Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: **Risikostyring med spesialisering i offshore sikkerhet.**	Vår semesteret, 2012 **Konfidensiell**
Forfatter: **Endre Halvorsen**	…… (signatur forfatter)
Fagansvarlig: **Terje Aven** Veileder(e): **Gunnar Anglevik, Statoil**	
Tittel på masteroppgaven: **Analyse og styring av aldrende sikkerhetssystemer** Engelsk tittel: **Analysis and management of aging safety systems**	
Studiepoeng: 30	
Emneord: **Sikkerhetssystem** **Aldring** **Teknisk tilstand Sikkerhet** **Gap analyser** **Pålitelighetsanalyser** **ALARP** **Kostnytte**	Sidetall: 50 + vedlegg/annet: 16 Stavanger, 15.06.2012 dato/år

Oppgaven foreslår underlag og beslutningsprosess om hvorvidt man skal videreføre eksisterende teknologi eller innføre ny teknologi i sikkerhets-systemene for å møte forlenget levetid.

Analyse og styring av aldrende sikkerhetssystemer

DISCOS systemer i Statoil

Halvorsen, Endre

Forord

Denne masteroppgaven er avslutningen av 2-årig masterstudie i risikostyring, spesialisering i offshore sikkerhet ved Universitetet i Stavanger. Oppgaven utgjør 30 studiepoeng.

Oppgaven er gjennomført i et samarbeid med Statoil og en tidligfasestudie som utføres internt i Statoil. Studien skal vurdere behov for oppgradering av alle Siemens Teleperm M-systemer offshore. En del av disse systemene er sikkerhetssystemer som vurderes delvis for seg selv. Dette ble en mulighet for meg til å utføre denne masteroppgaven i lys av denne studien og deretter inngå i studiegruppen når oppgaven blir ferdigstilt.

Min egen faglige bakgrunn er automasjonsingeniør fra Universitet i Stavanger i 1999. Jeg har arbeidserfaring som systemleverandør, leveranser av sikkerhetssystemer og prosjekterfaring i Statoil. Dette har vært et godt utgangspunkt for denne oppgaven.

Takk til alle som har gjort det mulig for meg å få utført denne oppgaven, og de som har kommet med gode innspill, diskusjoner og utfordringer.

Stavanger 15. Juni 2012

Endre Halvorsen

Forkortelser og Definisjoner

Forkortelse	Beskrivelse
B&G	Brann og Gass-deteksjonssystem
CPU	Central Processor Unit
HF	Human Factors
HMI	Human Machine Interface
DISCOS	Distributed Supervisory Control and Safety System (Hydro definisjon)
DNV	Det Norske Veritas
FFO	Flerfeltsoperasjoner
HAZOP	Hazard and operability study
HWFT	Hardware Fault Tolerance
IOR	Increased Oil Recovery
I/O	Inn og Utganger
MTTF	Mean Time To Failure
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MTO	Menneske Teknologi og Organisasjon
M2	En Type Notifikasjon i SAP
NAS	Nød-avstegningssystem
NPV	Net Present Value
OLF	Oljeindustriens Landsforening
PAS	Prosess-avstegningssystem
PS	Performance Standard
Ptil	Petroleumstilsynet
P01, P01	SAP versjoner
SAS	Safety and Automation System
SIS	Safety Instrumented System
SIF	Safety Instrumented Function
SFF	Safe Failure Fraction
SJA	Sikker Jobb Analyse
Teleperm M	Elektronisk prosess kontroll system, utviklet av Siemens i starten på 1980 årene
TFF	Target Failure Fraction
TTS	Teknisk Tilstand Sikkerhet
TST-database	Database for alle TTS verifikasjoner
TPM	Teleperm M
WBS	Work Breakdown Structure

Innhold

1 Innledning

1.1 Bakgrunn for oppgaven

Innretninger på Norsk kontinentalsokkel er designet og godkjent for en bestemt levetid. Om få år vil mer enn halvparten av innretningene på sokkelen ha passert sin opprinnelig tiltenkte levetid. Mange felter har fremdeles lønnsomme olje- og gassreserver som det er mulig å utvinne ved å forlenge innretningens levetid.

Eldre innretninger møter flere problemstillinger knyttet til aldring av de enkelte barrieresystemene. Systemene er introdusert i designet for å reduserer risiko for mennesker, miljø og materielle verdier. Under drift blir systemene og de enkelte barriere funksjonene testet og vedlikeholdt i henhold til et fastsatt vedlikeholdsprogram. Systemene er bygget på en teknologi som stadig er under utvikling og møter blant annet utfordringer knyttet til ytelse og support av teknologien. Systemene skal samtidig tilfredsstille krav fra myndighetene og operatørselskapenes interne krav.

Ombygninger og prosessendringer medfører at systemene må modifiseres, gjerne i forbindelse med prosjekter som er initiert for øke levetiden. Dette kan medføre utfordringer i forhold til tilgjengelig kapasitet i systemene og muligheten til å inkludere modifikasjonene i eksisterende system. Ved utvidelse eller utskiftning kan man enten holde seg til eksisterende teknologi eller skifte ut systemene til nyere teknologi.

Utskiftninger av sikkerhetssystemer offshore er komplekse prosjekter som vil pågå i lengre tidsperioder. Deler av arbeidet kan utføres og planlegges inn mot revisjonsstanser, mens andre deler må utføres under normale driftsforhold. Kostnadene forbundet med gjennomføring av slike oppgraderings prosjekter er betydelige, i tillegg er det fare for at driftsregulariteten og integriteten til sikkerhetssystemene påvirkes negativt under oppgraderingsperioden.

De finnes flere referanseinstallasjoner på Norsk sokkel hvor det er utfordringer knyttet til aldringsproblematikk, og hvor det utføres ulike tiltak for å robustgjøre sikkerhetssystemer. Noen utfører total utskiftning av sikkerhetssystem mens andre gjør mindre modifikasjoner for å holde seg innenfor minimumskravene. For å kunne gjennomføre en investeringsbeslutning må behovet og nytteverdien dokumenteres.

1.2 Formål med oppgaven

Hovedmålet med denne oppgaven er:

- Beskrive dagens rammeverk og metoder som kan benyttes for å vurdere aldring og levetid til de instrumenterte sikkerhetssystemene på eldre installasjoner på norsk sokkel. Systemene som skal gjennomgås inngår som en del av sikkerhet og automasjonssystemene.
- Identifisere hvordan aldring av sikkerhetssystemene kan påvirke ytelsen, dette inkluderer fysisk degradering og samspill mellom menneske, teknologi og organisasjon, men også å vurdere om det finnes andre problemstillinger knyttet til aldring av systemene.
- Vurdere og foreslå underlag, analyser og prosesser som er nødvendig for å kunne foreta beslutninger rundt forlenget levetid av sikkerhetssystemene.

1.3 Innhold i oppgaven

Kapittel 2. Beskriver hvordan sikkerhet og automasjonssystemene offshore er bygget opp og hva som regnes som et instrumentert sikkerhetssystem. Her forklares også forskjellen mellom et sikkerhetssystem og en sikkerhetsfunksjon. Figur 2-3 avgrenser systemet som denne oppgaven skal omhandle.

Kapittel 3. Gjennomgår regelverket som definerer funksjonelle krav til sikkerhetssystemene. Det beskrives i hvilke grad regelverket har tilbakevirkende kraft på eldre installasjoner. Det er disse overordnede kravene som danner referansen man måler mot i forbindelse med teknisk gap.

Kapittel 4-6. Beskriver problemstilling og hvilke alternativer som kan vurderes i forbindelse med en levetidsforlengelse. Anbefaler en prosess for å vurdere de ulike alternativene og involvering av ledelsen og beslutningstakerne.

Kapittel 7-8. Identifiserer ulike utfordringer i forbindelse med aldring av systemene. Basert på identifiserte farefaktorer analyseres systemene gjennom ulike metoder. Dataene som benyttes i analysene er hentet fra etablerte verktøy i Statoil.

Kapittel 9-10. Beskriver hvordan ledelsen og beslutningstakerne kan benytte informasjon fra analyser med tilhørende usikkerhet til å forta en beslutning. Kapitel 10 drøfter beslutningsprosessen.

<u>Oppsummert:</u>
Denne oppgaven foreslår underlag og beslutningsprosess om hvorvidt man skal videreføre eksisterende teknologi eller innføre ny teknologi i sikkerhetssystemene for å møte forlenget levetid.

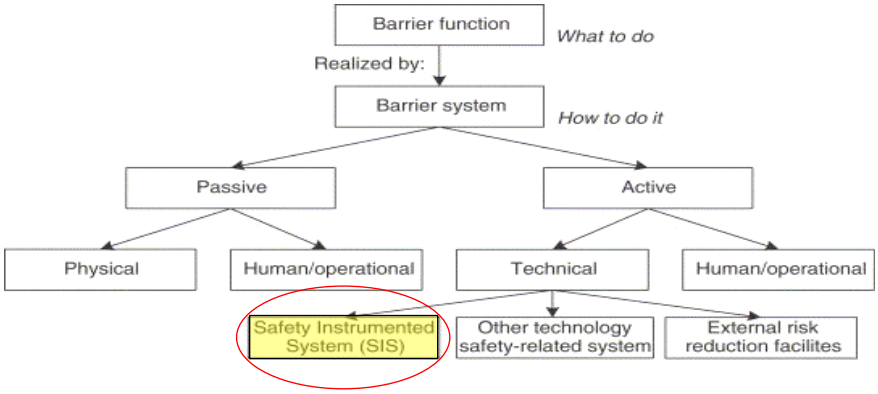
2 Sikkerhetssystemer og Automasjonssystem

2.1 SAS (Sikkerhet og Automasjons System)

Sikkerhet og automasjonssystem (SAS) utfører måling, prosesskontroll, sikkerhetskontroll og er grensesnittet mellom operatøren og prosessen på en installasjon. De ulike systemene inngår i et integrert system som kan bestå av utstyr fra en eller flere leverandører. Sikkerhetssystemene som inngår i SAS er nød-avstengningssystemet, prosess-avstengningssystemet og brann- og gassystemet. Selv om systemene er integrerte er det et myndighetskrav om at sikkerhetssystemene skal være uavhengig fra prosesskontrollsystemene. Dette betyr at sikkerhetskritiske funksjoner ikke skal implementeres i kontrollsystemet og at kontrollsystemet ikke skal kunne påvirke sikkerhetssystemet negativt. Se vedlegg C for en typisk SAS topologi i et offshore anlegg.

2.2 Sikkerhetssystemer (SIS)

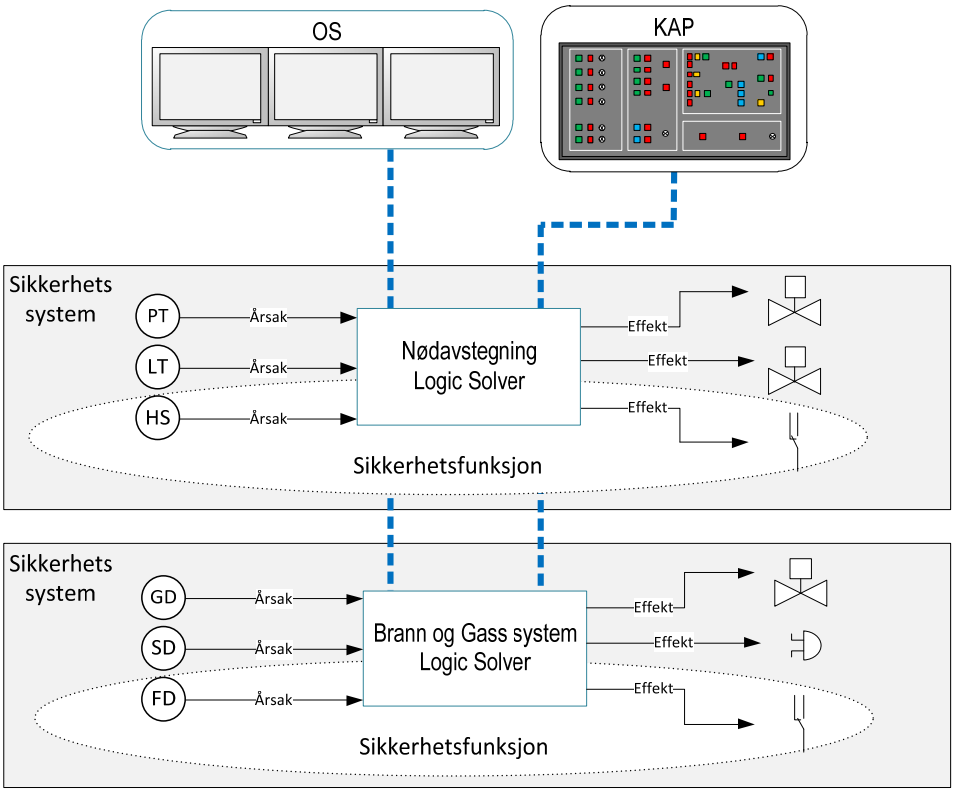
Et instrumentert sikkerhetssystem er et aktivt barrieresystem som ivaretar mange sikkerhetsfunksjoner eller barrierefunksjoner.



Figur 2-1 Barriererfunksjoner (Sklet)

2.3 Instrumentert sikkerhetssystem (SIS) og sikkerhetsfunksjoner (SIF)

Et instrumentert sikkerhetssystem benyttes til å detektere, stoppe eller forhindre en påbegynt farlig hendelse og/eller begrense denne hendelsens konsekvenser. Systemet inneholder minst en logisk enhet. Systemet er normalt uavhengig av andre systemer som for eksempel prosesskontrollsystemet. Et instrumentert sikkerhetssystem kan deles inn i fire ulike sub-systemer, sensor, logikkenhet, menneske/ maskin-grensesnitt og sluttelement. De ulike funksjonene som utføres i et slikt system er ofte referert til som sikkerhetsfunksjoner (SIF). Et instrumentert sikkerhetssystem kan ha mange ulike sikkerhetsfunksjoner. Figur 2.2 illustrerer nød-avstengningssystemet og brann- og gass-systemet med ulike sikkerhetsfunksjoner.



Figur 2-2 Sikkerhetssystem og sikkerhetsfunksjoner

2.4 Avgrensning av systemene som denne oppgaven omhandler

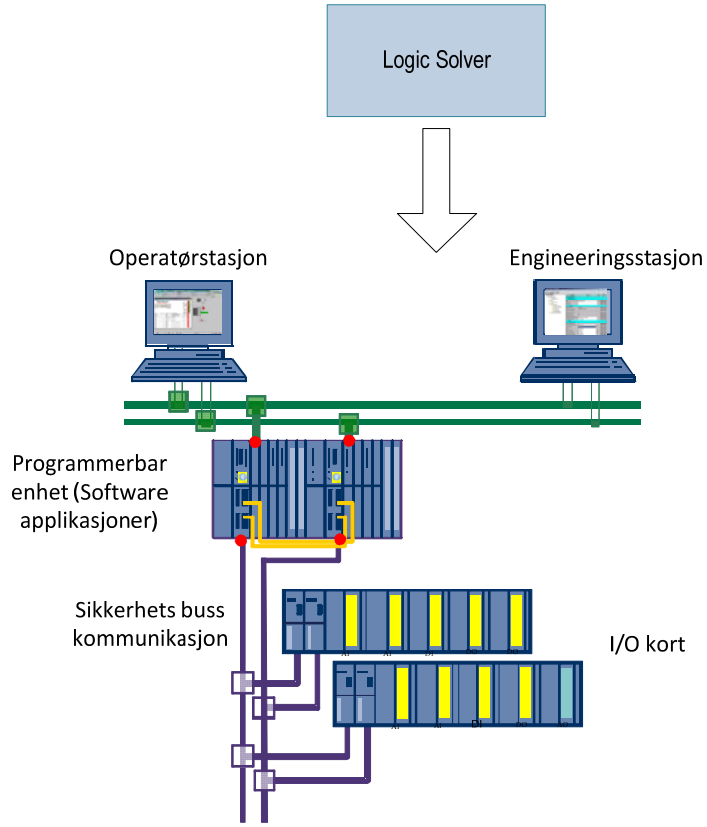
Denne oppgaven skal belyse problemstillinger knyttet til aldring av sikkerhetssystemene innenfor SAS offshore. Sikkerhetssystemene som inngår i SAS skal ivareta følgende:

1. Nødavstengningssystemet skal hindre eskalering av unormale tilstander til en farlig hendelse og begrense omfanget og varigheten av slike hendelser som oppstår.

2. Prosessavstengningssystemet skal registrere og vurdere en unormal prosesstilstand og iverksette nødvendig utstyrsstans og/eller prosess-seksjonalisering, for å forhindre, eventuelt minimere effektene.

3. Brann- og gass systemet skal kontinuerlig overvåke brann-og gass status og utføre sikkerhetsrelaterte funksjoner ved deteksjon av branntilløp, brann eller gasslekkasje.

Disse systemene inneholder mange ulike sikkerhetsfunksjoner i samme enhet. Selve kontrollenheten (logikk) kan deles inn i ulike elementer som, operatørstasjoner for alarm og status til operatør, vedlikeholdstasjon for å implementere endringer i systemet og programmerbar enhet som består av ulike typer programvare og som kommuniserer over buss mot inn- og utgangskort. Systemet er avhengig av strømtilførsel for å kunne operere i normal modus.



Figur 2-3 Elementer som inngår i logikk

2.5 Livssyklusen til sikkerhetssystemene

Livsløpet til et instrumentert sikkerhetssystem kan deles inn i flere hovedfaser. Første fase dekker analyse og design av de enkelte risikoreduserende funksjonene, ytelseskrav fastsettes, deretter følger realisering av de enkelte systemene. Under drift og operasjon sørger man for å måle ytelsen opp mot de fastsatte krav som er definert. Under operasjonsfasen kan det pågå modifikasjoner av systemene i forbindelse med ulike prosjekter.

3 Ansvar og regelverk

Virksomheten på norsk kontinentalsokkel reguleres gjennom petroleumsloven. Utvinningstillatelser blir tildelt gjennom konsesjonsrunder og departementet peker ut en operatør for utvinningstillatelsen som skal stå for den operative virksomheten i utvinningstillatelsen.

Regelverket for petroleumsvirksomhet på norsk kontinentalsokkel består blant annet av fem ulike forskrifter med tilhørende veiledninger som vist i figur 3-1. Kravene i forskriftene er i stor grad funksjonsbaserte og refererer videre til andre anerkjente standarder.

HMS-forskriftene i regelverket er risikobaserte, det vil si at forskriftene må tolkes som en funksjon av de spesifikke risikoer som gjelder i hver enkelt virksomhet. Kravene i HMS-regelverket er i hovedsak utformet som såkalte funksjonskrav. Det betyr at de angir hvilket sikkerhetsnivå som skal oppnås, men ikke hvordan. Dermed må den enkelte aktør fastlegge hvordan virksomheten konkret skal møte myndighetskravene.

Figur 3-1 HMS regelverk på Norsk kontinental sokkel

Aktøren må altså gjøre en vurdering av de spesifikke risikoforholdene som er knyttet til hver enkel aktivitet. Hvor krevende det er å oppfylle HMS-forskriftene er dermed avhengig av særegenheter ved hver enkel virksomhet. I kapitlene under beskrives lovverk og forskrifter som er relevante for de instrumenterte sikkerhetssystemene.

3.1 Petroleumstilsynets forskrifter

Forskriftene gjelder, med unntak av innretningsforskriften, for alle offshoreinstallasjoner. Innretningsforskriften er gjeldene fra 1.1. 2002, men har ikke tilbakevirkende kraft. For

sikkerhetssystemer gjelder at ved større ombygginger og modifikasjoner på eksisterende innretninger gjelder likevel forskriftene for det som omfattes av ombyggingen eller modifikasjonen. Større ombygginger og modifikasjoner kan være installering av en ny modul, større inngrep i hydrokarbonførende systemer eller større endringer av fysiske barrierer.

Under er et utdrag fra de ulike forskriftene som er relevante i forhold til vurdering av instrumenterte sikkerhetssystem.

3.1.1 Styringsforskriften

§5 Barrierer

- Barrierens funksjon skal alltid ivaretas
- Det skal være kjent om barrierene er svekket
- Det skal kompenseres for svekkede barrierer
- Krav til ytelse av barrierene skal defineres

3.1.2 Aktivitetsforskriften

(§26 sikkerhetssystemer)

- Det skal fastsettes på forhånd hvilke tiltak og begrensninger som er nødvendige ved overbroing eller utkopling av sikkerhetssystemer eller deler av systemene, eller når systemene er svekket på annen måte
- Status for alle overbroinger, utkoplinger og andre svekkelser skal være kjent til enhver tid

3.1.3 Innretningsforskriften

§8 Sikkerhetsfunksjoner

- Det skal fastsettes krav til ytelsen for sikkerhetsfunksjoner
- Status for sikkerhetsfunksjoner skal være tilgjengelig i det sentrale kontrollrommet

§ 21 Menneske-maskin-grensesnitt og informasjonspresentasjon

- Krav om oppgave- og funksjonsanalyser
- Alarmene som presenteres, er enkle å registrere og oppfatte og klart viser hvor de eventuelle avvikene og faresituasjonene har oppstått
- Alarmene kodes, kategoriseres og tildeles prioritet basert på alarmenes sikkerhetsmessige betydning og hvor raskt det må reageres for å unngå uønskede konsekvenser
- Alarmsystemene legger til rette for undertrykking og redusering av alarmer, slik at mental overbelastning av kontrollroms- personellet unngås under driftsforstyrrelser og ulykkeshendelser

§32 Brann og gassdeteksjonssystemet

- Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre system

§33 Nødavstegningssystemet

- Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre system
- Nødavstengningssystemet skal utformes slik at det går til eller forblir i en sikker tilstand dersom det oppstår en feil som kan hindre systemet i å virke
- Nødavstengningssystemet skal ha en enkel og entydig kommandostruktur
- Fra det sentrale kontrollrommet skal det være mulig å manuelt aktivisere funksjoner som bringer innretningen til en sikker tilstand ved svikt i de programmerbare delene av systemet

§34 Prosessikringssystemet

- Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer
- Systemet skal utformes slik at det går til eller forblir i en sikker tilstand dersom det oppstår en feil som kan hindre systemet i å virke
- Prosessikringen skal utformes med to uavhengige sikringsnivåer for beskyttelse av utstyr

3.2 IEC61508/IEC61511 og OLF 070

I veiledningene til forskriftene nevnes det at for sikkerhetssystemer bør IEC61508 og OLF070 benyttes. Ved utforming av alarmsystemene bør prinsippene i Oljedirektoratets publikasjon YA-710 følges.

Når man skal designe et sikkerhetssystem og dets funksjoner etter dagens krav, anvendes IEC61508/11 og OLF 070. Etter at analysefasen er utført bestemmer man hvilken risikoreduksjon som er nødvendig gjennom instrumenterte funksjoner for å redusere risikoen til et akseptabelt nivå. Oppsummert kan man dele inn kravene fra standardene på følgende måte:

1. Krav til ytelse gjennom PFD[1]. Det er definert som 4 ulike nivåer, SIL 1-4 og man skiller mellom funksjoner som er ”low demand” eller ”high demand”. PFD er sannsynligheten for at sikkerhetsfunksjonen ikke virker når man trenger den.

2. Strukturkrav definerer påkrevd feiltoleranse av hardware sub konfigurasjon (for eksempel logikk). Avhengig av kompleksiteten til komponenten skiller man mellom type A og type B komponenter. Standarden definerer 3 ulike feiltoleranseverdier 0,1 og 2. Avhengig av komponentens type og evne til å detektere farlige feil (SFF) stilles det krav til systemstruktur.

3. Unngåelse og kontroll av systematisk feil ved å følge teknikker og tiltak som beskrevet i standarden.

4. Software-krav inngår under systematiske feil. Det skilles mellom krav til programvareutvikling (IEC61508) og programvareapplikasjon (IEC61511)

[1] Probability of failure on demand

3.3 OLF122-Recommended guidelines for service life extension

OLF122 veiledningen har til hensikt å hjelpe operatøren/selskapet med en framgangsmåte til å vurdere og dokumentere sikker drift i en forlenget periode. I tillegg legger den et rammeverk for informasjon som bør inngå i en søknad om levetidsforlengelse.

Veiledningen beskriver blant annet at den tekniske integriteten til sikkerhetssystemer som NAS, B&G, PAS skal analyseres og evalueres. I tillegg sier veiledningen at gapanalyse mot innretningsforskrift skal utføres og at ALARP- prinsippet skal benyttes for å reduserer risiko.

Det er opprettet en egen arbeidsgruppe som arbeider med å revidere OLF122. Statoil bidrar med personell i denne arbeidsgruppen. Arbeidet er planlagt ferdigstilt i juni 2012.

4 Problemstilling

Statoil er i ferd med å gjennomføre en mulighetsstudie som vurderer behovet for oppgradering av DISCOS systemene på seks ulike installasjoner. Felles for de ulike installasjonene er at alle har systemer som er levert av Siemens og er baserte på Teleperm M-teknologien. Statoil-den gang Hydro bygget totalt syv installasjoner basert på denne teknologien, og disse er de eneste plattformene med Teleperm M-teknologi på norsk kontinentalsokkel. Hydro benyttet en rammeavtale mot Siemens som systemleverandør. Systemene er baserte på samme type design, og bruk av felles biblioteker og standard løsninger.

De seks installasjonene er:

- Brage
- Njord A
- Oseberg Sør
- Oseberg Øst
- Troll C
- Visund

Sikkerhetssystemene og Teleperm M-teknologien har vært i drift siden nittitallet. Brage ble satt i drift 1993

Installasjon	Oppstart offshore
Brage	September 1993
Njord A	September 1997
Oseberg Sør	September 2000
Oseberg Øst	Mai 1999
Troll C	1999
Visund	April 1999

Tabell 4-1 Oppstartsår offshore for de ulike installasjonene

Teleperm M-teknologien ble levert av Siemens frem til slutten av 90-tallet. Systemet er i ferd med å fases ut fra Siemens og vil ikke lengre bli support etter år 2014-2016. Dette er systemer som er levert til både land og offshorebasert industri. Det er levert mellom 15.000-20.000 Teleperm M-anlegg globalt (Wikipedia).

Hovedmålet med mulighetsstudien er å anbefale tiltak og konsept for å møte krav om forlenget levetid for SAS til 2030 på alle installasjonene. Studien skal fokusere på ulike behov innen tre ulike hovedsystemer:

1. Prosesskontrollsystemer (PCS)

2. Subseasystemer (SCU)

3. Instrumenterte sikkerhetssystemer (SIS)

Metoden som skal benyttes er ikke fastsatt og vil være ulik for de forskjellige typer system. Erfaringsmessig blir det utført ulike typer vurdering av systemer som har behov for oppgradering, men det finnes ikke en fastsatt metodikk i Statoil for hvordan slike behov skal vurderes.

Brage har alt Statoil startet prosessen rundt levetidssøknad til myndighetene. OLF122 danner grunnlag for søknaden. Den tekniske integriteten til de instrumenterte sikkerhetssystemene skal vurderes blant annet ved hjelp av GAP-analyser som skal identifisere avvik mot dagens krav (innretningsforskriften) og standarder. ALARP-prinsippet skal benyttes under evaluering av gap, i henhold til OLF122.

Tabellen 4.2 viser når de ulike installasjonene går ut på levetid.

Inst. navn	Inst. Type	Fase	Inst. Dato	design levetid	Operatør	Installasjons år	Design levetid utgår	SIS teknologi
BRAGE	JACKET 8 LEGS	I service	mai 93	20	Statoil	1993	2013	Siemens TPM
OSEBERG SØR	JACKET 6 LEGS	I service	januar 99	30	Statoil	1999	2029	Siemens TPM
OSEBERG ØST	JACKET 4 LEGS	I service	juni 98	20	Statoil	1998	2018	Siemens TPM
NJORD A	SEMISUB STEEL	I service	august 97	25	Statoil	1997	2022	Siemens TPM
TROLL C	SEMISUB STEEL	I service	august 99	25	Statoil	1999	2024	Siemens TPM
VISUND	SEMISUB STEEL	I service	august 98	30	Statoil	1998	2028	Siemens TPM

Tabell 4-2 Oversikt over Statoils innretninger på Norsk sokkel med Teleperm M-teknologi

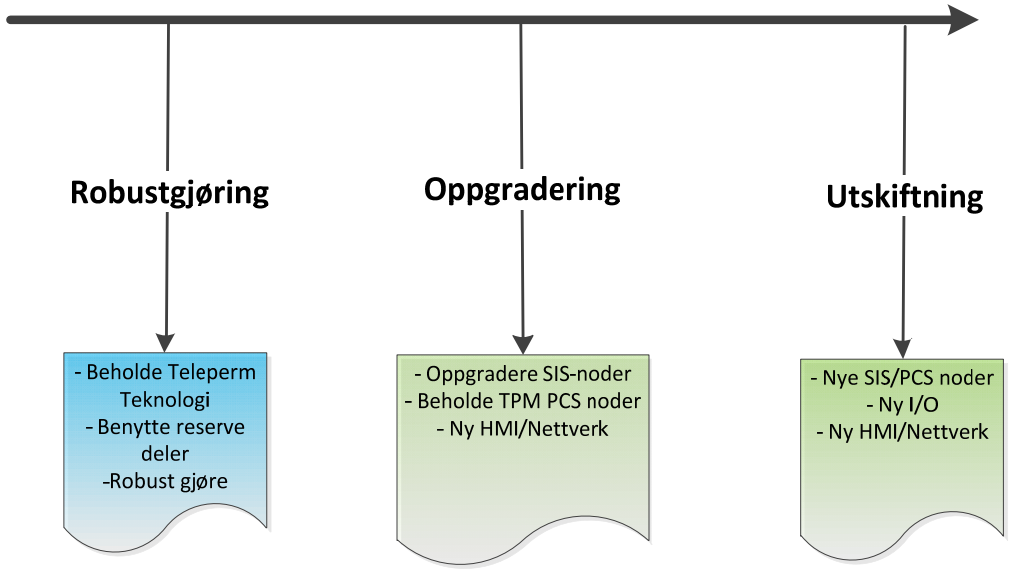
Systemene skal møte krav for forlengelse av drift av installasjonene frem til 2030. Med et tidsperspektiv frem mot 2030 for installasjonene vil systemene ha vært i drift i over 30 år. Statoils styrende krav (TR3034) til slike systemer beskriver en levetid på 20 år for node og I/O kort. HMI systemene har en vesentlig kortere levetid, definert til 6-8 år.

Å leve videre med TPM-teknologien i sikkerhetssystemene er forbundet med ulike typer risiko og utfordringer. Bekymringen er økende feilrater som følge av aldring av systemet. Feil i disse systemene kan resultere i uønskede hendelser i form av tapt sikkerhetsfunksjon eller tilgjengelighet (tapt produksjon). Man har lang erfaring med systemene i drift og kjenner til ulike typer feilfrekvens.

5 Alternativer

For å møte forlenget levetid frem til 2030 er det skissert 3 ulike alternativer som skal utredes. For SIS er det 2 ulike alternativer, enten beholde eksisterende teknologi eller skifte ut eksisterende systemer til ny teknologi.

Figur 5.1 viser to ulike strategier for SIS for å kunne møte en forlenget levetid frem mot 2030. Alternativ 1 er å beholde eksisterende system og teknologi, mens alternativ 2 er å oppgradere eller skifte ut sikkerhetssystemene. Det tredje alternativet i figuren inkluderer også PCS systemene, men det alternativet utredes ikke i denne oppgaven.



Figur 5-1 Alternativer som skal vurderes

1. Beholde eksisterende SIS teknologi

Ved å velge denne strategien vil man kunne utsette investeringen det innebærer å gå for en totalutskiftning. Dette alternativet kan allikevel medføre at ulike tiltak bør iverksettes for å redusere farekilder og tilhørende konsekvenser.

2. Skifte ut SIS med dagens teknologi.

Ved å skifte ut hele systemer vil man kunne designe systemer som vil være i samsvar med dagens ytelseskrav. Dette gjelder både i forhold til sikkerhet og tilgjengelighet. I tillegg vil man kunne designe inn overskuddskapasitet for å møte fremtidige modifikasjoner.

Oppgradering av sikkerhetssystemer offshore er kostbart og innebærer i seg selv en fare for sikkerheten og økonomisk tap. Gjennomføring av en utskiftning vil kunne utføres i stor grad under normale driftsforhold. For NAS/PAS-systemene vil produksjonstans være nødvendig for å få utført funksjonstest av nytt system.

6 Forslag til beslutningsprosess

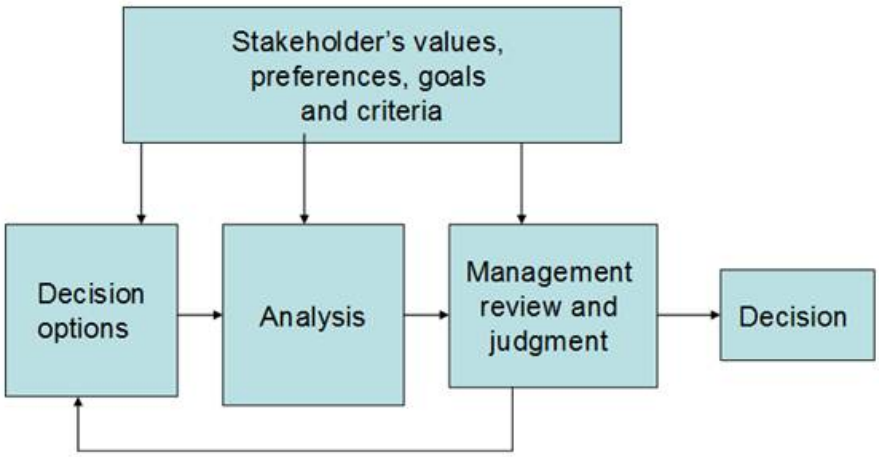
En beslutningsprosess i vurderingen om hvorvidt gammel teknologi skal beholdes eller ikke, må støttes opp av informative analyser og beskrivelse av usikkerhet. Beslutningsprosessen i denne sammenheng tar utgangspunkt i modellen (Aven) i figur 6-1.

Beslutningsprosessen kan deles inn i 4 ulike deler:

1. Identifisering av ulike alternativer for å møte forlenget levetid med sikkerhetssystemene
2. Analyse arbeid
3. Evaluering av resultat fra analyser
4. Valg av alternativ

Før en beslutning skal tas må underlaget fra analysene vurderes. Hva har blitt analysert og hvilke antakelser og usikkerhet eksisterer. Modellen skiller mellom analyser og ledelsesvurdering. Analysene skal utføres uten påvirkning fra mulige utfall av beslutning. Det er ledelsen som skal beslutte det beste alternativet som innebærer å finne en balanse mellom kostnader mot fordelen av tiltaket. Det er beskrevet mer om ledelsesvurdering i kapitel 9.

Beslutningsprosessen må også ses i sammenheng med en kontekst. I konteksten er de overordnede målene og de ulike parametere som skal overveies ved styring av risiko.



Figur 6-1 Model for beslutningsprosessen (Aven, 2008)

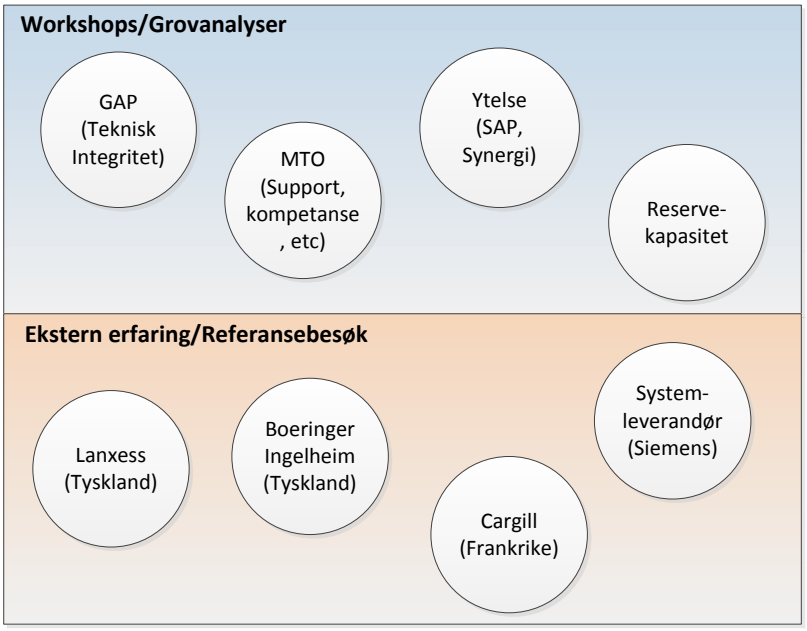
7 Analyser

Det er vesentlig å utføre en grundig identifisering for å sikre at alle aktuelle problemstillinger blir vurdert og inkludert som en del av beslutningsunderlaget. Farekilder som ikke blir fanget opp på dette stadiet kan fort bli utelatt for videre analyser og behandling.

Metode for å indentifisere problemstillinger forbundet med TPM-teknologi er basert på gruppearbeid og en form for grovanalyse. Resultatet er skissert i figur 7-1.

For å ytterligere identifisere farekilder har man oppsøkt andre selskaper med liknende problemstilling for å forsøke å lære av andre. Teleperm M-teknologien er som beskrevet i kapittel 3 benyttet i et stort omfang i Europa. Referansebesøkene gir innsikt i andre selskapers strategi og drivere for ulike tiltak.

Systemleverandør har også blitt involvert for å informere om videre support av teknologien.



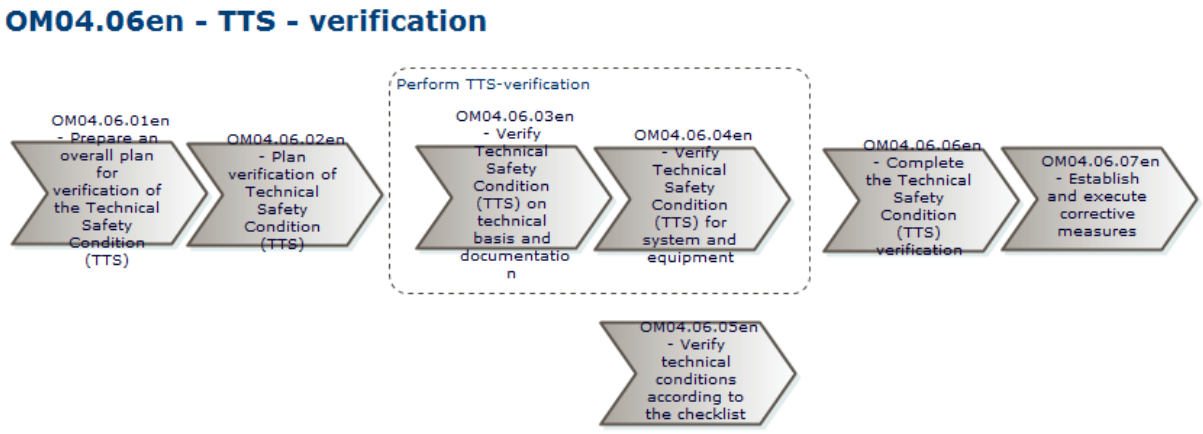
Figur 7-1 Metode for identifisering av farekilder ved eksisterende teknologi

Resultat fra figur 7-1 danner grunnlag for videre analyse arbeid for å behandle de ulike farekildene. Arbeidet skal resultere i et informativt underlag som skal benyttes i beslutningsprosessen, dette er videre beskrevet i kapitel 10.

7.1 Gap-analyse av teknisk tilstand

Gap-analyse av teknisk tilstand innebærer å vurdere gapet mellom den tekniske tilstanden til sikkerhetssystemene, og dagens krav og det ønskede referansenivået som er definert i ulike TR[2] dokumenter. Tilstanden skal møte overordnende myndighetskrav og anbefalinger fra en rekke internasjonale standarder. Statoils TR-hierarki er globale krav som dekker alle områder hvor Statoil opererer, og det utføres jevnlig verifikasjoner av sikkerhetssystemene gjennom en metode kalt teknisk tilstand sikkerhet, forkortet til TTS.

TTS-verifikasjon er en verifikasjonsmetodikk som ble utviklet av Statoil på begynnelsen av 2000-tallet for å kontrollere tilstanden til de tekniske sikkerhetsbarrierene på de ulike installasjonene. Verifikasjonene utføres av et utvalg av teknisk fagpersonell internt i Statoil (personellet må være uavhengige fra plattformorganisasjonen), og personell innleid fra eksterne selskap som for eksempel DNV. Resultatene fra verifikasjonene er benyttet til å utvikle indikatorer for å overvåke teknisk sikkerhetstilstand og utvikling på en systematisk måte.



Figur 7-2 Statoil arbeidsprosess i forbindelse med gjennomføring av en TTS-verifikasjon

Ved en TTS-verifikasjon "splittes" plattformen opp i subsystemer, og hvert enkelt subsystem har sin egen ytelsesstandard definert i henhold til myndighetskrav og selskapets interne krav. Dedikert personell med kjernekompetanse innenfor hvert enkelt subsystem arbeider intensivt on- og offshore i samarbeid med teknisk systemansvarlige, for å avdekke gap mellom krav og faktisk tilstand. Det benyttes egne sjekklister med veiledende sjekkpunkter og felles database for alle installasjoner for å sikre en enhetlig verifikasjon. Alle avvik registreres i en database, kalt TTS-databasen.

[2] Technical Requirements, del av Statoils styrende dokumentasjon

7.2 TTS gjennomføring og PSer

Installasjonene som Statoil-prosjektet vurderer har alle gjennomgått komplette TTS-verifikasjoner. De fleste er utført i løpet av 2011, men for Njord og Oseberg er de forrige verifikasjonene utført i 2006. For disse installasjonene er det planlagt nye verifikasjoner i løpet av 2012.

	2006	2007	2008	2009	2010	2011	2012
Visund						X	
Troll C						X	
Brage						X	
Njord	X						X
Oseberg Øst						X	
Oseberg Sør	X						X

Tabell 7-1 TTS oversikt – verifikasjoner 2006 – 2012

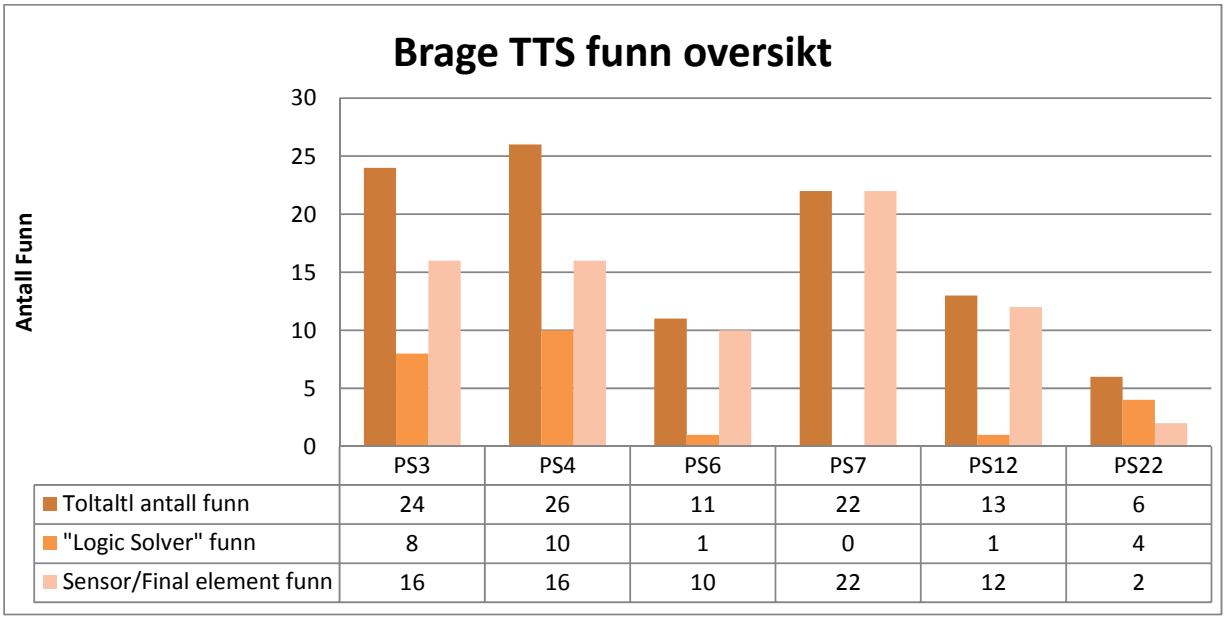
For å inkludere alle sjekkpunkter som er relevante for denne masteroppgavens definerte system, er alle ytelsesstandarder som inneholder krav til SIS-systemene identifiserte. Dette gjelder følgende PSer:

- PS 3 (Gassdeteksjon)
- PS4 (Nødavstegning)
- PS6 (Tennkildekontroll)
- PS7 (Branndeteksjon)
- PS12 (Prosessikring)
- PS22 (Menneske/maskin-grensesnitt og alarm system)

Deretter er det tatt ut rapporter fra TTS-databasen. Alle funn som tilhører de relevante ytelsesstandardene er gjennomgått, og relevante funn for SIS er identifisert.

7.2.1 Vurdering av TTS funn

Det er identifisert flere avvik mellom ønsket referansenivå og sikkerhetssystemene på alle seks TPM-installasjonene. Antall funn ligger rundt tjue for hver installasjon med unntak av Oseberg -plattformene. Her er antall funn betydelig lavere. Figur 7-3 og figur 7-4 viser resultat fra Brage installasjonen. Tilsvarende presentasjon av funn fra de andre installasjonene er i vedlegg B. Beskrivelse av funntekst er gitt i vedlegg D.



	PS3	PS4	PS6	PS7	PS12	PS22
Toltaltl antall funn	24	26	11	22	13	6
"Logic Solver" funn	8	10	1	0	1	4
Sensor/Final element funn	16	16	10	22	12	2

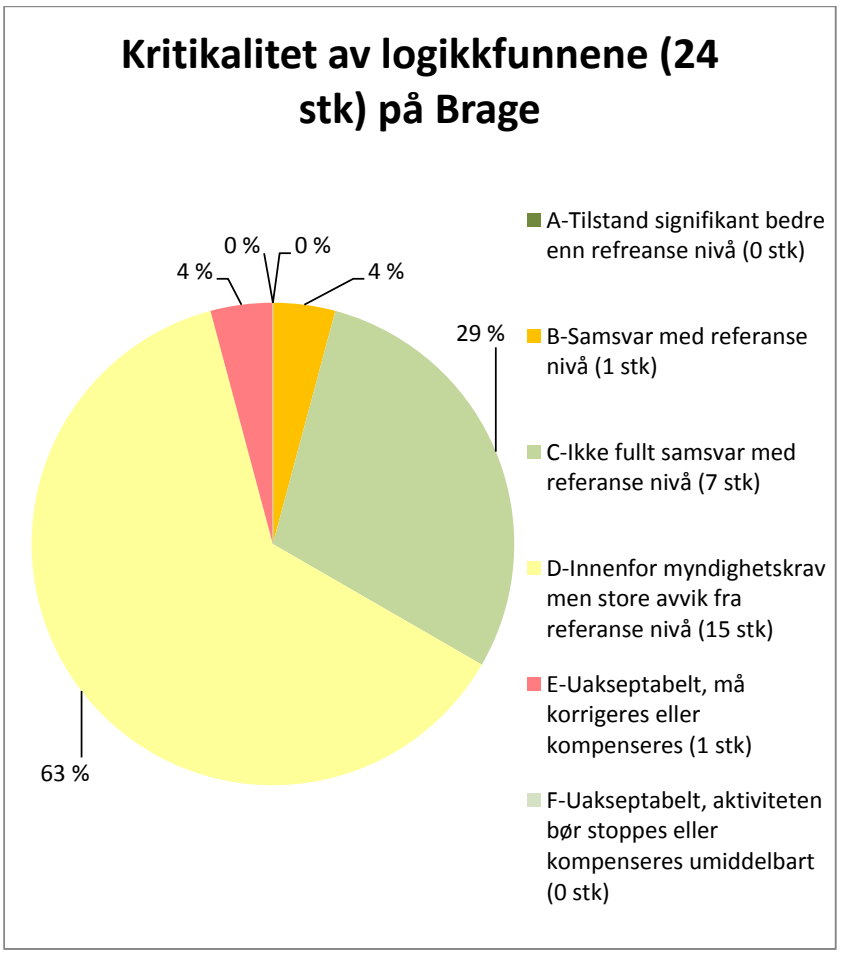
Figur 7-3 Fordeling av funn innenfor de ulike ytelsesstandardene

For Brage er det identifisert til sammen 103 ulike funn. Av disse funnene kan 24 stykker relateres til logikkelementet. Dette vil si at 23 % av alle funn i de relevante PSene er knyttet til logikk.

Ved vurdering av funntekst kan man se at det er mange felles funn på tvers av installasjonene. De fleste funn er mangler i design, og tiltak kan gjennomføres med eksisterende teknologi. For eksempel er det manglende funksjoner for å fjerne alle blokkeringer i NAS, PAS og B&G systemene. NAS-systemene mangler uavhengig funksjon for å isolere utganger til sikker tilstand uavhengig av logikk, utganger fra B&G er ikke designet failsafe[3] og mangler tilstrekkelig diagnose, og det mangler funksjonalitet for testing i drift. Det er også mangler i strømforsyningen til systemene.

Andre funn er relatert til systemteknologien og kan ikke utbedres uten at hele eller deler av systemet skiftes ut. For eksempel mangler man dokumentasjon for ytelsen av logikk, engineering verktøyene mangler funksjonalitet, logikk har ikke nødvendig tilgangskontroll, I/O kortene har ikke tilstrekkelig diagnose, HMI mangler alarmprioriteter og alarm skjuling.

[3] Engelsk, sikker tilstand ved feil



Figur 7-4 Kritikalitetsvurdering av logikkfunn

Alle funn blir vurdert i forhold til kritikalitet og veid opp mot et referansenivå som tilsvarer dagens krav til nye installasjoner. Gradene av kritikalitet er rangert fra A-F. Av de 24 funnene som tilhørte logikk er størstedelen klassifisert som (D) innenfor myndighetskrav, men store avvik fra referanse nivå som illustrert i figur 7-4. Kritikalitetsvurderingene av logikkfunn vurderes ulikt på de enkelte installasjonene. Njord har 17 funn innen logikkkategorien som er rangert som uakseptable i forhold til drift av plattformen. På Brage er ikke noen av funnene definerte som uakseptable.

Basert på TTS-metodikken og de funnene som har blitt identifisert, er det dokumentert et forholdsvis stort avvik mellom tilstand og ønsket referansenivå. Flere av funnene som er beskrevet peker på mangler i designet til sikkerhetssystemene.

Siden disse systemene ble designet og installert i løpet av nittiårene har det kommet nye forskrifter og standarder som er viktige for dagens design og realisering av SIS. Petroleumstilsynets Innretningsforskrift sier at IEC61508/11 og OLF070 bør benyttes. Disse standardene har hatt stor påvirkning for dagens systemer, som i stor grad dokumenterer samsvar i henhold til standardene. Programvareutvikling og sammenstilling av applikasjoner følger en systematisk metode beskrevet i standardene for å unngå feil i programvare.

Nytt regelverk har også resultert i et større skille mellom prosesskontrollsystemene og sikkerhetssystemene. Sikkerhetssystemene benytter i dag hardware og programvare som er utviklet og i samsvar med IEC61508/11. Teleperm M- systemene er i utgangspunkt laget for prosesskontroll og ikke utviklet som et sikkerhetssystem. Systemet mangler derfor flere sikkerhetsmekanismer og diagnosefunksjonalitet som skal oppdage feil og aksjonere.

Dagens sikkerhetssystemer har blitt mer komplekse, dette kan i seg selv øke faren for feil i systemene. De ulike elementene i SAS systemer har blitt mer sammenkoblet og man tar stadig i bruk ulike sikkerhetsbusser for å kommunisere signaler istedenfor tradisjonell hardware kobling. Bruk av busskommunikasjon, utvidet diagnose og sammenkoblingen i systemene stiller større krav til personellet som skal vedlikeholde og modifisere systemene.

Funksjonelle krav til systemene er også en del av kontinuerlig forbedring. Dette gjelder både krav i Ptil forskriftene, men også egne selskapsinterne krav som stadig forbedres og skal utgjøre beste praksis basert på erfaring. Dette gjelder for eksempel nye krav til redundante løsninger.

Teknisk gap kan resultere i ulike konsekvenser som hyppigere feil i systemet, feiloperering og utvidet vedlikehold. Brage er i en søknadsprosess om levetidsforlengelse. I forbindelse med levetidsforlengelse beskriver OLF122 at systemenes gap mot innretningsforskrift skal identifiseres. Dersom gapet vurderes til å være for stort, kan dette resultere i at levetidssøknaden ikke godkjennes av myndigheten.

7.2.2 Usikkerheter i TTS-dataene

TTS funnene er hentet fra TST-databasen i Statoil. Resultatet av verifikasjonen er kvalitetssikret av TTS-verifikasjonsteam. Deretter har alle funnene blitt gjennomgått av en egen ekspertgruppe som har vurdert alle funnene med hensyn til funntekst og kategorisering.

Man ser i stor grad at funnene er gjengangere på tvers av installasjonene. Når det gjelder funn relaterte til Teleperm M-teknologien så er alle funn felles for alle seks installasjonene. Dette gjelder funn både på design og på tilstand.

Ulikhetene mellom antall funn som kan relateres til logikk for Oseberg plattformene og de andre installasjonene er stor. Dette kan ha med bakgrunnskompetansen til verifikatøren. En verifikatør som har ansvar for PS3,4,6,7,12 skal dekke alle sjekkpunkter knyttet mot PSene. De fleste sjekkpunktene er mot sensor- og aktuatorelementet, mens logikkenheten kanskje er litt spesiell.

Generelt er det nok også hovedfokus på sensor og aktuator i sjekklistene for PS3,4,6,7,12. Det er normalt sensor- og aktuatorelementet som bidrar mest til farlige feil i pålitelighetsberegninger.

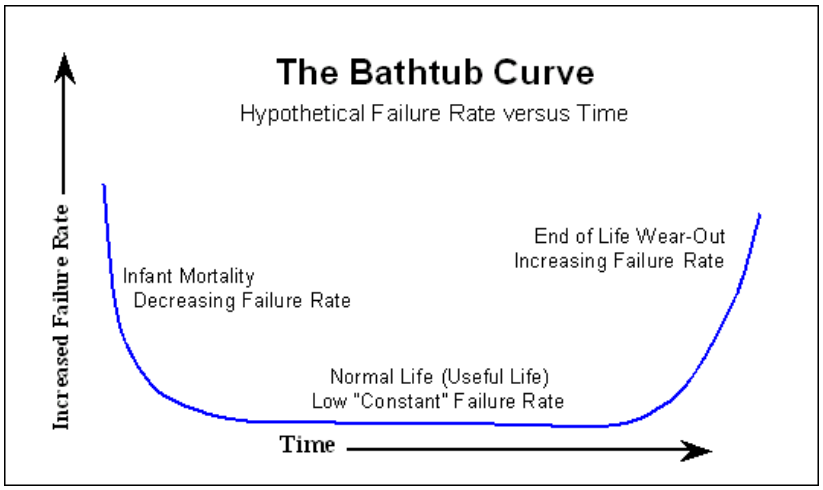
7.3 Analyser av feilrater

For å analysere feilrater til TPM systemene er bakgrunnsdata hentet ut fra følgende applikasjoner:

- Synergi (rapportering av uønskede hendelser)
- SAP(rapportering av feil og oversikt over reservedelsuttak)

Systemene er bygget opp av mange ulike komponenter. De fleste inneholder elektronikk og programvare. Faktorer som kan påvirkere degradering kan være kompleksitet og hvordan komponenten er bygget opp, miljøfaktorer som komponenten blir utsatt for under drift og hvordan komponentene vedlikeholdes. Det finnes anerkjente kilder (MIL) som beskriver ulike faktorer som kan påvirke feilrater til elektroniske komponenter.

En vanlig utvikling av feilrater over tid gir den typiske badekarkurven. Denne kjennetegnes ved avtagende feilrate i starten som følge av innkjøringsfeil. Den sterke økningen på slutten av tidsperioden indikerer at systemet er på vei inn i «wear out»-perioden. Dette betyr at komponentene påvirkers av aldring og er i ferd med å overstige sin konstruerte levetid.



Figur 7-5 Feilrate og Badekarskurve

Normal perioden i figur 7-5 viser en tilnærmet konstant feilrate. Dette er en vanlig antakelse innenfor pålitelighetsvurderinger av elektronisk komponenter og instrumenterte sikkerhetssystem, som følge av eksponentiell fordeling (denne distribusjonen er uten hukommelse).

Analysen av erfarte feildata vil være med på å avdekke om antakelsen om konstant feilrate er gjeldende for TPM systemene eller om systemene er i ferd med å nærme seg en fase hvor slitasje og alder påvirker feilraten. Økende feilrater kan ha store konsekvenser på systemenes ytelse. Systemene og de ulike sikkerhetsfunksjonene kan svikte når man har behov for dem. I tillegg vil økende feilrate påvirke tilgjengeligheten til systemene.

For å innhente tilstrekkelig datagrunnlag til å kunne vurdere utvikling av feilrater i sikkerhetssystemene er analysene baserte på data fra år 2000 til og med år 2011.

7.4 Rapportering av uønskede hendelser i Synergi

Synergi et er et IT-verktøy som Statoil benytter for å rapportere ulike typer hendelser. Både hendelser som har resultert i tap av sikkerhetsfunksjon og/eller tapt produksjon og hendelser som har potensiale for tap av sikkerhetsfunksjoner eller økonomisk tap.

Ved utvalgssøk i Synergidatabasen er alle hendelser registrert mot de samme ytelsesstandardene som er vurdert ved analyse av TTS-data. Dette er følgende PS'er:

- PS 3 (Gassdeteksjon)
- PS4 (Nødavstegning)
- PS6 (Tennkildekontroll)
- PS7 (Branndeteksjon)
- PS12 (Prosesssikring)
- PS22 (Menneske/maskin-grensesnitt og alarmsystem)

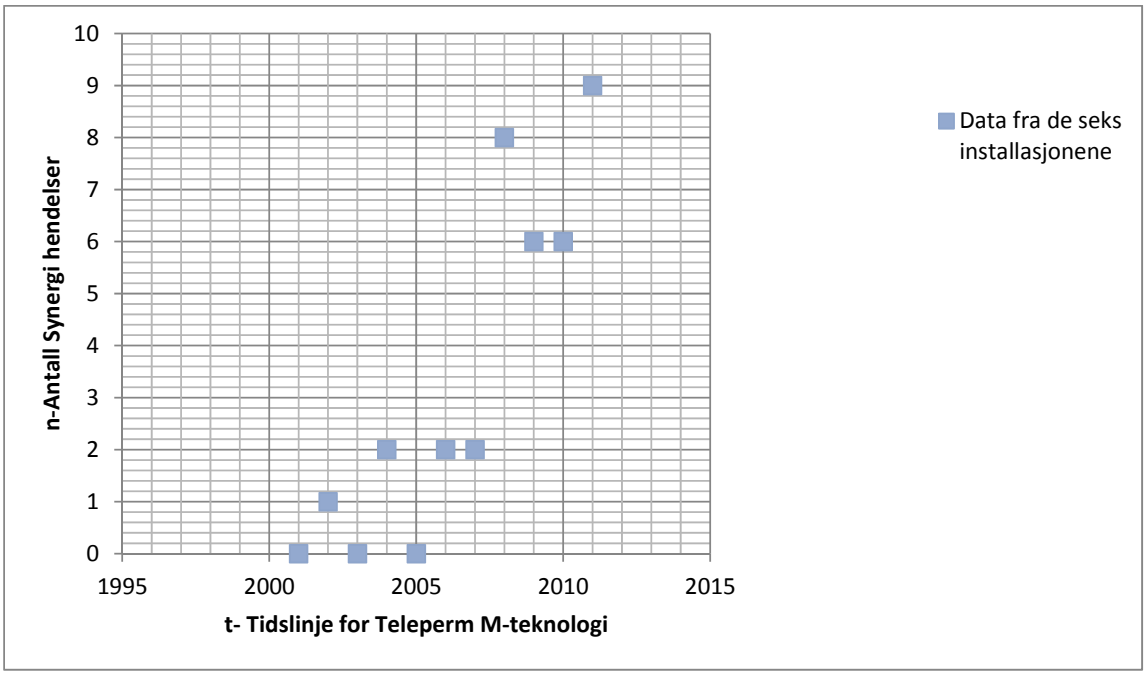
Synergidata er tilgjengelig for alle installasjoner i valgt tidsperiode. For detaljer rundt de ulike hendelsene er alle data tilgjengelige i vedlegg E.

7.4.1 Synergihendelser relatert til logikk

I løpet av perioden har det vært registrert ca. 2000 hendelser knyttet mot de aktuelle ytelsesstandardene på de seks ulike installasjonene. Blant disse er 36 hendelser relatert til DISCOS-systemene til de ulike plattformene. Tabell 7-2 viser tidsperiode og fordeling av hendelsene blant de ulike installasjonene.

TrollC		**Brage**		**Visund**		**Njord**		**OSØ**		**OSS**		**Sum**
År	Hendelser	År	Hendelser	År	Hendelser	År	Hendelser	År	Hendelser	År	Hendelser	
2000	0	2000	0	2000	0	2000	0	2000	0	2000	0	**0**
2001	0	2001	0	2001	0	2001	0	2001	0	2001	0	**0**
2002	0	2002	0	2002	0	2002	0	2002	0	2002	1	**1**
2003	0	2003	0	2003	0	2003	0	2003	0	2003	0	**0**
2004	0	2004	0	2004	0	2004	1	2004	0	2004	1	**2**
2005	0	2005	0	2005	0	2005	0	2005	0	2005	0	**0**
2006	0	2006	1	2006	0	2006	1	2006	0	2006	0	**2**
2007	2	2007	0	2007	0	2007	0	2007	0	2007	0	**2**
2008	0	2008	4	2008	1	2008	1	2008	1	2008	1	**8**
2009	4	2009	0	2009	1	2009	0	2009	1	2009	0	**6**
2010	2	2010	0	2010	3	2010	1	2010	0	2010	0	**6**
2011	4	2011	2	2011	3	2011	0	2011	0	2011	0	**9**

Tabell 7-2 Hendelser på de ulike installasjonene i perioden



Figur 7-6 Hendelser relatert til Teleperm M-systemene (prosesskontroll og sikkerhetssystem)

7.4.2 Resultat av gjennomgangen

Hendelsene er tilnærmet likt fordelt mellom økonomisk tap/tapspotensiale og tap/potensiale for tap av sikkerhetsfunksjon. Troll C skiller seg litt ut med flere antall hendelser relatert til Teleperm M-teknologien. Dette bekreftes i samtaler med teknisk systemansvarlig for systemene. Antall hendelser er sterkt stigende når man ser alle installasjonene i sammenheng de siste årene. Denne trenden er gjeldene også når man ser på de fleste enkelte installasjoner hver for seg.

7.4.3 Usikkerheter til datagrunnlag

Den største stigningen i antall hendelser inntreffer i 2008. Dette er året etter sammenslåingen av Statoil og Hydros olje og gassdivisjon. Samtaler med teknisk systemansvarlige for installasjonene peker på at det kan ha blitt økt fokus på rapportering etter sammenslåingen med Statoil.

Etter hvert som systemene blir eldre og ny teknologi blir tilgjengelig og tatt i bruk på andre installasjoner kan driftspersonell være mer fokusert på å dokumentere dårlige sider av systemene og potensialet for feil hendelser.

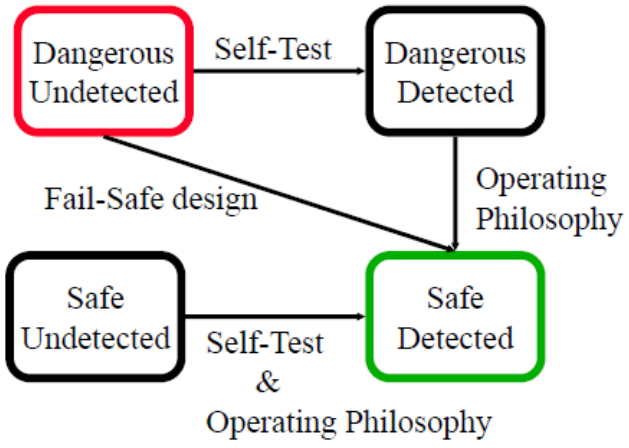
7.5 Rapportering av feil i SAP

Alle installasjoner rapporterer feil i sikkerhetssystemene inn i SAP via M2-notifikasjoner. Sikkerhetskritiske feil rapporteres inn med en spesiell kode som gjør at de hentes inn i en egen rapport kalt A10. A10 rapportene inneholder kun de farlige udetekterbare feilene som oppdages under funksjonstesting av sikkerhetsfunksjonene. Feiltoleranse for de ulike funksjonene er definert i et eget dokument (GL0114). Denne definerer antall årlige tillatte feil per antall utførte tester for de ulike barrierene, og ligger typisk mellom 0,5-1 %. Alle feil som oppdages må knyttes mot en tag, typisk feltutstyret/komponenten som testes, altså detektor, ventil, etc. Siden feilen knyttes opp mot feltutstyret er det vanskelig å finne logikkfeil i rapportene. Informasjon om type feil må identifiseres gjennom beskrivelsen i notifikasjonen.

M2-notifikasjonene inneholder alle typer feil som identifiseres under normal drift og vedlikehold. Alle M2-notifikasjoner i perioden fra 2000-2011 er derfor tatt ut fra SAP og gjennomgått. Å finne igjen denne informasjon i SAP er krevende, siden Hydro benyttet en annen versjon av SAP (P01), mens alle feil etter sammenslåingen er rapportert inn i Statoils versjon av SAP (P03).

Man skiller (IEC61511) mellom ulike typer feil i sikkerhetssystemene som vist i figur 7-7. De typer feil som klassifiseres som farlig og udetekterbare vil kunne resultere i tap av sikkerhetsfunksjon siden de ikke oppdages før man trenger funksjonen eller at man oppdager feilen under funksjonstest. For å unngå for høy andel av disse feilene er systemene designet med diagnostikk for å oppdage feil, i tillegg designes systemet «failsafe» slik at funksjonen går i sikker tilstand ved feil.

Detekterbare feil og reparasjonstid vil kunne resultere i utilgjengelige sikkerhetssystem som følge av «failsafe» design eller som etter en operativ vurdering og handling. Når barrieren ikke er å tilstede må kompenserende tiltak kunne iverksettes for å kunne opprettholde normal drift.



Figur 7-7 Ulike typer feilmodi (IEC61508/11)

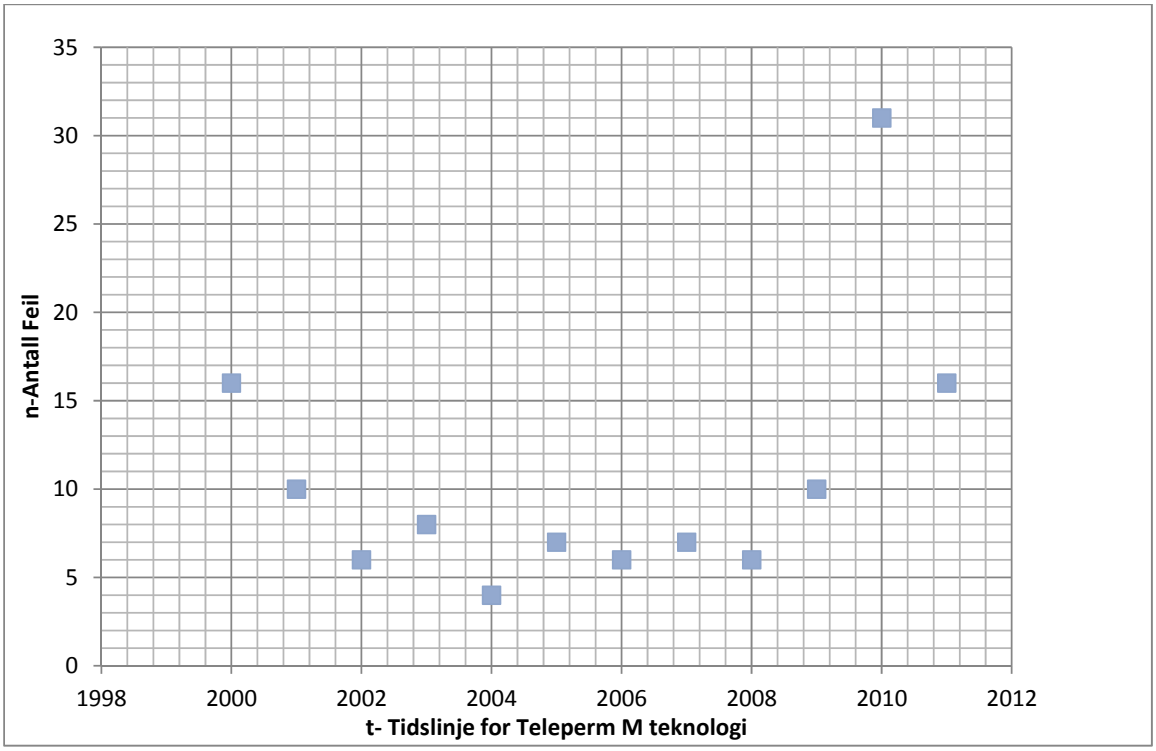
Alle feildata hentet fra SAP er tilgjengelig i vedlegg F.

7.5.1 Resultat av gjennomgangen

I perioden 2000-2011 har det blitt skrevet totalt 195.443 M2-notifikasjoner. For å identifisere hvilke M2er som kan relateres til Teleperm M-systemene har en utvalgsspørring filtrert ut alle notifikasjoner som inneholder et av følgende kriterieord i beskrivelsen: *DISCOS, SW, Node, I/O.* Dette reduserte antall notifikasjoner til 1037. Blant disse er alle M2er som kan relateres til Teleperm M-systemet filtrert ut ved manuell gjennomgang. Resultatet og fordelingen av M2er blant installasjonene og tidsperiode er beskrevet i tabell 7-3.

År	Akkumulert	Brage	Njord A	TrollC	OsebergS	OsebergØ	Visund
2000	16	2	3	3	7	1	
2001	10	1	4	2	3		
2002	6	3			2		1
2003	8			5	2	1	
2004	4			2	1		1
2005	7	3		2	1		1
2006	6		1	1	1	1	2
2007	7	1		2	1	2	1
2008	6	2		1	1	2	
2009	10	1	2	6			1
2010	31	21		3	2	5	
2011	16	4		4	5		3
Sum	**127**	**38**	**10**	**31**	**26**	**12**	**10**

Tabell 7-3 Antall M2 notifikasjoner relatert til DISCOS fordelt på de ulike installasjonene



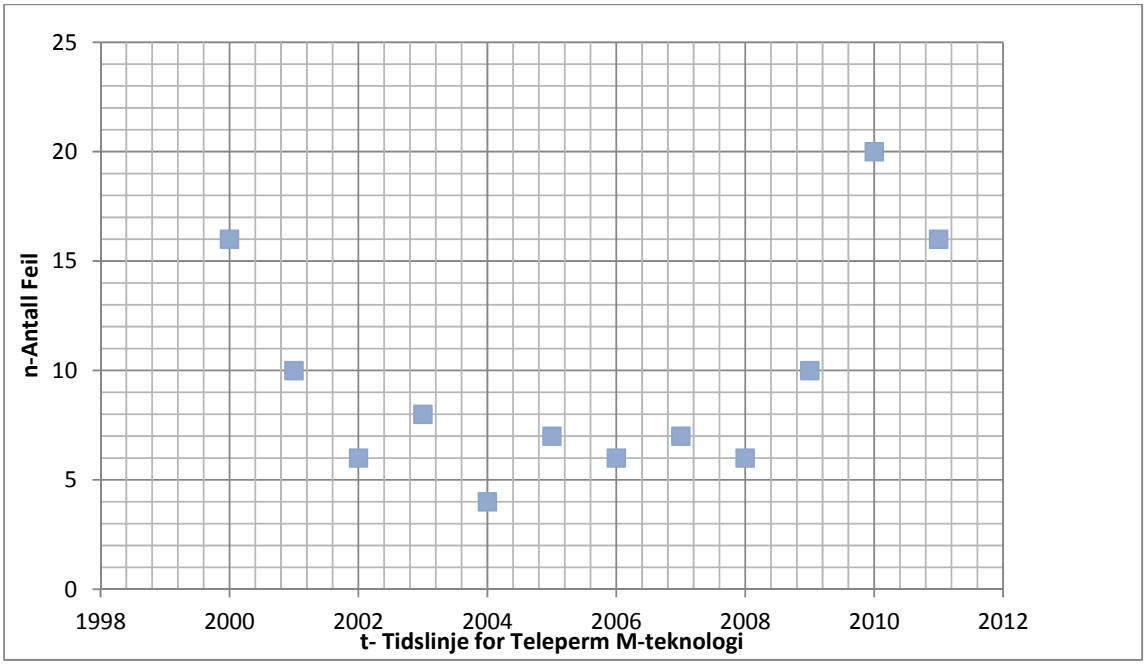
Figur 7-8 Feilregistreringer i SAP (M2) for perioden 2000-2011

Ved å akkumulere feil for alle installasjonene i et felles diagram kan vil man kunne se at feilraten er fallende fra år 2000, konstant mellom år 2002-2008. Fra år 2008 er den stigende.

7.5.2 Usikkerhet til datagrunnlag

Etter at søket i SAP er begrenset til antall M2er i henhold til søkekriteriet var det litt over tusen rapporter. Deretter er det utført manuell utvelgelse av rapporter som kvalifiserer til logikk feil. For eksempel er notifikasjoner som omhandler jordfeil som er detektert i systemet utelatt. Jordfeil antas å ha sin årsak fra feltinstrumentet/kabel.

År 2010 utpeker seg som et år med veldig mange M2er mot Teleperm-M på Brage. Det kan indikere at det ble ut ført mange jobber/kampanje mot ulike noder som lå inne med svikt. Ved å se bort fra denne type notifikasjoner vil total antall feil i år 2010 gå ned fra 31 til 20.



Figur 7-9 Følsomhetsvurdering ved korrigering av år 2010 og data fra Brage

7.6 Reservedelsuttak i SAP for DISCOS komponenter

Utstyr som har høy kritikalitet i forhold til operativ drift lagerføres i Statoil for raskt å kunne erstatte komponenter som feiler. DISCOS komponenter er kjøpt inn fra systemleverandør og plassert på lager i Statoil. Utstyret er plassert på både felles onshore-lager og egne offshore-lager for hver installasjon.

Ved gjennomgang av reservedelsuttak i SAP er det viktig at det er kun utstyr tatt ut fra lager på grunn av komponentsvikt som vurderes. Dette utføres ved å kun ta med arbeidsordre offshore som ikke er knyttet mot et nettverk eller en WBS, fordi dette er arbeidsordrer som er genererte i forbindelse med prosjekt eller modifikasjoner. Følgende typer arbeidsordre finnes i SAP og er relevante som uttak av reservedeler.

SAP kode 101-Arbeidsordre som har hentet utstyr direkte fra leverandør (ikke lagerført)
SAP kode 261-Arbeidsordre som har tatt ut utstyr fra offshore-lager
SAP kode 641- Arbeidsordre som har tatt ut utstyr fra onshore-lager

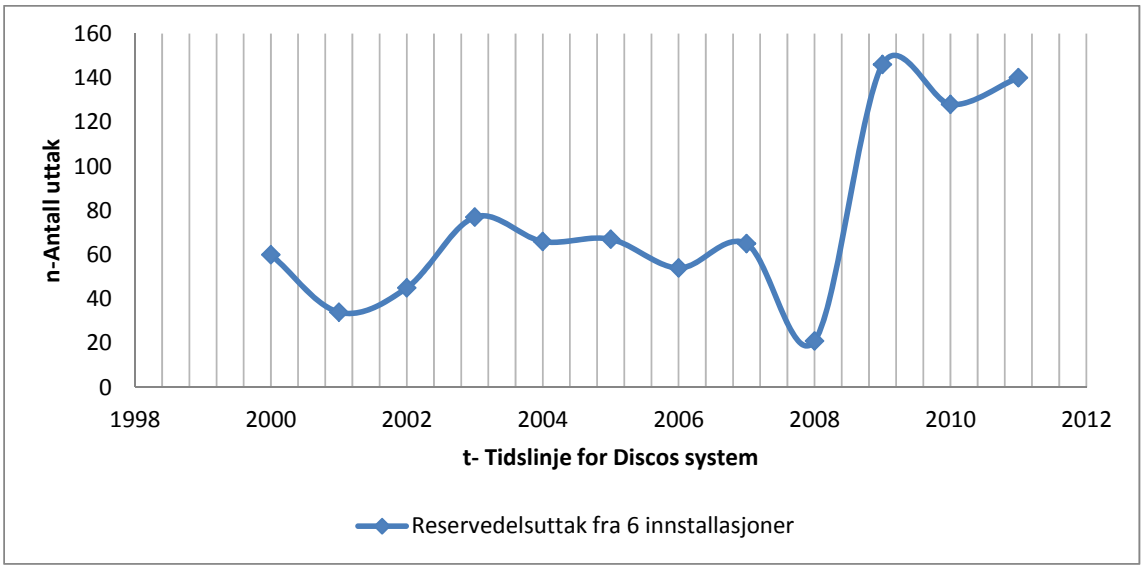
Oversikt av de ulike komponenter og uttak er tilgjengelige i vedlegg G.

7.6.1 Resultat av gjennomgangen

Tabell 7-4 gir en oversikt over antall reservedeler som er tatt ut av lager i perioden 2000-2011.

År	Antall Uttak
2000	60
2001	34
2002	45
2003	77
2004	66
2005	67
2006	54
2007	65
2008	21
2009	146
2010	128
2011	140

Tabell 7-4 Reservedelsforbruk offshore



Figur 7-10 Antall uttak av DISCOS-komponenter i perioden 2000-2011

Ut fra kurven kan man se at uttak er tilnærmet konstant frem til 2008 og deretter stigende. Uttaket av reservedeler støtter opp om fordelingen av antall M2-feil i figur 7-8.

7.6.2 Usikkerhet til datagrunnlag

Det finnes en del lagervarer på installasjonene som ikke er lagerførte i SAP. Dette er såkalte «ekornlagre» som består av restutstyr fra diverse modifikasjonsprosjekter som hatt reservedeler under ferdigstillelse av et prosjekt, og som enkelte ganger blir liggende uregistrert på installasjonen. Dette er utstyr som igjen benyttes i ulike arbeidsordre.

7.7 Anvendelse av driftsdata til pålitelighetsanalyse

Systemene og de ulike sikkerhetsfunksjonene er introdusert i designfasen som et risikoreduserende tiltak. De ulike typer feilmodi som kan inntreffe i selve systemet er gjennomgått under opprinnelig design og er ikke en del av denne vurderingen.

Man kan benytte statiske metoder for å forutse fremtidig feilrate som følge av aldring av sikkerhetssystemene. Metoden baseres på pålitelighetsmodellering. Figur 7-11 illustrerer hvordan feil i systemet resulterer i enten farlige udetekterbare feil eller utilgjengelig sikkerhetssystem.

Figur 7-11 Feil og mangler i DISCOS

Man har lang erfaring med systemene i drift og man har kjennskap til ulike typer feil og frekvens. Det som er av størst interesse i denne forbindelse er økende feilrate som følge av aldring av systemet.

7.7.1 MTTF vurdering (antatt konstant feilrate)

Datagrunnlag fra SAP i perioden 2001-2011 inkluderer alle registrerte feil i DISCOS systemene, se tabell 7-3. Det antas at totalt datagrunnlaget er representativt siden PCS og SIS er av samme hardware teknologi. Totalt antall noder er 173 stykk hvor 64 er SIS noder (NAS, PAS, F&G). Datagrunnlag er vedlagt i vedlegg F.

Man kan beregne MTTF for DISCOS system og for alle de seks ulike installasjonene:

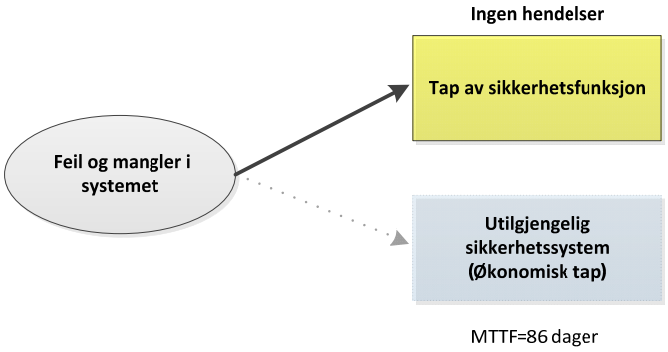
$$MTTF_{DISCOS=}\frac{1}{\lambda} = \frac{1}{\frac{127}{12 * 365}} = 35\ dager$$

$MTTF_{SIS=}$ 86 dager

7.7.2 Farlige udetekterbare feil

Siden 2000 har det blitt registrert 46 ulike hendelser i Synergi. Ved gjennomgang av hendelsene er det ikke funnet hendelser som har resultert i tap av sikkerhetsfunksjon. Feildata fra SAP og M2 notifikasjoner indikerer heller ikke uoppdagede farlige feil. Dette

indikerer at det ikke har vært registrert uoppdagede farlige feil (λ_{DU}) i DISCOS systemene i løpet av operasjonstiden. Uoppdagede farlige feil oppdages gjennom funksjonstest eller ved et reelt behov for funksjonen.



Figur 7-12 Type feilhendelser basert på erfaringsdata

7.7.3 Modell for feilrate

For å vurdere levetiden til sikkerhetssystemet kan man ta utgangspunkt i overlevelsesfunksjonen R(t). T er levetid og en storkastisk variabel med en tenkt kumulativ sannsynlighetsfordeling F(t).

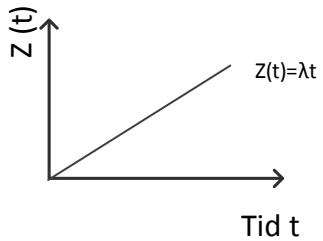
$F(t) = P(T \leq t)$
$R(t) = P(T > t) = 1 - F(t)$

Komponenter som inngår i sikkerhetssystemet består i veldig stor grad av ulike elektroniske komponenter. Man antar at disse komponentene har eksponentiell fordeling gitt ved:
$F(t) = 1 - e^{-\lambda t} \quad t \geq 0$
$R(T) = e^{-\lambda t}$

$f(t) = F`(t)$
$ET = \int_{-\infty}^{\infty} tf(f)dt$
$ET = \frac{1}{\lambda} \quad Forventet\ levetid\ er\ omvendt\ proporsjonal\ med\ \lambda$

Den eksponentielle fordeling har en spesiell egenskap i forbindelse med levetid, den er uten minne. Dette betyr at hvis en komponent lever ved en gitt tid, er sannsynligheten for at den lever videre det samme som da komponenten var ny, det vil si at der ikke er noen aldring. Dette er en forenkling som ikke nødvendigvis er realistisk i alle situasjoner.

For å utrykke egenskaper knyttet til aldring kan man benytte «hazardrate» som er definert ved:
$h(t) = \frac{f(t)}{1-F(t)}$
For eksponentiell fordeling blir $h(t) = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$

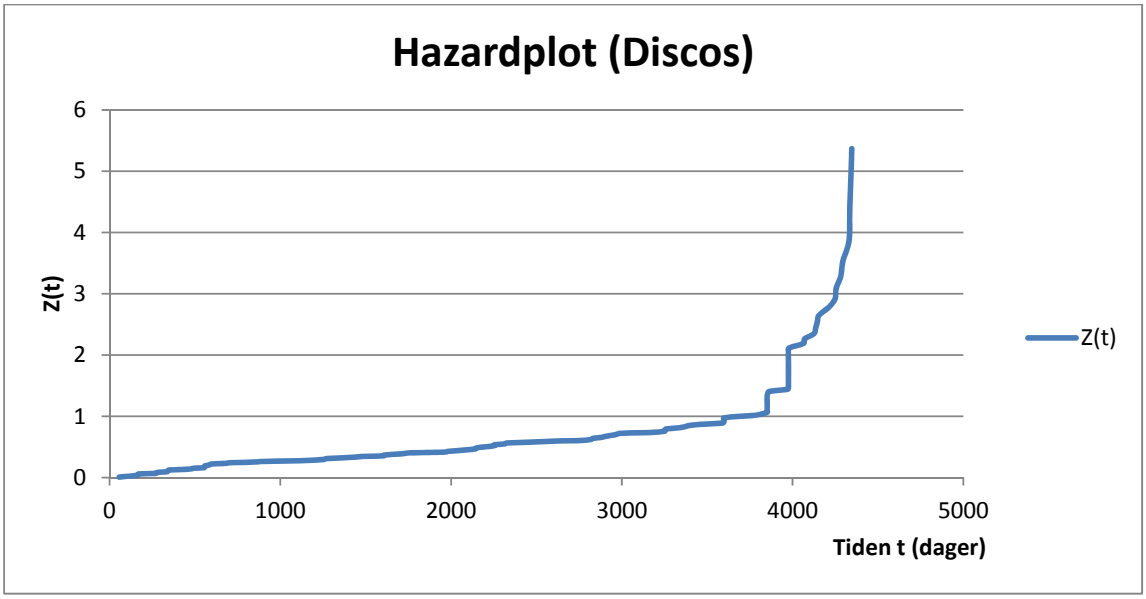


Figur 7-13 Hazardplot ved eksponentiell fordeling

Hazardplot i figur 7-13 viser den kumulative feilraten ved eksponentiell fordeling. Man kan se at kurven er lineær noe som betyr at feilraten er konstant.

7.7.4 Vurdering av feilfordeling

Det kan se ut som om antakelsen om eksponentiell fordeling ikke er tilfellet basert på tabell 7-6. Hazardplotting er en metode som gir mulighet for å avsløre levetidsfordelinger. Ved å analysere feildata fra perioden 2000-2011 kan man etablere et hazardplott basert på registrerte feil og tidspunktet feilen oppstod.



Figur 7-14 Hazardplot DISCOS

Hazardplottet i figur 7-14 er tilnærmet lineært frem til cirka 3000 dager som er frem til år 2008 (cirka 3000 d). Dette samsvar med forventet eksponentiell fordeling. Etter 3000 dager går kurven over til en konveks form som er typisk for en IFR[4] fordeling. Dette betyr at feilraten ikke er konstant etter 2008, men stigende.

Kurveformen fra 3000 dager kan passe bedre til en Weibull fordeling. Weibull fordeling blir ofte benyttet på samme måte som eksponentialfordelinger til å anslå pålitelighet til komponenter eller systemer som består av mange komponenter satt sammen. Forventet levetid i en Weibull fordeling er:

$$ET = MTTF = \int_0^\infty R(t)dt = \frac{1}{\lambda}\Gamma(1+\frac{1}{\beta})$$

Det er mulig å estimere parameterne β (form) og λ (skala) ut fra erfarte data og hazardplott. IFR kurve betyr at β>1. Det er mulig å estimere parameterne grafisk ved å ta logaritmen til både tiden og Z(t).

[4] Increasing failure rate

7.7.5 Usikkerheter til pålitelighetsanalysen

Funksjonaliteten til disse system avhenger av mange enkeltkomponenter og hvordan de er sammensatt. Sikkerhetssystemene består for det meste av seriekoblete komponenter og fungerer hvis og bare hvis-alle komponentene fungerer. Man må også anta at de ulike komponentene feiler uavhengig av hverandre. Det som gjelder for komponenter behøver ikke nødvendigvis gjelde for systemet.

Det er usikkerhet rundt valg av modell. Modellen er en forenkling av analyseobjektet for å kunne anvende analytiske metoder.

Når man benytter erfarte feil gjennom M2-notifikasjoner forutsetter man at de innsamlede dataene som benyttes er fra et representativt utvalg for å kunne beskrive sikkerhetssystemene.

7.7.6 Følsomhetsanalyse

Følsomhet er et mål på hvordan resultatet påvirkes dersom vi endrer på de ulike parameterne. Ved en Weibull fordeling kan man beregne forventet MTTF med ulik parameter verdier (λ, β).

7.8 MTO-analyse

Faktorer som påvirker ytelsen til sikkerhetssystemene kan utenom tekniske faktorer også være samspill mellom organisasjon, mennesker og teknologi. Systemene består i stor del av ulik type programvare som er nødvendig for at systemene skal fungere. Denne programvaren modifiseres nærmest kontinuerlig i forbindelse med ulike prosjekter som utføres. Dette krever kompetanse, metoder og prosedyre for å håndtere slike modifikasjoner på riktig måte.

Systemene inkluderer i tillegg menneske maskin grensesnitt (MMI) dette er grensesnittet mellom systemstatus og operatørene. Mange alarmer, menneskelige aksjoner og prosedyrer er knyttet til dette grensesnittet.

I tillegg er en forutsetning for integriteten til systemene at riktig vedlikehold utføres og at systemene testes etter gitte prosedyrer og intervaller. Ved feil i sikkerhetssystemene enten ved komponentsvikt eller andre type feilmodi vil systemene være avhengig av personell som kan identifisere årsaken og reparere systemet.

7.8.1 Kompetanse innen Teleperm M-teknologi

Det er en rekke ulike interne og eksterne organisasjoner involvert i ulike faser av livssyklusen til sikkerhetssystemene. Disse må ha tilstrekkelig kompetanse for å unngå blant annet feil bruk, og håndtering av komponenter, modifisere systemet, overvåke tilstanden og opererer systemet.

Personell som kan håndtere Teleperm M-teknologien aldres også og forsvinner ut av arbeidslivet eller over i andre oppgaver. Statoil utfører ofte omorganisering av både blant offshore og onshore personell noe som kan føre til at systemkompetanse forsvinner uten god erfaringsoverføring.

Statoil har også en egen organisasjon (FFO) som håndterer mindre endringer i systemene denne gruppen arbeider på tvers av alle Teleperm M-installasjonene og består av 2-3 personer. Det er allikevel Siemens som er hovedaktør og som utfører de fleste endringer i systemene. Underlag for endringer utarbeides av engineeringseselskap som for eksempel Aker og Aibel. Siemens har total 10-15 personer i Norge som har Teleperm M-kompetanse. Personellet sitter i Bergensavdelingen og arbeider mot Statoils anlegg.

Den største bekymringen er likevel ikke å finne applikasjons kompetanse, det vil si personell til å utføre endringer i applikasjonene, men system spesialister som kan løse mer komplekse utfordringer som kan oppstå i systemene. Support kanalene inn mot utviklingsmiljøet i Tyskland benyttes flere ganger i løpet av et driftsår.

Konsekvensene av manglende kompetanse kan resultere i feiltilstander i systemet, for eksempel introduksjon av programvare feil, manglende vedlikehold og man kan være dårlig rustet til å håndtere mer alvorlige systemfeil som oppstår.

Utenfor Norge finnes det flere selskaper utenom Siemens som har Teleperm-M kompetanse. Dette er selskaper som fungerer som systemintegratorer og engineeringselskaper med Teleperm-M kompetanse. Eksempler på selskaper som kan supportere Teleperm-M teknologi er for eksempel AT-plan og AkoTec i Tyskland.

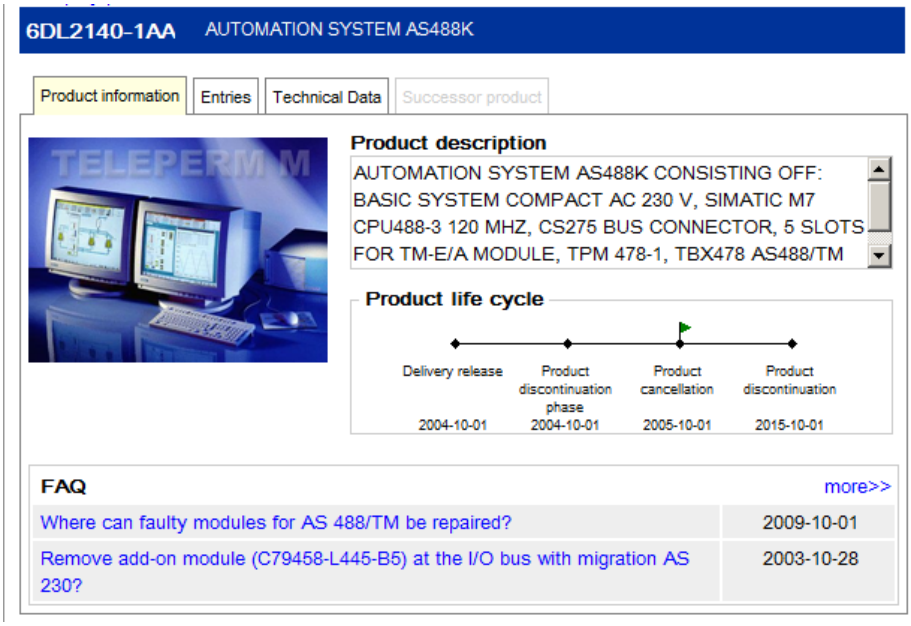
7.8.2 Support av Teleperm M teknologi

DISCOS systemet består av mange ulike komponenter. I forbindelse med reservedelsoversikt og forbruk er det identifisert over 300 ulike komponenter som inngår i DISCOS systemene. De fleste komponentene er levert av Siemens og er en del av Teleperm M-teknologien. I tillegg til lokal Siemens støtte i Norge benyttes også spesialiststøtte fra Siemens Tyskland. Etter samtaler med personell i Statoil nevnes at kanalene inn mot Tyskland benyttes jevnlig.

Teleperm M-teknologi er levert i stor utstrekning frem til slutten av 90-tallet. Globalt er det levert ca 15-20.000 anlegg (Wikipedia). Fra 2005 ble Teleperm M-teknologien som produkt faset ut av Siemens. Etter 2005 har Siemens forpliktet seg til å supportere utstyr og kompetanse i 10 år. Dette medfører at de fleste DISCOS komponenter ikke lengre supporteres etter 2015.

I praksis vil dette bety at kunder ikke lengre kan forvente å få levert eller reparert Teleperm komponenter hos Siemens. Spesialiststøtten i utviklingsmiljøet vil også oppheve. Statoil har utfordret systemleverandør til å forlenge supportavtalen til 2020, men leverandør har gitt tilbakemelding om at en slik forpliktelse ikke vil kunne gis. Det er mulig at leveranser av enkelte komponenter kan forlenges til 2016.

I og med at denne teknologien er levert til ulik industri globalt har det etablert seg et marked for omsetning av Teleperm M-komponenter. Dette er mindre selskaper som for eksempel (Classic Automation) som har spesialisert seg innenfor dette segmentet og tilbyr salg og reparasjon av Teleperm M-komponenter.



Figur 7-15 Typisk levetid for Teleperm M-komponenter (Siemens)

7.8.3 Human Factors

Som beskrevet i kapitel 3.1.3 stilles det krav til menneske-maskin-grensesnitt og informasjonspresentasjon. Statoil gjenspeiler disse kravene i et eget TR dokument[5].

«Humans factors» i denne sammenhengen handler om menneskelig feilhandlinger og om grensesnittet mellom menneskene og sikkerhetssystemene. Det utføres ofte HF-analyser ved design av nye kontrollrom og utvikling av skjermbilder og alarmsystem.

Eksisterende MMI på installasjonene har i ulik grad et gap mot gjeldende krav. Dette avviket skal identifiseres gjennom TTS metodikken og PS22[6].

[5] TR0926 Working Environment
[6] Performance Standard 22: Human Machine Interface & Alarm Management

7.9 Reservekapasitet i sikkerhetssystemene

I forbindelse med modifikasjonsprosjekt er det ofte behov for å utvide eksisterende sikkerhetssystemer. Systemene har begrensninger for hvor masse det er mulig å utvide eksisterende løsninger. Typiske prosjekter som initierer utvidelsesbehov er innfasing av nye subsea brønner, nye kompressormoduler, større prosessendringer i forbindelse med IOR prosjekt. Konsekvensene av manglende reservekapasitet kan resultere i at eksisterende system ikke har nødvendig kapasitet til å møte fremtidige prosjekter. I tillegg vil høy busslast kunne resultere i at viktige alarmer ikke kommer frem til operatør i kontrollrom ved en hendelse.

Når man vurderer reservekapasitet til systemene kan man dele systemets kapasitetsbehov inn i ulike elementer som:

1. I/O kapasitet
2. CPU kapasitet (minne, syklustid)
3. Buss kapasitet mellom noder og HMI

7.9.1 I/O kapasitet

Antall I/O i et sikkerhetssystem vil normalt være antall inn og utganger i systemet. Tabell 7-5 viser antall installerte inn og utganger på 2 av Teleperm-M installasjonene. Dataene viser antall benyttede I/O og forhåndsinstallerte reserve I/O.

		Brage	Njord A	OSS	OSØ	Troll C	Visund
Antall Brukt I/O	ESD	1100		900	1150	1400	
	PSD	600		1300	700	1300	
	F&G	5000		1400	2250	1900	
Antall-Reserve I/O	*ESD*	*210*			*500*		
	PSD	*214*			*300*		
	F&G	*574*			*900*		

Tabell 7-5 I/O oversikt på de ulike anleggene og systemene

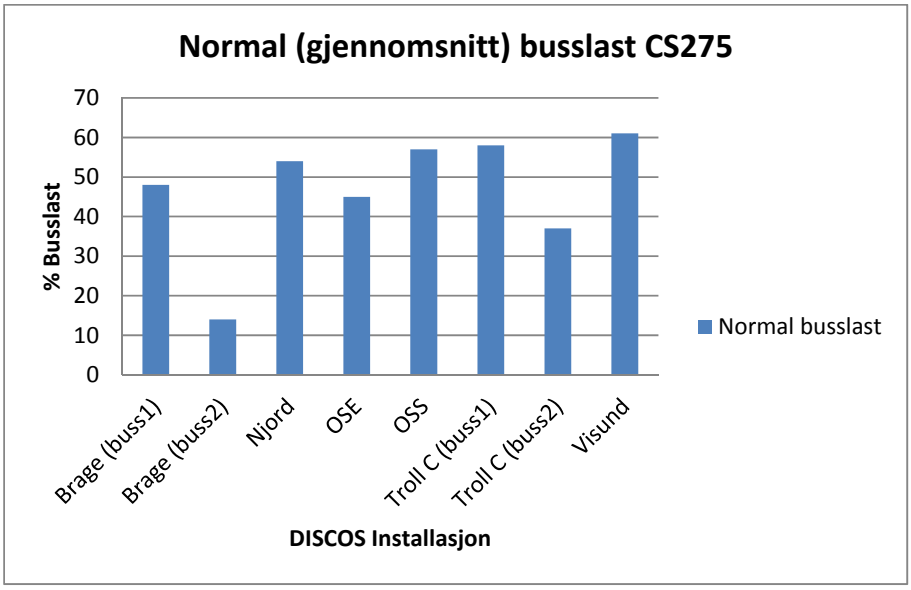
7.9.2 CPU kapasitet (minne, syklustid)

CPU kapasitet er avhengig av hvilken type CPUer som er benyttet i systemene. NAS, PAS, og B&G-systemene benytter såkalte AS235 og AS488 CPUer. AS488 har en høyere kapasitet enn AS235. Statoil har nylig kjøpt inn en stor beholdning av AS488 migrerings-kit for å kunne bytte ut AS235 noder ved behov for høyere kapasitet

Figur 7-16 AS488 Migrerings-kit

7.9.3 Busskapasitet, CS275-buss

Busskapasitet mellom Noder og HMI i DISCOS systemene er basert på Teleperm CS275-buss. Dette er en buss med datahastighet på 275 Kbit. Systemene har en øvre grense for gjennomsnittlig busslast som er satt til 60-70 %. Det er fordi at ved reelle hendelser vil lasten øke og i tillegg skal noe av kapasiteten reserveres systemmeldinger. Figur 7-18 viser gjennomsnittlig busslast på de ulike installasjonene.



Figur 7-17 Normal busslast

Brage og Troll C har splittet opp CS275 buss i to ulike buss segmenter for å utvide kapasiteten. Den ene bussen kalles safetybuss og den andre prosessbuss. Men safetybuss er ikke dedikert til kun sikkerhetssystemer. ESD systemene er koblet mot prosess buss.

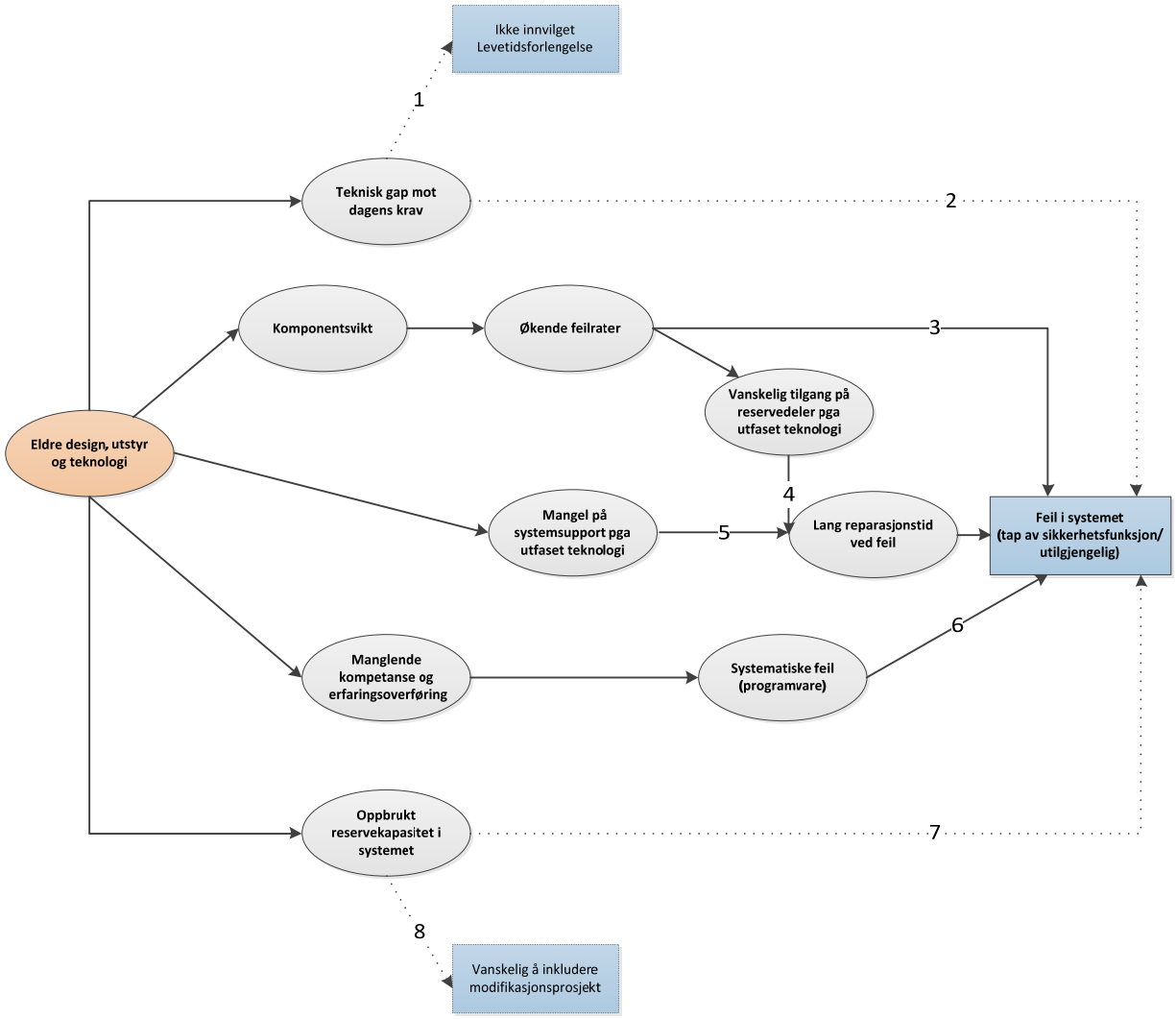
Ut av figur 7-18 ser man at flere av installasjonene er veldig nære eller overstiger maksimalt tillatt busslast. Også ved gjennomgangen av Synergi og M2-notifikasjoner ble det identifisert hendelser og feil som kan relateres til problemer med Node-HMI nettverk. Antall nye objekter og Teleperm M-telegrammer som systemet kan utvides med, kan beregnes ved å summere opp antall forventede data telegrammer.

8 Sammenstilling av de ulike aldringsfaktorene

Analysearbeidet i kapitel 7 startet med identifikasjon av ulike problemstillinger knyttet til aldringsproblematikken. Momentene ble analysert med bakgrunn i TPM-teknologien i sikkerhetssystemene.

8.1 Årsak og konsekvens sammenheng

For å forstå hvordan de ulike aldringsfaktorene kan påvirke systemet og hvordan de ulike årsakene påvirker hverandre kan man etablere en aldringsmodell. Modellen illustrerer de ulike faktorene og relasjonen til ulike hendelser.



Figur 8-1 Etablering av modell i forbindelse med aldring av SIS

Et resultat av aldring av systemene er at det utvikles ulike faktorer som igjen kan resultere i ulike hendelser. Forklaring til modell og de ulike sammenhengene:

1. Aldring har resultert i et teknisk gap mellom opprinnelig design og dagens krav. I forbindelse med søknad om levetidforlengelse skal teknisk integritet og gap mot nye krav vurderes.

2. Aldring har resultert i et teknisk gap mellom opprinnelig design og dagens krav. Dette avviket kan i seg selv kan også være en kilde til feil sammenliknet med dagens referanse som er etablert etter dagens beste praksis og standarder.

3. Aldring fører til degradering av enkelt komponenter som igjen resulterer i økende feilrater.

4. På grunn av utfasing av teknologi vil man ikke ha samme tilgang til reservedeler som kan resultere i lengre reparasjonstider og utilgjengelig sikkerhetssystem.

5. På grunn av utfasing av teknologi og systemsupport vil man ikke ha kanalen inn mot utviklingsmiljøet. Dette kan resultere i lang reparasjonstid og utilgjengelig sikkerhetssystem.

6. Aldring medfører at tilgang til kompetanse minsker og at systemkompetansen til systemene ikke videreføres til nytt personell. Dette påvirker systemene og mulighet for feil øker.

7. Aldring medfører at system komponentene fases ut av produksjon og tilgangen til reservedeler blir vanskelig. Dette påvirker igjen reparasjonstid og mulighet for å kunne utføre modifikasjoner innenfor samme teknologi.

8. Aldring medfører at designet sparekapasitet blir brukt opp. Enkelte deler av systemet har sprengt kapasitet som igjen fører til hyppigere feil. I tillegg vil man ha vanskeligheter med å inkluderer modifikasjoner.

8.1.1 Bayesian Belief networks (BBNs)

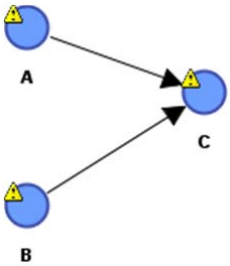
Aldringsmodellen kan overføres til et bayesianske nettverk siden det i stor grad er tegnet som et nettverk. Å konstruere dette nettverket gir en veldig god innsikt i hvordan de ulike faktorene påvirker hendelser og hvordan de ulike faktorene kan påvirke hverandre. Den kvalitative delen av analysen kan utføres ved å gjennomgå modellen og hver enkel node og link i detalj.

En kvantitativ analyse er veldig arbeidskrevende og er best egnet til å utføres ved hjelp av et dataverktøy, det finnes flere tilgjengelige verktøy på markedet, for eksempel (BayesianLab). Sannsynligheten som tildeles de ulike nodene er i stor grad subjektive men støttes i erfaringsdata. For å utføre beregninger må man gjøre en del antakelser knyttet til

avhengighet mellom nodene, for eksempel at noder er uavhengige når vi kjenner tilstanden til alle foreldre nodene deres.

Et Bayesiansk nettverk er en grafisk nettverksmodell som illustrerer koblingene mellom ulike faktorer og tilstandene til en eller flere utganger. En utgang kan for eksempel være den uønskede hendelsen «gasslekkasje» i prosessanlegget. Faktorene som kan påvirke denne hendelsen kalles risikopåvirkende faktorer eller RIF. [7]

Et Bayesiansk nettverk er bygget opp av noder og linker. Se figur 8-2 som viser et enkelt eksempel.

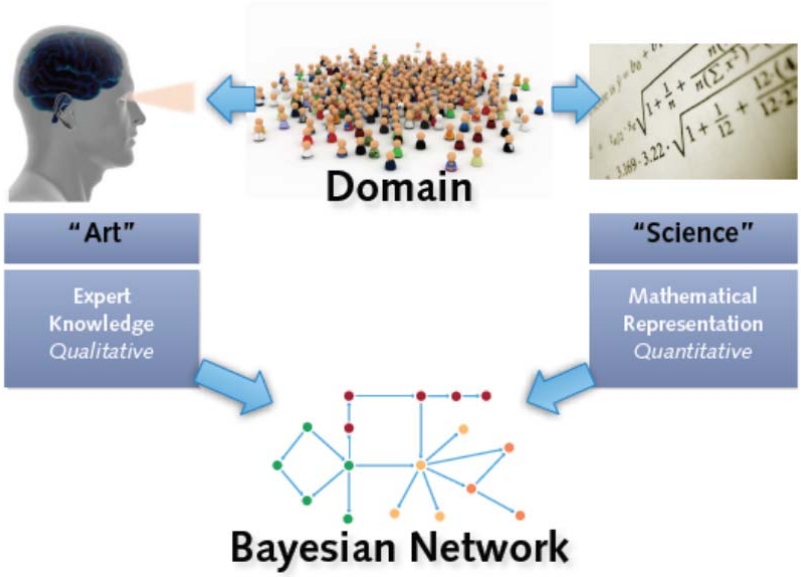


Figur 8-2 Eksempel på et enkelt Bayesiansk nettverk

Nettverket viser at nodene A og B begge har direkte påvirkning på noden C. A er en foreldre node til C (tilsvarende for noden B). Den sammensatte sannsynlighetsfordelingen til nettverker er gitt ved: $P(C,A,B)=P(C|A,B)P(A)(P(B)$

Disse nettverkene kan benyttes både som en kvalitativ og kvantitativ metoder i risikovurderinger. Bayesianske nettverk har evnen til å inkludere både kvalitative kunnskap gjennom strukturen på de ulike nodene og linkene mellom dem. Ved å gi nodene ulike parameter kan den kvalitative kunnskapen inkluderes til nettverket. Figuren 8-3 viser hvordan ulike type kunnskap kan samles inn under en felles form for presentasjon.

[7] Risk Influencing factor



Figur 8-3 Nettverk som representerer både kvalitativ og kvantitativ kunnskap

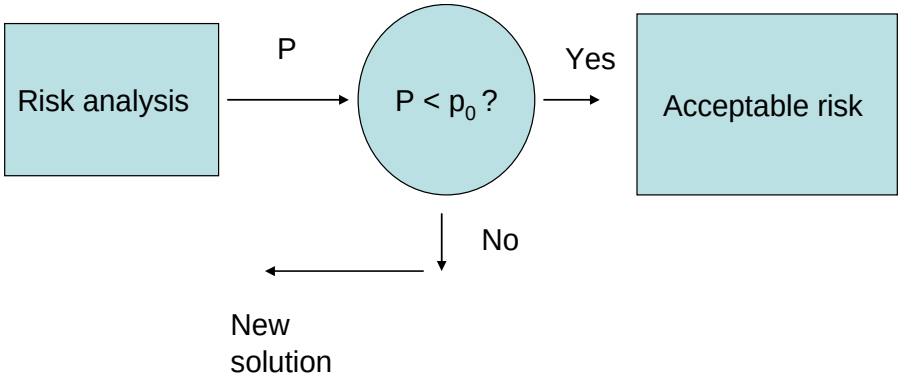
9 «Management review»

Underlaget fra analysene skal støtte opp om en beslutning og må gjennomgås av ledelsen og beslutningstakerne før beslutningen utføres. Gjennomgangen bør ha fokus på bakgrunnsinformasjon i analysene og hvilke antakelser som er gjort. Resultat fra analysene må vurderes i lys av faktorer som (Aven):

1. Hvilke alternativer vurderes
2. Hvilke mål for ytelse vurderes
3. Faktum at analysene representerer vurdering
4. Vanskeligheter med å bestemme fordeler og ulemper mellom alternativene
5. Faktum at analysene er basert på modeller som er en forenkling av virkeligheten

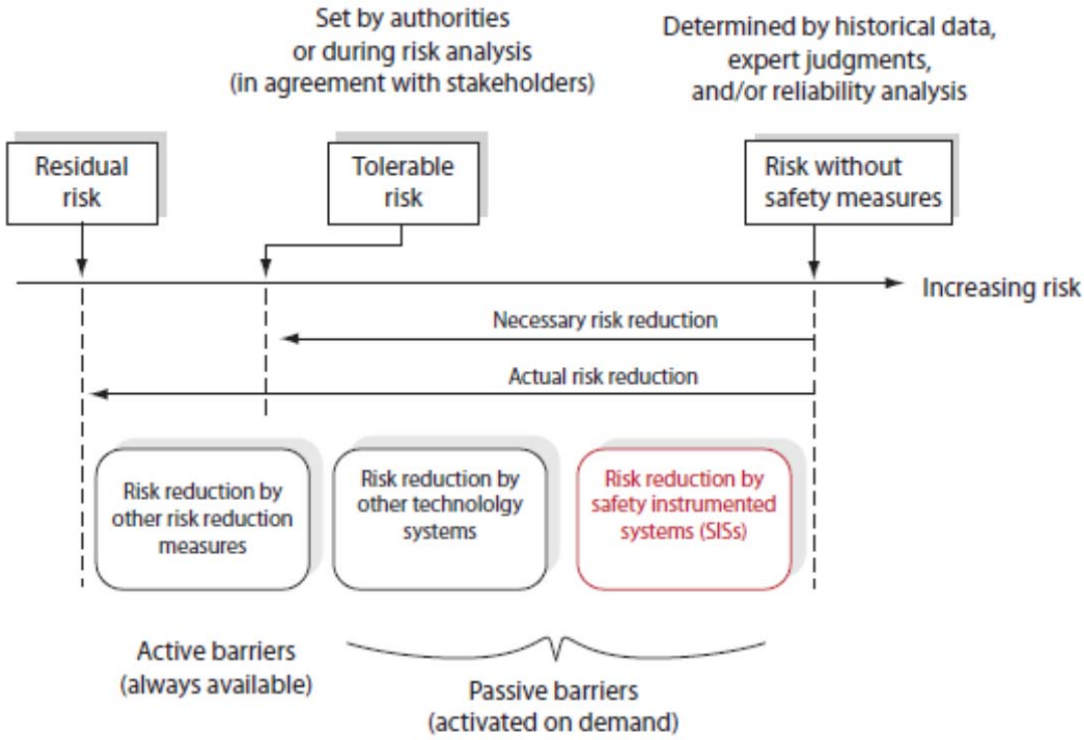
9.1 Akseptkriterier

I risikoanalyser er det vanlig å definere akseptkriterier for risiko før risikoanalysen utføres (ISO31000).



Figur 9-1 Akseptkriterier i forbindelse med risikoanalyser

For sikkerhetssystemene i drift har Statoil definert minimumskrav til sikkerhetskritiske feil hvor «logikk» inngår som et element i de ulike sikkerhetsfunksjonene. De instrumenterte sikkerhetssystemene er introdusert i design som et risikoreduserende tiltak for å kunne oppnå akseptabel risiko, se figur 9-2.



Figur 9-2 SIS som risikoreduksjon

Ytelseskravene fra designfasen av sikkerhetssystemene er ikke definert på samme måte som man vil gjøre i henhold til dagens krav (IEC61508/11) hvor blant annet ytelseskrav til sikkerhetsfunksjonen defineres av PFD[8] og tilgjengelighet gjennom MTBF. Man antar i den forbindelse at feil distribusjonen er eksponentiell og dermed at feilraten er konstant.

Ptil og aktivitetsforskriften sier at det skal være kjent hvilke krav til ytelse som er satt til barriere funksjonene. Statoils har fastsatt (GL0114) et minimum ytelseskrav til sikkerhetsfunksjoner offshore som gjelder for eldre installasjoner. (TFF[9]= antall feil pr antall utførte tester)

PS	Funksjoner	Target Failure Faction
3	Gassdeteksjon	1 %
4	ESD	0.5-2%
7	Branndeteksjon	0.5-1%
12	PSD	0.2-2%

Tabell 9-1 Ytelseskrav til ulike sikkerhetsfunksjoner i Statoil

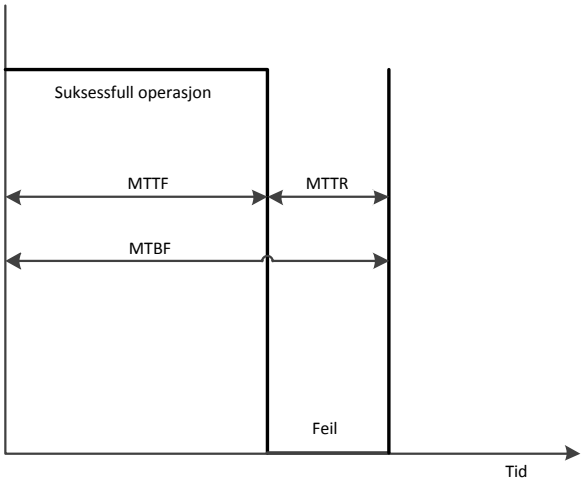
Guideline (OLF070) for applikasjoner i henhold til IEC61508/11 beskriver hvordan man kan oppnå minimum SIL krav for typiske sikkerhetsfunksjoner offshore. Feilbidraget fra «logikk» (CPU + I/O, singelt system) baseres på generiske feildata (datahåndbok) og operere med λ_{DU}=1*10-6 pr time. Samlet for TPM installasjonen vil dette kunne beregnes. Totalt antall «logikk» enheter (ESD, PSD, F&G) = 64 stykk.

$$Forventet\ pålitelighet\ i\ løpet\ av\ 10\ år = 1 * 10^{-6} * 64 * 10 * 8760 = 5{,}6\ DU\ feil$$

Man forventer 6 DU feil i løpet av en 10 års periode for alle SIS systemene. Dette er farlige feil som ikke oppdages av systemet ved hjelp av diagnosemekanismer og resulterer i tapt sikkerhetsfunksjon. Dette kan sammenliknes mot analyseresultat i kapitel 7.7.1.

For reparerbare systemer som SIS er tilgjengelighet viktig. Tilgjengelighet er «oppetid» til systemet. Tilgjengelighet er avhengig av hvor ofte systemet feiler og tiden det tar og reparerer systemet. ($MTBF = MTTF + MTTR$). Resultat fra analyse arbeidet i kapitel 7.7 indikerer en økende feilrate.

[8] Probability of failure of demand
[9] Target Failure fraction



Figur 9-3 Tilgjengelighet til systemene

$MTTR = Mean\ Time\ to\ Repair$
$MTBF = Mean\ Time\ between\ Failures$
$MTTF = Mean\ Time\ to\ Failure$

Det er vanskelig og kan være uheldig å definere absolutte akseptkrav til sikkerhetssystemene i form av feilrater og tilgjengelighet til systemene. Kravet vil være avhengig av antall komponenter som inngår i systemet. Det kan også være ulemper ved å tallfeste akseptkriterier for sikkerhetssystemer, det kan resultere i feil fokus for å møte kravet og i tillegg er ikke analyse verktøyene nøyaktige nok til å møte et slikt absolutt krav. Dette kunne delvis løses ved å definere et akseptabelt område for feilrate og MTTF.

Når man skal designe et sikkerhetssystem og definer ytelseskrav kan det være mer hensiktsmessig å definere ytelseskarakteristikk. Dette vil typisk være industri standarder som IEC61508/11 og beste praksis beskrevet i interne TR dokumenter. Gap-analysen i kapittel 7-1 kan være en slik tilnærming for eksisterende offshore installasjoner.

9.2 Kost-nytte analyser

Økonomisk analyse av de to ulike alternative for SIS for å møte forlenget levetid frem til 2030 er av stor betydning. Dette gjelder både kortsiktige og langsiktige virkninger. De ulike virkningene vil også kunne vurderes ulike mellom installasjonene. Lavere MTTF og utilgjengelig sikkerhetssystemer som et resultat av feil feilrater resulterer i utsatt produksjon, reparasjon, testing og re-start av produksjon.

Man kan beregne forskjell i nåverdi basert på feilfrekvens som de to ulike alternativene representerer fra pålitelighetsanalysen i kapitel 7-3.

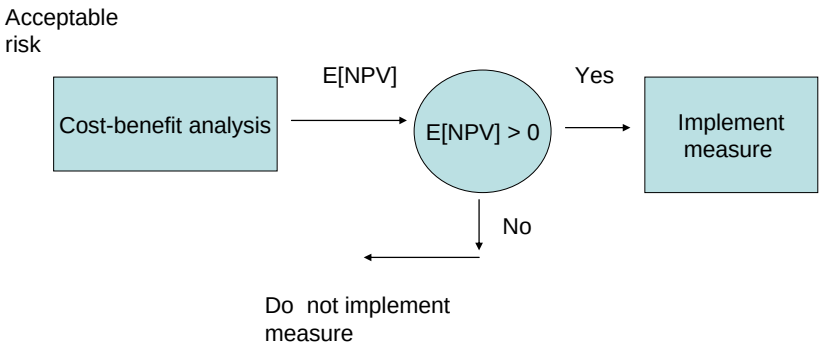
Tilleggskostnadene med et utskiftnings løsning fremfor videre bruk av eksisterende teknologi relateres i all hovedsak til investeringsutgifter. Investeringsutgiftene består i innkjøp av

utstyr, engineering, installasjon og testing. Et grovestimat +-30 % kan utføres ved å benytte kostnøkkel pr I/O som inngår i systemet. Et typisk nøkkeltall pr I/O og alt inkludert ligger mellom 30.000-70.000 pr signal.

Følgende fremgangsmåte kan benyttes (Aven):

1. Beregn frekvensen f av feilaktige nedstengninger pr år.
2. Beregn forventet tapt produksjon for en feilaktig nedstengning i år, i=1,2,…,n.
3. Beregn forventet tap for år i.
4. Diskonter de forventede årlige tapene til samme referanseår.
5. Olje som ikke produseres som følge av nedtegninger er ikke tapt men utsatt produksjon. Det kan antas at denne oljen blir igjen i reservoaret og kan produseres jevnt fordelt over de årene som er igjen i feltes levetid. Dette betyr at det er en fortjeneste knyttet til hver forventet tapsverdi. Ved å diskontere disse verdiene til referanse året fås en nåverdi.
6. Beregn total nåverdi.
7. Utfør følsomhetsanalyser basert på ulike feilrater, oljepris og diskonteringsfaktor.

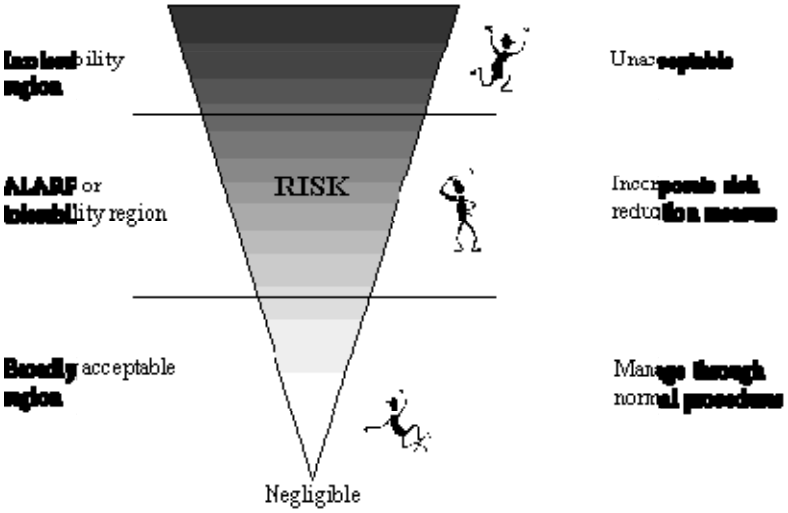
Ved å vurdere nåverdien til de ulike alternativene som vist i figur 9-4 kan man vurdere om begge alternativene er lønnsomme eventuelt om det ene er mer lønnsomt enn det andre.



Figur 9-4 Kostnytte analyser for å vurdere tiltak

9.3 ALARP vurdering

ALARP prinsippet innebærer at risikoen skal reduseres så langt som praktisk mulig. ALARP er en systematisk prosess hvor formålet er å redusere risikoen utover minimumskrav (myndighetskrav).



Figur 9-5 ALARP prinsipp

ALARP-prinsippet tar utgangspunkt i et mål for individuell risiko og hvor risiko deles inn tre ulike områder.

1. Et ikke akseptabelt område. Risikoreduserende tiltak må iverksettes

2. Et midt mellom område, kalt ALARP område, der risikoen kan tolereres hvis nytteverdien er betydelig. Forutsetningen for dette er at det innføres risikoreduserende tiltak såfremt kostnadene ved tiltaket ikke er uforholdsmessig[10] store i forhold til risikoreduksjonen som oppnås.

3. Et område hvor risikoen er lav og generelt akseptert.

Hvis man er innenfor ALARP regionen skal altså riskreduserende tiltak iverksettes hvis det ikke kan dokumenteres uforholdsmessig store kostnader i forhold til hva man oppnår. Prinsippet favoriserer sikkerhet. ALARP prinsippet inngår i rammeforskriften for Norsk offshore virksomhet (Ptil)

Det finnes ulike fremgangsmåter for å vurdere «Grossly disproportionate». Forslag til en metode er beskrevet av (Aven).

[10] Grossly disproportionate to the improvement gained

10 Drøfting av beslutningsprosessen

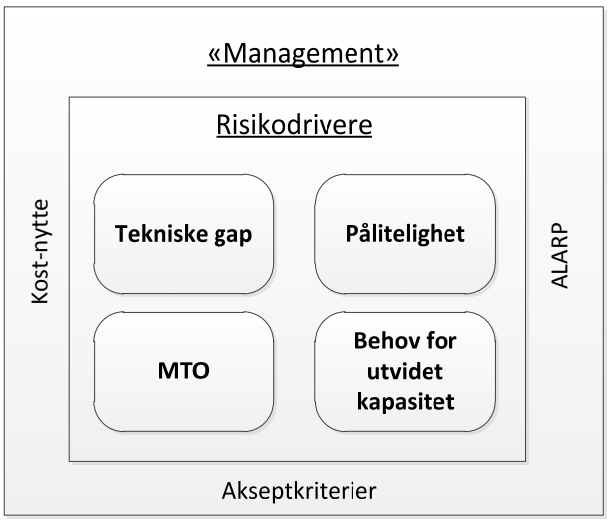
Det har blitt utført flere oppgraderingsprosjekter av sikkerhetssystemer offshore på eksisterende Statoil installasjoner. Eksempler på prosjekter som har oppgradert SIS i Statoil er:

- Statfjord feltet
- Oseberg Feltsenter
- Gullfaksfeltet
- Snorre A
- Sleipner

Behovet for oppgradering av SIS blir initiert av driftsmiljøet og «eier» av systemene. Dette blir ofte utført i forbindelse IOR-prosjekter på den enkelte installasjon. I forbindelse med denne oppgaven har det vært forsøkt å få identifisert hvilket underlag som beskriver oppgraderingsbehovet av SIS i disse prosjektene. Det virker som om beslutningene er begrunnet i TTS-funn, men de ulike funnene er ikke nærmere beskrevet i forhold til mulige tiltak. Det er også enkelte subjektive beskrivelser om ulike utfordringer innen support og kompetanse fra systemleverandør. Det virker uklart hvilke analyser og vurderinger som er nødvendige for å oppnå et tilstrekkelig beslutningsunderlag.

Det finnes en rekke ulike interessenter når et utskiftningsbehov skal vurderes. Både internt i Statoil men også eksternt som systemleverandøren. Disse interessentene bør identifiseres og vurderes i forhold til deres rolle og ansvar.

Når et prosjekt blir initiert skal det gjennom ulike faser (beslutningspunkt) før realisering av prosjektet. Den første fasen er mulighetsstudie, her vurderes ulike alternativer og om man har behov for å se nærmere på enkelte alternativer. En slik studie blir påvirket av prosjektdeltakere og deres vurderinger. Å sette ut en slik studie til systemleverandøren kan føre til at resultatet blir påvirket av deres interesser.



Figur 10-1 Forslag til analyse underlag

11 Konklusjon

Det blir stadig mer aktuelt å vurdere gjenstående levetid til sikkerhetssystemer offshore. Om få år vil mer enn halvparten av innretningene på Norsk sokkel ha passert sin tiltenkte levetid. Denne oppgaven identifiserer ulike faktorer i forbindelse med aldring som man kan ha stor nytteverdi av.

Levetidsøknader til myndigheten skal baseres på OLF122, retningslinjen er under revisjon og ny versjon blir tilgjengelig i juni- 2012. Teknisk gap skal indentifiseres og man skal vurdere hvorvidt man kan oppnå redusert risiko ved å innføre tiltak basert på ALARP prinsipp.

Sikkerhetssystemenes skal være i samsvar med definerte ytelseskrav, men også tilgjengeligheten til systemene er viktig. Utilgjengelige sikkerhetssystemer medfører utsatt produksjon og et tilhørende økonomisk tap.

Modeller for å forutse feilrater kan være et nyttig hjelpemiddel for å vurdere om systemene er innenfor akseptable rammer og til å forutse fremtidig utvikling av feilraten. Nyere modeller som Bayesianske nettverk kan også være nyttige å bruke i en feilmodell, ved å oppdatere ny kunnskap til modellen kan man analysere systemet med ny bakgrunnskunnskap.

Beslutningene rundt strategi og eventuelle tiltak for å møte levetidsforlengelse av sikkerhetssystemer må baseres på et informativt underlag. Usikkerhet, bakgrunnskunnskap og følsomhet må inngå som en del av underlaget. Det er ikke nødvendigvis alderen til et sikkerhetssystem som er det viktigste, men hvordan man evner å styre prosessen rundt aldringsproblematikken.

12 Referanser

Aven, T. (u.d.).
Aven, T. (2008).
BayesianLab. (u.d.). Hentet fra http://www.bayesia.com/en/products/bayesialab.php
Classic Automation. (u.d.). Hentet fra http://www.classicautomation.com/
datahåndbok, P. (u.d.).
GL0114. (u.d.).
IEC61508/11. (u.d.).
IEC61511. (u.d.).
ISO31000. (u.d.). Risikostyring Prinsipper og retningslinjer.
MIL. (u.d.). MIL-HDBK-270, Electrical Conductivity.
OLF070. (u.d.).
Ptil. (u.d.).
Siemens. (u.d.).
Sklet, S. (u.d.).
TR3034. (u.d.). TR3034 SAS. Statoil.
Wikipedia. (u.d.).

13 Vedlegg til oppgaven A-G

Vedlegg A: Informasjon og fakta om Teleperm M-installasjoner på Norsk sokkel

Brage er et oljefelt med noe gass. Brage-plattformen er en integrert bolig-, prosess- og boreplattform med stålunderstell. Feltet kom i drift i 1993 og nådde topp produksjon i 1998 med 120 000 fat i døgnet. I dag produserer feltet ca. 25.000 fat per døgn. Oljen transporteres i en rørledning til Oseberg A-plattformen for videre transport gjennom Oseberg Transport System (OTS) til terminalen på Sture i Øygarden kommune. Gassen transporteres i en egen rørledning til Statpipe for videre transport.

Njord-feltet er bygd ut med en flytende stålplattform, Njord A, med et integrert dekk med bore- og prosesseringsanlegg og boligkvarter. I den første fasen av feltets levetid ble oljen hentet opp gjennom 11produksjonsbrønner, mens fire injeksjonsbrønner sendte gassen ned igjen i reservoaret som trykkstøtte. Fra desember 2007 ble en ny fase innledet hvor også gassen på feltet utvinnes. Til sammen ble det investert 1,15 milliarder kroner i utstyr for gasseksport og 450 millioner kroner i nye produksjonsbrønner. Feltet produserer omkring 20.000 fat olje per døgn, mens gasseksporten gjennomsnittlig er på seks millioner kubikkmeter per døgn. Oljen fra Njord fraktes i rørledning fra plattformen til lagerskipet Njord Bravo, som ligger oppankret like ved plattformen. Skipet har lagerkapasitet på 110.000 kubikkmeter olje og er ankret opp i en tårnbøye som igjen er forankret til sjøbunnen med et åttepunkts forankringssystem. Fra Njord Bravo lastes oljen over til tankskip for transport til markedet. Gassen fra Njord-feltet eksporteres gjennom en 40 kilometer lang rørledning koblet til rørledningen Åsgard Transport. Åsgard Transport forbinder feltet med Kårstø gassanlegg og rørledningene videre til gassmarkedet i Europa.

Olje- og gassfeltet Visund, i blokk 34/8 og 34/7, ligger 22 kilometer nordøst for Gullfaks-feltet i Tampen-området. Produksjonen startet våren 1999. Feltet er bygget ut med en flytende bore-, prosesserings- og boligplattform. Brønnene på feltet er knyttet til plattformen med fleksible stigerør. Oljen går i rørledning til Gullfaks for lagring og eksport. Gasseksporten til kontinentet startet 7. oktober 2005. Visund Nord er en separat undervannsutbygging om lag 10 kilometer fra plattformen.

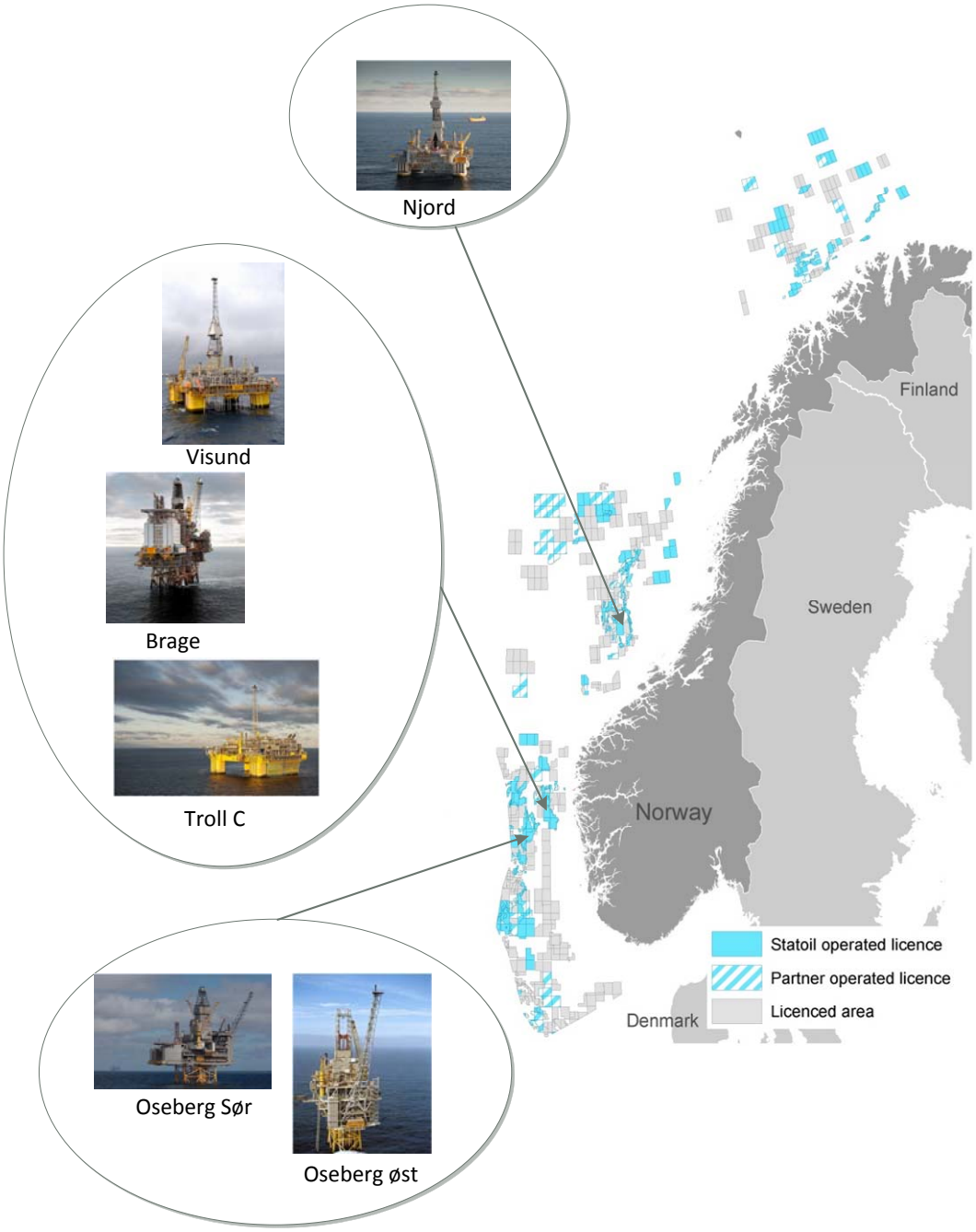
Troll-feltet ligger i nordre del av Nordsjøen, om lag 65 kilometer vest for Kollsnes i Hordaland. Feltet strekker seg over et område på 750 kvadratkilometer i blokkene 31/2, 31/3, 31/5 og 31/6 i Nordsjøen. Troll er selve hjørnesteinen i norsk gassproduksjon og det største gassfunnet som er gjort i Nordsjøen. Feltet inneholder om lag 40 prosent av de samlede gassreservene på norsk kontinentalsokkel. Troll er også blant de største oljefeltene på den norske kontinentalsokkelen; i 2002 var oljeproduksjonen på over 400.000 fat per døgn

Statoil er driftsoperatør for Troll A-, B- og C-plattformen og ilandføringsrørene, mens Gassco er operatør på vegne av Gassled for gassbehandlingsanlegget på Kollsnes. Statoil er teknisk

tjenesteyter for driften av Kollsnes. Det er ventet at de enorme gassreservoarene 1400 meter under havoverflaten vil kunne produsere i minst 70 år.

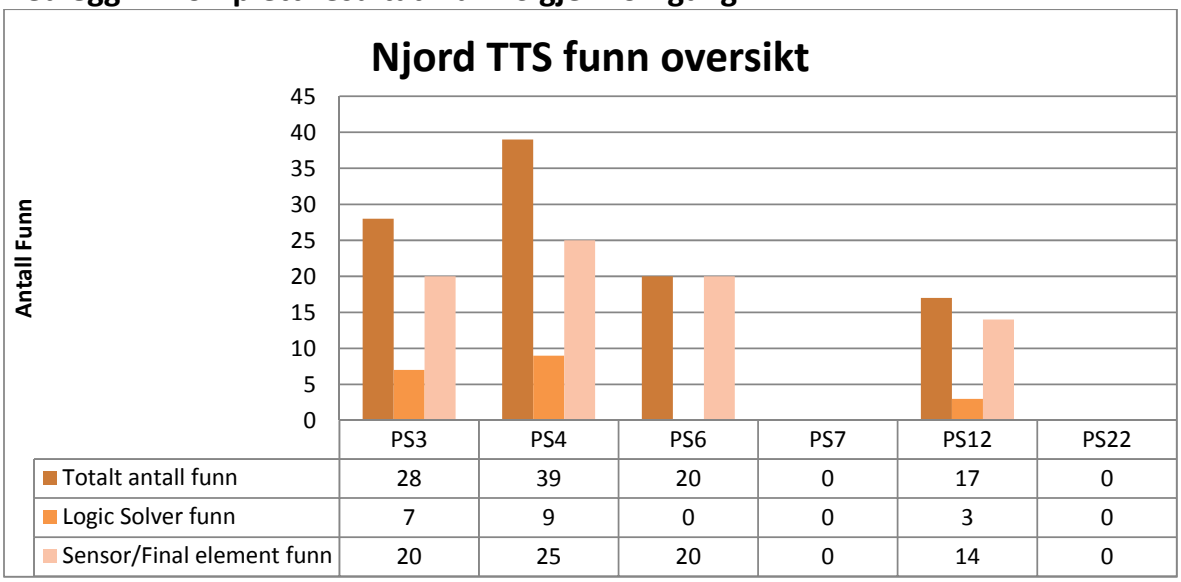
Oseberg Sør-feltet, som består av flere strukturer sør for Oseberg-feltet, er bygget ut med en integrert bore-, bolig- og produksjonsplattform med stålunderstell, og ble satt i drift vinteren 2000. En havbunnsinstallasjon med fire brønner på K-strukturen er knyttet opp mot Oseberg Sør plattformen. I 2004 kom en ny lignende havbunnsinstallasjon i drift på J-strukturen. Det er planlagt 34 brønner på feltet. Havdypet er om lag 100 meter. Oljen føres via Oseberg Feltsenter og Oseberg Transport System til Stureterminalen.

Den minste av plattformene i Oseberg-området, **Oseberg Øst**, ligger 25 kilometer nordøst for Oseberg feltsenter. Feltet er bygd ut med en integrert bore-, bolig- og produksjonsplattform med utstyr for førstetrinnsprosessering. Oljen går gjennom andre- og tredjetrinnsprosessering på Oseberg feltsenter før den transporteres i oljerørledningen Oseberg Transportsystem til Stureterminalen. Maksimal produksjon er på om lag 75.000 fat olje pr. dag. Vann og gass blir injisert i reservoaret for å øke oljeutvinningen.



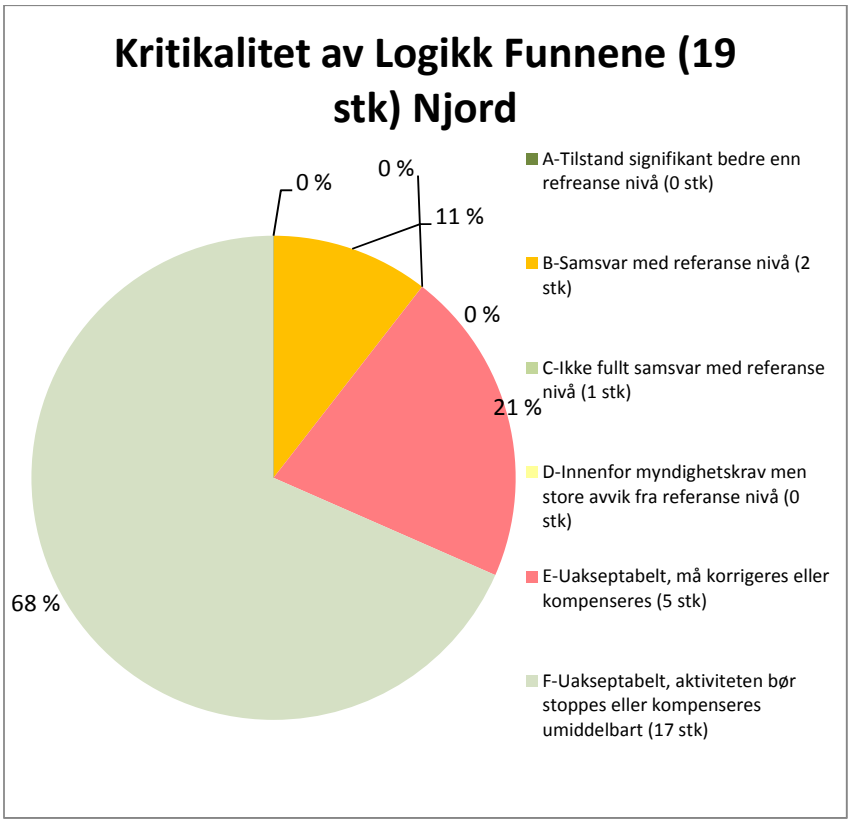
Figur 13-1 Teleperm M-installasjoner på norsk kontinental sokkel

Vedlegg B: Komplett resultat fra TTS gjennomgang

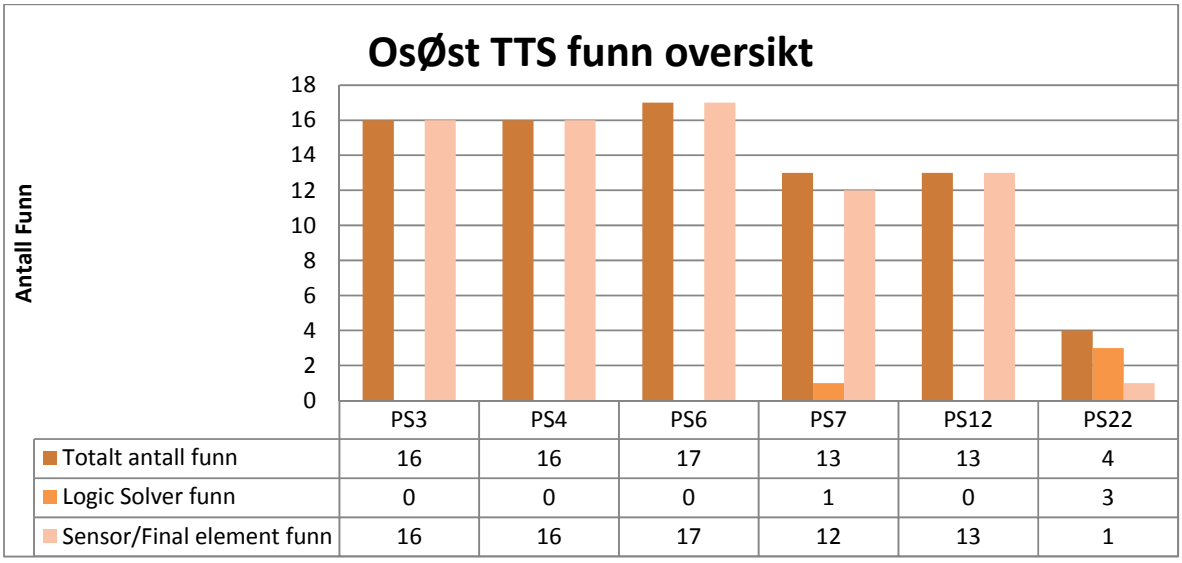


	PS3	PS4	PS6	PS7	PS12	PS22
Totalt antall funn	28	39	20	0	17	0
Logic Solver funn	7	9	0	0	3	0
Sensor/Final element funn	20	25	20	0	14	0

Figur 13-2 TTS resultat Njord A

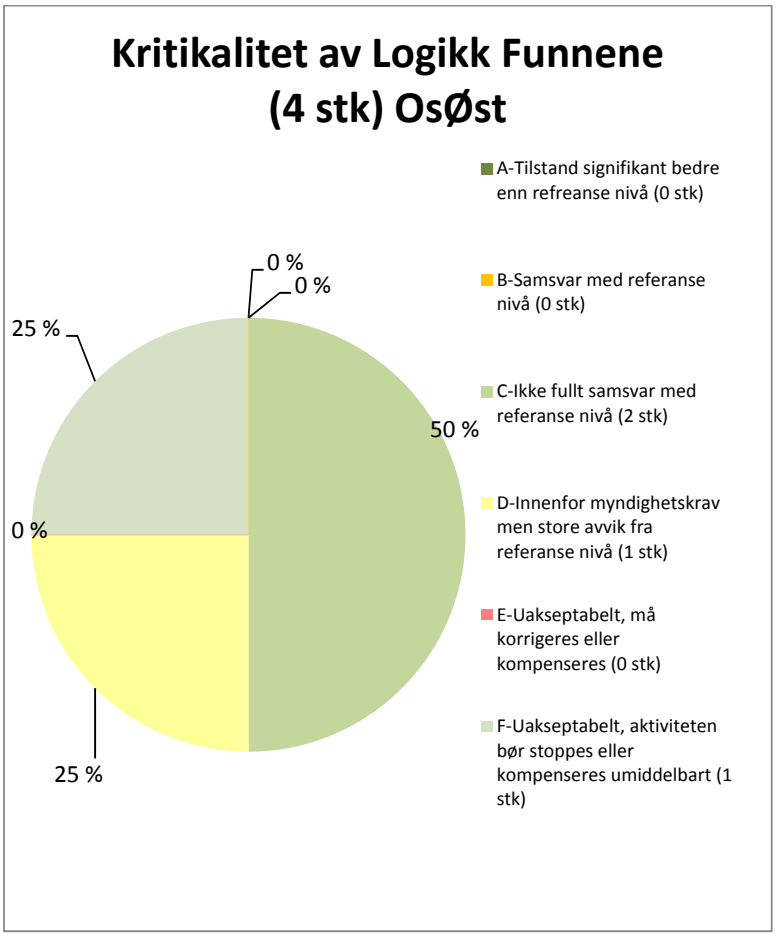


Figur 13-3 Kritikalitet av funn Njord A

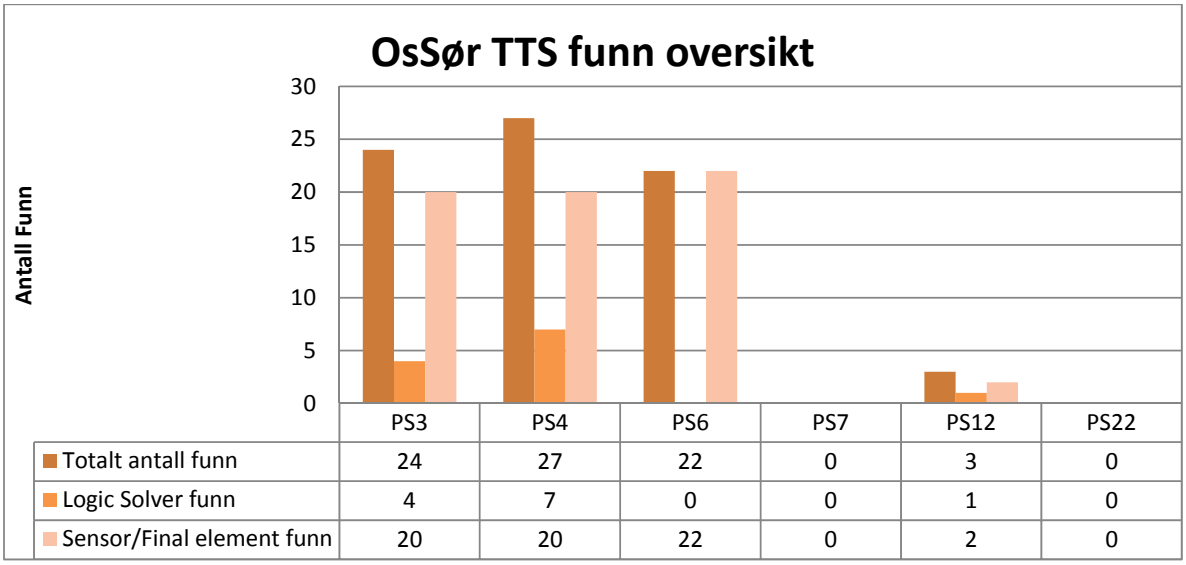


	PS3	PS4	PS6	PS7	PS12	PS22
Totalt antall funn	16	16	17	13	13	4
Logic Solver funn	0	0	0	1	0	3
Sensor/Final element funn	16	16	17	12	13	1

Figur 13-4 TTS resultat Oseberg Øst

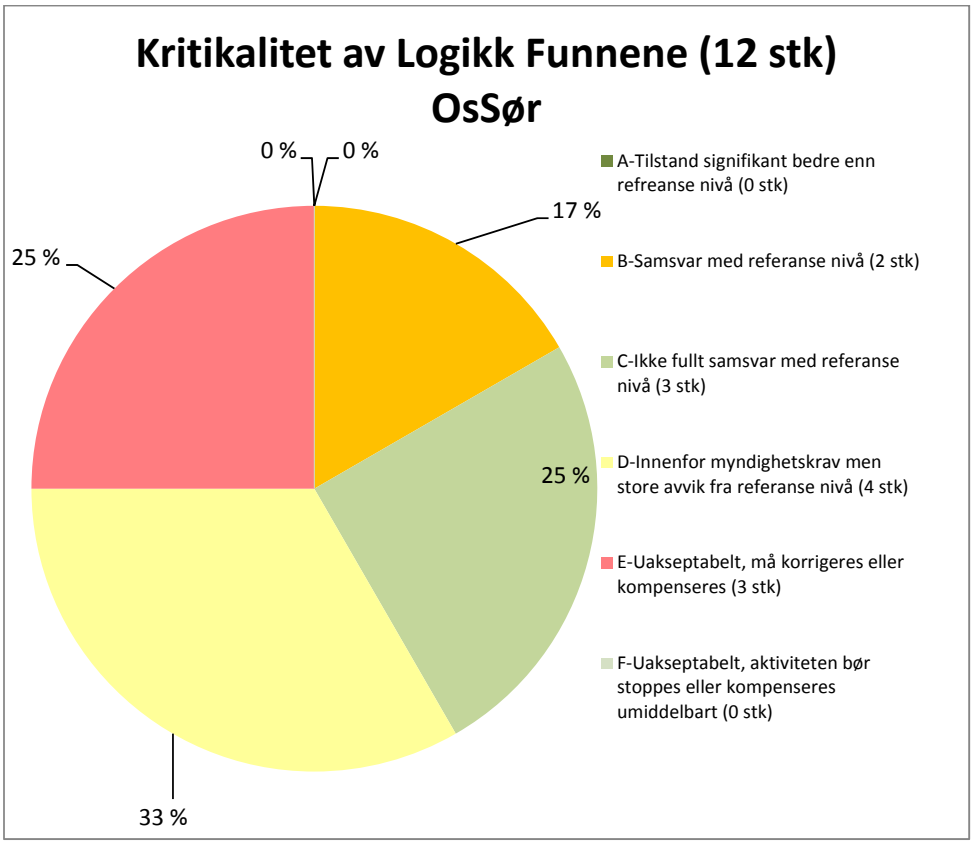


Figur 13-5 Kritikalitet av funn Oseberg Øst

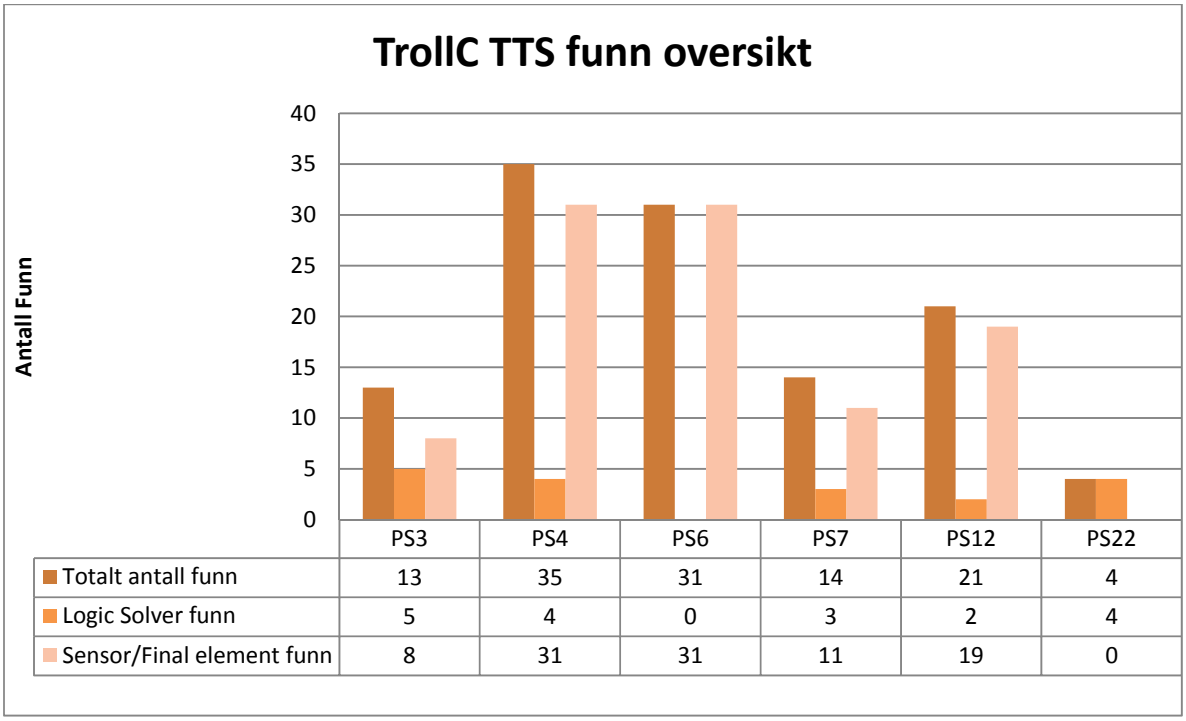


	PS3	PS4	PS6	PS7	PS12	PS22
Totalt antall funn	24	27	22	0	3	0
Logic Solver funn	4	7	0	0	1	0
Sensor/Final element funn	20	20	22	0	2	0

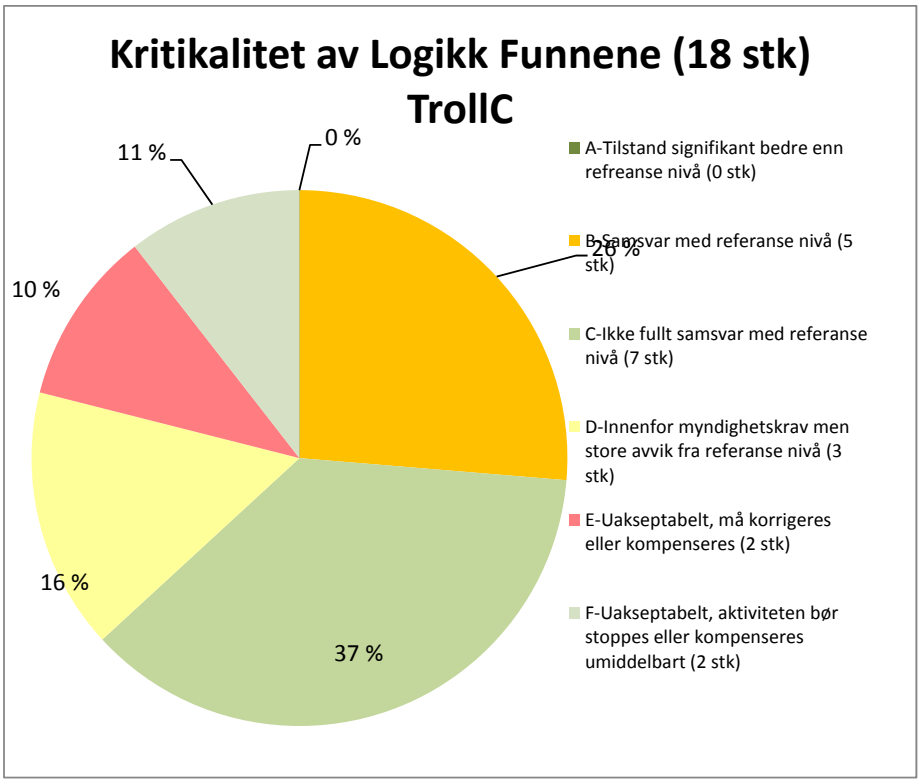
Figur 13-6 TTS resultat Oseberg Øst



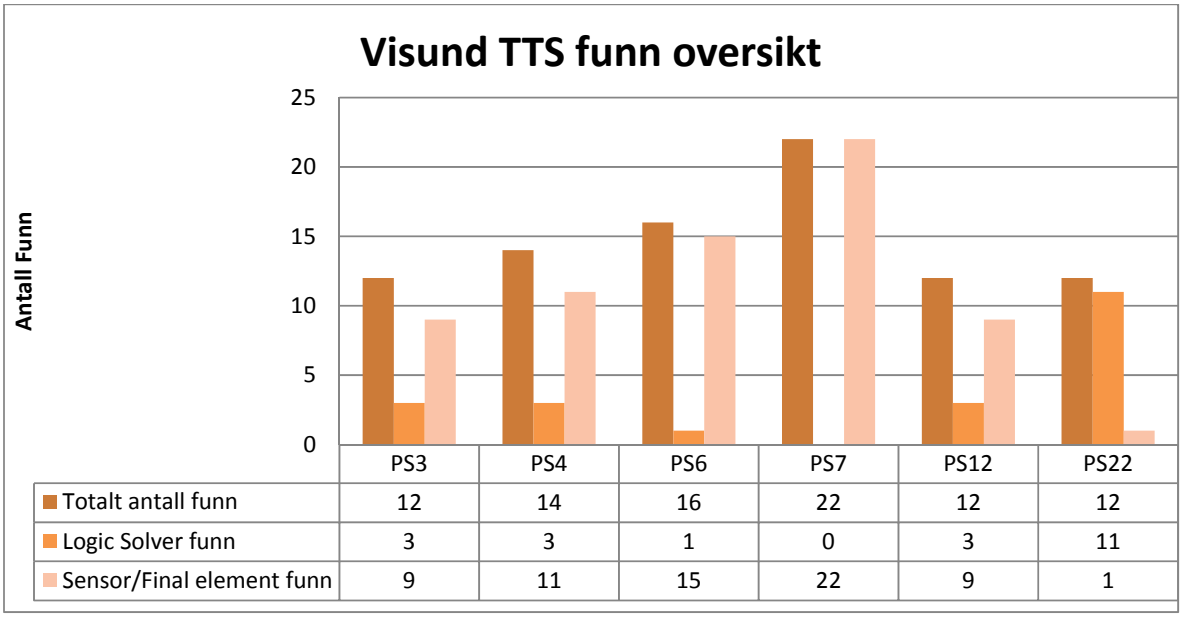
Figur 13-7 Kritikalitet av funn Oseberg Øst



Figur 13-8 TTS resultat Troll C

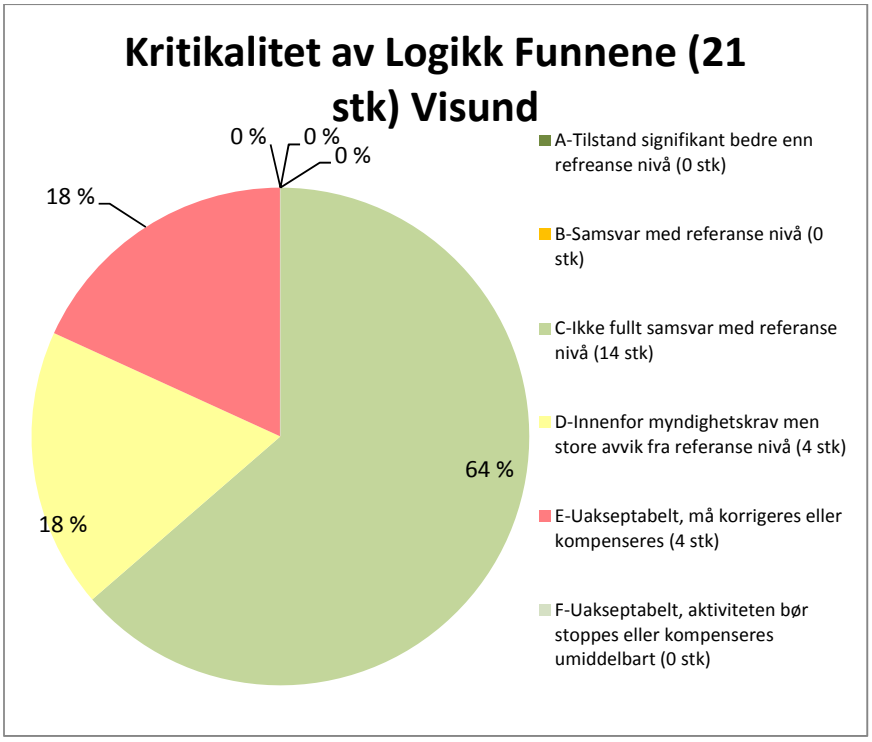


Figur 13-9 Kritikalitet av funn Troll C



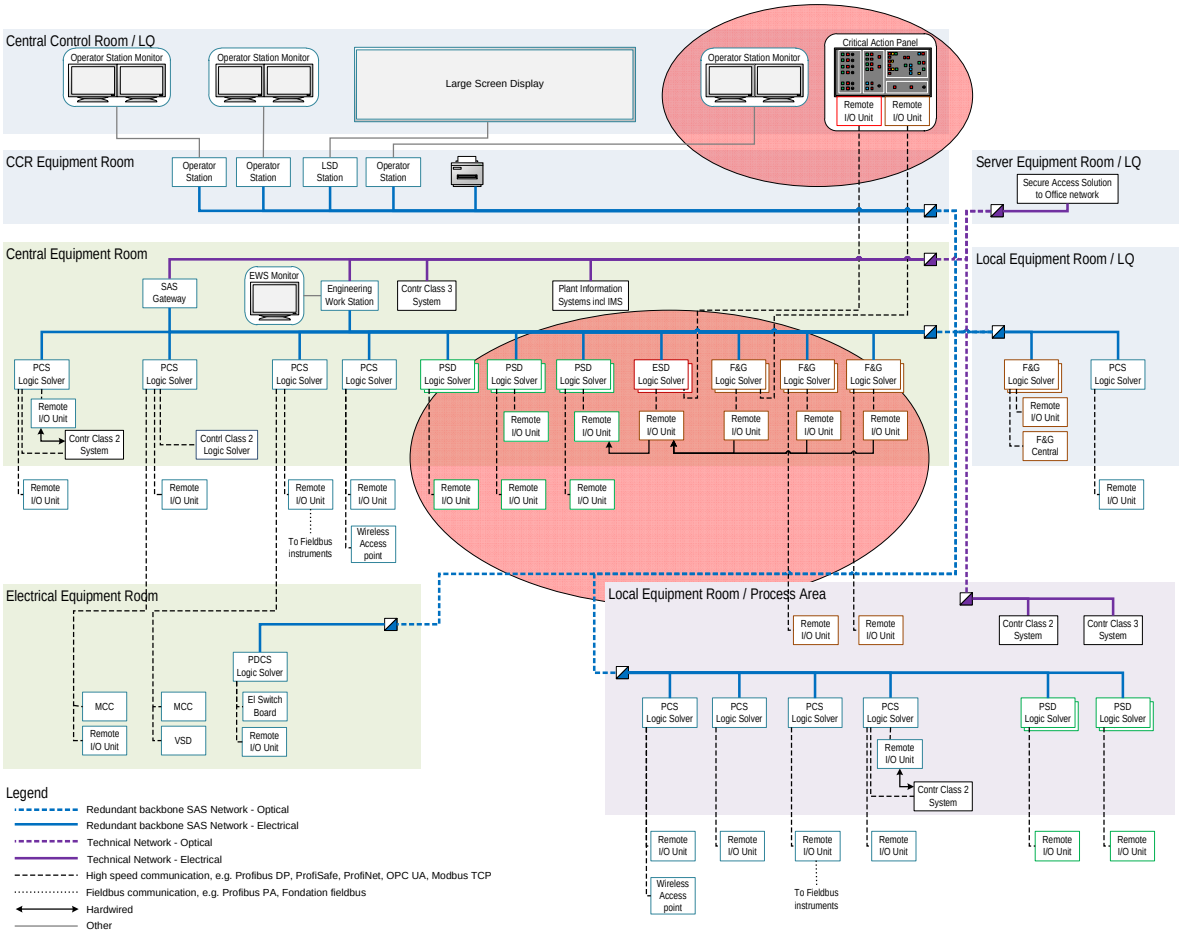
	PS3	PS4	PS6	PS7	PS12	PS22
Totalt antall funn	12	14	16	22	12	12
Logic Solver funn	3	3	1	0	3	11
Sensor/Final element funn	9	11	15	22	9	1

Figur 13-10 TTS resultat Visund



Figur 13-11 Kritikalitet av funn Visund

Vedlegg C: Topologi for et typisk Sikkerhet og Automasjonssystem



Vedlegg D: Datagrunnlag TTS

Vedlagt elektronisk (Excel)

TTS_funn_Discos.xls

Vedlegg E: Datagrunnlag Synergi

Vedlagt elektronisk (Excel)

Synergirapport_data.xls

Vedlegg F: Datagrunnlag M2 fra SAP

Vedlagt elektronisk (Excel)

M2_analyse_discos.xls

Vedlegg G: Datagrunnlag reservedelsuttak fra SAP

Vedlagt elektronisk (Excel)

Forbruk_deler.xlsx