter operatører/leverandører begrepet HIPPS i en vid og varierende betydning. Det synes derfor å være et definisjonsspørsmål hva som skal regnes som en HIPPS-

løsning. I dag er det ingen enhetlig praksis når det gjelder bruk av dette begrepet, og samme system kan av ulike aktører omtales både som HIPPS og PPS. Tilsvarende blir en FCS-løsning av minst én ventil-leverandør omtalt som HIPPS.

I den generelle oversikten i kapittel 4 over hva som finnes av trykkbeskyttelses-system på norsk sokkel inkludert landanlegg, er det også tatt med løsninger som strengt tatt ikke er ensbetydende med HIPPS dersom begrepet tolkes snevert. På denne måten får vi med hele spekteret av "HIPPS-liknende" applikasjoner, noe som anses vesentlig i en slik oversikt.

1.3 Oppbygging av rapporten

I Kapittel 2 beskrives en "standard" HIPPS-løsning, og det gis en kort diskusjon av de enkelte elementene; sensor, logikk og ventil, inklusiv testing. Det sies også litt om totalkonfigurasjonen (redundans/-interlock).

Kapittel 3 oppsummerer det som står om HIPPS i ulike standarder og regelverk, med hovedvekt på NORSOK og IEC 61508/61511.

Kapittel 4 presenterer en mest mulig komplett oversikt over alle HIPPS-installasjoner offshore og på landanlegg. Først gis en oversikt over ulike varianter av HIPPS, med definisjon av begrepene som er brukt av oljeselskap på norsk sokkel. Sentral informasjonen om de ulike HIPPS-installasjonene er samlet i en tabell.

I Kapittel 5 er det samlet tilgjengelige erfaringsdata for HIPPS. Dette er kombinert med generiske pålitelighetstall (OREDA/PDS) til å presentere estimat for sviktintensiteter for elementene i en HIPPS-løsning. Dessuten er testing av HIPPS behandlet.

I stor grad har arbeidet bestått i å samle og systematisere informasjon og data. Men rapporten avsluttes med å se på en del utfordringer, og gir en oppsummering med enkelte konklusjoner/anbefalinger.

1.4 Forkortelser

Under listes en del (primært engelske) forkortelser som er brukt i rapporten.

ALARP	As Low As Reasonably Practicable
B&G	Brann og Gass
CHAPS	Gas Inlet Concept for High Availability Protection System
CSU	Critical Safety Unavailability
EUC	Equipment Under Control (IEC 61508)
FCS	Flare Control System
FTO	Fail To Operate (Farlige feil)
DU	Dangerous Undetected (feilmode, IEC 61508)
GAMAB	*Globalement Au Moins Aussi Bon* ("Totalt minst like bra")
HEART	Human Error Assessment and Reduction Technique
HIPPS	High Integrity Pressure Protection System
IOPS	Instrumented Overpressure Protection System
ISS	Instrumented Safety System
LA	Level Alarm

MEM	Minimum Endogenous Mortality
NAS	Nødavstengningssystem
NE	Normally Energised
OPPS	Over Pressure Protection System
OREDA	Offshore Reliability DAta base
PAS	Prosessavstengningssystem
PC	Process Control
PDS	Pålitelighet (og tilgjengelighet) av Datamaskinbaserte Sikringssystemer
PFD	Probability for Failure on Demand
PLC	Programmable Logic Controller
PPS	Pipeline Protection System
PS	Pressure Switch
PSV	Pressure Safety Valve
PT	Pressure Transmitter
TIF	Test Independent failures (from PDS). Systematic failures in the IEC 61508 notation
QSV	Quick closing Shut off Valve
SD	Safe Detected (Feilmode, IEC 61508)

2 Standard HIPPS-løsninger

2.1 Litteratur

Det finnes svært lite offentlig tilgjengelig litteratur på området HIPPS. For eksempel finnes det i Bibsys[1] bare tre tilslag på stikkordet HIPPS, se referanser /1/, /2/, /3/. På webben er det mye fra diverse leverandører, men dette forteller stort sett at leverandøren kan tilby tjenester på området og gir lite detaljer.

Det finnes en rekke rapporter som behandler spesifikke HIPPS-løsninger (bl.a. en rekke SINTEF- og konsulentrapporter). Disse er fortrolige. Det er også rapportene fra de to forskningsprosjektene

- Subsea OPPS Feasibility Study, /4/
- Subsea HIPPS Development Study, /5/.

2.2 Bruksområder for HIPPS

Det finnes mange forskjellige anvendelser av HIPPS, men generelt er HIPPS benyttet for å redusere kostnader; og enkelte ganger kan resulterende kostnadskutt være nødvendig for å forsvare en utbygning.

Avhengig av anvendelse kan en for eksempel gruppere (typisk) bruk av HIPPS på følgende måte:

- For liten fakkelkapasitet / PSV kapasitet (vil i rapporten omtales som *prosess HIPPS*)
  - Ved behov for fakling i forbindelse med ”normalproduksjon”
  - Ved full stopp/blackout
  - For oppstart med gassfyllt rørledning
  -
- Beskyttelse av rørledninger og stigerør
  - Transport, mellom plattformer og til/fra land (jfr *PPS*)
  - Havbunn, som del av systemet for å koble brønnene til plattformen (vil omtales som *subsea HIPPS*)

Merk at også trykkavlastningsystemet, *FCS* (med hurtigåpnende ventil) ofte omtales som en HIPPS-løsning, se Avsnitt 4.1. Imidlertid vil HIPPS i snever betydning begrense seg til et system der trykkbeskyttelsen skjer ved *hurtiglukkende* ventil. Da faller både FCS og PPS utenfor, og i den systematiske oversikten i Kapittel 4 lar vi HIPPS, PPS og FCS være tre separate kategorier.

Der fakkelkapasiteten (PSV-kapasitet) er grunnen til at en velger en HIPPS-løsning, er det flere varianter, alt avhengig av hvor begrensningene ligger i forhold til standard dimensjonering. Dette er den helt typiske HIPPS-løsning som krever hurtiglukkende ventil, (typisk krav er en lukketid på høyst 2 sekunder). Statoil omtaler slike HIPPS-ventiler som QSV (Quick closing Shut off Valve), og den betegnelsen brukes også i denne rapporten.

For tilfellet med for liten fakkelkapasitet / PSV kapasitet, har en følgende:

[1] Omfattende litteraturdatabase ved NTNU

- Behov for fakling under ”normalproduksjon” kan oppstå i forbindelse med for eksempel blokkert utløp eller som et resultat av at kontrollventiler på innløp feiler åpne. Gass-/væskeproduksjonen er da i henhold til designspesifikasjon, men underdimensjonert PSV og/eller fakkel medfører at HIPPS må innstalleres.

- Behov for HIPPS i forbindelse med full *blackout* er i dag mest relevant for landanlegg med destillasjon. Her kan bortfall av kraft føre til at alle tanker med oppvarming, på grunn av restvarmen og varm føde, får for høyt trykk slik at fakkelen blir overbelastet på grunn av samtidig fakling fra mange kolonner. HIPPS brukes da til å stenge for føde og for eksempel damp.

- Hvis en ser på det etterhvert så omtalte ”oppstartscenariet”, er dette et resultat av at rørledning(er) over tid ”pakkes” med gass i forbindelse med en prosessnedstenging. Dersom en ved oppstart feilopererer en ventil, eller opplever ”choke-kollaps”, kan den situasjonen oppstå at PSV og/eller fakkelsystemet ikke klarer å ta unna all gassen som kommer inn på plattformen. Dessuten vil PAS funksjonen ofte ikke være rask nok til å hindre overtrykking utover designtrykk. En HIPPS-løsning vil da kunne brukes for raskt å stenge tilførselen av gass (HIPPS er såvidt SINTEF bekjent ennå ikke benyttet i denne applikasjonen).

For *rørledninger* er det ofte installert overtrykksbeskyttelse (dvs PPS) der det er sprang i designtrykk (*spec. break concept*), eller der høytrykksledninger kobles inn mot lavtrykks-systemer. Disse systemene har gjerne en innebygd treghet i form av tiden det tar å bygge opp trykket i rørledningen. Selve lukketiden er derfor sjelden kritisk. Hvis rørledningen blokkeres for eksempel fordi mottakeren har en nedstenging, kan produsenten derfor ofte forsette å levere inn i rørledningen i lengre tid før kritisk trykkgrense nås.

Subsea HIPPS er løsninger der HIPPS-ventilene er plassert på havbunnen, som regel for å unngå krav om at rørledninger og stigerør skal kunne tåle fullt brønninnstengingstrykk. For disse systemene får en bl.a. problemstillingen med begrenset tilgjengelighet for vedlikehold av ventiler, osv.

Når driftserfaring fra ulike systemer skal vurderes og sammenlignes er det viktig å skille på type fluid (medium). En mulig inndeling her vil være
- tørrgass
- våtgass
- stabilisert olje
- brønnstrøm
- damp

Det vil for eksempel ikke uten videre være mulig å overføre en konstruksjon og et vedlikeholdsregime for tørrgass i et distribusjonsanlegg i Tyskland til en undervanns-anvendelse i Barentshavet. Slitasjen på komponentene, avleiringer og tilstoppinger er svært avhengig av de lokale forholdene. Dette må også gjenspeiles i de feilrater etc. som kan brukes når en skal vurdere løsningene.

2.3 Typisk oppbygging

En standard HIPPS-løsning består av en trykksensor som via en logikk stenger en eller flere (hurtigvirkende) ventiler når det målte trykket i mediet kommer over en viss verdi. Hvis HIPPS

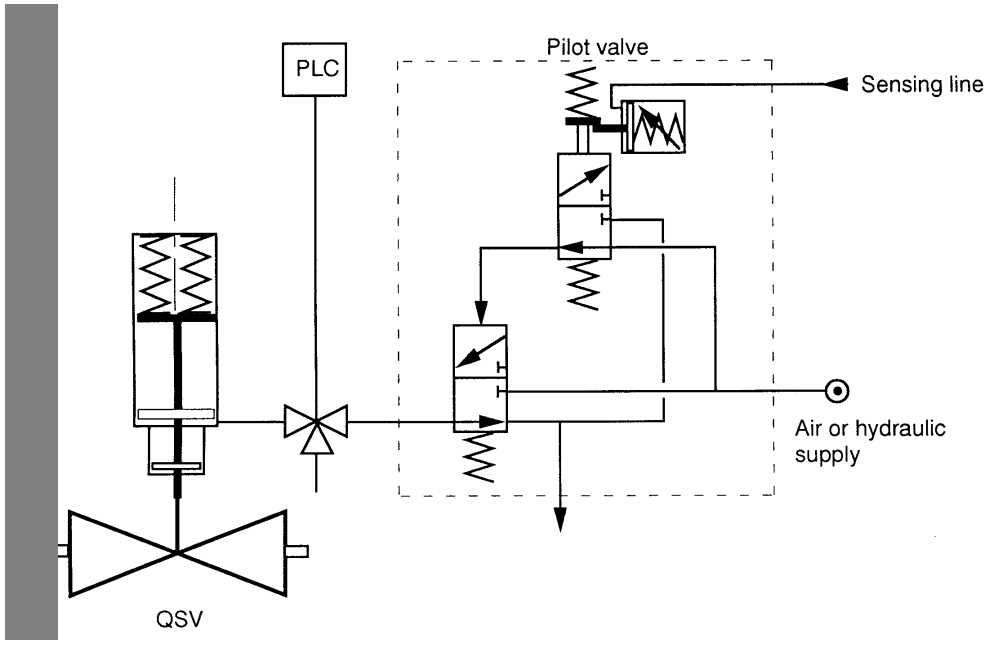
skal erstatte en mekanisk barriere er det er et sentralt poeng at HIPPS-barrieren skal være helt uavhengig av alle øvrige sikringssystemer (PCDA, PAS, NAS).

Den "klassiske" HIPPS-løsningen slik den blir brukt på gassdistribusjonsnettet bla. i Tyskland, er vist i Figur 1. Her er vist en enkel (ikke redundant) ventil med logikk uten votering. Løsningen som er skissert i denne figuren danner utgangspunkt for de fleste løsninger som finnes i dag. Trykksignalet fra prosessen gir via et pneumatisk system stengesignal til ventilen (QSV). I aktivert stilling (åpen QSV) føres forsyningstrykket gjennom den øverste pilotventilen (stilling som i figuren) og presser den andre pilotventilen til motsatt stilling slik at forsyningstrykket har fri tilgang til aktuatoren som åpner ventilen. Øverst til høyre på figuren ses mekanismen som brukes til å stille inn det prosesstrykket ventilen skal stenge ved. Når dette trykket nås, skifter den øverste pilotventilen stilling slik at oversiden av den andre pilotventilen bløs av (skifter til stillingen vist i figuren). Aktuatoren bløs så av gjennom den nederste piloten, og ventilen stenger p.g.a. fjærkreftene.

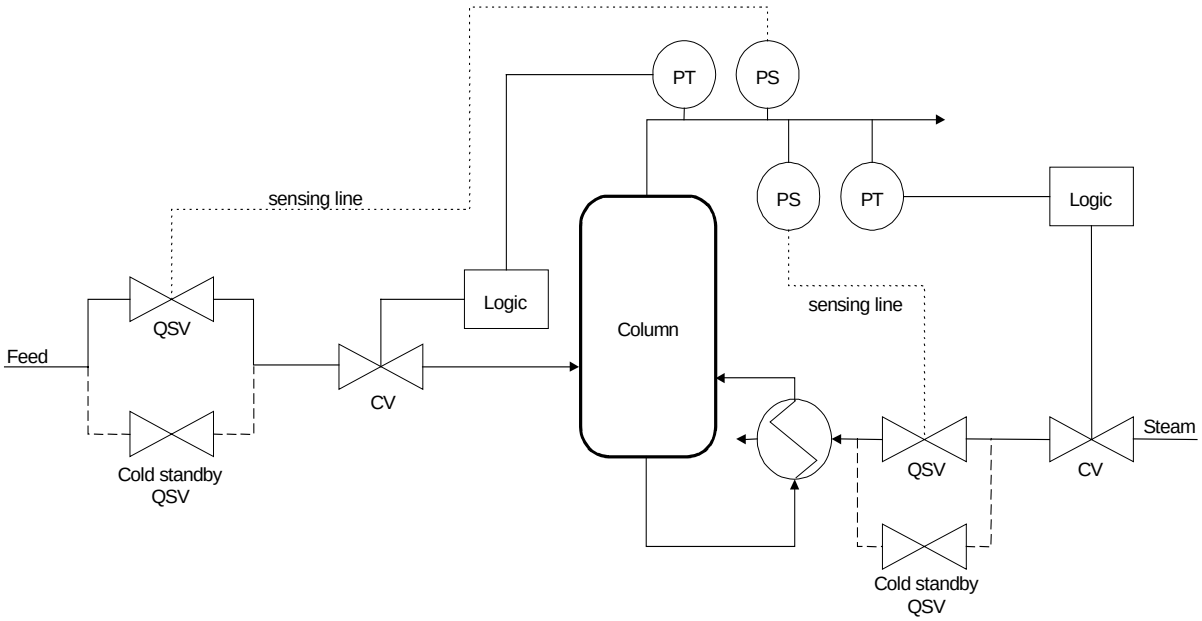
Det er også lagt inn en ventil (styrt av PLC) som kan blø av trykket slik at ventilen kan testes for å se om den virker (selvlukkende). Trykket bløs av ventilmotoren og det registreres med endebryterne at ventilen forlater åpen tilstand og kommer til lukket posisjon. Gangtiden registreres for å overvåke tilstanden til ventilen. Det finnes nå også systemer som kan brukes til å lekkasjeteste ventilen direkte i røret, samt avansert signalbehandling for å registrere forandringer i momenter og krefter ved lukking/åpning av ventilen.

Den aktuelle standarden, DIN 3381, ref /6/, gjelder egentlig bare for trykk opp til 100 bar, men prinsippene fra denne standardløsningen kan også brukes for høyere trykk.

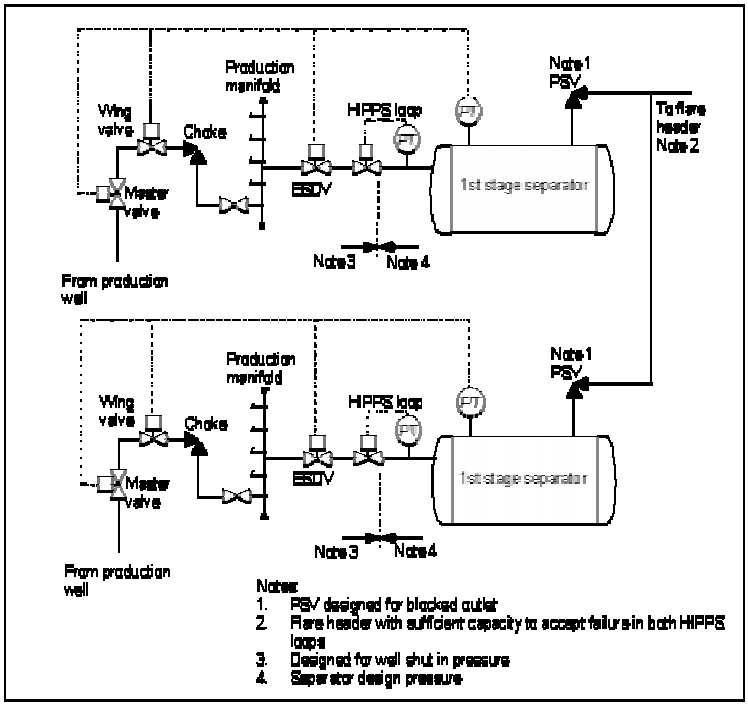
Figur 2 viser en typisk HIPPS- anvendelse ved for lav faklingskapasitet på en destillasjons-kolonne. Her er det installert en enkel HIPPS-sløyfe ("loop") både på føde og damp til kolonnen. Det er direkte pneumatisk aktivering av den åpne QSVen fra trykkbryteren, PS. Merk at regulering av kontrollventilen her utgjøre en ekstra barriere (”Kårstø varianten”).



Figur 1 Original direktevirkende pneumatisk HIPPS-konfigurasjon (DIN 3381)

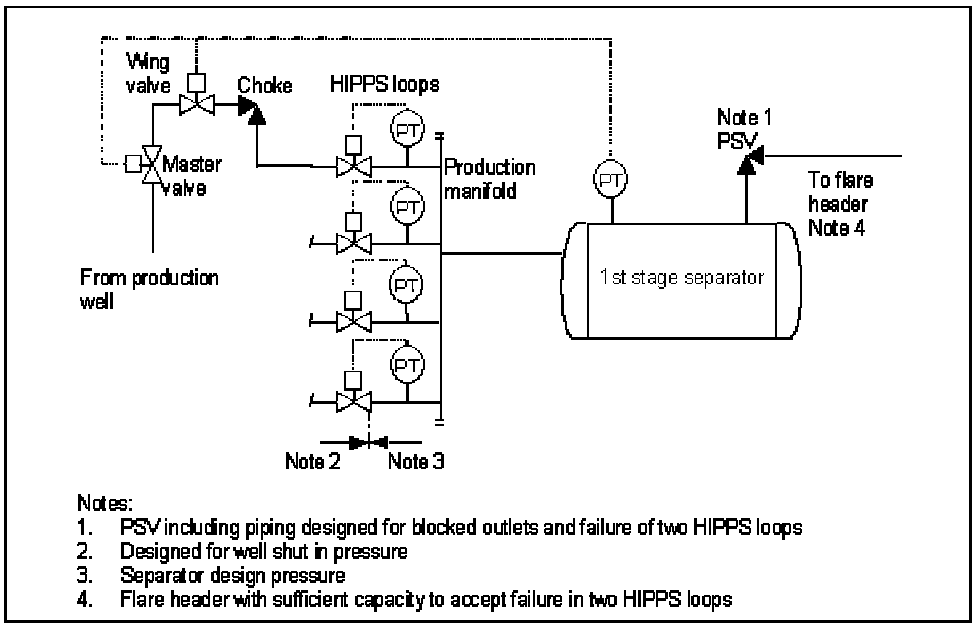


Figur 2 HIPPS-løsning med PS, pneumatisk aktuering og QSV for føde og damp til kolonne. Her utgjør også trykktransmitter (PT), logikk og kontrollventil (CV) en barriere.



Figur 3 HIPPS arrangement for to parallelle separatortog (fra Norsok P-001)

Figur 3 viser en annen HIPPS anvendelse. Her er det installert HIPPS på hvert av de to parallelle separatortogene for å kunne redusere fakkel designkapasiteten. Figur 4 viser et annet eksempel hvor en har flere parallelle løp inn til samme separator og hvor det for å redusere PSV (og fakkel) designraten er installert HIPPS på hver linje.



Figur 4 HIPPS arrangement for flere løp inn til samme separator (fra Norsok P-001)

2.4 Sensor

Det er to forskjellige måter for å generere et signal når prosesstrykket når et forhåndsbestemt nivå:

- Ved hjelp av en trykkbryter (PS) som styres direkte fra prosesstrykket, jfr Figur 1 og Figur 2;
- Ved hjelp av en analog sensor (trykktransmitter, PT), som enten går til en forsterker, eller inn til en eller annen form for logikk som også kan ha votering.

Løsningen med analog transmitter er å foretrekke, da denne kan overvåkes uten å påføre et trykk slik at den utløses.

I tillegg til det trykkfølsomme elementet, er tilkoblingen til prosessen et viktig punkt. Her er det flere forhold som er kritiske:

- Mulighet for tilstopping p.g.a. voks, hydrat, mekanisk skade osv. Plassering av transmitter og isolering av transmittertubing (impulsrør) er her viktige elementer;
- Mulighet for test og overvåking;
- Muligheten for at en sensor ikke kobles inn igjen etter test/vedlikehold eller utilsiktet kobles ut, slik at den ikke virker når det blir behov for den.

Ved testing er det viktig at en sikrer at alle testventiler etc. kommer i riktig posisjon etter testen. Dette kan sikres ved prosedyrer, men aller helst ved mekaniske løsninger der for eksempel skapet ikke lar seg lukke uten at alt står i riktig posisjon.

For å gi ekstra god overvåking og testing av transmittere i HIPPS-funksjonen er overføring av verdien fra disse til for eksempel styresystemet nyttig. Her kan en da overvåke og sammenligne verdien fra HIPPS med verdier fra andre transmittere. Hvis avviket mellom disse overskrider en viss grense, kan det gis alarm og test/vedlikehold blir igangsatt.

På markedet finnes det mange fullgode transmittere som benyttes i HIPPS-løsninger. Nå kommer også nye transmitterne fra ABB, Moore og Rosemount som har innebygget ekstra selvtest/ diagnose av elektronikken. Disse er sertifisert for å kunne brukes i løsninger som bygges og drives i henhold til IEC 61508.

Merk at en av og til benytter endebrytere (posisjonsbryter) på ventiler som sensor isteden for (eller som supplement til) trykkmåler. Dette kan gjøres hvis trykkoppbygningen og dermed behovet for HIPPS skyldes utilsiktet nedstenging av denne ventilen, og en finner det "uhensiktsmessig" å plassere trykkmålere oppstrøms denne. Dette representerer ikke en standard HIPPS-løsning, men er en variant som forekommer i.f.m. PPS. Endebrytere representerer som regel en mindre pålitelig deteksjonsmåte enn trykktransmittere. I tillegg trengs det ofte logikk for å hindre aktivering ved normal operasjon av ventilen, noe som fører til mer komplekse og mindre pålitelige systemer.

2.5 Logikk

Det finnes i hovedsak tre forskjellige teknologier som brukes i HIPPS logikkenheter:

- Pneumatisk, jfr Figur 1
- Elektronisk (fast fortrådet);
- Programmerbar logikk.

Hvilken teknologi som benyttes er ikke sentralt, så lenge den oppfyller kravene som stilles. De enkelte løsninger har imidlertid sine sterke/svake sider.

- Pneumatikk systemer er enkle og velutprøvde men kan vanskelig bygges med innebygget selvtest/diagnose. En må derfor basere seg på manuell testing.
- I likhet med pneumatiske systemer representerer også fast fortrådede systemer ("hardwiret solid state") forholdsvis enkel teknologi som kan designes for å feile til sikker tilstand. Begge typene systemer krever mye planlegging og fysisk omkobling for å forandre logikken og blir derfor sjelden forandret når de først er satt i drift.
- Programmerbare systemer er i utgangspunktet like sikre som fast fortrådede, og tillater dessuten utstrakt grad av selvtest og diagnostisering. De er imidlertid enklere å modifisere enn pneumatiske og fast fortrådede systemer. Dermed kan terskelen for å gå inn og gjøre endringer bli lavere, noe som også kan medføre at logikken for sikkerhetsfunksjonene etterhvert blir mer komplisert og uoversiktlig.

Som nevnt over er det ofte et viktig poeng at HIPPS skal være uavhengig av andre sikringssystemer. Dette kravet kommer av at en ofte har erstattet en mekanisk uavhengig barriere med HIPPS, eller at HIPPS erstatter PAS funksjonen. For da å oppfylle kravet om to uavhengige barrier i tillegg til regulering, må HIPPS være uavhengig. Å knytte HIPPS opp mot NAS systemet er heller ingen god løsning. En slik løsning komplisere både NAS og HIPPS-funksjonene, og reduserer forståelsen av HIPPS som et 100% uavhengig trykksikringssystem.

For lettere å kunne overvåke HIPPS fra kontrollrommet, er det som sagt en fordel å koble HIPPS til det generelle styresystemet på anlegget. En slik kobling må imidlertid kun være enveis slik at feil i styresystemet ikke kan påvirke HIPPS på noen måte. Dette fordi behovet for HIPPS nettopp kan skyldes en feil i styresystemet.

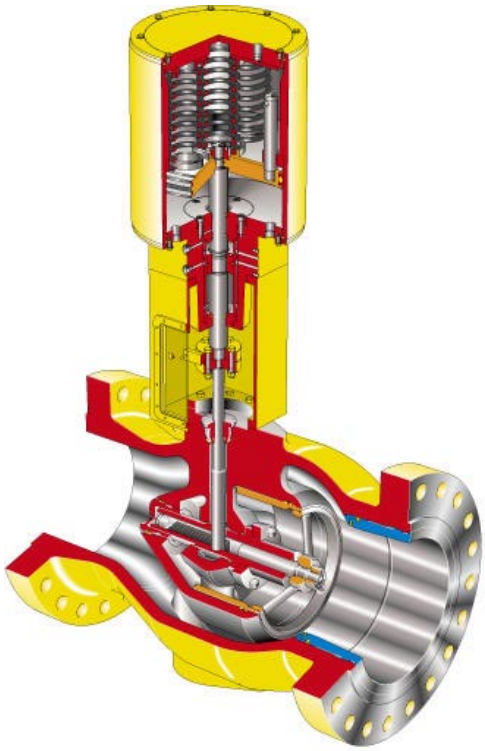
Direktevirkende pneumatisk logikk har vært mye brukt sammen med trykkbrytere (bl.a. på Kårstø).

En fast fortrådet (*hardwiret solid state*) løsning er ofte brukt i kombinasjon med redundante trykktransmittere. Logikken består da av trippforsterkere med etterfølgende voteringselement.

Programmerbar løsning er ofte brukt i PPS, i kombinasjon med trykktransmittere.

2.6 Ventil/aktuerende element

Vanligvis benyttes (hurtiglukkende) ventiler som aktuerende element (sluttelement). Det finnes selvsagt mange potensielle leverandører, men den dominerende er Mokveld med sin spesielle ventil, se Figur 5. Disse *axial flow* ventilene (RZD-X-SAV) har et trykk-balanseringssystem som bl.a. muliggjør hurtig lukking.



Figur 5 Mokveld ventil (RZD-X-SAV) anvendt i HIPPS-løsninger

I forhold til en spjeld/kule eller seteventil, har denne konstruksjonen vist seg å fungere bra i HIPPS-anvendelser.

Valtek har også levert en rekke HIPPS-ventiler av typen *butterfly*. Disse har særlig vært brukt for avstenging av damptilførsel til separator-kolonner (Kårstø).

Videre leverer en annen leverandør hurtiglukkende (under 1 sekund) sluseventiler (*gate*-ventiler), som er brukt subsea. Disse ventilene baserer seg på dobbel “block and bleed” prinsippet. Ventilaktuatorene er uten fjær-retur. Trykket i produksjonsrøret brukes som drivkraft for å lukke ventilene. Her vil 1” kryssover ventiler (”fail open”) sørge for hydraulisk forbindelse mellom

over-og underside av stempelet i aktuator. Straks kryssover ventilen åpner, enten som følge av et signal fra trykksensorer, eller ved bortfall av elektrisk eller hydraulisk kraft, vil hydraulikkvæsken hurtig bli overført fra "åpne" til "lukke"-siden av stempelet, og HIPPS-ventilene stenger raskt. For å unngå hydratdannelse mellom HIPPS-ventilene, er det koblet opp injeksjonsporter for metanol. Annulus bleed er også tilkoblet mellom ventilene for å kunne utføre lekkasjetest, og eventuelt blø av en mindre lekkasje.

Én leverandør opplyser at også 12" kuleventiler er levert i en HIPPS-applikasjon på et landanlegg i Midt-Østen. Disse ventilene har under testing vist seg å lukke på under 2 sekunder. De leveres med to forriglede *bypass* ventiler for full funksjonstesting under produksjon (*online* testing), samt fasiliteter for delvis funksjonstesting (*partial stroke* testing).

En helt annen variant av beskyttelse mot overtrykk er det såkalte *Flare Control System* (FCS). Dette systemet forhindrer overtrykking av lukket fakkel ved hjelp av hurtigåpnende ventiler, se Avsnitt 4.1.4.

I tillegg til de rent mekaniske og hydrauliske egenskaper er det i hovedsak to forhold ved en ventil som er viktig i mange HIPPS-anvendelser:

- Lukketid
- Tetthet i lukket posisjon

Med hensyn til tetthet i lukket posisjon vil kritikalitet av dette avhenge av den enkelte applikasjon. I flere anvendelser vil det finnes andre sikkerhetsfunksjoner, slik som tilgjengelig PSV-/fakkelkapasitet og prosessikringssystemet, som når det reagerer vil forhindre videre trykkoppbygging fra en lekkasje gjennom HIPPS-ventilen. Da er tetthet til QSV i lukket posisjon ingen viktig egenskap.

HIPPS installeres ofte fordi det er viktig å ha en barriere som reagerer raskere enn de andre. For standard ventiler regner en som en tommelfingerregel at lukketiden er 1 sekund pr. tomme (dvs at en 10" ventil stenger tar omtrent 10 sekunder å stenge), mens en HIPPS-ventil kan stenge på under 2 sekunder. Med så korte reaksjonstider vil en få voldsomme mekaniske påkjenninger ved nedstengning, spesielt hvis det er væskefraksjoner i strømningen. Design av ventilen er derfor svært sentralt.

Det må også nevnes at for PPS benyttes av og til et relé som sluttelement. Dette kan f.eks. trippe kraftforsyninga til en gasskompressor.

2.7 Totalkonfigurasjon/redundans

Grad av redundans har stor betydning for sikkerhet og regularitet. De fleste anvendelser trenger ikke redundans for å oppnå nødvendig sikkerhet. Høye krav til sikkerhetstilgjengelighet kan imidlertid medføre to ventiler i serie og/eller dubliserte/tripliserte trykkmålere. Dette kan bl.a. være påkrevet for å oppnå en ønsket SIL-klasse.

Som oftest er HIPPS-løsningene redundante ut fra krav til regularitet, dvs for å

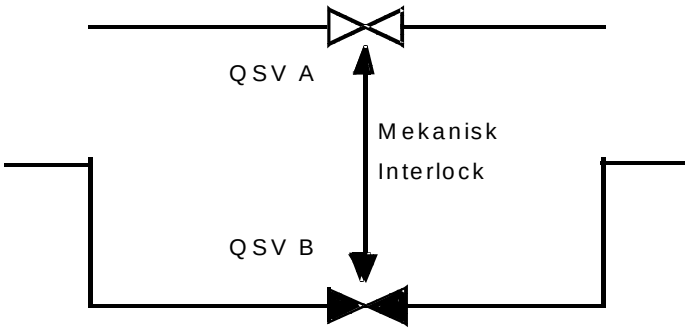
- kunne teste systemet uten å stoppe produksjonen;
- unngå nedstengning på grunn av enkle feil på HIPPS.

For eksempel er det i Norsok P-001, /13/, spesifisert alternative løsninger for en HIPPS-sløyfe (dvs. den totale funksjonen med sensor, logikk og ventil). I Avsnitt 4.4 gis det fire kombinasjoner av brytere, transmittere og trippforsterkere[2]:

- direktevirkende trykkbryter (jfr Figur 1);
- enkel trykktransmitter med trippforsterker;
- doble trykktransmittere med trippforsterkere i 1oo2 votering;
- triple trykktransmittere, votert 2oo3.

For å kunne teste transmittere uten å gjøre noe med logikken, er 2oo3 votering av transmittere mye brukt. En kan da trykke opp en og en transmitter og registrere at den går i alarm, uten å koble ut noe i logikken. Som påpekt i /13/ vil voteringslogikken for 2oo3 gjøre systemet noe mer komplekst, noe som også kan virke negativt på sikkerhet/pålitelighet.

For systemer der nedetid på grunn av funksjonstesting ikke kan aksepteres, vil en løsning som vist i Figur 6 kunne benyttes. Her er to HIPPS-ventiler, QSV A og QSV B installert i parallell, mens bare ett løp normalt er åpent. Da begge ventilene må være stengt for å blokkere røret, er det viktig at den forgreiningen som ikke er operativ (der det kan drives test/vedlikehold) er blokkert. En løsning der to ventiler må stenge for å blokkere røret, vil sikkerhetsmessig bli dårligere enn én enkelt ventil. Hver ventil vil kunne isoleres ved hjelp av to manuelle blokkventiler (slik at grenen kan avstenges når ventilen tas ut til overhaling).



Figur 6 Ventil i *standby* for å kunne teste uten driftsstans

Dersom ventilen B er stengt under normal drift, vil denne åpnes i forbindelse med full testing av ventil A, som da er åpen. Ved hjelp av et spesielt nøkkelsystem (mekanisk *interlock*) sikres at ikke begge ventiler er oppe samtidig. Hver ventil har plass til to nøkler (én svarer til at ventil kan åpnes, og én til lukking). Normalt befinner en nøkkel seg i hver ventil og én i kontrollrommets nøkkelskap.

Prosedyren starter med at en henter "startnøkkel" fra kontrollrommet som settes i B, slik at B kan åpnes. (Da vil i en kort periode begge ventiler være åpne.) Deretter fjernes "lukke-nøkkelen" som var i B og overføres til A, slik at A kan stenges. Deretter bringes den nøkkelen som opprinnelig var i A til nøkkelskapet i kontrollrommet. Dette er da startnøkkel ved den motsatt prosedyre for

[2] Forsterker (komparator) som kan justeres slik at utgangen slår om når inngangen passerer en innstilt verdi.

åpning av A. Merk at hvis en ikke avslutter denne prosedyren midt i, vil den perioden da begge ventiler er åpne samtidig være meget kort. Det er også en egen nøkkel i bruk under selve testingen.

Til slutt påpekes at totalløsningen må lages slik at den svikter til en på forhånd definert tilstand ved farlige feil (*fail-safe).* Da stenging av ventilen er sikker tilstand, lages systemet slik at brudd på hydraulikkrør/lufttilførsel eller bortfall av energi fører til at ventilen lukkes (NE - ”Normally Energized”).

3 HIPPS i regelverk og standarder

Formålet med dette avsnittet er å diskutere bruken av HIPPS opp mot relevante standarder og forskrifter, herunder:

- NORSOK
- ISO 10418 (API RP 14C)
- IEC 61508 / IEC 61511
- selskapsspesifikke kravdokumenter

Det er beskrevet hva hver av disse referansene sier om bruk av HIPPS og hvordan dagens praksis stemmer overens med dette.

Videre diskuteres hva ODs regelverk sier om bruken av HIPPS og hvordan dette forholder seg til ovenfor nevnte referanser.

3.1 NORSOK

Bruk av HIPPS er omtalt i følgende Norsok standarder:

- P-001, ”Process design” Rev. 4, Oct. 1999, ref /13/
- P-100, ” Process systems”, Rev. 1, August 1997, ref /14/

P-001, ”Process design” inneholder et eget avsnitt om bruk av HIPPS (avsnitt 4.4). Tabell 1 nedenfor oppsummerer de viktigste punktene fra avsnitt 4.4 i denne Norsok standarden

Under spesifikke systemkrav (redusert PSV- og fakkelkapasitet) merker vi oss at med hensyn til *hydraulisk kapasitet* skal PSV, fakkelrør, væskeutskiller og flammetårn designes for samtidig feil av to HIPPS-sløyfer. Dette kravet kommer til anvendelse når flere enn to linjer med HIPPS rutes inn til samme fakkelrør. Kravet er ikke formulert slik i klartekst i standarden, men følger av Figur 3 i aktuelle avsnitt av standarden P-001, og teksten i tilknytning til denne. SINTEF er usikker på hvor gjennomtenkt konsekvensene av å gi et såvidt bastant krav er.

I kapittel 43.2.2.4 (under *Flare*) av Norsok P-100 står det at dersom HIPPS brukes for å redusere nødvendig fakkelkapasitet, så skal det dokumenteres at sikkerheten opprettholdes på sammen nivå som om en brukte ISO 10418/API RP 14C. Ellers er det ikke funnet noe konkret om HIPPS i P-100.

Legg spesielt merke til at NORSOK P-001 sier at HIPPS ikke skal *erstatte* PSV i prosessanlegg for å beskytte trykktanker, rør og utstyr, men kan brukes for å *redusere* krav til fakkel-kapasitet. I spesielle scenarier, slik som ”oppstartsscenariet” (ref. avsnitt 2.2), bør det kunne vurderes å avvike fra dette absolutte kravet.

Tabell 1 HIPPS i Norsok standard P-001, ”Process Design” (Avsnitt 4.4).

Stikkord	**Innhold i Norsok standard P-001, ”Process design”**
Anvendelse	HIPPS skal bare anvendes i tilfeller hvor bruk av konvensjonell trykkavlastning (PSV) er vurdert som upraktisk (for eksempel p.a.e.ekstreme kostnader). Følgende konkrete anvendelser aksepteres: - som ersatning for PSV ved overtrykksbeskyttelse av undervanns rørledninger - i prosessanlegg for å redusere krav til PSV og fakkel kapasitet
Pålitelighets-krav	I de tilfeller HIPPS brukes som trykkbeskyttelse-system skal systemet ha en like god eller bedre pålitelighet enn konvensjonell trykkavlastning (PSV). Alternativt, kan IEC 61508 metodikk brukes for å fastsette et SIL (Safety Integrity Level) krav til den spesifikke anvendelsen.
Generelle systemkrav	- systemet skal være i overenstemmelse med DIN 3381 - stengetid for HIPPS-ventiler skal være maks 2 sekunder - det skal være uavhenhig og dedikert instrumentering - det skal være lokal reset - systemet skal være ”fail safe close” - Dersom HIPPS består av flere ”sløyfer” skal disse være uavhengige av hverandre - det skal alltid utføres en tredje parts verifikasjon av design, instrallasjon og prosedyrer
Spesifikke systemkrav	<u>Ved beskyttelse av rørledninger:</u> - To HIPPS-sløyfer i serie kan være nødvendig for å oppnå påkrevd pålitelighet. Når maks trykket i rørledningen er mindre enn det hydrostatiske testtrykket, kan én enkel HIPPS-sløyfe være tilstrekkelig. - Dersom en intern lekkasje gjennom HIPPS-ventilen er kritisk mht overtrykking av nedstrøms utstyr, skal det installeres en liten PSV. Maks tillatt intern lekkasjerate skal aldri overstige 50% av PSV kapasiteten. <u>For å redusere krav til PSV og fakkelkapasitet:</u> - HIPPS skal ikke erstatte PSV i prosessanlegg for å beskytte trykktanker, rør og utstyr, men kan brukes for å redusere krav til fakkel kapasitet - I prosessanlegg med parallelle utstyrstog kan HIPPS brukes for å forhindre at samtidig fakling blir et design kriterium. Dette kan redusere designkrav til flammetårn betraktelig - Én HIPPS-sløyfe per tog vil normalt gi en tilstrekkelig pålitelighet. - Med hensyn til *hydraulisk kapasitet* skal PSV, fakkelrør, væskeutskiller og flammetårn designes for samtidig feil av to HIPPS-sløyfer - Med hensyn til *varmestråling* skal flammetårn, som et minimum, designes for feil av én HIPPS-ventil
Andre krav	Det settes krav om at HIPPS skal funksjonstestes hver tredje måned for å oppnå påkrevd pålitelighet. Intern lekkasje gjennom HIPPS-ventilene skal testes årlig. Av regularitetshensyn kan det være nødvendig å installere HIPPS-ventiler i parallell for å muliggjøre testing under produksjon.

3.2 ISO 10418 (API RP 14C)

I ISO 10418, ”Analysis, design, installation and testing of basic surface process safety systems for offshore installations” (Ref /16/) behandles ikke HIPPS eksplisitt. Det henvises imidlertid flere steder til at et instrumentert sikringssystemer (ISS) kan erstatte tradisjonell API RP 14C sekundærbeskyttelse (PSV) gitt at ISS designes og implementeres i henhold til IEC 61508.

Det er ellers verdt å merke seg følgende formulering angående overtrykk i ISO 10418 (se avsnitt 6.2.11): *“protection from overpressure might be provided by a PSH, which could be used to initate isolation of the affected equipment before rupture can occur, ...”*. I tidligere versjoner har API

RP 14 C sagt at (jfr. avsnitt 3.4): *"the PSH prevents rupture by shutting in the affected equipment before pressure becomes excessive"*. I ISO 10418 er det altså en tilsynelatende lemping på dette absolutte kravet om at det skal være en PSH som beskytter mot overtrykk. Delvis på bakgrunn av dette har OD i sitt nye utkast til regelverk formulert følgende krav (fra RP14C):

"Prosessikring skal utformes med to uavhengige sikringsnivåer for beskyttelse av utstyr."

3.3 IEC 61508 og IEC 61511

Den internasjonale standarden IEC 61508, "Functional safety of electrical/electronic/ programmable electronic (E/E/PE) safety–related systems", beskriver en framgangsmåte for å oppnå et akseptabelt sikkerhetsnivå for et gitt utstyr/installasjon ved bruk av instrumenterte sikkerhetssystemer. IEC 61508 er en generisk standard og legger grunnlag for videre utvikling av bransjespesifikke standarder, herunder IEC 61511 som er prosessindustriens svar på dette.

Ifølge IEC 61508/61511 skal det gjennomføres en risikoanalyse for å beregne risikoen knyttet til det utstyret som skal beskyttes (dvs "*EUC risiko*"). Videre skal akseptabel risiko angis, og herav utledes krav om risikoreduksjon som stilles til de risikoreduserende systemer.

IEC 61508 skiller mellom tre ulike typer av risikoreduserende systemer (og standarden fokuserer på de første av disse tre):

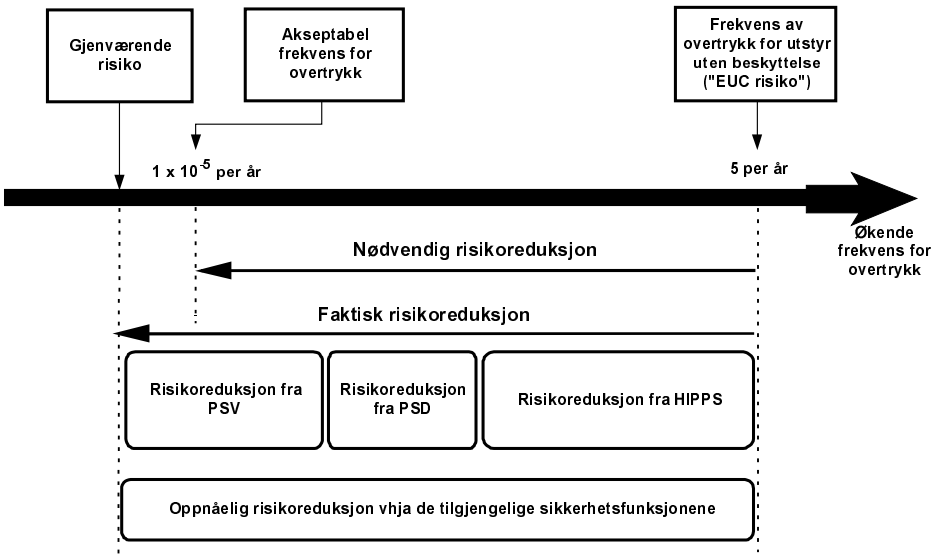
- instrumenterte sikkerhetssystemer, (som f.eks. NAS, PAS B&G, HIPPS, osv.)
- sikkerhets-relaterte systemer basert på annen teknologi, (som f.eks. en PSV)
- andre eksterne risiko-reduserende fasiliteter (som f.eks. en brannvegg, bruk av prosedyrer, osv.)

Disse tre kategoriene av sikkerhetssystemer skal alene eller i kombinasjon med hverandre redusere risikoen til et akseptabelt nivå for den faren ("hazard") som vurderes. Dette er illustrert i Figur 7 nedenfor, hvor én del av overtrykksbeskyttelsen for utstyr (en separator) består av HIPPS.

For subsea HIPPS er det behov både for ekstra noder og kommunikasjon, og IEC 61508 stiller krav om at styresystemet på plattformen som kommuniserer med subsea HIPPS logikken i størst mulig grad gjøres uavhengig av øvrige plattform sikkerhetssystemer (PAS) og ikke påvirkes av feil i disse systemene. Det kreves uavhengighet mellom subsea kommunikasjon og topside systemer for PAS og HIPPS (se Del 1, 7.6.2.7).. Hvis feil i PC system kan gi demand til PAS eller til instrumentert system (som kan står for testing av HIPPS ventiler), må PC system vare adskilt fra og være uavhengig av disse systemene (se Del 1, 7.5.2.4.d).

IEC 61508 standarden er etterhvert hyppig referert og den henvises til både i ISO 10418 og i det kommende regelverket. Det bør i denne forbindelse nevnes at industrien i samarbeid med SINTEF og OLF utarbeider en retningslinje for bruk av IEC 61508/61511, /9/.

Det bør understrekes at hverken IEC 61508 eller 61511 går konkret inn på HIPPS-anvendelse men at de snarere angir en risikobasert metodikk for fastsettelse av krav til slike systemer.



Figur 7 Risikoreduksjon iht IEC 61508 ved hjelp av HIPPS, PAS og PSV

3.4 Operatørenes egne spesifikasjoner

Lenge var det kun Statoil og Elf som opererte HIPPS-anlegg i Norge. Det er opplyst at Norsk Hydro nå har HIPPS på Visund (1997), men dette er ikke bekreftet av NH. Videre har Norsk Hydro såkalt IOPS (Instrumented Overpressure Protection System) på Snorre TLP. Hydro planlegger dessuten å installere HIPPS på totalt 14 linjer på den nye Tune modulen på Oseberg D.

Statoil
Statoil arbeider nå med å fullføre sin egen spesifikasjon med tittel "General Specification. HIPPS in Offhore & Onshore Applications". Disse retningslinjene gir detaljer på beste design praksis for de ulike applikasjonene av HIPPS i Statoil. Ulike anvendelsesområder for HIPPS er beskrevet. Dokumentet gir også en rekke sikkerhetskrav, og presenterer akseptkriterier (stort sett knyttet til hyppighet for overtrykking). Retningslinjene er basert på IEC 61508. Bl.a. behandles også SIL-allokering, og dokumentet gir eksempler på hvordan et SIL2 eller SIL3 krav skal oppfylles.

Norsk Hydro (NH)
På forespørsmål har NH opplyst at de foreløpig ikke har noen egne spesifkasjoner på HIPPS men at en i hovedsak følger Norsok P-001.

Elf Norge
ELF opplyser å ha sine egne spesifikasjoner som ikke er rene HIPPS-spesifikasjoner, men et system som refereres til som "CHAPS" (*Concept for High Availability Protection Systems*). Her vurderes ikke bare selve HIPPS-barrieren isolert sett, men hele sikkerhetsfunksjonen inkludert effekten fra prosess-kontrollsystemet, PAS systemet og eventuelt andre risikoreduserende tiltak; (altså analogt til en IEC 61508 tilnærming).

3.5 ODs regelverk

OD's gjeldende og framtidige regelverk nevner ikke HIPPS eksplisitt, men sier heller ikke at det er forbudt å bruke HIPPS. Det er imidlertid en forutsetning at løsningen med HIPPS blir sikkerhetsmessig like bra som den konvensjonelle løsningen den erstatter. Dette betyr da at hvis

HIPPS f.eks. brukes for å begrense fakkelraten, dvs som en del av prosessikringssystemet, gjelder følgende krav:

- systemet må være uavhengig av andre systemer, f.eks. fra regulering og NAS
- det skal i utgangspunktet være to fysisk og funksjonellt forskjellige systemer for overtrykkbeskyttelse

Hvis en tenker seg en løsning med PAS og HIPPS p.g.a. at en ikke har fullkapasitets fakkel i henhold til API RP 520/521, må dette da behandles som et avvik i forhold til kravene ovenfor. Også i OLF retningslinjene, /9/, blir HIPPS behandlet som et avvik fra standard løsninger, og krever spesiell dokumentasjon ihht. IEC 61508.

4 HIPPS-installasjoner

I dette kapittelet gis en oversikt over de HIPPS-løsninger (inklusiv varianter av HIPPS), som finnes i Norge.

4.1 Ulike varianter av HIPPS

I kapittel 2 ble "standard HIPPS" beskrevet. I dette avsnittet ser vi også på en del konsept som har liknende funksjonalitet, og som av og til derfor omtales som HIPPS. Vi ser her på følgende betegnelser/type system som er registrert i bruk.

OPPS - Over Pressure Protection System (Elf)
CHAPS - Gas Inlet Concept for High Availability Protection System (Elf)
IOPS - Instrumented Overpressure Protection System (Saga)
FCS - Flare Control System
PPS - Pipeline Protection System
Subsea HIPPS - Subsea High Integrity Pipeline Protection System

I tillegg innfører vi i denne rapporten begrepet *prosess HIPPS* som representerer en konvensjonell HIPPS med hurtiglukkende ventil.

Merk at slik Elf bruker begrepene OPPS og CHAPS, er dette betegnelser på et totalsystem bestående av en rekke overtrykksbarrierer, hvorav den egentlige "HIPPS-barrieren" bare utgjør én av disse. Hvis en bruker denne notasjonen er derfor OPPS og HIPPS to helt forskjellige ting. Til dels har vi noe av samme "problem" med Statoil, som til dels har brukt HIPPS om totalsystemet av flere barrierer. I en del anvendelser (Kårstø gass-terminal) inkluderes dedikerte og oppgraderte kontrollventiler som en del av HIPPS-konseptet, hvor da HIPPS defineres som totaliteten av kontrollventil-barrieren og den egentlige HIPPS-barrieren, jfr Figur 2.

I denne rapporten vil vi i hovedsak tolke HIPPS, OPPS, osv. som betegnelse på én spesifikk overtrykksbarriere, mens vi ikke har noen slik betegnelse for å representere totaliteten av alle barrierene. De beskrivelsene som gis under i Avsnittene 4.1.5. - 4.1.7. vil imidlertid være et unntak fra dette; da vi her beskriver de enkelte operatørenes egen notasjon. Under gis en kort beskrivelse av de sju HIPPS-begrepene som omtales i rapporten.

4.1.1 Prosess HIPPS

Dette er den typiske situasjon illustrert i Figur 2. En HIPPS-sløyfe består her av en eller flere trykkmålere i prosessen, som ved høyt trykk sender stengesignal til en hurtiglukkende HIPPS ventil(er) som stenger tilførselen av prosessmediet.

4.1.2 Subsea HIPPS

Fra en subsea installasjon vil en ofte (pga kostnader) unngå å dimensjonere stigerøret opp til plattformen for fullt brønntrykk. Nedstrøms ventilene (ving/master) på subsea ventiltre, og evt også nedstrøms subsea manifold når det er flere brønner, installeres derfor en hurtiglukkende "HIPPS-ventil. Ved stenging topside og begynnende trykkoppbygning i stigerøret vil da trykksensor gi lukkesignal til denne HIPPS-ventilen.

Så langt har en ikke *subsea* HIPPS-anvendelser i Norge. På Gullfaks fase II er det imidlertid identifisert en brønn hvor en forventer å se trykk på omkring 440 bar. Designtrykket for rørledninger og mottakssystem er her 390 bar. For å unngå å måtte øke designtrykket til 440 bar,

har en valgt å montere HIPPS-ventil nedstrøms choken på denne brønnen. HIPPS-ventilen vil virke som en sikkerhetsventil og stenge dersom trykket overstiger 390 bar (merk: leverandør bruker her "HIPPS" i betydningen High Integrity Pipeline Protection System). Et tilsvarende system er benyttet *topside* på plattformer tidligere, men dette er første gang det blir installert et kvalifisert system subsea. En egen opptrekkbar HIPPS kontrollmodul for styringen av systemet er plassert på manifolden.

Også på Kristin er det planer om å installere en subsea HIPPS-løsning for beskyttelse av rørledning og stigerør.

4.1.3 Pipeline Protection System

PPS betegner en kategori HIPPS-anvendelser som brukes for å kunne operere en rørledning med to ulike trykklasser. I et slik "*spec break*" konsept utnyttes at trykket i fluidet avtar langs en eksportledning. En oppnår derfor betydelige kostnadsbesparelser ved å dimensjonere deler av rørledningen for lavere trykk enn eksporttrykket. Ved blokkering på lavtrykksiden av rørledningen er det behov for å stenge tilførselen inn i rørledningen. Oftest har en her god tid før avstenging er nødvendig.

Som kompenserende beskyttelse benyttes et automatisk nedstengingssystem, PPS, som består av sensor + logikk/signaloverføring+aktuering. Sensorer skal registrere evt. blokkering av "utløpet" av rørledningen (hos mottaker), og her brukes enten

- trykkmåler, som indirekte viser at en ventil har stengt (eller blokkering på annen måte), og/eller
- posisjonsbryter, som viser at ventil har stengt

Logikken er typisk et programmerbart system. En har ofte behov for signaloverføring (f.eks. via satellitt) tilbake til eksportsiden, eller mellom ulike PPS på samme ledning (der f.eks. aktivering av PPSen på en del av rørledningen kan trigge PPSen "oppstrøms".

Aktueringen kan være å
- lukke ventil på utløpssiden, og slik blokkere for videre fylling av rørledning, og/eller
- trippe eksport-kompressorer.

4.1.4 Flare Control System

FCS er betegnelse på et system som ved hjelp av hurtigåpnende ventiler forhindrer overtrykking av fakkelsystemet, i tilfeller hvor en har valgt å bruke lukket og slukket fakkel . Dette er i prinsippet vesensforskjellig fra et egentlig HIPPS-konsept, og i rapporten brukes derfor FCS om denne type system, selv om leverandør omtaler det som HIPPS. Systemer av typen FCS vil ikke diskuteres i særlig grad i rapporten, men de tas med i total-oversikten over HIPPS-installasjoner i Avsnitt 4.2.

4.1.5 Over Pressure Protection System

OPPS ble benyttet på Frigg, og er designet for beskyttelse av "sales gas header network". Dette systemet ble tatt i bruk i 1987 (etter at Alwyn ble koplet til TP1 plattformen) og erstatter tradisjonell "full flow PSVer" i form av tre uavhengige barrierer:

- En "initiell" barriere som består av en dedikert funksjon implementert i kontrollsystemet for å stoppe kompressorer og lukke ventiler så snart en ventil på havbunnen ikke er fullt åpen.
- En "primær" barriere som omfatter dedikerte trykktransmittere som tripper kompressorene og ventilene ifølge prinsippene i API RP 14C.

- En "sekundær" barriere som består av et sett triplikerte trykktransmittere som tripper dedikerte "sluttelement" via et eget programmerbart logisk system. Denne sekundære barrieren kan oppfattes å være ekvivalent med HIPPS-konseptet.

4.1.6 Gas Inlet Concept for High Availability Protection System

CHAPS ble benyttet på NEF (Nordøst Frigg) og lille-Frigg for beskyttelse mot overtrykk av innløpsseparator, da innløps rørledning ikke var utstyrt med full PSV kapasitet. Dette konseptet inkluderer fire uavhengige barrierer:

- En "initiell" barriere som består av en dedikert funksjon i prosesskontrollsystem for å lukke innløpsventiler så snart en hendelse som initierte overtrykk inntreffer; (en slik initierende hendelses vil være en ventil nedstrøms separatoren som er ikke fullt åpen, og enhver hendelse som initierer PAS).
- En "primær" barriere som omfatter dedikerte trykktransmittere som lukker innløpsventilene via PAS.
- En "sekundær" barriere som består av et sett tripliserte trykktransmitere som tripper dedikerte "aktuerende element" via programmerbart logisk system innebygd i ISS. Denne sekundære barrieren kan oppfattes å være ekvivalent med HIPPS-konseptet.
- Full PSV kapasitet på tank.

En variant av CHAPS / OPPS, kalt *Frøy Gas Lift Separator OPPS*, blir benyttet på Frøy. Dette systemet blir i denne rapporten ikke beskrevet, men blir kort referert som *Gas lift OPPS*.

4.1.7 Instrumented Overpressure Protection System

IOPS er en "avart" av HIPPS som er brukt på Snorre og Vigdis (driftstart oktober 2000). Følgende type beskyttelse er implementert:

- Nivåmåler på førstetrinns separator (LALL) utløser stenging av isolasjonsventilen mellom første og annen trinns separator: Beskytter mot gassgjennomblåsing fra første til annen trinns separator. Det er for liten PSV kapasitet på annet trinns separator, og dette kan drmed ses på som en prosess *HIPPS-variant.*
- *Dedikert nivåmåler* på førstetrinns separatorer (LAHH) utløser stenging av isolasjonsventil på produksjonsmanifolder: Beskytter mot høyt væskenivå i Snorre og i Vigdis 1.trinns separator (to ulike system).
- Beskyttelse mot høyt væskenivå i Snorre og i Vigdis produsert vann i avgassingstank (to ulike system).
- Beskyttelse mot høyt væskenivå i Snorre testseparator.

Nivåmålere gir signal både til IOPS-noden og PAS-noden.

4.2 Oversikt over HIPPS-installasjoner i Norge

Tabell 2 gir en oversikt over (kjente) HIPPS-løsninger i norsk olje/gass-virksomhet. Oversikten er ordnet etter operatør og installasjon (felt). Systemet er så klassifisert etter HIPPS-variant, og det gis kjent informasjon over sensor, logikk og *sluttelement* (typisk *ventil*).

I siste kolonne gis ulik utfyllende informasjon. Der det er gitt opplysninger om standarder som er fulgt (eller oppnådd sikkerhetsklasse) er dette angitt i tabellen.

Tabell 2 **Oversikt over Norske HIPPS-installasjoner**

Ope-ratør	År	Instal-lasjon	Type system	Sensor	Logikk	Ventil - *sluttelement*	Medium	Funksjon / beskrivelse
Elf	1987	Frigg-feltet	OPPS	Foxboro 821GH	Dual ASEA master 140 controllers	4" Neles (stenger *fuel gas supply* linjer til turbin som driver kompressor; kun aktivt til 1994)	Tørrgass	Ett system. To (tidligere 5) grupper av tripliserte PTer. Spesiell voter-ingslogikk, basert på gjennomsnittsverdien i hver gruppe. Innstengningstrykk på gass: 20 barg. Lukketid < 1 sek. Initierer også stenging av 3 NAS ventiler og stopper kompressor på Alwyn, (fremdeles aktivt).
	1994-1999	Lille Frigg	CHAPS	Rosemount 821GH Triplisert trykktransmitter	Bailey (nå ABB) INFI90 (MFP02)	2x9" Mokveld RZD-X	Våtgass, kondensat	Ett system. Overtrykksbeskyttelse av innløps-separator Innstengningstrykk på gass: 530 barg. Lukketid <2 sek Initierer også subsea nedstenging (via subsea control enhet), lukking av innløps "sealine" ESV og PAS
	1996	Frøy	Gas lift OPPS	Rosemount 1151GP Triplisert trykktransmitter	Bailey (nå ABB) INFI90 (MFP02)	2" Petro kuleventil	Tørrgass	Overtrykksbeskyttelse av DEG system Trykktransmitter mellom choke og "vessel". Lukketid 2 sekunder, men kravet til responstid på flere minutter
Norsk Hydro	1996	Njord	FCS SIL2	Fisher-Rosemount 3051 trykktransmitter 1oo2 votering	HIMA Planar F Hardwired Solid state TUV AK6	16" og 24" Fisher Posiseal Butterfly, (SAAS)	Gass	Lukket fakkelsystem med hurtigåpnende ventiler Åpningstid <2 sek DIN V19250
	1998	Oseberg Gass	FCS SIL2	Fisher-Rosemount 3051 trykktrans 1oo2 votering	HIMA Planar4 Solid state TUV AK7	20" Fisher Posiseal Butterfly, (SAAS)	Gass	Lukket fakkelsystem med hurtigåpnende ventiler Åpningstid <2 sek
	1999	Oseberg Sør	FCS SIL2	Fisher-Rosemount 3051 trykktrans 1oo2 votering	HIMA Planar 4 Solid state TUV AK7	20" Fisher Posiseal Butterfly,(SAAS)	Gass	Lukket fakkelsystem med hurtigåpnende ventiler. Åpningstid <2 sek
	1997 og 2000	Snorre TLP	IOPS	Nivå-transmitter	logikk implementert i PAS og NAS	16" BEL (NAS) sluseventil	Gass	- Beskytter mot gassgjennomblåsning, (*partial flow* PSV) - Beskytter mot høyt væskenivå
	1997	Visund	Prosess HIPPS		HIMA Planar F Hardwired Solid state TUV AK6			

	TBI	Tune / Oseberg D	Prosess HIPPS SIL3	Moore trykktransmitter XTC 345G (0-150 barg)	HIMA Planar 4. Hardwired Solid state TUV AK6	4" Mokveld. RZD-X-SAV. hydraul. solenoid 14 ventiler	Gass	Beskytter nedstrøms utstyr mot overtrykk pga begrenset fakkelkapasitet. Totalt 2x7 =14 linjer. 1oo1 votering hver linje; tåler at 2 av 14 linjer ikke stenger. IEC 61508
Statoil	1991	Kårstø gass terminal	Prosess HIPPS	Pneumatisk trykkbyter, Tiefenbach	Direktevirkende pneumatisk aktuering, Walter styreventil	10"-12" Valtek Butterfly	Damp	8 linjer (hver med to ventiler i parallell)
	"	"	Prosess HIPPS	Pneumatisk trykkbyter, Tiefenbach	Direktevirkende pneumatisk aktuering Walter styreventil	10"-12" Mokveld RZD-X-SAV	Gass	6 linjer (hver med to ventiler i parallell)
	1993	Kårstø, Sleipner kondensat	Prosess HIPPS	Pneumatisk trykkbyter	Direktevirkende pneumatisk aktuering	10"-16" Valtek Butterfly	Damp	5 linjer (hver med to ventiler i parallell)
	"	"	Prosess HIPPS	Pneumatisk trykkbyter	Direktevirkende pneumatisk aktuering	16" Mokveld RZD-X-SAV	Gass	1 linjer (med to ventiler i parallell)
	1993	Kårstø Statpipe ekspansjon				10" Mokveld RZD-X-SAV	Gass	2 ventiler (*slam shut* ventiler)
	2000	Kårstø modifik-asjon	Prosess HIPPS			4" - 12" Mokveld. RZD-X-SAV	Gass, olje	I alt 56 ventiler på prosessanlegg.
	"	"	Prosess HIPPS			8" - 12" Valtek Butterfly	damp	10(?) ventiler på prosessanlegg.
	1996	Kollsnes gassterm. Troll landanlegg	PPS SIL3	Fisher - Rosemount 3051 trykktransmitter 2oo3 votering	HIMA Planar F Hardwired Solid State 2oo3 votering TUV AK6	6x24" Mokveld. RZD-X-SAV. Lucifer solenoid, Midland quick exhaust	Tørrgass	Beskytter 3 gassbehandlingstog pga begrenset fakkelkapasitet. HIPPS på hvert tog. By-pass ventilene er utstyrt med overvåket , mekanisk forrigling. Lukketid<2 sek. DIN V19250, API RP14C
	"	"	PPS SIL3	Fisher-Rosemount 3051 trykktrans 2oo3 votering	HIMA Planar F Haedwiret Solid State TUV AK6	Signal virker direkte på elektrisk hovedbryter på kompressorene	Tørrgass	På alle fem eksportkompressorer, for beskyttelse mot for høyt eksport-trykk

	1999	Åsgard transport, Kårstø	PPS SIL3	Fisher-Rosemount 3051 trykk-transmitter *eller* posisjonsbryter, 2oo3 votering	HIMA F51 Safety PLC, programmerbar TUV AK6	Mokveld?	Tørrgass	HIPPS for ilandføringstasjonen fra Åsgard feltet for beskyttelse av Kårstø anlegget (inkl landledning Kårstø-Kalstø), (betegnet LPPS; L=Land) Vil senere inkludere PPS for transport-rørledningen fra Åsgard, (betegnet OPPS; O = *Offshore*).
	1997	Åsgard A	Prosess HIPPS		HIMA Planar F Hardwired Solid state	10x10" Mokveld RZD-X-SAV-2	Brønnstrøm	10 ventiler, flowline DIN V19250
	"	"	PPS		"	5x4" Mokveld RZD-X-SAV	Gass	5 ventiler, stopper *fuel gas* til kompressor DIN V19250
	"	"	FCS		"	2x24" Mokveld RZD-X-SAV	Gass	2 ventiler ("Flare quick opening valve") DIN V19250
	1998	Åsgard B	Prosess HIPPS	Trykk-transmitter	HIMA Planar F Hardwired Solid state	9x10" + 2x12" Mokveld RZD-X-SAV	Gass	11 ventiler DIN V19250
	"	"	Prosess HIPPS	"	"	12" Mokveld RZD-X-SAV	Gass	1 ventil, *Excess gas* DIN V19250
	"	"	PPS		"	4x4" Mokveld RZD-X-SAV	Gass	4 ventiler, stopper *fuel gas* til kompressor DIN V19250
	1995	Gullfaks A	FCS		HIMA Planar F Hardwired Solid state. AK6	2x24" Mokveld RZD-X-SAV	Gass	For flare, vent&blowdown system DIN V19250
	1999	"	FCS			30" Mokveld RZD-X- SAV	Gass	1 ventil ("flare quick opening valve")
	2000	"	Prosess HIPPS		HIMA Planar 4 Hardwired Solid state, AK6	2x16" Mokveld RZD-X-SAV	Gass	2 ventiler DIN V19250
	1995	Gullfaks C	FCS		HIMA Planar F Hardwired Solid state, AK6	2x24" Mokveld RZD-X-SAV	Gass	For flare, vent&blowdown system DIN V19250
	2000	"	Prosess HIPPS		HIMA Planar F Hardwired Solid state, AK6	4x2" Mokveld RZD-X-SAV		Mokveld: Fuel Gas compr. HIPPS Boo? DIN V19250
	TBI	Gullfaks II	Subsea HIPPS	Trykk-transmitter		FMC Gate-ventil (KOS)	Brønnstrøm	

	1995	Norne	PPS	Fisher Rosemount 3051 trykktransmitter 2oo3 votering	HIMA Planar 4 Hardwired Solid state, AK6	8" Mokveld, RZD-X-SAV	Gass	1 ventil, eksport system DIN V19250
	1997	Heidrun	FCS		HIMA Planar F Hardwired Solid state, AK6	2x18" Mokveld RZD-X-SAV	Gass	For flare, vent&blowdown system "HP Flare Header Fast operation valve"
	1996	Veslefrikk A	Prosess HIPPS	Analog 1oo1	HIMA Planar F Hardwired Solid State	2x8" Mokveld RZD-X-SAV	Gass	
	"	Draupner E Zeepipe phase IIB	PPS			30" + 20" Mokveld RZD-GX-SAV, RZD-X-SAV	Gass	2 ventiler
	1995	Sleipner Vest	Prosess HIPPS	Trykk-transmitter, 2oo3 votering	Tricon TMR PLC 2oo3	5x24" Mokveld RZD-X-SAV		Redusert flare-kapasitet, se SINTEF studie '91. Implementert?
	1996	Sleipner "B"	PPS		HIMA H51, HRS Safety PLC	2x20" Mokveld RZD-X-SAV (hydraktuering)	Olje	(i alt 4 ventiler) Oljeeksport
	1997	Zeepipe IIA Kollsnes/ Sleipner (Emden)	PPS SIL3	Fisher-Rosem. 3051 trykktrans *eller* Posisjonsbryter (scenarieavh.) 2oo3 votering	HIMA H51, HRS Safety PLC Logikk implementert i NAS/PAS	NAS ventil (Mokveld?‘)	Gass	Sikkerhetssystem for å kunne operere rørledningen med to ulike trykklasser (”spec. break” prinsipp) (Eksportgass) DIN V19250
	1991	Gass-eksport Kårstø	PPS	Trykkbryter	"Direktevirkende pneumatisk"	8" Mokveld RZD-X-SAV	Gass	I alt 3x2 = 6 Mokveld ventiler for gasseksport Kårstø. Dessuten 4 ventiler for "Draupner Backflow Letdown"
	1999	Europipe II Kårstø/ Emden	PPS SIL3	Fisher-Rosem. 3051 trykk-transmitter, 2oo3 votering *eller* Posisjonsbryter scenarieavh.	HIMA H51, HRS Safety PLC, (inkludert satelitt kommunikasjon) TUV AK6	8" Mokveld RZD-X-SAV	Gass	Sikkerhetssystem for å kunne operere rørledningen med to ulike trykklasser (”spec. break” prinsipp) (Eksportgass)
	TBI	Kristin	Subsea HIPPS	Trykk-transmitter, (2ooN votering)	Subsea kontroll enhet	2x10" Mokveld?	Våtgass	Beskytter subsea rørledninger og Kristin stigerør…. 12 linjer, hver med 2 HIPPS-ventiler i serie (evt 12 enkle ventiler)

Når det gjelder HIPPS-"varianter", vil SINTEF foreslå at en standardiserer i form av følgende hovedvarianter:

- HIPPS [med hurtiglukkende ventil, QSV], der en har "undervariantene"
  - *prosess* HIPPS, og
  - *subsea* HIPPS
- PPS, [for rørledninger der ventilens lukketid er irrelevant]
- FCS, [hurtigåpnende ventil]

Bortsett fra "spesialvariantene" OPPS og CHAPS (tidligere Elf) og IOPS (tidligere Saga), er alle systemene i tabellen klassifisert i henhold til dette.

4.3 Oppsummering

Tabell 3 gir en oppsummering av noe av informasjonen samlet i Tabell 2. Oversikten begrenser seg til de system som er tatt i bruk. I tabellen under vil OPPS inkludere både systemene OPPS og *Gas Lift OPPS* fra Tabell 2.

Oversikten er tilnærmet, og er basert på informasjon fra mange ulike kilder som ikke er fullstendig komplett. Noe av informasjonen her er derfor basert på skjønn. En ser likevel at det nå er installert i størrelsesorden 100 systemer av ulike kategorier HIPPS, og at disse har til sammen ca 400 driftsår. Medium-kategorien "Gass/olje" inkluderer alle muligheter unntatt "tørgass" og "damp".

Når det gjelder prosess HIPPS-løsninger er det her antatt at det i alle tilfelle er dupliserte ventiler, dvs. alle systemer har ventil i kald *standby*. Antall installerte ventiler er dermed det dobbelte av antall systemer. For PPS skal 3 av 15 "system" trippe eksportkompressor. De øvrige 12 har hovedsaklig to avstengingsventiler i serie.

Tabell 3 Oversikt over installerte *systemer* (pr 2000)

System	Totalt antall	Antall system fordelt på medium			Ca. antall driftsår	(Typisk) redundans
		Tørrgass	Gass/olje	Damp		
prosess HIPPS	72	-	54	18	259	Ventil i kald *standby*
PPS	15	5	10	-	57	Redundant ventil
FCS	13	-	13	-	45	Enkle ventiler
OPPS	2	2	-	-	17	Triplisert PT
CHAPS	1	-	1	-	5	Triplisert PT
IOPS	6	-	6	-	4	Enkelt
Sum	109	7	84	18	387	-

5 Data og erfaringer med HIPPS

Her presenteres det som er funnet av erfaringsdata. Dels gjengis eksplisitte data på HIPPS-løsninger, dels mer generiske data.

5.1 Mottatte driftsdata for HIPPS

SINTEF har mottatt noe informasjon om driftserfaring og rapporterte svikt. Dette er referert under, (se forøvrig Avsnitt 5.4).

TotalFinaElf
Når det gjelder OPPS (på Frigg fra 1987)) gjelder:

- Det har ikke vært registrert noen nedstengninger p.g.a. overtrykkshendelser.
- Det er derfor heller ikke registrert noen farlige feil, dvs svikt av typen, FTO ("ikke avstengning ved demand") under operasjon. Denne feilmoden er heller ikke registrert i forbindelse med testing.
- Det er registrert 3 PT feil som førte til nedstenging, dessuten 4 hendelser der PT ble påvirket ved prosessendringer, f.eks. "line changeover"; dvs. totalt 7 nedstengninger. P.g.a. spesiell voteringslogikk vil ikke dette gi noe klart svar på hvor mange PTer som har sviktet.
- Det er registert 29 PT loop feil uten nedstengning.
- En har hatt 4 svikt i logikk, som har ført til automatisk degradert operasjon (1oo1), og 5 andre logikk feil detektert under selv-test/kontinuerlig monitorering.
- Galvanisk skille for PTer ble skifet etter 3 år, da disse forårsaket ”drift” pga temperatur effekter. Med den nye typen ble problemet unngått.

Antall svikt inkluderer altså de som ble funnet under funksjonstesting.

For CHAPS (Lille-Frigg) gjelder at i løpet av 5 års drift er

- Ingen nedstengninger registrert p.g.a. overtrykkshendelser;
- Ingen FTO feil registrert;
- Ingen systemnedstengninger p.g.a feil i CHAPS registrert.

Evt. svikt funnet under funksjonstesting ville vært inkludert.

For *Gas Lift OPPS* (Frøy) gjelder at i løpet av 4 års drifter

- Ingen nedstengninger registrert p.g.a. overtrykkshendelser
- Ingen FTO feil registrert
- Ingen systemnedstengninger p.g.a feil i Gas lift OPPS registrert..

Evt. svikt funnet under funksjonstesting ville vært inkludert.

Norsk Hydro
For IOPS beskyttelse på Snorre TLP gjelder at kun ett system ble installert i 1997, de øvrige i oktober/november 2000. En har derfor meget begrenset driftserfaring og driftsdata, men oppgir følgende to hendelser:

- Under oppstart og uttesting av IOPS systemet i september 2000 var det en IOPS-trip og prossessnedstengning p.g.a. feil ved eksisterende PAS-solenoide for isolasjonsventil på produksjonsmanifold. Årsaken var en internlekkasje av hydraulikk-olje, trolig p.g.a. slitasje / aldring som førte til at ventilen mistet hydraulikk og stengte.

- November 2000 var det en feil på nivåmåler (LAHH) for Vigdis 1. trinns separator som ga IOPS-trip og nedstengning av Vigdis prosess. Årsaken var løse forbindelser i kabel-tilkopling på nivåmåler.

Statoil
SINTEF har som input til denne studien fått tilgang til en rapport som viser observert pålitelighet av HIPPS i Statoil, se /21/. Tabell 4 viser eksponeringsdataene (antall ventilår) som ligger til grunn for analysen.

Tabell 5 resymerer observert sviktintensitet, (dvs feilrate = 1/MTBF). Først gis total feilrate, dvs feil både av "severity class" "critical", "degraded" og "incipient"; jfr OREDAs feilklassifisering. Deretter gis raten av de "critical" feil som har de farlige (sikkerhetskritiske) feilmodene, "Delayed operation" og "Fail-to-close on demand", evt "Fail-to-open on demand". Merk at flere feil er "delayed operation" og det er usikkerhet med hensyn til kritikaliteten av disse.

Tabell 4 Eksponeringsdata for HIPPS, Statoil. Underlag for pålitelighetsberegninger.

Installasjon	**Applikasjon**	**Antall ventiler**	**Installasjons-dato**	**Antall ventilår**
Troll Kollsnes	PPS og Prosess HIPPS (normalt åpen)	6	1996-07-01	24
Sleipner B		4	1996-08-01	16
Kårstø		50	fra 1991-09-01	253
Sum		60	-	293 [2)]
GFA / GFC [1)]	FCS (normalt stengt)	4	1995-01-01	22
Heidrun		2	1997-03-16	11
Sum		6	-	33

[1)] Gullfaks A / Gullfaks C
[2)] 151 år for Mokveld-ventiler og 142 år for Valtek-ventiler (benyttet for damp)

Tabell 5 Pålitelighetsdata for HIPPS, Statoil.

Applikasjon	**Total feilrate, λ pr 10^6 time** [1)]	**Ikkedetekterbar, farlig feilrate, λ_{DU} pr 10^6 time**		
		Delayed operation	***Fail to operate on demand***	**Sum**
Prosess HIPPS / PPS	7.4	0.8	3.5 [2)]	4.3
FCS	34.6	6.9	13.8 [3)]	20.7

[1)] I tillegg til "farlige feil" inkluderer dette degraderte feil og "*incipient*" feil.
[2)] Fail-to-close on demand
[3)] Fail-to-open on demand

Merk at det ser ut til at dataene i Tabell 5 muligrens kan oppfattes som feilrate for den totale HIPPS-sløyfa. I Tabell 6 er feilraten fordelt (prosentvis) på "subunit failed". En ser at det i mange tilfelle ikke foreligger eksakt informasjon om dette, og muligens kan det ikke utelukkes at det har vært trykkmåler, logikk eller ventil som har feilet. For normalt lukkede ventiler (FCS) ser en imidlertid at det primært er ventilen som har sviktet. Merk også at dette er reelle data for det *totale* antall feil, inklusiv hva en ville kalle systematiske svikt (som i PDS kvantifiseres ved TIF-sannsynligheten).

Tabell 6 Feilrate fordelt på utstyr. Prosentvis fordeling av raten av farlige feil, λ_{DU} fordelt på "subunit" (jfr OREDA)

Applikasjon	***Entire equipment*/ ukjent**	**Aktuator** [1)]	**Ventil**	***Control & monitoring***
Prosess HIPPS / PPS	73%	9%	9%	9%
FCS	17%	17%	50%	17%

1) Feilene her gjelder "Maintainable item": pilotventil, og skal vel ikke regnes med i feil på hovedventilen, etter den inndelingen som er fulgt i denne (OD-)rapporten.

5.2 Generiske pålitelighetsdata

Her presenteres en del generiske data for relevante komponenter. I Tabell 7 presenteres noen PDS-data, se /18/, som særlig bygger på OREDA, bl.a. /19/. Videre gir Tabell 8 en del data fra OLF retingslinjene for IEC 61508, /9/. Merk at disse dataene i stor grad er basert på /18/.

Merk at β-faktoren i Tabell 8 gjelder for en 1oo2 votering. I samsvar med /9/ og modifisert PDS-metodikk, /22/, justeres denne med en voteringsfaktor, C_{kooN} (k<N), se Tabell 9. Det betyr at β for en kooN votering er gitt som

$$\beta_{kooN} = C_{kooN} \cdot \beta \ ,$$

der β f.eks er gitt i Tabell 8 (gyldig for 1oo2).

Tabell 7 Pålitelighetsdata fra PDS, /18/.

Komponent	**Total kritisk feilrate, λ pr 10^6 time**	**Ikkedetekter-bar "sikker" (SO) feilrate λ_{SU} pr 10^6 time**	**Ikkedetekter-bar "farlig" (FTO) feilrate λ_{DU} pr 10^6 time**	**TIF-sann-synlighet (testuavhengige feil)**
Trykkbryter/Nivåbryter	3.4	0.9	0.2	0.001 - 0.005
Trykktransmitter	1.3	0.4	0.1	$3 \cdot 10^{-4}$ - $5 \cdot 10^{-4}$
Nivåtransmitter	3.1	0.8	0.1	$3 \cdot 10^{-4}$ - $5 \cdot 10^{-4}$
Logikk, inkl. I/O kort (enkel PLC)	32.0	1.6	1.6	$5 \cdot 10^{-5}$ - $5 \cdot 10^{-4}$
Feltbuss-kopler	0.2	0.02	0.001	10^{-5}
XV/ESV inkl. aktuator	1.6	0.3	1.3	10^{-6} - 10^{-5}
Blowdown ventil inkl. aktuator (jfr FCS) [1)]	1.6	0.3	1.3 [1)]	10^{-6} - $\cdot 10^{-5}$
Ventil på ventil-tre (wing, master)	1.6	0.5	0.8	10^{-6} - 10^{-5}
Solenoid / pilot-ventil	4.2	1.8	1.4	-
PSV	1.2	0.2	1.0	10^{-3}

1) PDS bruker samme FTO rate som for XV/ESV, selv om det her er en annen feilmode (her Fail-To-Open og ikke Fail-To-Close) Jfr Appendix A i /9/.

Tabell 8 Pålitelighetsdata fra Appendix A i /9/ (se Table A.3)

Komponent	**Test-intervall**	**Ikkedetekterbar "farlig" feilrate λ_{DU} , pr 10^6 time**	**TIF-sann-synlighet [2)]**	**β - faktor (1oo2)**
Trykktransmitter	12	0.1	$3 \cdot 10^{-4}$	2% (5% for TIF)
Nivåtransmitter	12	0.1	$3 \cdot 10^{-4}$	
Logikk, inkl. I/O kort (enkel PLC)	6	1.6	$1 \cdot 10^{-4}$	1% (50% for TIF)
XV/ESV inkl. aktuator	6	1.3	$5 \cdot 10^{-6}$	2% 5% for TIF)
Blowdown ventil inkl. aktuator (jfr FCS) [1)]	6	1.3 [1)]	$5 \cdot 10^{-6}$	
Ventil på ventil-tre (wing, master)	6	0.8	$5 \cdot 10^{-6}$	
Solenoid / pilot-ventil	6	1.4	- [3)]	2% - 10% [4)]

[1)] /9/ bruker samme FTO rate som for XV/ESV, selv om det her er en annen feilmode.
[2)] Foreslått TIF-sannsynlighet, gitt eksponert detektor
[3)] TIF for solenoid/pilot er inkludert i tall for ventil/aktuator
[4)] β = 10% for pilotventiler på samme ventil, ellers β = 2%

Tabell 9 Modifiseringsfaktor for β, basert på voteringslogikk.

Votering	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
C_{kooN}	1.0	0.3	2.4	0.15	0.8	4.0

5.3 Anbefalte generiske HIPPS-data

Tabell 10 under gir anbefalte feildata for HIPPS-anvendelser. Merk at disse i stor grad baserer seg på de anbefalte data i PDS og OLFs IEC-retningslinjer. Pålitelighetsdata for QSV som en har mottatt fra Mokveld tyder på at disse ventilene har meget høy pålitelighet. Imidlertid fører Statoil-dataene (se foran) til en viss usikkerhet med hensyn til en slik konklusjon. En har derfor valgt å fortsatt bruke samme data som for ESV. Dette er muligens konservativt, men SINTEF mener at ytterligere dokumentasjon er nødvendig for å verifisere at QSVer *generelt* er mer pålitelige enn standard ESVer.

Når de gjelder normalt lukkede ventiler (FCS anvendelse) viser Statoil-dataene meget høy feilrate. Dette er reflektert i tabellen under. Da Statoil informasjonen bygger på et forholdsvis lite materiale, er det også her behov for nærmere undersøkelser.

Når det gjelder β-faktorene er disse tenkt benyttet i kombinasjon med modifiseringsfaktorene i Tabell 9 (se over).

Tabell 10 Anbefalte generiske data for HIPPS.

Komponent	**Ikkedetekter-bar "sikker" feilrate λ_{SU} pr 10^6 time**	**Ikkedetekter-bar "farlig" feilrate λ_{DU} pr 10^6 time**	**TIF-sann-synlighet**	**β - faktor (1oo2)**
Trykkbryter/Nivåbryter	0.9	0.2	0.002 [1)]	5% (10% for TIF)
Trykktransmitter	0.4	0.1	$3 \cdot 10^{-4}$ [1)]	2% (5% for TIF)
Nivåtransmitter	0.8	0.1	$3 \cdot 10^{-4}$ [1)]	
Fast fortrådet logikk, failsafe [2)]	1.0	0.01	$0.5 \cdot 10^{-5}$	1% (50% for TIF)
Programmerbar logikk, failsafe, (inkl. I/O kort)	1.0	0.1	$5 \cdot 10^{-5}$	1% (50% for TIF)
XV/ESV inkl. aktuator	0.3	1.3	$5 \cdot 10^{-6}$	2% (5% for TIF)
Blowdown ventil inkl. aktuator, (jfr FCS)	1.0	10.0 [3)]	$5 \cdot 10^{-6}$	
QSV, inkl. aktuator	0.3	1.3	$5 \cdot 10^{-6}$	
Solenoid / pilot-ventil	1.8	1.4	- [4)]	2% - 10% [5)]

[1)] TIF-sannsynlighet, gitt eksponert detektor.

[2)] Ifølge leverandør-data kan en ha enda bedre verdier her (spesielt for λ_{DU}). Ifølge disse data er λ_{DU} for fast fortrådet logikk bedre enn programmerbar logikk med *mer enn* én dekade.

[3)] Nærmere vurdering nødvendig av denne høye verdien.

[4)] TIF for solenoid/pilot er inkludert i tall for ventil/aktuator.

[5)] β = 10% for pilotventiler på samme ventil, ellers β = 2%

5.4 Testing/vedlikehold/nedetid

Her beskrives *typisk* omfang av ulike former for testing av HIPPS, og problemstillinger knyttet til nedetid av systemet. Ofte har det vært benyttet 3 måneders testintervall for HIPPS. Det kan være unntak fra dette, basert på pålitelighetsberegninger, kritikalitetsvurderinger eller operasjonelle hensyn. Bruk av *delvis* funksjonstesting og økt diagnostikk vil her kunne inngå som en løsning for å øke testintervallet. Under refereres informasjon om testing for tre hovedvarianter av HIPPS.

Testing av QSV med direktevirkende pneumatisk trykkbryter PSHH.
Typisk utføres utvendig visuell inspeksjon av QSV under drift månedlig. Denne inspeksjonen inneholder en visuell bekreftelse på at alle ytre komponenter til QSV og kontrollkretsen, medregnet PSHHene og styreventil (solenoid) til QSVs aktuator, er på plass.

Alle QSVer funksjonstestes med et intervall på tre måneder. Ventilene skal stenge ved spesifisert trykk og innen systemets responstid. Responstiden er den tiden som går fra trykkets settpunkt nås ved kontrollenheten, til sikkerhetsventilen er helt stengt (inkluderer altså funksjonstiden til den pneumatiske kontrollkretsen, som kan være opp til et halvt sekund). Under funksjonstesten økes trykket sakte inntil kontrollenheten utløses og ventilen stenger. Det er gjennomsnittet, dvs. aritmetisk middel, av tre slike målinger som benyttes som systemets responstid.

Testene utføres når anlegget er i drift. Den QSV som skal testes må isoleres ved hjelp av dens oppstrøms og nedstrøms blokkventiler, og blokkventilen på sensorlinja fra prosessen må være låst i stengt posisjon (ref. interlock-system prosedyre, indikert i Avsnitt 2.7). Nåleventiler i HIPPS-

kabinettet gjør det mulig å teste en QSV mens den parallelle er i drift. Slike nåleventiler kan også isolere sensorlinja mellom prosessen og PSHHen og koble ut den aktive QSVen.

Hensikten med funksjonstesten er:
- å sjekke PSHH settpunktene, og
- å sjekke systemets responstid.

En QSV funksjonstest vil kreve to personer som står i radiokontakt med hverandre, én ved HIPPS kontrollkabinettet og den andre ved QSVen som skal testes.

Testing av QSV med elektronisk (fast fortrådet) logikk og trykktransmitter PT.
Typisk testing foregår ved å isolere én og én trykktransmitter (kontrolleres ved hjelp av mekanisk forriglet manifold), injisere testtrykk på prosessiden av transmitteren, og lese av nødvendige inngangsdata til logikkortene, på skjermbilder osv. Etter at alle PTene er testet hver for seg, tester man logikken og utgangene ved å sette trykk på én transmitter og så introdusere en feil (kortslutning/brudd) på en av de gjenværende for å får 2oo3 logikken til å trippe ut. Testen verifiseres ved at ventilen stenger og lukketiden dokumenteres. Dette gjentas så for alle 2oo3 kombinasjoner av transmitterne. Dersom det av operasjonelle grunner ikke er mulig å lukke ventilen fullt så ofte, så skal testen i alle fall inkludere solenoid-ventilene på ventilkontrollen, og eventuelt delvis lukking av ventilen foretas.

Testing av et slikt *prosess* HIPPS-anlegg, eller tilsvarende PPS, er ressurskrevende, og en må involvere flere mennesker i testen enn ved en vanlig sløyfetest. Typisk er det én person ved transmitteren, én ved logikkenheten (kabinettet), én på VDU/skjerm og én ved ventilen, altså i alt fire personer. Et HIPPS-system med 2oo3 votering og to ventiler i serie tar typisk 4 timer å teste.

Når det gjelder periodisk testing, refereres følgende eksempel.

1) for ”standard” HIPPS på innløpsseparator med bruk av QSVer:
- 3 måneder: funksjonstest av instrumenter/QSV.
- 12 måneder: samme som 3 mnd., samt kalibrering av transmittere.
- 12 måneder: lekkasjetest av QSV.
- 60 måneder: full demontering og inspeksjon av QSV.

2) for trip av eksport-kompressorer i tilfelle for høyt eksport-trykk, ved at krafttilførselen til kompressormotor brytes:
- 3 måneder: funksjonstest av instrumenter til kompressorer.
- 12 måneder: samme som 3 mnd. samt kalibrering av transmittere og kontroll av høyspentbryters utkoplingsfunksjon.
- 12 måneder: test av gasstrykk, oljetrykk og akkumulatortrykk på høyspentbryter.

Felles for begge systemer er test av UPS, samt alarmer for HIPPS-kabinett.

Testing av QSV med programmerbar logikk.
Også her kan ulike periodiske tester kombineres. Som eksempel ser vi under på test av OPPS på Frigg. Dette representerer kanskje et "ekstrem"-tilfelle med hensyn til antall forskjellige tester. TotalFinaElf opplyser at følgende periodiske tester benyttes for dette systemet:

- Daglige *modulation test* for å vise respons av transmittere (dette er nå erstattet med kontinuerlig monitorering - se under).

- Automatisk ukentlig output testing med ASEA controller.
- Månedlig aksjons-testing ved å brute kraft-tilførsel til transmitter input for å fremprovosere full aksjons test gjennom systemet.
- OPPS-ventil-testing i samsvar med normal ESV-testrutiner.

I tillegg har en for OPPS en rekke system for kontinuerlig overvåking:

- Kontinuerlig ASEA intern system monitorering.
- Kontinuerlig sammenlikning av middelverdi av trykkmålinger).
- Analoge transmitter-kretser blir kontinuerlig monitorert for feil, og middelverdi-voteringslogikken blir rekonfigurert for å ekskludere feilede transmittere. Hvis to transmittere feiler initieres en ”fatal feil” shutdown.
- Middelverdi av sikkerhets-gruppen er kontinuerlig sammenliknet med en ekvivalent transmitter fra prosessmonitoreringssystemet, og det gis en allarm hvis disse avviker med mer enn a predefinert verdi.
- Kontinuerlig monitorering av ventilposisjonsbrytere for å identifisere latent feil under ventil operasjoner eller *spurious* bevegelse av ventilene.
- Kontinuerlig modulasjonsmonitorering (jfr modulasjonstesting, se over). Denne funksjonen ble modifisert for å unngå daglig modulasjonstest da det ble funnet at normale prosessfluktuasjoner beviste at transmitterne i virkeligheten var åpne for prosessfluid. Det gis en allarm hvis det ikke er noen "modulasjon" i løpet av et forhåndsdefinert tidsintervall.

Dessuten utføres for OPPS preventiv kalibreringer av PTer med 6 måneders intervall. Kalibreringen utføres ved å erstatte et komplett sett PTer etter tur med et kalibrert sett. Alle transmittere blir også testet før en linje tas i bruk etter å ikke ha vært trykksatt over en lengre periode.

6 Utfordringer og krav

I dette avsnittet ser en på de viktigste problemstillingene og utfordringene i forbindelse med bruk av HIPPS. Bl.a., hva er godt nok? Hvilke krav er det naturlig å stille?

6.1 Krav til HIPPS

Som påpekt tidligere er det et problem at HIPPS i dag brukes for å betegne en rekke ulike systemer, samtidig som det også er flere forskjellige begrep som anvendes for samme type system. Det er derfor viktig først å klassifisere og inndele disse systemene i ulike kategorier. Som nevnt i Avsnitt 4.2 vil SINTEF foreslå at en standardiserer begrepsbruken, og begrenser seg til å inkludere følgende varianter når en diskuterer HIPPS-problematikk: *prosess* HIPPS og *subsea* HIPPS (begge med hurtiglukkende ventil), PPS og FCS.

Under vil altså HIPPS være en samlebetegnelse for alle disse fire variantene (men alltid referere til en spesifikk HIPPS-barriere og ikke totalen av flere barrierer). Da FCS er såvidt forskjellig fra de andre systemene, kunne en vurdere å ikke inkludere dette. Siden enkelte bruker betegnelsen HIPPS også om dette systemet, er det i denne rapporten tatt med for oversiktens skyld.

Noen naturlige problemstillinger i tilknytning til de ulike HIPPS-variantene er:
- Tilpasning til IEC 61508 og SIL-krav.
- Valg av akseptkriterier for risiko.
- Er HIPPS like sikkert som standard løsninger (API RP14C løsninger)?
- Kan HIPPS erstatte begge nivåene av prosessikring?
- Arkitektur, bl.a. krav til redundans og uavhengighet av andre barrierer.
- Designkrav, (sensor, logikk og aktuerende element).
- Krav til prosedyrer.
- Krav til operasjon/utkopling.
- Krav til testing/testrutiner.
- Krav i forbindelse med endringer/modifikasjoner.
- Krav til klare ansvarsforhold, administrasjon og ledelse.
- Krav til data og beregninger.

Det er klart at flere av disse spørsmålene må behandles separat for de ulike HIPPS-variantene, idet svarene kan være ganske forskjellige for *prosess/subsea* HIPPS, PPS og FCS. Vi starter med å se på generelle krav til risikovurdering, ut fra IEC 61508, og behandler deretter de enkelte problemstillingene.

6.2 IEC 61508 og krav til risikoevaluering

Standardene IEC 61508 og 61511 gir generelle retningslinjer for gjennomføring av risikoevaluering. Flere punkter er meget relevante for vurdering/aksept av HIPPS-løsninger (se også Avsnitt 3.3). Bl.a. gjelder følgende:

- Evalueringen må knyttes til hele livssyklusen. Det er et sentralt poeng at det valgte integritetsnivået for sikkerhetsfunksjonen opprettholdes gjennom hele livssyklusen, og også i

forbindelse med endringer/modifikasjoner. Dette er ikke minst relevant for HIPPS, som ofte innføres som en modifikasjon på et eksisterende anlegg.
- Alle risiki skal identifiseres; dvs en skal finne alle relevante scenarier hvor overtrykks-beskyttelsen trer i kraft, og inkludere alle operasjonsmodi (og overgang mellom disse). Spesielt kan dette medføre at det må gjennomføres dynamiske prosess-simuleringer for å kartlegge behovet for / omfanget av HIPPS-barriere.
- Krav om å formulere akseptkriterierer for risiko. For denne type system kan en knytte et slikt kriterium til PFD *(Probability of Failure on Demand*), dvs sannsynligheten for at funksjonen svikter, gitt en *demand*. Et annet relevant mål på risiko i forbindelse med HIPPS er hyppighet av overtrykking av EUC (Equipment Under Control).
- SIL-krav for sikringsfunksjonen/systemet skal spesifiseres. Ut fra dette kan det for HIPPS-løsninger være aktuelt å stille krav om at det skal tilfredsstille f.eks. SIL3.

Disse punktene blir nærmere diskutert under.

6.3 Mål på risiko og akseptkriterier.

Dette avsnittet gir en forholdsvis generell diskusjon. En kommer tilbake til detaljer for de enkelte HIPPS-varianter i Avsnitt 6.4 under.

Påliteligheten, dvs. evnen til å utføre tiltenkt funksjon (i rett tid) er det essensielle ved disse systemene. Fra IEC 61508 har en målet *PFD* (Probability of Failure on Demand) som er en aktuell parameter for å evaluere påliteligheten av en sikkerhetsfunksjon som HIPPS. Risokoakseptkriteriet kan ut i fra dette relateres til PFD (f.eks. at en skal ha PFD < 10^{-4}), eller tilsvarende formuleres som et SIL krav.

Mens *PFD* egentlig representerer et pålitelighetskrav for barrieren, vil akseptert frekvens for overtrykking av EUC (Equipment Under Control) være et mer fullverdig akseptkriterium med hensyn til risiko. Hyppigheten av overtrykking vil også ta hensyn til demandraten, som er direkte proporsjonal med risikoen, og i en viss forstand trekkes også konsekvensen inn (ved at en kan se på hyppighet av ulike grader av overtrykking) . Det kan være naturlig å spesifisere ulike grader av overtrykking for EUC, og tilpasse akseptkriterier til hver av disse. En kan f.eks. formulere ett akseptkriterium for hyppighet av trykk over designtrykk, og et annet kriterium for trykk over testtrykk.

Bruk av hyppighet for overtrykking har også den konsekvens at en "tvinges" til å ta hensyn til den totale frekvensen når en skal vurdere om løsningen er akseptabel (uansett årsak til overtrykkingen). Bruk av PFD som anbefalt i IEC 61508 har den uheldige side at en begrenser seg til å kvantifisere utilgjengeligheten som følger av hardware feil, mens systematiske feil (som i PDS kvantifiseres ved TIF-sannsynligheten) holdes utenfor enhver kvantifisering. Dette er en uheldig praksis for sikkerhetskritiske system. Kvantifiseringer bør gi et realistisk bilde av reell risiko, når en tar alle type feil i betraktning. Dette er ikke minst viktig når hardware har høy pålitelighet.

Valg av type akseptkriterium (f.eks. at det skal basere seg på PFD) er et sentralt trinn i en risikoevaluering, og valg av *akseptgrense* (f.eks. 10^{-4}) kan være en utfordrende oppgave. I utgangspunktet er det operatøren som selv skal definere og begrunne sine akseptkriterier. Generelt kan valget knyttes opp til ulike prinsipp. De mest kjente er (se Vedlegg A):

- *ALARP*, (*As Low as Reasonably Practicable*), jfr del 5 av IEC 61508, /7/,
- *Comparison Criteria* (se NORSOK Z-13), tilsvarende *GAMAB*, eller
- *MEM* (Minimum Endogen dødelighet), som kort sagt går ut på at aktiviteten ikke skal gi signifikant "tilleggsrisiko".

ALARP er først og fremst et prinsipp for risikoforbedring og kostnadseffektivitet, og gir ikke støtte for å velge de egentlige akseptgrensene.

Ofte er NORSOKs sammenlikningskriterium ("Comparison Criteria") benyttet for å formulere akseptkriterier for system av typen HIPPS. Da setter en det krav til HIPPS-løsningen at påliteligheten skal være lik eller bedre enn det systemet den erstatter, f.eks. en PAS ventil og en PSV.

I enkelte tilfeller vil innføring av HIPPS med sikkerhet føre til øket risiko, slik at sammenlikningskriteriet ikke er aktuelt. Da kan det være naturlig *å ta utgangspunkt* i MEM-prinsippet (Vedlegg A). Dette baserer seg på at en har en "iboende" risiko for å omkomme ved uønskede hendelser (trafikkulykker, utøvelse av idrett osv), og at den aktuelle "aktiviteten" ikke skal gi signifikant bidrag til denne "utgangs-risikoen". I utgangspunktet gjelder MEM-prinsippet for en *virksomhet*, men en tilsvarende tankegang må kunne brukes mer generelt. Da kan en f.eks. kreve at innføring av HIPPS ikke skal bidra med mer mer enn 1% (10%) økning i lekkasjefrekvensen for utstyret under vurdering (dvs det ekstra bidraget fra overtrykking av EUC). En slik betraktning om "ikke signifikant bidrag" kan være til god *støtte* også når en fastsetter akseptkriterier (dvs. selve akseptgrensen).

Et sentralt poeng i IEC 61508 er at en skal ha kontroll over *totalrisikoen* i forbindelse med operasjon av EUC. Dette prinsippet anses som spesielt viktig i forbindelse med bruk av HIPPS av flere årsaker

- HIPPS innføres ofte i forbindelse med modifikasjoner av eksisterende anlegg og representerer gjerne et ”tillegg” til tidligere utstyr. Slike utvidelser kommer dessuten ofte ”bolkvis” og bør derfor forsøkes sett i sammenheng.
- HIPPS øker ofte kompleksiteten i anlegget og setter nye krav til driftsoperatørene. Det er derfor sentralt at de risikovurderinger som gjøres ifm innføring av HIPPS ikke bare sammenligner rene designløsninger, men også tar hensyn til endrete krav til operasjon og vedlikehold.

Dersom en konsekvent benytter et kriterium som bare vurderer tilleggsrisikoen ved innføring av HIPPS, vil en ved hjelp av risiko-/pålitelighetsanalyser kunne vise at det meste er akseptabelt ("tar du den, så tar du den"). Et middel for å motvirke en sånn fare at derfor å sette stenge krav til evaluering av totalsystemet og definere akseptkriteriet deretter, for eksempel som akseptabel frekvens for årlig overtrykking. I forbindelse med slike vurderinger bør en, i tillegg til de rent kvantitative vurderingene, også vurdere kvalitativt aspekter som økt kompleksitet av totalanlegget, konsistent bruk av teknologi, brukergrensesnitt, godhet av prosedyrer (for eksempel for bypass), drift og vedlikehold. Krav om slike ”totalanalyser” kan bidra til enklere, mer enhetlige løsninger.

6.4 Designkrav

I dette avsnittet vurderes en del spørsmål av typen:

- Hvilke typer akseptkriterier for risiko er det naturlig å bruke (jfr diskusjon i 6.3 over) for ulike HIPPS applikasjoner?
- Er HIPPS like sikkert som standard løsninger (API RP 14C løsninger)? Kan spesielt HIPPS erstatte begge nivåene av prosessikring (PSV og PAS)?
- Bør det stilles determimistiske krav mht
  - uavhengighet mellom barrierer?
  - enkeltfeil skal ikke være kritiske?
  - redundans / diversitet?
  - type/design for sensor, logikk og aktuerende element?

Under gis separate diskusjoner for hver av de fire HIPPS-variantene (se Avsnittene 4.1.1 - 4.1.4), med hovedvekt på *prosess HIPPS*. De "krav" som antydes her er stort sett i overensstemmelse med dagens praksis, og vil kreve en grundigere vurdering hvis de evt skal innføres som "absolutte krav" for aktuelle HIPPS-kategori

6.4.1 Prosess HIPPS

Som diskutert i avsnitt 2.2 brukes HIPPS ofte for å erstatte manglende fakkel- og/eller PSV-kapasiteten. En typisk HIPPS sløyfe består da av en eller flere trykkmålere som ved høyt trykk sender stengesignal til en QSV som stenger tilførselen av prosessmediumet. Slike system har en etterhvert samlet betydelig erfaring med.

Valg av akseptkriterium kan i prinsippet avhenge av flere forhold, deriblant

- om en vil vurdere overtrykking i forhold til designtrykk eller testtrykk, eller begge deler.
- om en ser på overtrykking av fakkel og/eller av selve prosessutstyret,
- om det er ett eller flere parallelle løp inn mot samme utstyret, for eksempel en separatoren, hvor hver linje er beskyttet med HIPPS (som planlagt på Tune),
- om en har flere parallelle prosesseringstog (som på Kollsnes) hvor hvert enkelt tog er beskyttet med HIPPS for å unngå samtidig nedblåsning fra flere tog,
- om HIPPS *erstatter* sekundærbarrieren, dvs en full-flow PSV (selv om noe PSV kapasitet fremdeles er tilgjengelig), eller om HIPPS er installert for å *redusere* PSV og fakkel-kapasitet.
- Om PAS er rask nok til å kunne oppfattes som egen barriere (evt for noen scenarier)

Merk at det er naturlige koplinger mellom flere av disse alternativene. Hovedtilfellene blir diskutert under.

For prosess HIPPS vil et naturlig akseptkriterium være å si at løsningen med HIPPS (sammen med evt andre barrierer) skal være like god som en standard API RP 14C løsning, dvs PAS+en full flow PSV. En beregner da PFD (pluss TIF-sannsynlighet for å vurdere systematiske feil) for begge disse løsningene og foretar en sammenligning. Det er imidlertid en del ”fallgruber” knyttet til bruk av dette kriteriet

- Feildata for PSV er i stor grad basert på resultater fra testing. Dvs en har trykket ventilen opp til settpunktet pluss en viss prosent, si 5%, og dersom den da ikke åpner registreres dette som en svikt. Hvorvidt ventilen ville ha åpnet ved økt påtrykk vet en ikke, men det må forventes å være sannsynlig. Mao er det en viss fare for at en sammenligner med en ”for dårlig” PSV

pålitelighet siden det i en gitt overtrykkssituasjon som oftest kan være godt nok at ventilen åpner ved f.eks. +10% eller i verste fall før testtrykket nås.

- Det må på forhånd være klart definert hvilke kriterier som ligger til grunn for selve sammenligningen. Vil svikt i overtrykkssikringen (dvs PAS+HIPPS) bety at en overstiger designtrykket men ikke testtrykket til nedstrøms utstyr, eller vil begge trykkgrensene kunne overskrides? Normalt (når HIPPS installeres) vil det være PSV kapasitet for å kunne ta termisk ekspansjon og/eller forventet lekkasje gjennom HIPPS ventilen. I enkelte tilfeller vil tilgjengelig PSV kapasiteten også være tilstrekkelig til å forhindre trykk over testtrykk i utstyret (avhengig av trykk og strømningsforhold – dette må verifiseres med dynamiske simuleringer).
- Når sammenligningskriteriet er formulert på denne måten tar det ikke høyde for antall demand på overtrykkssikringen.

SINTEFS konklusjon på denne diskusjonen blir:
Dersom sammenligningskriteriet skal brukes som akseptkriterium er det viktig å definere klart hvilket trykk en egentlig ser på. Dersom det er testtrykket som er kritisk, mangler en i dag data som sier hvor god en PSV egentlig er (og dermed hva en skal sammenligne HIPPSen med). Generelt, synes det derfor bedre å operere med et akspetkriterium som tar utgangspunkt i årlig akseptert frekvens for å overstige henholdsvis designtrykk og testtrykk.

En slik formulering av akseptkriteriene har også den fordel at den har generell gyldighet (uavhengig av designløsning osv). Deterministiske/kvalitative krav kan naturligvis komme i tillegg.

Hvis HIPPS og andre barrierer (evt. PAS) ikke er funksjonelt uavhengige er det viktig at muligheten for fellesfeil mellom disse funksjonene vurderes.

Et hovedtilfelle vil være at HIPPS erstatter en full-flow PSV, men der PAS funksjonen/annen barriere fremdeles er tilgjengelig sammen med noe PSV kapasitet. Det bør understrekes at en løsning hvor HIPPS fullt ut erstatter en PSV kun vil være akseptabel for helt spesielle scenarier med lav frekvens, slik som for eksempel ”oppstartsscenariet” (ref. avsnitt 2.2).

Et annet hovedtilfellet vil være der HIPPS er installert for å *redusere* PSV og fakkel designkapasiteten; dvs en kan tåle feil på minst én HIPPS sløyfe. Dette kan gjelde anlegg der en har flere parallelle prosesseringstog og hvor HIPPS er installert på hvert tog for å beskytte fakkel mot samtidig nedblåsning fra flere tog (jfr.Figur 3). En annen mulighet vil være tilfeller hvor flere parallelle løp er rutet inn til samme separator og hvor det for å redusere PSV (og fakkel) designraten er installert HIPPS på hver linje inn til separatoren (jfr.Figur 4).

For begge (alle) tilfeller med parallelle prosesseringstog/løp anbefaler en altså å knytte akseptkriteriet til hyppigheten av overtrykking som en følge av at HIPPS på et eller flere tog/løp feiler; dvs. beregne frekvensen av de (nedstengnings)tilfeller hvor en vil ha utilstrekkelig PSV og/eller fakkelkapasistet. For det siste tilfellet hvor en har flere parallelle løp rutet inn mot samme separator sier forøvrig NORSOK P-001 at en skal designe fakkel for samtidig feil av to HIPPS sløyfer. Etter SINTEFs oppfatning kan det diskuteres hvorvidt et slikt absolutt krav bestandig er hensiktsmessig. Dersom en for eksempel har en viss rest-kapasistet i fakkelsystemet, kan effekten bli at en velger å splitte innløpet i et stort antall linjer for å ”tilpasse” seg kravet. Dette medfører økt kompleksitet og mere utstyr og har derfor andre sikkerhetsmessige ulemper.

Inntil i dag er såvidt SINTEF bekjent HIPPS ikke benyttet til å erstatte begge nivåer (PAS og PSV) av prosessikringen. Dersom en slik løsning skal diskuteres er det igjen viktig at en vurderer

ulike trykknivåer og konsekvenser av overtrykk. Ofte vil PAS funksjonen være for ”treig” til å motvirke trykk over design, men kan være rask nok til å forhindre overtrykking utover testtrykk. *Det bør i utgangspunktet ikke tillates å erstatte begge nivåer av prosessikring med HIPPS dersom detda blir slik at svikt i HIPPS kan gi trykk over testtrykk med påfølgende fare for at prosessen går til brudd.*

For *prosess HIPPS* må det generelt stilles strenge krav til et pålitelig og hurtigvirkende system. Spesielt bør det kreves at HIPPS er helt uavhengig av øvrige sikrings-/reguleringssystem. Videre bør i utgangspunktet alle sløyfer være uavhengige. Et absolutt krav om at enkeltfeil ikke skal være kritisk vil ofte være for stengt dersom en betrakter en enkelt HIPPS sløyfe (som for eksempel har et SIL2 krav). Krav om at enkeltfeil ikke skal være kritisk vil først og fremst komme til anvendelse når en betrakter totaliteten av alle barrierer. Det bør i denne sammenheng påpekes at argumenter som at ”vi trenger ikke designe for to samtidige feil” ofte ikke er forenlig med bruk av et risikobasert akspetkriteirum iht IEC 61508. Enten designer en i forhold til standarder, og da kan prinsippet ”vi trenger ikke designe for to samtidige feil" komme til anvendelse. Hvis en derimot avviker fra standarder, og velger å bruker en risikobasert angrepsmåte, er SINTEF av den oppfatning at en ikke kan velge å beholde "det en liker" av standarden, som f.eks. nevnte prinsipp.

På sensor-siden er det åpenbart store fordeler ved å bruke trykktransmitter framfor trykkbryter. Muligheten som en transmitter gir for kontinuerlig overvåking vil bl.a. minimere muligheten for feilmoden "tilstopping av impulsrør", og gir betydelig sikkerhetsgevinst framfor en bryter som bare testes med måneders mellomrom. For nye HIPPS-installasjoner synes det rimelig å sette krav om bruk av trykktransmittere, (og anbefaling/krav om 1oo2 eller 2oo3 votering for SIL 3 eller bedre).

På logikksiden bør det settes krav om fast fortrådet system, som feiler til sikker tilstand. SINTEF oppfatter dette som den sikreste løsningen. Det oppfattes også som en fordel (sikkerhetsmessig) at endring av logikken da bare kan gjennomføres etter grundig planlegging (fysisk omkopling).

Det er i de fleste HIPPS applikasjoner helt avgjørende at systemet har høypålitelig, hurtiglukkende ventil(er). Det er flere slike på markedet. Testing av at ventilen lukker er meget sentral for påliteligheten til systemet. En form for overvåking, med bl.a. relativt hyppig bevegelse av ventilen anbefales. Intervallet for full funksjonstesting må vurderes spesielt, (se Avsnitt 6.7 under). Krav til produksjonstilgjengelighet kan føre til at en benytter løsningen med to ventiler i parallell for å muliggjøre full funksjonstesting under produksjon.

6.4.2 Subsea HIPPS

Dette systemet består også av trykkmåler(e), logikk og en eller flere hurtiglukkende ventiler, og har mange likhetstrekk med prosess HIPPS-løsningene. Flere av kommentarene ovenfor gjelder derfor også for subsea HIPPS. Imidlertid har en enda ingen erfaring med subsea HIPPS, og en får enkelte tilleggsproblem både sikkerhetsmessig og regularitetsmessig, spesielt knyttet til tilgjengelighet i forbindelse med vedlikehold osv.

Ved fastsettelse av akseptkriterium bør en igjen vurdere konsekvensen av HIPPS-svikt. I tilfeller der konsekvensen kan være brudd på rørledning og/eller stigerør synes det fornuftig å definere et kriterium som sier noe om akseptert hyppighet av overtrykking utover for eksempel testtrykk. Det kan i denne sammenheng være aktuelt å skille mellom brudd som skjer i umiddelbar nærhet av tilknyttet installasjon (dvs på stigerøret / innenfor sikkerhetssonen) eller brudd som skjer på rørledningen utenfor sikkerhetssonen. Fra et slikt risikobasert akseptkriterium vil en kunne utlede krav til integritet for subsea HIPPS funksjonen. Kravet vil avhenge av hvilke andre sikkerhetsfunksjoner som er tilgjengelig (PAS, PSV på stigerøret, ”weak link” på rørledningen, osv).

Når det gjelder design av undervannsanlegg, har en tradisjonel hatt noe andre nedstengnings-filosofier enn topside. Blant annet er elektrisk ”fail-safe” prinsippet lite utbredt subsea. Subsea HIPPS introduserer imidlertid et krav om dette også subsea. Videre har subsea styrepanelet på topside ofte vært integrert i øvrige plattformsystemer. Dette medfører at det forsubsea HIPPS kan være vanskelig å opprettholde krav om full uavhengighet av øvrige kontroll og sikringssystem siden en må ha visse muligheter for å operere HIPPS-ventilene fra plattform. Det er generelt viktig at det styresystemet på plattformen som kommuniserer med subsea HIPPS logikken i størst mulig grad gjøres uavhengig av øvrige plattform sikkerhetssystemer (som PAS) og ikke påvirkes av feil i disse systemene, se krav i IEC 61508-1, referert i Avsnitt 3.3 foran.

På grunn av problem med å skifte ventil ved feil, kan det være ønskelig å ha to HIPPS ventiler i serie fra starten av. Hvis én svikter, kan den da låses åpen, og en fortsetter drift med én ventil.

6.4.3 Pipeline Protection System, PPS

Problemstillingen her er ganske forskjellig fra *prosess HIPPS.* Karakteristisk for PPS er at en ofte har meget god tid (noen ganger opp til flere timer) før situasjonen blir kritisk mht overykking av rørledningen. Det er derfor ikke naturlig å sette samme strenge krav til rask reaksjonstid og høy sikkerhet av *PPS*, som til *prosess HIPPS*. SINTEF oppfatter det derfor ikke som noe sentralt problem at PPS integreres med NAS/PAS. Siden responstid sjelden er dimensjonerende legger en gjerne inn tidsforsinkelser for aktiveringen hos eksportør (for å slippe unødvendige nedstengninger). Direkte (telefonisk) kontakt mellom eksportør og mottaker kan derfor inngå som en barriere, eller som et middel til å redusere demand på det automatiske nedstengingssystemet. Det er derfor karakteristisk at prosedyrer blir en sentral del av beskyttelsessystemet, se avsnitt 6.5 under.

Ved bruk av PPS i forbindelse med *spec break* konseptet, er situasjonen den at en i utgangspunktet har en rørledning designet for fullt innstengninstrykk hele veien, hvor en nedgraderer nedstrøms delen av rørledningen til en lavere trykklasse. Dermed kan dette konseptet aldri bli like sikkert som ”opphavet” og sammenligningskriteriet blir derfor upassende. Mulige akspetkriterier blir da å definere hvor stor tilleggsrisiko en er villig til å akseptere og/eller definere en akseptabel hyppighet for overtrykking av rørledningen (se diskusjonen ovenfor).

For PPS er det samme krav til deteksjon som for øvrige HIPPS-varianter. I tilfelle posisjonsbryter skal tillates brukt som sensor, må det stilles krav om redundans (med votering som fremmer sikkerhet, dvs 1oo2, 2oo3 e.l.).

Siden logikken ifm PPS ofte er knyttet til signaloverføring via satelitt, synes et programmerbart system å være den foretrukne løsning. Overføring må være failsafe. Det er også et viktig poeng å sikre tilstrekkelig tilgjengelighet av signaloverføringen.

Det synes ikke å være problem med å bruke ordinære ESV som aktuerende element i PPS. Alternativt (i kombinasjon) brukes også tripping av eksportkompressor.

6.4.4 Flare Control System, FCS

Et FCS vil bestå av en hurtigåpnende ventil, i parallell med en sprengblikk, plassert mellom PSV og fakkel. En produserer altså da med slukket fakkel (uten pilot). Dette medfører at en har installerter en "kanon" for tenning av fakkel, i det øyeblikk en har overtrykking og ventilen åpner.

Tilsvarende som for PPS vil her sammenligningskriteriet være upassende siden en her tar utgangspunkt i et åpent rørstykke (mellom PSV og fakkeldunk), og en fakkel der det konstant

brenner en pilotflamme. Siden FCS legges i parallell med sprengblikk, må en imidlertid kunne anta at faren for overtrykking er så godt som eliminert. Likevel bør en sette krav til åpning av FCS system (uten sprengblikk). Dvs, at et akseptkriterium kan knyttes til hyppighet av demand uten at FCS åpner.

Hovedforskjellen på en FCS-løsning og konvensjonell løsning er at en ved bruk av FCS er avhengig av å tenne fakkel. Da kommer en også fort over i problemstillingen med hvor stor risiko det er forbundet med å få et uantent utslipp fra fakkeltippen. Konsekvensene av dette vil avhenge av fakkelhøyde, egenvekt på gassen som slippes ut, osv. og må verifiseres ved hjelp av spredningsberegninger. Så lenge ikke annet er dokumentert, bør en imidlertid basere seg på at dette har betydelige sikkerhetskonsekvenser, og en må sette krav til akseptabel hyppighet av åpning av fakkel uten samtidig tenning. Merk at problemstillingen er forholdsvis fjern fra vanlig HIPPS-problematikk, og vil ikke følges nærmere opp i denne rapporten.

6.5 Prosedyrer

Det er spesiell grunn til å understreke behovet for å dokumentere klare prosedyrer for operasjon og vedlikehold av HIPPS systemer, og ikke minst at operatøren kan sannsynliggjøre at dette også er prosedyrer som brukerne er fortrolige med og er innstilt på å følge.

Det er viktig å sette krav til at prosedyrerene dekker alle mulige driftsmodi, slik som normal operasjon, oppstart, nedstengning og test/vedlikehold. Videre bør det understrekes at det påhviler operatør et ansvar for å tenke igjennom mulige faresituasjoner knyttet til operasjon av HIPPS i alle operasjonsmodi. Det er ofte de "unormale" situasjoner som viser seg å være kritisk (overbroing, skifte av modus, vedlikehold, ...). Det er i denne forbindelse viktig at prosedyrene gir klare retningslinjer knyttet til muligheten for overbroing av deler av HIPPS funksjonen (f.eks. en av to ventiler) og spesifiserer hvilke kompenserende tiltak som i så fall skal settes inn.

Det er viktig at HIPPS ses i sammenheng med de andre funksjonene (slik som PAS) som utgjør den totale overtrykksbeskyttelsen. Ved utforming av prosedyrer må det derfor sikres at det også legges restriksjoner på operasjon av de øvrige beskyttelsesnivåene. Dette kan ofte være en utfordring rent operasjonelt fordi operatørene ikke er vant til å legge begrensninger på utkobling av for eksempel en PAS funksjon.

I forbindelse med PPS er det ofte et viktig poeng at en *ikke ønsker* for rask aktuering. En har som regel god tid til å åpne ventil som blokkerer rørledningen før kritisk trykk nås, og en ønsker naturligvis ikke å trippe eksportstrømmen unødig. Derfor legges det gjerne inn tidsforsinkelse som medfører at aktivering ikke skjer umiddelbart. Hvis oppheving av aktueringssignalet når blokkerende ventil åpnes, skjer på bakgrunn av (telefonisk) kontakt, fås en sammenblanding av prosedyrer og automatisk system, noe som kan svekke påliteligheten. Videre kan det være et generelt problem at ”lang” tid i seg selv introduserer feil for eksempel ved at aksjoner kan utsettes og glemmes (evt glemmer en å gi beskjed i forbindelse med "vaktskifte"). Det er derfor viktig at stringent bruk av prosedyrer vies stor oppmerksomhet i forbindelse med operasjon av PPS.

6.6 Produksjonstilgjengelighet og degradert system

Det er ofte en konflikt mellom krav om høy sikkerhet og høy produksjonstilgjengelighet. I utgangspunktet skal arkitekturen i systemet gi maksimal tilgjengelighet, samtidig som krav til sikkerhet er oppfylt, f.eks. 2oo3 transmittere, full redundans i logikken, redundant strømforsyning

osv. For system med høyt integritetskrav (SIL3 eller høyere) bør det også stilles krav til maksimal utkopling for deler av anlegget (degradert operasjon); for eksempel hvor lenge man kan operere med bare en CPU i et redundant system, og hvorvidt feil på én av flere ventiler i serie skal medføre nedstengning.

Krav/ønske om kort nedetid fører også til at en vil ha kritiske deler på lager, samt tilgjengelig personell som kan installere reservedelene på kort varsel. Da dette alltid er kritiske systemer vil en sikkerhetskritisk feil som oftest kreve øyeblikkelig innsats for å få anlegget raskt i drift, noe som vil være ressurskrevende. En leverandør opplyser som eksempel at de har en løpende kontrakt med Statoil drift på Kollsnes for 24-timers telefonstøtte.

6.7 Testing

I tillegg til krav/anbefalinger om ulike typer selvtest/overvåking som bygges inn i nye HIPPS-løsninger, bør det settes minimumskrav mht full funksjonstesting. For HIPPS systemer virker det ikke urimelig at en kan forlenge perioden noe ut over 3 måneder, som er anbefalingen f.eks. i NORSOK, se Avsnitt 3.1. Imidlertid bør det ikke være "fritt fram" for å "regne seg" fram til et vilkårlig testintervall. Det er ulike fallgruber med bruk av pålitelighetsdata, og hvis en nøyer seg med å sette krav til *PFD* (*Probability for Failue On Demand*, jfr IEC 61508), kan en fort regne seg fram til et "tilfredsstillende" intervall for funksjonell testing som vil bli urimelig langt. Grunnen til at SINTEF her sier "urimelig" skyldes at det er usikkerhet både mht pålitelighets-modellering og data, se avsnitt 6.9 under.

Totalt betyr dette at SINTEF anbefaler at en velger en robust angrepsmåte her. Det innebærer dels at forlengelse av intervall for funksjonell testing bare bør skje gradvis. Videre bør det settes en øvre grense for dette intervallet. SINTEF er av den oppfatning at i dag bør denne grensen høyst være 1 år. Dette gjelder full funksjonstesting, med lukking av ventil i løpet av spesifisert tid. Det er som regel ikke samme behov for å sette krav til lekkasjetesting av ventilen.

6.8 Endringer / modifikasjoner

Det er et potensielt problem med HIPPS at systemet skal tre i funksjon når alt annet har feilet. Det er ofte et selvstendig, frittstående anlegg, gjerne med et eget programmerings-språk, grensesnitt osv. Dette medfører at operatørenes erfaring med HIPPS blir begrenset til selve testingen. Derfor kan det være naturlig å trekke inn leverandøren når det skal gjøres endringer, siden denne besitter den spesialkompetansen som er nødvendig.

Det understrekes at endringer av HIPPS-løsninger ikke kan foretas uten videre. Spesielt skal de programmerbare systemene gjennomgå en full gjennomgang for å verifisere at endringen ikke går ut over sikkerhetsintegriteten i systemet.

6.9 Pålitelighetsdata og -beregninger

Det må stilles krav til dokumentasjonen av at akseptkriterier er oppfylt, samt at analysene er reproduserbare. Dette vil normalt medføre at det kreves verifikasjon av analyser av uavhengig tredjepart.

I forbindelse med beregning av pålitelighet og risiko er det viktig å sette krav til gyldighet av inngangsdata. For hver komponent kreves sviktintensitet (feilrate), feilmodefordeling, graden av selvtest og testintervall. Sviktintensiteten defineres normalt som 1/MTTF, (der MTTF= Mean Time To Failure). Det er viktig å kunne sannsynliggjøres at inngangsdata er relevante for den konkrete anvendelsen. Spesielt for høypålitelige løsninger (som SIL 3) bør det stilles krav om at data så langt som mulig er "installasjons-spesifikke" og også støtter seg til reelle driftsdata.

Vedrørende pålitelighetsberegning (av PFD) bemerkes følgende:

- Standard-modellene for beregning av PFD bygger på en del forutsetninger (som ikke alltid blir presisert). Spesielt antas i denne beregningen at sviktintensiteten er *konstant*, dvs en "gammel" komponent svikter med samme sannsynlighet som en "ny". Dette er en tvilsom antakelse for mekaniske komponenter, og medfører at en ikke må ta beregnet PFD altfor bokstavelig. Det gjelder spesielt for lange testintervall, hvor antakelsen om konstant sviktintensitet vil føre til en underestimering av den virkelige PFD.

- Det vil være sammenheng mellom observert sviktintensitet og testintervall. Relativt korte testintervall vil føre til forholdsvis mye forebyggende vedlikehold, ved at flere degraderte "svikt" oppdages og korrigeres før de har utviklet seg til kritisk feil; (*critical failure* i OREDA svarer til tap av viktig funksjon). Pålitelighetsdata samlet for en slik situasjon kan derfor ikke uten videre brukes hvis en går over til lengre intervall.

- Når en skal se på fellesfeil bl.a. for et større antall løp er dette "problematisk" beregningsmessig. Standard beta-faktor - modell er lite egnet til å håndtere dette, og beregningen for større antall løp blir noe vilkårlig. Det er behov for å etablere/anbefale en felles metodikk for å håndtere dette på en entydig måte.

- Når det gjelder operatørens rolle i regnestykket som leder fram til risikomålene PFD og hyppighet av overtrykking, kan det generelt være behov for oppklarende retningslinjer. Dette gjelder blant annet for systemer det manuell intervensjon vil utgjøre en ekstra barriere (f. eks. for PPS), der det kan være uenighet om en skal ta høyde for denne barrieren eller ikke. Generelt kan det sies at dersom en velger å ta høyde for mulig manuell intervensjon, bør dette dokumenteres, blant annet gjennom at operatøren har tilstrekkelig tid til å diagnostisere situasjonen og gjøre nødvendige tiltak. Ellers er estimering av menneskelig pålitelighet fremdeles et vanskelig område, hvor lite operasjonsspesifikke data er tilgjengelig, og hvor generiske data eventuelt bør brukes med omhu. I dag er en av de mest benyttede teknikker i så måte databasen HEART, /23/.

- IEC 61508 krever ikke kvantifisering av systematiske feil. Dette inngår imidlertid i PDS-metoden, der systematiske feil kvantifiseres ved TIF-sannsynligheten, og total sikkerhetsutilgjengelighet kvantifiseres ved *CSU = Critical safety unavailability*. Grovt regnet kan en bruke *at CSU = PFD + TIF*. En vil anbefale at en selv om IEC 61508 benyttes, fremdeles kvantifiserer TIF-sannsynligheten, jfr. OLFs retningslinjer, /9/.

7 Konklusjoner og anbefalinger

SINTEF er av den oppfatning at et av hovedproblemene med HIPPS i dag er at begrepet har en noe upresis betydning. Det finnes et konglomerat av ulike systemer som omtales dels som HIPPS-løsninger, men der også andre betegnelser brukes. Disse systemene er også til dels ganske forskjellige, og krever ulike regelverk og form for tilsyn. SINTEF vil derfor anbefale at OD spesifiser og eksplisitt definerer en del *standard HIPPS-kategorier,* f.eks. følgende

- *Prosess HIPPS,* [med hurtiglukkende ventil for å redusere eventuelt erstatte kravet til PSV og fakkel designkapasitet];
- *Subsea HIPPS,* [med hurtiglukkende ventil *subsea*];
- *PPS,* [beskyttelse av rørledninger der ventilens lukketid er "irrelevant"];
- *FCS,* [hurtigåpnende ventil for trykkavlastning ifm faklings-problematikk].

Etter SINTEFs oppfatning bør en i framtiden unngå å operere med andre begrep, som dels er i bruk i dag.

For hver av de valgte variantene synes det naturlig å spesifisere en del krav og anbefalinger (til standardisering) som, hvis de er oppfylt, i utgangspunktet vil gi en akseptabel løsning. Krav og anbefalinger bør knytte seg både til teknologi, operasjon/prosedyrer og testing/vedlikehold.

SINTEF vil i Avsnitt 7.1 begrense seg til å antyde hvordan en del slike krav/anbefalinger kan se ut; se også kapittel 6. Avsnitt 7.2 gir en del anbefalinger med hensyn til videre arbeid med HIPPS-problematikken.

7.1 Standard krav

SINTEF anbefaler at det spesifiseres generelle krav, dels tilpasset ulike "standard" HIPPS-kategorier. Den følgende lista inneholder en del slike naturlige krav/anbefalinger:

- Det stilles krav om at de ulike HIPPS-varianter bygges og opereres iht *IEC 61508*. I denne sammenhengen må det understrekes at det påhviler operatør et ansvar for å tenke igjennom mulige faresituasjoner knyttet til operasjon av HIPPS i alle operasjonsmodi.

- *Akseptkriterier* bør ta utgangspunkt i *total*risikoen og påliteligheten av (total)barrierene, og slik ta hensyn til *demand*-raten. Det er naturlig at operatøren formulerer akseptkriterier med hensyn til hyppighet av overtrykking av de system som beskyttes av HIPPS. En kan f.eks. se på hyppigheten av både trykk over designtrykk, og trykk over testtrykk.

- Det bør settes stenge krav til evaluering av totalsystemet, spesielt i forbindelse med *utvidelser/modifikasjoner*. I slike vurderinger bør det spesifiseres at en skal vurdere bl.a. økning i *kompleksitet* av totalanlegget, spesielt evt. mangel på enhetlige løsninger. Dette gjelder både teknologi, bruker-interface, prosedyrer og vedlikehold.

- En bør gå vekk fra trykkbryter (PS), og gå over til bruk av trykktransmitter (PT) som sensor.

- Fasttrådet logikk anbefales for prosess HIPPS og subsea HIPPS.

- Klare og entydige prosedyrer for operasjon og vedlikehold må dokumenters. Dette gjelder alle operasjonsmodi, og overgang mellom disse. Ikke minst må det sannsynliggjøres at brukerne er fortrolige med og er innstilt på å følge prosedyrene.

- En må velger en robust angrepsmåte ved valg av testintervall. Det innebærer dels at forlengelse av intervall for funksjonell testing bare bør skje gradvis. Videre bør det settes en øvre grense for dette intervallet (høyst være 1 år). En skal mao ikke helt fritt kunne "regne seg" fram til et vilkårlig langt intervall, som gir akseptabel PFD verdi i forhold til gitte SIL-klasse.

- Risikoevalueringen skal ta hensyn til alle feilkategorier som reelt inntreffer under operasjon; dvs en må ta hensyn til systematiske feil i tillegg til hardware feil (i notasjonen til IEC 615608).

- Pålitelighetsanalyser må så langt som mulig basere seg på relevante, reelle driftsdata.

- Krav om at kompetanse opprettholdes i drift. Oppfølging av drift og vedlikehold; uavhengig sjekk av arbeid.

- Det er viktig at muligheten for fellesfeil mellom HIPPS-sløyfer og mellom HIPPS og andre sikkerhetssystemer vurderes.

7.2 Anbefalinger mht videre arbeid

Mht ODs videre arbeid med HIPPS-problematikken anbefales følgende

- Detaljer og spesifiser krave som antydet i Avsnitt 7.1 (jfr også Kapittel 6 der flere punkter er utdypet).

- Foreta en vurdering av kravet i NORSOK vedrørende feil på to løp ifm fakkelkapasitet, *uavhengig* av det totale antall løp.

- Når det gjelder subsea HIPPS er det behov for en systematisk gjennomgang bl.a. av krav med hensyn til uavhengighet.

- Foreta en gjennomgang av operatørenes rolle og hvordan en skal ta hensyn til dette i risiko-analyser; inklusiv kvantifisering av menneskelig pålitelighet.

- Foreta en gjennomgang og vurdering av bruk av prosedyrer og "tidsforsinket operasjon" i forbindelse med PPS. Her fås en sammenblanding av prosedyrer og automatisk system, som kan svekke påliteligheten. Dessuten har en her det spesielle problemet at den lange responstiden i seg selv kan representere et problem.

- I takt med at HIPPS blir et "helt vanlig" system kan det være en utfordring å etterse at kompetanse for involverte personer for operasjon av disse system i alle faser er tilfredsstillende. Videre må tilsyn sikre at drift/vedlikehold er i henhold til forutsetninger og planer.

- Se på metoder for vurderinger av økning i kompleksitet av totalanlegget, spesielt evt. mangel på enhetlige løsninger. Dette gjelder både teknologi, brukergrensesnitt, prosedyrer og

vedlikehold.

- Bedre pålitelighetsdata bør fremskaffes, spesielt på QSVer og ventiler i FCS anvendelser. Det kan være behov for å innskjerpe at operatørenes (interne) rapporteringsrutiner må legges opp slik at de avdekker *årsak* til svikt, (spesielt når det gjelder sikkerhetskritiske system), og at datainnsamlingen følges opp med pålitelighetsanalyser som et ledd i kontinuerlig forbedring.

- Beregningsmetode for håndtering av fellesfeil bl.a. for et stort antall løp bør vurderes. Her har en i dag ikke noen anerkjent felles metode, og ulike operatører/konsulenter står nokså fritt til å velge angrepsmåte. Generelt er standardisering ønskelig når det gjelder analysemodell.

8 Referanser

/1/ T. Onshus, R. Aarø, B. F. Lund *HIPPS Applications and Acceptance Criteria.* Paper OTC 7828 presented at the 1995 OTC Offshore Technology Conference, May 14, 1995, Houston Texas.

/2/ Aarø R., Lund B.F. and Onshus T. *Subsea HIPPS Design Procedures.* Paper OTC 7829 presented at the 1995 OTC Offshore Technology Conference, May 14, 1995, Houston Texas.

/3/ Lund B.F., Aarø R. and Onshus T. *HIPPS Concepts for a Subsea Field Scenario*. Paper OTC 7830 presented at the 1995 OTC Offshore Technology Conference, May 14, 1995, Houston Texas.

/4/ *Subsea OPPS Feasibility Study*. Executive Summary Report STF75 F93011, (og i tillegg 9 delrapporter).

/5/ *Subsea HIPPS Development Study*. Executive Summary Report. STF75 F95029, (og i tillegg 9 delrapporter).

/6/ DIN 3381. *Sicherheitseinrichtungen für Gasversorungsanlagen mit betriebsdrüke bis 100 bar*, Deutsche Industrie Normen.

/7/ IEC 61508. *Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrical Commission, Part 1-7. (Part 2, 6, 7: First edition, 2000-04).

/8/ IEC 61511. *Functional safety: Safety Instrumented Systems for the process industry sector*. International Electrical Commission, Part 1-3.

/9/ 066 OLF *Guidelines on the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian continental shelf*, January 2001.

/10/ API RP 14C, *Recommended practice for analysis, design, installation and testing of basic surface systems for offshore production platforms.* API recommended practice 14C, American Petroleum institute (API), fifth edition, March 1994.

/11/ API RP 520. *Design and installation of pressure relieving systems in refineries.*

/12/ API RP 521. *Guide for pressure relieving and depressuring systems.*

/13/ NORSOK P-001, *Process design*, Rev. 4, Oct. 1999.

/14/ NORSOK P-100, *Process systems,* Rev. 1, August 1997.

/15/ NORSOK Z-13. Risk and emergency preparedness analysis, Rev. 1, Mars 1998. Utarbeidet av Norwegian Technology Standard Institution (NTS).

/16/ ISO 10418, *Analysis design, installation and testing of basic surface process safety systems for offshore installations*, Rev. 4, 07-05-1999.

/17/ prEN 50126. *Railway applications. The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS*). European Standard. CENELEC, European Committee for Electrotechnical Standardisation.

/18/ *Reliability Data for Control and Safey Systems. 1998 Edition.* SINTEF report STF38 A98445.

/19/ OREDA Phase III, computerised data base on topside equipment, (Offshore Reliability Data).

/20/ *Reliability Assessment Shut-off Valves*, AEA/MOK/18298167/Rev.2. AEA Technology consulting, May 2000.

/21/ *Pålitelighet av HIPPS*, Statoil Memo, PTT KU OPTEK 21009, 8.86.862, February 2001.

/22/ P. Hokstad og K. Corneliussen, Improved common cause failure model for IEC 61508 . SINTEF rapport STF A00420.

/23/ J.C. Williams, *HEART - A proposed method for assessing and reducing human error.* Proceedings of the 9th advances in reliability technology sympsium, 1986.

9 VEDLEGG A. Prinsipper for risikoakseptkriterier.

A.1 Krav til akseptkriterier

Når operatøren fastesettere akseptkriterium bør en ta hensyn til

- (observert) risiko i liknende aktiviteter
- bidrag til totalrisikoen (hvis en f.eks. ser på introduksjon av ny risiko)
- allmennhetens/de berørtes grad av aksept av den aktuelle risikoen
- krav om kontinuerlig risikoforbedring
- teknologiske og økonomiske muligheter for å kontrollere/redusere risikoen

Under presenteres tre prinsipp for akseptkriterier for risiko

- ALARP
- GAMAB
- MEM

Disse er alle er referert i Appendix D av prEN 50126, /17/.

A.2 ALARP (As Low As reasonably Practicable)

Dette prinsippet praktiseres bl.a. i Storbritannia, og refereres i flere standarder, bl.a. i NORSOK Z-13, /15/ og IEC 61508, /7/. Her vil endelig risiko i en virksomhet klassifiseres i tre klasser. Kort sagt er disse definert ved at

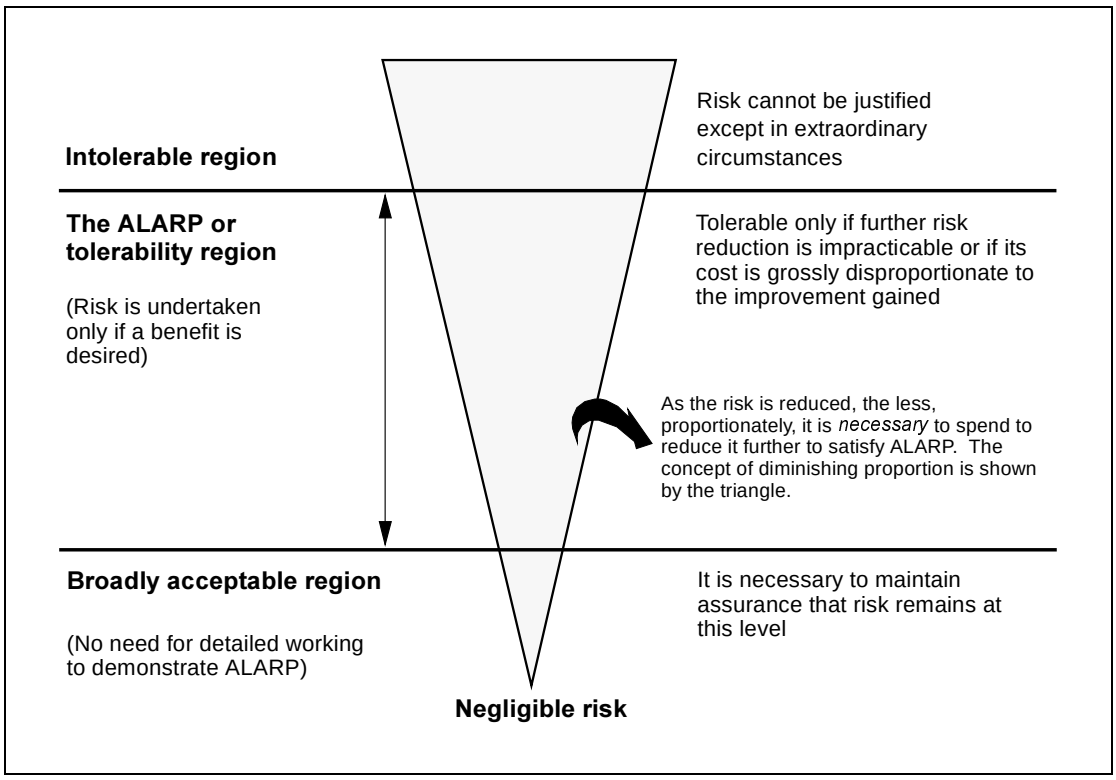
a) risikoen så stor at den overhodet ikke er akseptabel; eller

b) risikoen er, eller har blitt gjort, så liten at den er ubetydelig; eller

c) risikoen faller mellom de to tilfellene spesifisert i a) og b) over **og** har blitt redusert til det "lavest mulig" nivå, basert på en kost-nytte vurdering

ALARP prinsippet sier at hvis risikoen faller mellom de to ekstrem-områdene ("uakseptabel" og "akseptabel") skal risikoen reduseres til et nivå som er "Reasonably Practicable". De tre områdene er også illustrert i Figur under

Begrepet ALARP kan brukes både når kvalitative og kvantitative risikomål benyttes. Enkelte bruker begrepet ALARA (As Low As Reasonably Achievable), som essensielt har samme betydning. Merk at dette (disse) prinsipp ikke gir konkret råd om hvilke risikogrenser (tallverdier) som skal brukes for å skille mellom de tre regionene.



Figur A.**1 — Tolerable risk and ALARP (fra IEC 61508, del 5)**

A.3 GAMAB

GAMAB-prinsippet praktiseres en del i Frankrike.

GAMAB = *Globalement Au Moins Aussi Bon.*

Dette innebærer at en ny løsning sammenliknes med tidligere aksepterte løsninger, og at den nye løsningen totalt sett skal være minst like god som "ethvert ekvivalent eksisterende system". Jfr. også "Comparison Criteria", referert i Annex A.1.5 i NORSOK Z-13, /15/.

Når dette prinsippet velges, befris altså beslutningstaker for selv å spesifisere en akseptabel risikogrense.

A.4 MEM. (Minimum Endogenous Mortality)

MEM prinsippet brukes en del i Tyskland.

MEM = *Minimum Endogenous Mortality*

En tar her utgangspunkt i at mennesker omkommer av en rekke "teknologiske faktorer", f.eks. sport/underholdning, egenaktiviteter (bl.a. i hjemmet), arbeidsmaskiner, transport. Disse dødsfall resulterer i en viss sannsynlighet for død pr år ("endogen" dødelighet). Merk at død p.g.a. sykdom ikke er inkludert. I vel utviklede land er denne sannsynligheten lavest for aldersgruppen 5-15, og betegnes "Minimum Endogenous Mortality":

$R_m = 2 \cdot 10^{-4}$ omkomne pr person pr år

Poenget med MEM prinsippet er at det spesifiseres at risikoen som følge av en bestemt virksomhet ikke skal påvirke dette tallet signifikant. Det kan f.eks. bety at personrisiko som følge av en virksomhet ikke skal overstige 10^{-5} omkomne pr person pr år.

Her vil altså beslutningstaker fremdeles selv måtte sette akseptgrensen, men prinsippet gir betydelig støtte til å sette denne grensen.