Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: **Master i Risikostyring / ERM**	Vårsemesteret, 2010 Åpen
Forfatter: **Sindre Utne**	..... (signatur forfatter)

Fagansvarlig: **Eirik Bjorheim Abrahamsen (Universitetet i Stavanger)**

Veileder(e): **Eirik Bjorheim Abrahamsen (Universitetet i Stavanger)**
Arvid Eikeskog (Stiftelsen Polytec)
Gudmundur Kristjansson (Gassco)

Tittel på masteroppgaven:

Usikkerhet knyttet til pålitelighetsvurderinger i instrumenterte sikkerhetssystemer

Studiepoeng:
30sp

Emneord: Usikkerhet / usikkerhetsanalyse Pålitelighet / pålitelighetsanalyse Sikkerhets relaterte systemer Safety Integrity Level (SIL) IEC 61508 PDS OLF 070	Sidetall: **94 sider** + vedlegg/annet: **21 sider** Stavanger, 15. juni 2010

FORORD

Denne masteroppgaven er skrevet ved Institutt for industriell økonomi, risikostyring og planlegging ved Universitetet i Stavanger (UiS) under vårsemesteret 2010. Oppgaven er en del av et toårig masterprogram i risikostyring.

Tittelen på oppgaven er "Usikkerhet knyttet til pålitelighetsvurderinger i instrumenterte sikkerhetssystemer", der denne er skrevet i samarbeid med Gassco AS. Oppgaven er basert på en litteraturstudie av to metoder for pålitelighetsanalyser, og en casestudie av et instrumentert sikkerhetssystem (SIS). De to metodenes håndtering av usikkerhet i relasjon til prediksjoner av fremtidig sikkerhetsutilgjengelighet utgjør hovedfokus. Det antas at leseren av denne oppgaven har tatt et introduksjonskurs i pålitelighetsteori eller har tilsvarende kunnskaper.

Jeg vil takke min veileder på UiS, Førsteamanuensis Eirik Bjorheim Abrahamsen, for å ha veiledet meg gjennom ulike problematiske emner. Jeg vil også takke mine andre veiledere, Gudmundur Kristjansson (Gassco AS) og Arvid Eikeskog (Stiftelsen Polytec), for gode råd i løpet av dette semesteret.

Stavanger, 15. juni 2010

Sindre Utne

SAMMENDRAG

Sikkerhetsinstrumenterte systemer (SIS) er uavhengige systemer som blant annet er installert for å redusere risikoen knyttet til personell, miljø og verdier i mange industrier og bransjer, inkludert landbasert- og offshoregassindustri. Betydningen av et velfungerende SIS gjør på denne måten påliteligheten til en viktig faktor, der avhengigheten av blant annet menneskelig interaksjon introduserer aspekt av usikkerhet knyttet til vurderinger av systemers tilgjengelighet på etterspurt tid.

Denne oppgaven dokumenterer resultatene av en analyse der formålet har vært å undersøke i hvilken grad metoder for kvantifisering av sikkerhetsutilgjengelighet i SIS justerer, håndterer og tar høyde for usikkerhet knyttet til SIL (Safety Integrity Level) verifisering. SIL kravene introduseres i IEC 61508 standarden som kom i 1998, og er nærmere beskrevet i OLF 070 som er veiledende retningslinjer for å forenkle implementeringen av kravene i norsk petroleumsindustri. Oppgaven er på denne måten avgrenset til å fremskaffe førstehånds erfaring fra anbefalte metoder for verifisering av SIL kravene fra de to metodiske tilnærmingene som foreslås og inkluderes i OLF 070: den generelle tilnærming i IEC 61508 og PDS metoden som er utviklet av SINTEF.

En litteraturstudie har blitt gjennomført for å identifisere ulikheter i de to metodenes håndtering av usikkerhet, herunder modellusikkerhet, ufullstendighetsusikkerhet og datausikkerhet. Resultatene fra analysen indikerer at konsekvent bruk av begge metodene for gjennomføring av SIL verifisering, vil kunne representere usikkerhet. Grad av usikkerhet forbundet med de to metodene vil være avhengig av hvilket bakenforliggende risiko- og sannsynlighetsperspektiv som ligger til grunn for vurderingen, der begge metodene ut i fra et prediktivt epistemisk sannsynlighetsperspektiv ser ut til å være tilknyttet usikkerhet i ufullstendighet og inndata. Dette oppstår dersom pålitelighetsanalytikeren følger fremgangsmåten for de to metodene uten i tillegg å generere inngående kunnskap og betrakte tilhørende usikkerhet omkring angitt system.

Oppgaven har derfor utviklet en alternativ metodisk tilnærming for å inkludere kunnskapsakkumulasjon og usikkerhetsvurderinger i tilknytning til pålitelighetsvurderingene som foretas for å verifisere et system i henhold til underliggende SIL krav. Den alternative metodiske tilnærmingen uttrykker behovet for en systematisk og strukturert måte for å identifisere scenarioer som kan medføre fare eller operasjonelle problemer knyttet til det aktuelle system. Sannsynlighet for svikt på etterspurt tid (PFD) er her et mål på usikkerhet, vurdert og basert på tilgjengelig informasjon og kunnskap.

INNHOLDSFORTEGNELSE

FIGURLISTE

TABELLISTE

FORKORTELSER

CSU	Critical Safety Unavailability
DC	Diagnostic Coverage
DU-RH	Dangerous Undetected Random Hardware failures
DU-S	Dangerous Undetected Systematic failures
DU	Dangerous Undetected failures
E/E/PE	Elektriske, elektroniske og/eller programmerbare elektroniske komponenter
EUC	Equipment Under Control
FMECA	Failure Mode, Effect and Criticality Analysis
FMEDA	Failure Mode, Effect and Diagnostic Analysis
HIPPS	High Integrity Pressure Protection System
IEC	International Electrotechnical Commission
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety-Related Systems
IEC 61511	Functional Safety – Safety Instrumented Systems for the Process Industry
ISO	International Standard Organization
MFDT	Mean Fractional Dead Time
MooN	M ut av N
MTTR	Mean Time To Restoration
OLF	Oljeindustriens Landsforening
OLF 070	Veiledning til IEC 61508 og IEC 61511 i norsk olje- og gassindustri
OREDA	Offshore Reliability Database
PDS	Påliteligheten til Datamaskinbaserte Sikkerhetssystemer
PFD	Probability of Failure on Demand
PFH	Probability of a dangerous Failure per Hour
P_{TIF}	Probability of Test Independent (systematic) Failures
Ptil	Petroleumstilsynet
QRA	Quantitative Risk Assessment

SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Intergrity Level
SIS	Sikkerhetsinstrumentert system (Safety Instrumented System)

DEFINISJONER

Aleatorisk usikkerhet	Iboende og naturlig usikkerhet som er knyttet til et system eller en prosess (Janbu, 2009)
Epistemisk usikkerhet	Manglende kunnskap om ytelse i et system eller en prosess (Aven, 2003)
Farlig feil	"Failure which has the potential to put the safety-related system in a hazardous or fail-to-function state" (OLF-070, 2004) En liten del av disse feilene, "dangerous detected failures", vil oppdages ved automatiske selvtester. De residuale kritiske feilene som ikke oppdages ved automatiske selvtester betegnes som "dangerous undetected failures"
Feil	Feil for en komponent eller et system vil i denne oppgaven betraktes som å "nå", eller å være i, en tilstand der komponenten eller systemet ikke vil kunne fullføre tiltenkt funksjon (M. Rausand & Høyland, 2004)
Sikkerhets-instrumenterte systemer	"En fellesbetegnelse for automatiske systemer som har til formål å detektere potensielt farlige situasjoner ved å bringe systemer eller komponenter til en sikker tilstand dersom farlige hendelser skulle inntreffe" (Lundteigen, 2009)
Pålitelighet	"The ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time" (ISO8402, 1986).
Sannsynlighet	I denne oppgaven vil sannsynlighet bli definert som grad av tro
Sikre feil	"Failure which does not have the potential to put the safety-related system in a hazardous of fail-to-function state" (OLF-070, 2004) En liten del av disse feilene, "safe detected failures", vil oppdages ved automatiske selvtester. De residuale sikre feilene som ikke oppdages ved automatiske selvtester betegnes som "safe undetected failures"
Systematisk feil	"Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or

	other relevant factors" (IEC 61508-4, 1998)
Tilfeldig hardware feil	"A failure occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware" (IEC 61508-4, 1998)
Usikkerhet	I denne oppgaven representerer usikkerhet et begrep som uttrykker vår grad av kunnskap omkring systemet

1 Introduksjon

Norsk olje og gassindustri er underlagt myndighetskrav i form av forskrifter som skal regulere forhold av betydning for helse, miljø og sikkerhet. Forskriftene stiller blant annet krav til konstruksjon og design av systemer, til drift av systemene, til beskyttelse av miljøet og til arbeidernes arbeidsvilkår.

Formålet med gasstransport og prosesseringssystemer er i stor grad å forsyne konsumenter med gass til en akseptabel grad av pålitelighet og kvalitet til så lave kostnader som mulig. Økt kostnadseffektivitet stiller krav til kontinuerlig drift av både transportsystemer og prosessanlegg for å ivareta og optimalisere nytteeffekten av systemene. Således har man i moderne samfunn forventning om kontinuerlig tilgjengelighet på etterspurt tid, kombinert med forventninger om høy sikkerhetsgrad og sikkerhetsstandard for systemene. Politiske krav og direktiver for å opprettholde høy effektivitet og høy sikkerhet har videre vært retningsbestemmende for både drift og design i industrien. Innenfor området har således metoder for risiko- og pålitelighetsvurderinger blitt viktige for å sikre langsiktig effektivitet og god sikkerhet.

I sikkerhetsarbeid for landbasert- og offshoregassindustri nyttes ofte *instrumenterte sikkerhetssystemer* (Safety Instrumented System – SIS) for å se til at risikoen er innenfor akseptable rammer. SIS er en fellesbetegnelse for automatiske systemer som har til formål å detektere potensielt farlige situasjoner ved å bringe systemer eller komponenter til en sikker tilstand dersom farlige hendelser skulle inntreffe (Lundteigen, 2009).[1] Kvaliteten til SIS er med dette avgjørende for hvor stor risikoreduksjon som oppnås. I industrien er det innført standarder og retningslinjer som definerer gjeldende krav for de instrumenterte sikkerhetssystemene, samt krav for å kontrollere at disse ligger innenfor gjeldende risikoakseptkriterier. Kravene er i stor grad knyttet til såkalte *Safety Integrity Level* (SIL-nivå) og *Probability of Failure on Demand* (PFD) (Safetec, 2010).

1.1 Bakgrunn

Sikkerhets- og pålitelighetsanalyser har som beskrevet en viktig rolle i SIS. Analysene benyttes for å beslutte og kvalifisere SIS under bestemte forhold med et gitt funksjonalitets-

[1] Mer informasjon om SIS foreligger i delkapittel 3.1

og pålitelighetskrav. Når SIS blir satt i drift, kan det hentes inn data for å oppdatere sikkerhets og pålitelighetsanalysene for å verifisere at et gitt SIS fortsatt møter spesifiserte krav (Lundteigen, 2009).

De oppgitte kravene til kalkulasjoner og metoder for pålitelighetsanalyser av SIS er gitt i forskrifter og standarder. Nasjonale og internasjonale myndigheter gir generelle krav til SIS design, implementering og drift, mens disse refererer til detaljerte implementeringskrav som videre er samlet i internasjonale standarder som IEC 61508 og IEC 61511. IEC 61508 ble introdusert i 1998, mens IEC 61511 ble publisert i 2003. I denne oppgaven er disse to standardene referert til som "IEC-standardene".

Sikkerhets- og pålitelighetsanalysene bygger videre på en rekke antakelser om systemer og hvilke forhold disse driftes under, der avhengigheten av menneskelig interaksjon i SIS gjør pålitelighet og usikkerhet til viktige parametre. Dersom beslutningstakere ikke er klar over graden av usikkerhet som er knyttet til ulike metoder for pålitelighetsvurderinger, kan resultatene feiltolkes eller potensielt sett lede til at beslutninger for å ivareta nødvendig risikoreduksjon tas på feil grunnlag.

Uheldigvis er det flere aspekt i en pålitelighetsanalyse som forårsaker usikkerhet knyttet til de endelige resultatene. Usikkerheten avhenger i hovedsak av hvorvidt modellen, inndataene og den metodiske tilnærmingen gjenspeiler de viktigste egenskapene og forholdene til systemet det tas utgangspunkt i (Lundteigen, 2009). Stor grad av usikkerhet i pålitelighetsvurderinger kan således antas å redusere validiteten til resultatene, og dermed øke risikoen for å ta feil beslutninger. Det bør med dette nedlegges innsats og ressurser for å minimere denne usikkerheten.

1.2 Formål

Oppgaven med å beslutte påliteligheten til SIS kan som nevnt være en kompleks og vanskelig prosess. Det foreligger mange metoder, og terminologien bak de ulike metodene har ulike styrker og svakheter når det kommer til håndtering av usikkerhet ved kvantifisering av systempålitelighet. Forutsetninger og forenklinger som foretas gjør at usikkerhet i pålitelighetsanalysene oppstår som følger av begrensninger relatert til å reflektere systemet i det virkelige liv og dets omgivelser. Formålet med denne oppgaven blir å undersøke i hvilken grad metoder for kvantifisering av sikkerhetsutilgjengelighet i SIS justerer, håndterer og tar høyde for usikkerhet knyttet til SIL verifisering.

Dette hovedformålet kan videre deles inn i følgende delmål:

- Gjennomføre en litteraturstudie og bli kjent med metodene som benyttes for å kvantifisere sikkerhetsutilgjengelighet, herunder PFD
- Diskutere ulike tilnærminger for å tolke sannsynlighet og usikkerhet
- Illustrere ulikheter mellom metoder knyttet til kvantifisering av PFD i en enkelt case
- Diskutere styrker og svakheter i ulike metoders håndtering av usikkerhet
- Eventuelt å foreslå nødvendige forbedringer for å inkorporere håndtering og effekter av usikkerhet på en praktisk måte i en alternativ metodisk tilnærming

Det er som nevnt viktig å være klar over at kvantifisering av pålitelighet og sikkerhetsutilgjengelighet er assosiert med usikkerhet. Dette betyr at resultatene som oppnås fra denne typen analyser kan betraktes som kvantifiserte prediksjoner, betinget på tilgjengelig bakgrunnsinformasjon og pålitelighetstendenser i den operasjonelle fasen. Det foreligger videre i oppgaven en antakelse om at fokus på usikkerhet vil påvirke pålitelighetskalkulasjoner og sikkerhet i systemer, samt i hvilken grad kvantitative prediksjoner kan betraktes å representere systemers lokale operasjonelle driftsforhold.

Mer informasjon om hvordan usikkerhet er operasjonalisert og vil bli undersøkt i denne oppgaven, foreligger i delkapittel 2.2.

1.3 Avgrensning

Bakgrunnen for denne oppgaven er Gassco sitt behov for vurdering av barriereeffektivitet for landbaserte gass- og prosessterminaler, med hensyn til barrierenes funksjonalitet, tilgjengelighet, sårbarhet og pålitelighet. Formålet med denne oppgaven var således å fremskaffe førstehånds erfaring omkring anbefalte metoder for verifisering av SIL krav fra de to metodiske tilnærmingene som foreslås og inkluderes i OLF 070 (2004): den generelle tilnærming i IEC 61508 og PDS[2] metoden som er utviklet av SINTEF.

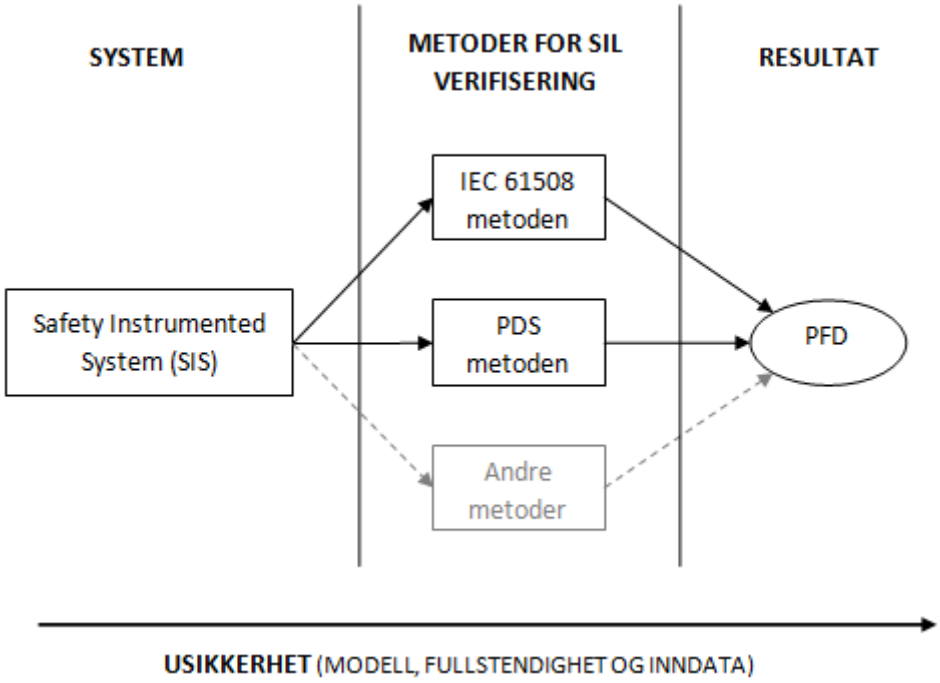
Oppgaven retter oppmerksomheten mot kvantifisering av sikkerhetsutilgjengelighet, herunder PFD, i systemer som opererer på etterspørsel (forespørsel). På denne måten vil oppgaven kun ha fokus på de metodiske PFD kalkulasjonene for hardware sikkerhetsintegritet, og vil ikke betrakte andre semi-kvantitative og kvalitative krav til sikkerhetsintegritet for SIS. Oppgaven er videre begrenset til "low demand" SIS. Denne typen

[2] Påliteligheten til Datamaskinbaserte Sikkerhetssystemer (PDS)

systemer er barrierer mot konsekvenser som vanligvis assosieres med høy energi og initierende hendelser med lav frekvens (Janbu, 2009). Grunnlag og vurderinger for fastsettelse av SIL kriteriene (akseptkriterier) som er beskrevet i OLF 070 og IEC-standardene vil ikke bli nærmere diskutert, mens forutsetninger og forenklinger som foretas for å kvantifisere PFD i henhold til metodene for SIL analyser vil bli nærmere betraktet.

Oppgaven er videre basert på et prediktivt Bayesiansk sannsynlighets- og risikoperspektiv, hvor reduksjon av usikkerhet er relatert til kunnskapsakkumulasjon og ekspertvurderinger. Dette er i stor kontrast til et klassisk relativ frekvens perspektiv hvor usikkerhet kun diskuteres i forhold til probabilistiske resultater. Oppgaven er først og fremst opptatt av ideene og prinsippene, og vil således forenkle matematikken der det er nødvendig for ikke å bli for teknisk og detaljert. Det forutsettes likevel at leseren av denne oppgaven er kjent med pålitelighetsanalyser. Dette hindrer forklaring av enkelte grunnleggende element og reproduksjon av materiale fra introduksjonskurs i pålitelighetsanalyse.

Til tross for at oppgavens empiriske utgangspunkt og underliggende betraktninger omhandler landbaserte gass- og prosessterminaler, vil oppgaven likevel kunne ha anvendelse ut over dette området.



Figur 1.1 - Avgrensning av oppgaven

Figur 1.1 viser oppgavens avgrensning til de to metodene det refereres til i OLF 070; IEC 61508 metoden og PDS metoden. Figuren illustrerer også usikkerhetskategoriene som ligger til grunn for operasjonaliseringen av usikkerhet i denne oppgaven.

Oppgaven vil videre forstå sannsynlighet for svikt på etterspurt tid når det både refereres til (1) PFD, (2) sikkerhetsutilgjengelighet og (3) sikkerhetstap. Disse begrepene vil dels bli nyttet om hverandre slik det også gjøres i faglitteratur på området.

1.4 Struktur

Kapittel 2 beskriver metoden for hvordan arbeidet i oppgaven er utført. Operasjonaliseringen som anvendes for å identifisere og validere ulike tilnærminger for å håndtere usikkerhet blir også presentert. Det bemerkes i den anledning som viktig at leser blir introdusert for operasjonaliseringen i en tidlig fase av oppgaven. Leser vil på denne måten kunne ha de ulike usikkerhetskategoriene i underbevisstheten når det teoretiske fundament og de ulike risiko- og usikkerhetsperspektivene dernest blir presentert.

I kapittel 3 blir det teoretiske grunnlaget for oppgaven presentert. Dette inkluderer en kort oversikt over SIL konseptet, og bakenforliggende krav til barrierer og sikkerhetsfunksjoner i sentrale regelverk og standarder. Andre del av kapittelet presenterer det teoretiske fundament som utgjør basisen for diskusjoner omkring usikkerhetsbetraktningene som drøftes i oppgaven.

Tilnærminger for usikkerhetsvurderinger blir nærmere presentert i kapittel 4. Dette innebærer en kort presentasjon av noen velkjente vurderingsteknikker for kvantitative usikkerhetsbetraktninger, herunder sensitivitetsanalyse og betydningsmål. Disse vil bli nærmere betraktet i kapittel 8, men presenteres tidlig i oppgaven for å være tilknyttet øvrige deler av det teoretiske fundament.

Formålet med kapittel 5 er å gi en enkelt og konkret beskrivelse av de mest relevante aspektene knyttet til kvantifiseringen av sikkerhetsutilgjengelighet som benyttes i de to metodene, IEC 61508 og PDS. Ulikhetene dem i mellom vil bli forsøkt illustrert gjennom komparasjon.

Kapittel 6 presenterer resultater fra systemanalyse av en case. Appendiks B inneholder kalkulasjonene og en nærmere systembeskrivelse, mens kapittelet presenterer generelle observasjoner og resultater etter anvendelse av metodene.

I kapittel 7 blir det drøftet hvordan de underliggende faktorene og ulikhetene kan påvirke nivået av usikkerhet i metodenes utilgjengelighetskalkulasjoner, herunder PFD prediksjoner. Dette vil bli gjort med utgangspunkt i operasjonaliseringen av usikkerhet, og i relasjon til oppgavens teoretiske fundament.

For å møte utfordringer i tilknytning til IEC 61508 og PDS metoden, så er det i kapittel 8 utviklet en alternativ metodisk tilnærming for å kvantifisere de aktuelle usikkerheter som foreligger, og effektivt implementere disse i kalkulasjoner av sikkerhetsutilgjengelighet. De ulike sekvensene i den alternative metodiske tilnærmingen er illustrert med utgangspunkt i en systemanalyse av caset som presenteres i appendiks B.

Konklusjonene fra oppgaven blir deretter presentert i kapittel 9.

2 Metode

For å kunne svare på oppgavens problemstilling er det nødvendig med kunnskap og innsikt, der det legges opp en strategi rundt vurdering og analyse for å kunne besvare de aktuelle forhold på en best mulig måte. En del av denne strategien går ut på å avgjøre hvilke metoder oppgaven skal benytte for å besvare problemstillingen. Metode blir i denne oppgaven brukt om fremgangsmåte for innsamling, gjennomgang og analyse av problemstillingen.

2.1 Datainnsamling og valg av metode

Det finnes en rekke metoder for å samle inn data, der majoriteten av disse blir kategorisert som kvalitative eller kvantitative. I denne oppgaven vil det sentrale fokus ligge innenfor metoder for kvantitative undersøkelser av systempålitelighet, med innslag av kvalitative aspekt og vurderinger. Således vil oppgaven nytte metodetriangulering som karakteriser en kombinasjon av både kvantitative og kvalitative aspekt. Denne fremgangsmåten innebærer liten grad av formalisering, er fleksibel og gjør at undersøkelsesopplegget til dels har blitt tilpasset underveis. Oppgaven har videre en induktiv tilnærming, der rapporter og standarder som omhandler metodene, IEC 61508 og PDS, har dannet datagrunnlag for en litteraturstudie (dokumentanalyse/innholdsanalyse) og vært det empiriske utgangspunktet for analyse av problemstillingen. En litteraturstudie er i denne oppgaven relatert til å systematisk søke og sammenfatte litteratur som er knyttet til problemstillingen.

Gjennom dialog med Gassco ble det besluttet at ulikheter i metodene skulle illustreres i en enkel systemanalyse av en case, for så å diskutere resultatene. Valget av denne tilnærmingen var basert på antakelsen om at nødvendig informasjon og innsikt best ble oppnådd og illustrert gjennom en kort praktisk illustrasjon med påfølgende diskusjon.

2.1.1 Systemanalysen av caset

Systemanalysen av caset ble gjennomført med relevant datamateriale, men som på grunn av konfidensialitetsbegrensninger ikke er direkte tilknyttet angitt system. Som det understrekes i systemanalysen, kunne ikke faktiske feildata for det analyserte systemet inkluderes i oppgaven. Tilgang ble videre gitt til nødvendig informasjon om systemet. Gjennom

deltakelse på møter, og ved kontinuerlig dialog med Gassco, var det således mulig å få en rask forståelse av systemet og datamaterialet som anvendes.

Det ble gjennomført to kalkulasjoner med utgangspunkt i de to metodene, IEC 61508 og PDS. En kalkulasjon med utgangspunkt i grunndata fra systemet, og en kalkulasjon med utgangspunkt i oppdaterte applikasjons- og anleggsspesifikke data. Gjennom analysen ble førstehånds erfaring ved bruk av de ulike metodene oppnådd, og det var mulig å gjøre en komparasjon der det ble hentet ut informasjon om hvordan de ulike metodene resulterte i ulike prediksjoner, usikkerhetsvurderinger og betraktninger for sannsynlighet for svikt på etterspurt tid (PFD).

2.2 Operasjonalisering av usikkerhet

Med utgangspunkt i oppgavens problemstilling har det vært nødvendig å få frem ulikheter for å kunne identifisere og validere ulike tilnærminger for å håndtere usikkerhet ved kvantifisering av systempålitelighet. Det har i oppgaven derfor blitt valgt å operasjonalisere[3] og relatere usikkerhet i metodene til styrker og svakheter i:

- Modellen: modellen kan beskrives som analysens forsøk på å representere systemet (Parry, 1996), altså i hvilken grad metodene er i stand til å fange opp vesentlige faktorer i systemet, inkludert dets operasjonelle forhold. I praksis må ofte flere motstridende interesser balanseres, blant annet at:
    - den metodiske tilnærmingen bør være tilstrekkelig enkel og håndterlig
    - den metodiske tilnærmingen skal være tilstrekkelig realistisk slik at resultatene er av praktisk relevans

- Fullstendighet: en annen kilde til usikkerhet er ufullstendighet i vurderinger. Denne usikkerheten er enten kjent men ikke inkludert i vurderingene, eller ukjent og ikke inkludert i vurderingene (Drouin, et al., 2009). Fullstendigheten i vurderingene er videre sterkt knyttet til faktorer som representerer modellen.
    - Kjent usikkerhet kan være som følger av unnlatelse av faktor som for eksempel ulike feilmodi

[3] Operasjonaliseringen er relatert til forventede ulikheter, styrker og svakheter i metodene. Data om mulige påvirkningsvariabler er samlet fra flere kilder, blant annet: (Drouin, et al., 2009; Stein Hauge, Lundteigen, Hokstad, & Håbrekke, 2010; IEC61508, 1998; Janbu, 2009; Lundteigen, 2009; OLF-070, 2004)

  - Ukjent usikkerhet rundt fullstendighet kan skyldes manglende måter å håndtere effekter, som for eksempel effekter fra menneskelige og organisatoriske faktorer og/eller feilmekanismer.

- Inndata (input) til analysen: I hvilken grad dataene er relevante for å fange opp fremtidige resultater/hendelser?
  - Bruk av pålitelighetsdata er vanligvis basert på enkelte forutsetninger i den statistiske modellen. Dette kan være standard forutsetninger som for eksempel konstant feilrate og lignende
  - Historiske data er ikke det samme som fremtidige data, selv for samme komponent. De historiske dataene er gjerne basert på ulike forsøk under ulike driftsforhold, og i enkelte tilfeller ulike egenskaper
  - Inndata kan være ufullstendig som følger av få testobservasjoner, feil testing eller ved å ikke inkludere alle feiltyper i kalkulasjonene

Overnevnte kategorier kan ikke betraktes som gjensidig utelukkende, der ulike forhold vil kunne være representert ved flere faktorer. Styrker og svakheter i overnevnte punkter kan videre bidra til å gi uttrykk for hvilken av de to metodene som justerer, håndterer og tar høyde for usikkerhet ved å relatere og reflektere systemet i lokale operasjonelle forhold og dets omgivelser.

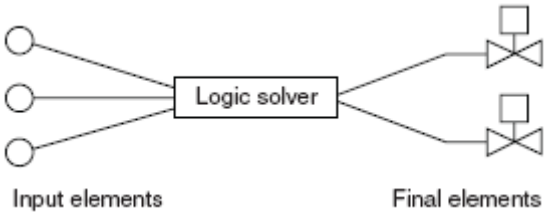
3 Teori og relevante bestemmelser

Dette kapittelet retter oppmerksomhet mot SIS, IEC-standardene og tilhørende SIL krav. Hensikten er å gi en kort oversikt over SIL konseptet, og bakenforliggende krav til barrierer og sikkerhetsfunksjoner i sentralt regelverk og standarder.

Andre del av kapittelet inneholder det teoretiske fundament som utgjør basisen for diskusjoner omkring usikkerhetsbetraktningene i metodene som drøftes i oppgaven.

3.1 Sikkerhetsinstrumenterte systemer (SIS)

Vår sikkerhet blir i økende grad håndtert av instrumenterte sikkerhetssystemer (SIS) der elektriske, elektroniske og/eller programmerbare elektroniske komponenter (E/E/PE) i sikkerhetssystemer samhandler med mekaniske, pneumatiske og/eller hydrauliske systemer. SIS er som tidligere nevnt en fellesbetegnelse for automatiske systemer, som har til formål å detektere potensielt faglige situasjoner ved å bringe systemer eller komponenter til en sikker tilstand dersom farlige hendelser skulle inntreffe (Lundteigen, 2009). Denne oppgaven vil forstå SIS som et uavhengig sikkerhetssystem som er installert for å redusere risikoen knyttet til driften av landbaserte gass- og prosessanlegg (M. Rausand & Høyland, 2004). Områder, systemer eller utstyr der hvor SIS ivaretar sikkerheten kalles normalt ”equipment under control” (EUC). Et SIS fungerer således som en barriere som har til hensikt å beskytte EUC mot potensielle farlige hendelser som for eksempel for høy eller lavt trykk, temperatur og flytende nivåer. Dersom SIS unnlater å utføre tiltenkt funksjon kan hendelsen utvikle seg til farer og ulykker som utblåsning, eksplosjon og lignende.



Figur 3.1 - Skisse av enkelt instrumentert sikkerhetssystem (SIS) (Lundteigen, 2009)

SIS kan videre deles opp i tre delsystemer slik det er illustrert i figur 3.1; elementer for input, logiske løsninger og sluttelementer. Disse tre delsystemene nyttes for å utføre en

sikkerhetsinstrumentert funksjon (SIF). SIF er en funksjon som er implementert i et SIS, og som er ment å oppnå eller å opprettholde en trygg tilstand med hensyn til en bestemt prosessetterspørsel (M. Rausand & Høyland, 2004). En SIS kan bestå av en eller flere SIFer.

Slik vil det kunne betraktes at SIS har følgende hovedfunksjon (M. Rausand & Høyland, 2004):

1. når et forhåndsdefinert prosessavvik forekommer i utstyr eller i et spesifisert system, skal avviket *bli detektert* (input elements) av SIS *sensorer*, og de nødvendige *handlingselementene* (final elements) aktiveres og oppfyller deres intenderte funksjon
2. SIS skal ikke aktiveres sporadisk uten tilstedeværelse av et forhåndsdefinert prosessavvik i utstyret eller i et spesifisert system

3.2 Krav til barrierer og sikkerhetsfunksjoner

Overordnede krav til barrierer og sikkerhetsfunksjoner (SIS) gis av myndigheter. I Petroleumstilsynets (Ptil) regelverk sies det blant annet at ytelseskrav til sikkerhetsfunksjoner skal etableres (Ptil, 2003), og at data må samles inn og benyttes for å vurdere ytelsen (Ptil, 2001 (a), 2001 (b)). Ptil refererer med dette til IEC-standardene og OLF 070.

IEC-standardene omhandler krav, prinsipper og metoder for sikkerhets- og pålitelighetsvurderinger, og viser på hvilket tidspunkt slike vurderinger skal utføres. Hovedformålet med standardene er å definere en enhetlig tilnærming til sikker og pålitelig SIS design, implementering og drift. Til tross for at enkelte prinsipper, begreper og metoder har vært brukt i tidligere standarder, så representerer IEC 61508 og IEC 61511 en videreutvikling. Standardene tar ikke bare for seg tekniske aspekt, men også arbeidsprosesser, rutiner og verktøy som er nødvendig for å spesifisere, utvikle og vedlikeholde operative SIS (Lundteigen, 2009; Smith & Simpson, 2004).

IEC 61508 (1998) er hovedstandarden for SIS. Standarden er en generisk prestasjonsbasert standard som dekker det meste av de sikkerhetsmessige aspektene omkring SIS. Som sådan, mange av emnene som dekkes av standarden ligger utenfor omfanget i denne oppgaven. Hovedformålet med IEC 61508 er å beskrive en (risikobasert) metodikk for å spesifisere og realisere SIS slik at et akseptabelt nivå av funksjonell sikkerhet oppnås (OLF-070, 2004; SINTEF, 2010). IEC 61511 (2003) er videre spesielt utviklet for prosessindustrien, der

standarden i hovedsak tar utgangspunkt i SIS design med ”velprøvd” utstyr, og henviser til IEC 61508 for nytt utstyr (Lundteigen & Hauge, 2008).

Mens IEC-standardene beskriver en risikobasert tilnærming for å avgjøre SIL krav, angir OLF 070 (2004) minimum SIL krav til de vanligste SIF for olje- og gassinstallasjoner. OLF 070 er retningslinjer som har blitt utviklet av Oljeindustriens Landsforening (OLF), der formålet har vært å forenkle implementeringen av IEC-standardene. Retningslinjene dekker likevel ikke en fullbyrdes risikobasert tilnærming slik som IEC 61508. Siden Ptil krever at enhver ny tilnærming til SIS skal være bedre eller lik nåværende praksis, så inkluderer OLF 070 kalkuleringer av PFD for typiske SIF, samtidig som den foreslår korresponderende SIL-nivå som minimum SIL krav. Den underliggende forutsetningen er at SIF er i henhold til kravene i ISO 13702 (1999) og ISO 10418 (2003) (Lundteigen, 2009).

For å beskrive ønsket ytelse for sikkerhet og pålitelighet, kreves det videre en kvantitativ og en kvalitativ pålitelighetsvurdering for å oppfylle de kravene som er gitt i IEC-standardene. Det foreligger to typer av sikkerhetskrav (Lundteigen, 2009):

- Funksjonelle sikkerhetskrav som beskriver hva sikkerhetsfunksjonen skal utføre
- Krav til sikkerhetsintegritet som beskriver hvor godt sikkerhetsfunksjonen skal utføre funksjonen

3.2.1 Sikkerhetsintegritet

Sikkerhetsintgritet er et fundamentalt begrep i IEC-standardene, og er definert som *”probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period of time”* (IEC61508, 1998). Sikkerhetsintegritet kan med dette tolkes som pålitelighet. Sikkerhetsintegritet deles videre inn i fire nivå krav som kalles Safety Integrity Levels (SIL). En SIL er definert som et *”discret level (one out of a possible four) for specifying the safety integrity requirements of the safety function to be allocated to the E/E/PE safety related systems…”* (IEC61508, 1998). For å dokumentere samsvar med IEC-standardene og gjeldene krav, så må en pålitelighetsanalyse av SIS dokumentere at beregnet sannsynlighet for svikt på etterspurt tid (PFD) tilfredsstiller de kvantitative hardware kravene, som vist i tabell 3.1.

IEC 61508 har ytterligere krav til hardware verifikasjon i tillegg til PFD kravene. Disse kalles arkitektoniske begrensninger og er semi-kvalitative krav som uttrykkes som Safe Failure Fraction (SFF), systemtype A og B, og hardware fault tolerance (HWFT). SFF er brøkdelen av

alle feil som defineres som ”sikre”, der en ”sikker” feil er en feil som ikke gir tap av sikkerhetsfunksjonen eller en feil som umiddelbart oppdages og blir korrigert. Type A systemer er videre systemer med lav kompleksitet, slik at ulike feil og drift under feil forhold kan oppdages. Type B systemer er mer komplekse systemer, typisk programmerbare enheter. For slike systemer er det ikke mulig å oppnå en komplett oversikt over eventuelle feil og konsekvenser av disse. HWFT er videre antallet feil som tolereres før sikkerhetsfunksjonen ikke lenger fungerer. For eksempel vil et en ut av tre system (1oo3) kun trenge en av komponentene for å fortsatt fungere som en sikkerhetsbarriere. Således er systemets toleranse for feil før sikkerhetsfunksjonen bortfaller lik 2 (HWFT = 2).

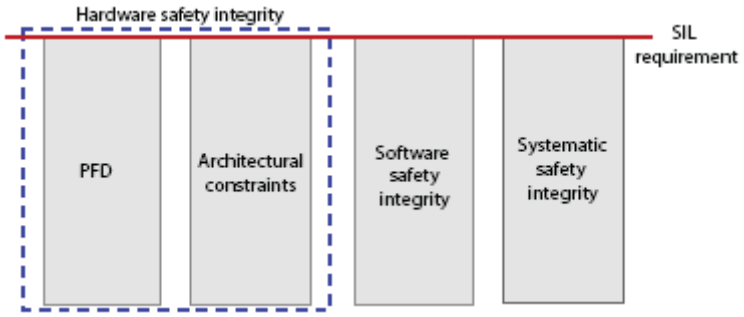
Tabell 3.1 - SIL nivå for sikkerhetsfunksjoner (IEC 61508, 1998)

Safety Integrity Level	**Low Demand Mode of Operation** *(average probability of failure to perform its design function on demand – PFD)*	**Continuous / High Demand Mode of Operation** *(probability of a dangerous failure per hour - PFH)*
SIL 4	$\geq 10^{-5}$ til $< 10^{-4}$	$\geq 10^{-9}$ til $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ til $< 10^{-3}$	$\geq 10^{-8}$ til $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ til $< 10^{-2}$	$\geq 10^{-7}$ til $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ til $< 10^{-1}$	$\geq 10^{-6}$ til $< 10^{-5}$

Tabell 3.1 viser krav til hardware PFD verifikasjon, der SIL 1 er minst og SIL 4 er det mest pålitelige nivået. IEC 61508 metoden, PDS metoden og OLF 070 bruker sannsynligheten for svikt på etterspurt tid (PFD) for et SIS som opererer på forespørsel, og sannsynligheten for en farlig feil per time (Probability of a dangerous Failure per Hour – PFH) for SIS som driftes kontinuerlig (Lundteigen, 2009). Begge disse sannsynlighetene refererer til sikkerhetsutilgjengeligheten i SIS. PFD nivået for en SIL 2 sikkerhetsfunksjon er for eksempel $1x10^{-3}$ og $1x10^{-2}$. Dette betyr at en SIL 2 sikkerhetsfunksjon må utføre sin tiltenkte funksjon i (minst) 99 av 100 tilfeller. De spesifikke nivåene av PFD er relatert til feilraten for farlige feil per time. Mer informasjon om feilrater i de ulike metodene er presentert i kapittel 5.

I tillegg til hardware kravene, så må det vises overensstemmelse med software- og systematiske sikkerhetskrav. Software kravene er kvalitative krav som uttrykker nivået av funksjonell sikkerhet og kvalitetssikringsprogram som kreves for software utvikling, testing og integrasjon. Dette innebærer teknikker for å unngå og kontrollere systematiske feil i softwaren. Unngåelse og kontroll er også hovedfokus i de kvalitative kravene for systematisk

sikkerhetsintegritet. Krav til systematisk sikkerhetsintegritet, tilsvarende krav til software sikkerhetsintegritet, uttrykkes i form av tilstrekkelighet i håndtering av funksjonell sikkerhet og nødvendig kvalitetskontroll.



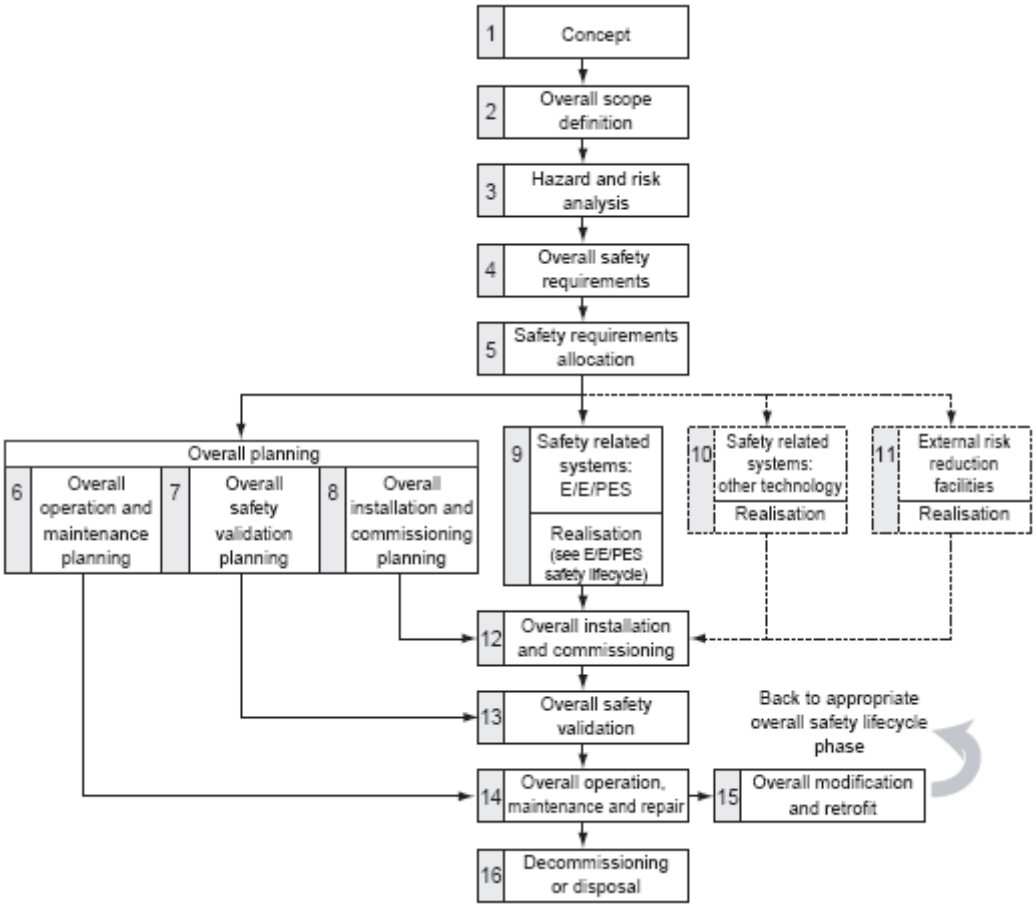
Figur 3.2 - Illustrasjon av kategorier for sikkerhetsintegritet og SIL (Lundteigen, 2009)

I IEC 61508 metoden er verifisering av tilstrekkelig hardware sikkerhetsintegritet en tostegs prosess: det er først nødvendig å beregne pålideligheten til SIF og sammenligne resultatet med SIL krav. For det andre er det nødvendig å beslutte de designmessige begrensningene. Systematisk sikkerhetsintegritet og software sikkerhetsintegritet blir som nevnt her håndtert ved kvalitative kravspesifikasjoner (Lundteigen, 2009). PDS metoden verifiserer også tilstrekkelig sikkerhetsintegritet gjennom samme prosess som IEC 61508 metoden, men i motsetning til IEC 61508 metoden, så forsøker PDS metoden også å kvantifisere de systematiske feilene. Dette er nærmere diskutert i senere kapitler av oppgaven.

3.2.2 Safety Lifecycle modellen

I tilnærmingen til å ta opp en fyllbyrdes sikkerhetsrelatert tilnærming fra sensor til aktuator, med tekniske så vel som ledelsesaspekt, beskriver IEC 61508 en livssyklusmodell for sikkerhet. Modellen kan betraktes som en instrumentell modell for sikkerhetsplanlegging og iverksettelse i ulike livssykluser for sikkerhet, og består av 16 faser som er illustrert i figur 3.3. Hver og en av disse fasene er nærmere beskrevet i IEC 61508-1, 7 (1998). Grovt sett kan fasene videre deles inn i tre ulike grupper:

- Fase 1-5: Analyse
- Fase 6-13: Realisering
- Fase 14-16: Drift



Figur 3.3 - Safety Lifecycle modell (IEC 61508-1, 1998)

3.2.2.1 Analyse

Etter betraktning av funksjoner og utstyr under kontroll (EUC), samt dets miljø, definerer en funksjonell sikkerhetsplan ansvar, organisasjon og planlegging for utvikling av SIS. Fare- og risikoanalyser gjennomføres deretter for å identifisere nødvendige sikkerhetsfunksjoner for å ivareta og kontrollere risikoene i tilknytning til EUC. Derfor sier man at IEC 61508 standarden er en risikobasert tilnærming. De overordnede sikkerhetskravene defineres og dokumenteres i en sikkerhetsmessig kravspesifikasjonsrapport (Safety Requirement Specification – SRS) (Janbu, 2009).

3.2.2.2 Realisering

En etterlevelsesanalyse blir deretter gjennomført i starten av realisasjonsfasen, der pålitelighetskalkulasjoner av sikkerhetsfunksjoner (SIF) blir gjennomført for å evaluere om

kravene fra SRS rapporten ivaretas (Janbu, 2009). På dette tidspunktet har akkurat detaljert design startet, og dataene som er tilgjengelige for pålitelighetsvurderinger varierer mye. OLF 070 anbefaler bruk av generiske data for etterlevelsesanalyser, men dette eksisterer ikke alltid ettersom man for eksempel ved ny teknologi mangler driftsdata for systemene.

Under realisering oppdateres design med tilgjengelig leverandørdata og mer spesifikke krav fra SRS. En funksjonell sikkerhetsvurdering (Functional Safety Assessment – FSA) skal deretter gjennomføres for å verifisere hardware, software og integrert system mot spesifiserte krav. Deretter gjennomføres installasjon og igangkjøring etter forhåndsdefinerte planer. En samlet validering blir deretter utført før systemet settes i drift (verifikasjonsanalyse/-rapport).

3.2.2.3 Drift

Drift bør utføres i henhold til definerte planer. Denne fasen betraktes i IEC-standardene å være veldig viktig for å samle inn feltdata. Det betraktes i livssyklusene for drift at disse dataene kan benyttes som inndata til generiske databaser, men også som inndata for å verifisere at SIS møter definerte SIL krav. Eventuelle nødvendige modifikasjoner gjennomføres, før systemet vender tilbake til relevante faser i livssyklusen frem til systemet er ute av drift. Prosessen for å verifisere at SIS møter de spesifiserte kravene (SIL nivå) skal videre følge gjentakende evalueringer så lenge systemet er i drift.

3.2.2.4 Usikkerhet knyttet til livssyklusmodellen

Et viktig moment knyttet til pålitelighetsvurderinger er analytikernes kunnskap om systemets egenskaper, noe som er spesielt sårbart i tidlige faser av livssyklusen og ved nyutvikling av teknologi. I tidlige faser er det nødvendig å betrakte ulike scenario, konsekvenser og datatilhørighet. Enkelte karakteristikker i systemene, som for eksempel skjulte feil, trenger ikke alltid å bli avdekket og betraktet i slike faser. Dette øker usikkerheten som følger av ufullstendighet i betraktninger, og kan lede til ukonservative data som tas med i videre analyser. Analysene må også betrakte og forstå systemets atferd for å kunne vurdere dette ut fra best mulig egnet modell, og således redusere usikkerhet knyttet til modellen.

Usikkerhet i tilknytning til inndata for vurderinger er særlig stor i tidlige faser av livssykluser, der disse blir oppdatert etter hvert som nye generiske data samles inn. SIS blir videre testet av leverandører for å kunne kompensere med data i forhold til lave feilfrekvenser. Det kan

videre være stor usikkerhet knyttet til disse dataene på grunn av unaturlige testforhold. De beste generiske dataene oppnås når SIS blir plassert og driftet i feltmiljøet hvor det skal driftes. Bayesiansk oppdatering er velegnet for å implementere nye data i forhold til allerede eksisterende generiske data som er forbundet med stor usikkerhet. Oppdateringen kan derfor redusere usikkerheten til tross for manglende data, der ekspertvurderinger i slike tilfeller bør nyttes (Janbu, 2009).

3.2.3 Usikkerhet i relasjon til detaljkrav og akseptkriterier

Det er videre viktig å påpeke at dersom et angitt SIL krav skal ha mening, så må dette ikke alene forstås som et skarpt skille på aksept og/eller ikke aksept. Om analyseberegningene for et alternativ gir et bestemt PFD som er like utenfor SIL kravene så er ikke alltid dette alene av betydning – man kan avhengig av situasjonen likevel akseptere dette nivået. Det interessante er i større grad hvordan denne kalkulasjonen, kontra alternative kalkulasjoner med alternative parametre, kommer ut i forhold til hverandre både når det gjelder pålitelighet og risiko. Samlet sett kan en vurdere sikkerheten som fullt ut forsvarlig, til tross for at sikkerhetsutilgjengeligheten for systemet ligger like utenfor akseptkriteriene. Dette kan begrunnes i at usikkerheten i kalkulasjonene av sikkerhetsutilgjengeligheten kan være minimal, men at prediksjonen likevel ligger rett utenfor akseptkriteriet for systemet – og da bør aksepteres. Som en motsetning til dette, så kan et system i forhold til akseptkriteriene bli godkjent til tross for at det er skyhøy usikkerhet i underliggende prediksjoner og tidligere observasjoner. Som nevnt så må det vises varsomhet ved bruk av disse kravene, der et for sterkt fokus på krav kan begrense kreativiteten og driven for å finne frem til totalt sett bedre løsninger og tiltak (Aven, 2007). Bruken av akseptkriterier under SIL verifikasjon kan betraktes som et stort felt som alene ville kunne utgjøre en masteroppgave, og vil ikke bli nærmere drøftet i denne oppgaven. Det er likevel viktig å ta med seg den underliggende prinsipielle forståelsen om at en predikert sannsynlighet for svikt på etterspurt tid (PFD) ikke alene trenger å være tilstrekkelig for å anse godheten av systemet – dette må også betraktes ut i fra grad av usikkerhet knyttet til angitt prediksjon.

3.3 Risiko- og usikkerhetsperspektiver

Risiko omhandler hendelser (A), og fremtidige konsekvenser (C) av disse hendelsene. Det er ikke mulig å direkte fastslå om disse hendelsene vil inntreffe eller ikke, og eventuelle

konsekvenser dersom det skulle inntreffe. Det er med andre ord usikkerhet (U) knyttet til både hendelser (A) og konsekvenser (C). Hvor trolig det er at en hendelse med en spesifikk konsekvens vil inntreffe kan uttrykkes ved hjelp av sannsynligheter (P), fortrinnsvis med basis i gitt kunnskap[4] (bakgrunnskunnskap) (K) (Aven, Røed, & Wiencke, 2008).

Med bakgrunn i dette kan "risiko beskrives ved (C, C*, U, P, K), der C er mulige konsekvenser (inkludert initierende hendelser A), C* er prediksjoner av C, U er usikkerheten knyttet til hva C kommer til å være, P er våre sannsynligheter for C, gitt bakgrunnskunnskapen K" (Aven, 2008b; Aven, et al., 2008).

Det er videre viktig å betrakte hvordan usikkerhet knyttet til fremtidige hendelser og konsekvenser av disse skal forstås. Usikkerhet ble i delkapittel 2.2 operasjonalisert og kategorisert for å kunne evaluere ulike bidrag fra modell-, fullstendighet- og datausikkerhet. Disse kan videre betraktes og forstås ut i fra to hovedtyper av usikkerhet, aleatorisk usikkerhet og epistemisk usikkerhet (Parry, 1996).

Aleatorisk usikkerhet representerer den iboende og naturlige usikkerheten som er knyttet til et system eller en prosess. Det er for eksempel umulig å predikere eksakt hvor mange tilfeller et SIS vil mislykkes i å respondere. Dette skyldes blant annet variasjon i systemet som ikke kan elimineres på grunn av iboende tilfeldigheter som forårsaker hendelser med stokastiske egenskaper (Janbu, 2009). Dette er grunnen til at aleatorisk usikkerhet også ofte refereres til som "stokastisk usikkerhet" (Mosleh, Siu, Smidts, & Lui, 1995).

Noen hendelser i prosesser og systemer er likevel til en viss grad forutsigbare. Våre prediksjoner er basert på vår kunnskap omkring fenomenet på et gitt tidspunkt. Hvis det foreligger kunnskap om hvordan et bestemt fenomen forårsakes, er det enklere å predikere utfallet. For å kunne predikere må man således ha en metodisk modell. Egenskapene som definerer modellen, slik som parametre og initierende hendelser, er basert på tilgjengelig kunnskap. Usikkerhet oppstår fra begrensninger knyttet til å nøyaktig vurdere ulike egenskaper, altså den bakenforliggende kunnskapen. Denne typen usikkerhet refereres ofte til som *epistemisk* usikkerhet, og kan defineres som manglende kunnskap om ytelse i et system (Aven, 2003). I motsetning til aleatorisk usikkerhet, så kan epistemisk usikkerhet reduseres ved å samle mer informasjon samt øke kunnskap om underliggende forhold.

Usikkerhet kan som nevnt ovenfor defineres som manglende kunnskap om forhold knyttet til et system. Pålitelighetsanalyser uttrykker videre usikkerheten knyttet til fremtidige hendelser, ofte i tilknytning til sannsynligheter. Et sannsynlighetsuttrykk er med dette en

[4] Kunnskap vil i denne oppgaven være relatert til grad av tro

bekjennelse av manglende kunnskap, fordi den uttrykker usikkerheten knyttet til den ukjente hendelsen (Janbu, 2009).

Det foreligger videre flere teoretiske sannsynlighetsperspektiver, der fortolkningen av disse vil være avhengig av hvilket syn og bakenforliggende perspektiv som ligger til grunn. Oppgaven deler disse sannsynlighetsperspektivene inn etter realistfortolkning og subjektiv fortolkning.

3.3.1 Realistfortolkning

I pålitelighetsanalyser er det vanlig å uttrykke feilrater og PFD som karakteristikker for systemet det tas utgangspunkt i. Dette er i følge realistfortolkningen, som betrakter sannsynlighet som et mål på egenskaper, akkurat lik enhver annen fysisk egenskap (Watson, 1993). Ulike lover, reguleringer og standarder, inkludert IEC-standardene, er likevel godt egnet til denne fortolkningen av sannsynligheter. For eksempel så må det for et spesifikt SIS kunne vises at sannsynligheten for å forvente en farlig uoppdaget feil er mindre eller lik et gitt SIL nivå, for at man skal ligge innenfor gjeldende risikoakseptkriterier og således samsvare med kravene i IEC-standardene og OLF 070. En slik fortolkning gir likevel ingen mening dersom påliteligheten ikke antas å være et ”tenkt objektivt” mål på egenskapene i verden (Janbu, 2009). Denne fortolkningen er problematisk og samtidig i konflikt med kunnskap ut over det som ville vært antatt som målbart, slik som for eksempel lokale driftsforhold og ekspertvurderinger. Det foreligger likevel tre kjente perspektiver innenfor en realistfortolkning: det klassiske perspektivet, relativ frekvens perspektivet og apriori perspektivet. Som en samlebetegnelse for de tre perspektivene vil oppgaven i tillegg til å benytte realistfortolkning referere til disse som et klassisk sannsynlighetsperspektiv, noe som også er mye benyttet innenfor fagmiljøet i risiko- og pålitelighetsanalyse.

3.3.1.1 Klassisk sannsynlighetsperspektiv

Den klassiske sannsynlighetsfortolkningen er den eldste fortolkningen med opprinnelse fra sannsynligheter i sjansespill (Bedford & Cooke, 2001). Perspektivet er basert på antakelsen om at alle sannsynligheter er like, noe som vil kunne være egnet for spillsituasjoner som for eksempel å trille en terning. Det klassiske perspektivet er dermed mindre overbevisende i forhold til pålitelighetsanalyser, hvor sannsynligheten for en eller null feil innenfor et tidsintervall ikke nødvendigvis vil være like sannsynlig.

3.3.1.2 Relativ frekvens sannsynlighetsperspektiv

Relativ frekvens perspektivet definerer sannsynligheten for en hendelse som andelen av ganger en hendelse inntreffer i en tenkt uendelig populasjon av observasjoner gjort under identiske forhold. I relativ frekvens fortolkningen antas det gjerne at det finnes "objektive" sannsynligheter som kommer til uttrykk ved gjentatte forsøk og observasjoner. Dette er derimot problematisk, spesielt for systemer der hvor feil sjelden oppstår (slik som SIS). Sannsynligheten avhenger videre av den kunnskap og de forutsetninger som gjøres, der påliteligheten som fremkommer er basert på en vurdering som er utført av noen med basis i en viss kunnskap, og således ikke er "objektiv" (Aven, 2007).

3.3.1.3 A priori sannsynlighetsperspektiv

Som en parallell til utviklingen av relativ frekvens perspektivet ble det utviklet et a priori perspektiv som også integrerer den andre fortolkningen av sannsynlighet; grad av tro (Watson, 1993). I dette perspektivet så viser a priori kunnskap til tidligere kunnskap om et forhold, snarere enn å anslå de siste observasjoner samt å predikere fremtiden. A priori betraktes i enkelte tilfeller å være både "objektiv" og subjektiv; "objektiv "i den forstand at a priori kunnskap skal være basert på tilgjengelige data og ikke egne betraktninger, men også subjektiv siden evalueringen er basert på betraktninger om tidligere observasjoner (Janbu, 2009). A priori kunnskap er derfor å betrakte som grensen mellom frekventist og den Bayesianske tilnærmingen til statistikk.

3.3.2 Subjektiv fortolkning

Den subjektive fortolkningen av sannsynlighet definerer sannsynlighet som grad av tro. Av dette følger det at usikkerheten som er forbundet med den subjektive sannsynligheten er ren epistemisk på grunnlag av å være kunnskapsbasert. Subjektive sannsynligheter er i praksis ofte benyttet i kombinasjon med andre tilnærminger der det foreligger manglende datakvalitet. Bayesiansk oppdatering som er basert på ekspertvurderinger er et eksempel på det. I oppgaven vil det også vises til den subjektive fortolkningen når det refereres til et Bayesiansk perspektiv.

3.3.2.1 Prediktivt epistemisk sannsynlighetsperspektiv

Den prediktive epistemiske tilnærmingen er en fullbyrdes subjektiv tilnærming til risiko og risikovurderinger og definerer sannsynligheter som et mål på usikkerhet. I motsetning til realistfortolkninger hvor fokus er innenfor estimering av "objektive" statistiske faktorer, slik som PFD og feilrater, så fokuserer det prediktive epistemiske perspektivet på å predikere observerbare mengder (Aven, 2007). De observerbare mengdene og faktorene er fenomener som gjerne er ukjente på vurderingstidspunktet, men som oppstår (eller kan forekomme) i fremtiden. Eksempler på dette kan være feil på etterspørsel (failure on demand) og antall dødsfall. I dette perspektivet er det således bortkastet tid å betrakte usikkerhet i statistiske mengder slik som PFD, der usikkerheten antas å være rent epistemisk. Det vil si at perspektivet betrakter usikkerhet å kun oppstå som følger av begrensninger relatert til å forutsi (predikere) fremtidige hendelser (Janbu, 2009). Perspektivet vurderer med dette sannsynlighet som et subjektivt mål på usikkerhet om hendelser og utfall (konsekvenser), vurdert og basert på tidligere bakgrunnsinformasjon og kunnskap (betinget av bakgrunnsinformasjonen) (Aven, 2008a).

3.3.3 Oppsummerende betraktninger

Bruken av frekvens som et mål på sannsynlighet har blitt kritisert med det argument at det kan være farlig å feste sin tillit til tidligere frekvenser for å forutse fremtidige hendelser. Realistfortolkningen er imidlertid den vanligste måten å betrakte sannsynlighets- og pålitelighetsvurderinger. Den anses av enkelte som "objektiv" og således også "ukontroversiell" som grunnlag for beslutninger. Men den er også i konflikt med en viktig del av pålitelighetsvurderingene, nemlig den subjektive fortolkningen og således bruken av ekspertvurderinger. Behovet for "objektiv" tolkning av resultatene er å forstå som en sannsynlighet som er rent statistisk basert på stokastiske lover og sjanseprosesser (Janbu, 2009). Men som et resultat av de "objektive" vurderingenes manglende inkludering av kunnskap, så oppstår behovet for epistemologisk tolkning. I denne oppgaven vil sannsynlighet bli definert som *grad av tro* som er i stor kontrast til det "objektive" synet (Watson, 1993).

4 Tilnærminger for usikkerhetsvurderinger

Risiko- og pålitelighetsanalyser vil til en viss grad involvere usikkerheter som følger av vurderingsprosessene som foreligger. Usikkerhetsvurderinger kan derfor være nyttig når kritiske beslutninger rundt verifisering av sikkerhetsintegritet blir tatt under stor usikkerhet. Dette kapittelet presenterer med dette noen velkjente vurderingsteknikker for kvantitative usikkerhetsbetraktninger.

Hovedforskjellen mellom en pålitelighetsvurdering og en usikkerhetsvurdering er at pålitelighetsvurderinger uttrykker aleatorisk usikkerhet omkring fremtidig atferd i systemer, mens usikkerhetsvurderinger hovedsakelig uttrykker epistemisk usikkerhet knyttet til informasjon (utdata i modell) som uttrykkes i pålitelighetsparametrene (Janbu, 2009). Det vil si usikkerheten knyttet til prediksjon.

Det foreligger en rekke tilnærminger for å vurdere og håndtere usikkerhet knyttet til ulike typer av analyser. I denne oppgaven har det blitt tatt utgangspunkt i to teknikker for å analysere effekten av usikre inndata på modellens utdata:

- Sensitivitetsanalyse: metode for å analysere hvordan usikkerhet (variasjon) i utdata kan relateres til ulike kilder av variasjon i modellens inndata
- Betydningsmål (sensitivitetskoeffisienter): metode som benyttes for å identifisere den (de) dominante bidragene til feil i et system

Disse metodene kan nyttes for å beskrive usikkerhet knyttet til inndata for analysen, men også modellusikkerhet ved å endre ulike forutsetninger og antakelser for å se hvordan dette påvirker nivået av usikkerhet. Usikkerhet knyttet til ufullstendighet kan videre beskrives gjennom sensitivitetsanalyser eller konservative tilnærminger, der modell og/eller inndata oppdateres.

4.1 Sensitivitetsanalyser

Sensitivitetsvurderinger som benyttes i pålitelighetsanalyser beskriver hvor sensitiv påliteligheten er for endringer i inndata for ulike parametre eller modellantakelser for systemet. Slike analyser utføres for å hente informasjon om (NASA, 2002):

- Indikasjon på grad av respons i pålitelighet som følger av en endring i ulike parametre av inndata, og således hvilket inndata parameter som er mest sensitivt
- Identifisering av hvilke komponenter der datakvaliteten er sensitiv eller ikke for analysen

Dersom endringen i utdata, altså PFD estimatet, er stort i forhold til endringen i inndata, så sies det at systemet er sensitivt til inndata parameteren som ble endret (Janbu, 2009). Det er videre viktig å bemerke at sensitivitetsanalyser ikke beskriver nivået av usikkerhet i relasjon til usikre inndata, kun effekten av endringer (sensitivitet). Parametre med høy sensitivitet trenger derfor ikke å være assosiert med høy grad av usikkerhet. Men usikre inndata som betraktes å ha stor innvirkning på resultatene anses likevel ofte å være tilknyttet et tilsvarende nivå av usikkerhet. I tilknytning til sistnevnte, er det da i stor grad parametre med stor sensitivitet som blir videre betraktet i ulike usikkerhetsvurderinger. Parametre med lav sensitivitet betraktes ofte som ikke vesentlige fordi disse ikke forventes å utgjøre signifikante endringer i utdata. Det er videre viktig å bemerke at dersom en faktor for en komponent har en sikker verdi, så spiller ikke systemets sensitivitet ovenfor denne faktoren noen rolle.

4.2 Betydningsmål

En sensitivitetsanalyse gir informasjon om hvordan variasjoner i pålitelighet kan forekomme som følger av endringer i relasjon til inndata fra komponenter i ulike modeller. Noen komponenter i systemer er likevel av større betydning for systempåliteligheten enn andre komponenter. Om det tas utgangspunkt i for eksempel to komponenter som modelleres i en parallellstruktur, så er levetiden til systemet lik levetiden til den komponenten med lengste levetid. Om de to komponentene derimot modellers i en seriestruktur, så er levetiden til systemet lik levetiden til den komponenten med minst levetid. En seriestruktur kan dermed tenkes å måtte kompenseres med komponenter som har høyere pålitelighet, for å oppnå tilsvarende systempålitelighet som parallellstrukturen. Det er med dette viktig å betrakte komponentenes sensitive betydning med hensyn til både påliteligheten til komponentene (inndata) og systemets struktur (modell) for å ivareta en funksjon, og samtidig forstå at like komponenter kan ha ulik betydning avhengig av struktur (Janbu, 2009).

I større og mer komplekse systemer kan det være vanskelig å forstå betydningen av ulike komponenter uten å foreta en videre analyse. Det er derfor ofte av stor interesse å rangere komponenter med hensyn til enkelte kvantitative følsomhetskoeffisienter kalt

betydningsmål. De ulike betydningsmålene kan benyttes for å rangere de relative verdiene for komponentene med hensyn til forbedringspotensial, bidrag til utilgjengelighet og betydning for systemets funksjon. Informasjonen som hentes inn etter rangeringsprosessen kan med dette brukes til å endre design, sette opp redundans, redusere risikoer, beslutninger om ressurstildeling, justering/betinging av parametre, osv. I det følgende vil det bli presentert to kvantitative betydningsmål, der disse vil bli nærmere diskutert i delkapitel 8.2.1.

4.2.1 Birnbaum's betydningsmål (Birnbaum's measure)

Birnbaum's betydningsmål beskriver pålitelighetsbetydningen av komponent *i* som (Aven, 2006):

$$I_i^B = \frac{\partial h}{\partial p_i} = h(1_i, p) - h(0_i, p)$$

Man kommer altså frem til Birnbaum's mål ved å partiellderivere systempåliteligheten med hensyn på p_i, der dette kan skrives som differansen mellom systempåliteligheten når komponent *i* betraktes som perfekt ($h(1_i, p)$), til situasjonen der hvor komponenten har feilet ($h(0_i, p)$). Merk at målet kun avhenger av systemets struktur og påliteligheten til de andre komponentene, altså ikke den underliggende påliteligheten til komponent *i*. Dette kan betraktes som en svakhet ved Birnbaum's betydningsmål siden det anses som et viktig mål på den spesifikke komponenten, men likevel er uavhengig av påliteligheten til den aktuelle komponenten som måles (Janbu, 2009).

Dersom I_i^B er stor så vil en liten endring i komponentens pålitelighet medføre en etter måten relativ stor endring i systempåliteligheten (Aven, 2006). En feil i en slik komponent er dermed avgjørende for den totale systempåliteligheten.

4.2.2 Mål for forbedringspotensial (Improvement potential)

Improvement potential er en utvidelse av Birnbaum's betydningsmål, og har sitt navn på bakgrunn av at det er forbedringspotensialet i systempåliteligheten som måles ved å anta at en komponent *i* er en perfekt komponent der p_i=1 (Janbu, 2009). Målet er basert på differansen mellom $h(1_i, p)$ og $h(p)$, og betegnes for en komponent *i* som:

$$I_i^A = h(1_i, p) - h(p)$$

Siden rangering etter dette betydningsmålet gir en indikasjon på hvilke komponenter som er mest vesentlige for å forbedre den totale systempåliteligheten, så kan det dermed også tolkes som hvilken av komponentene det også vil være mest sannsynlig å betrakte dersom en feil skulle oppstå (Janbu, 2009).

4.3 Oppsummerende betraktninger

Det er i mange sammenhenger vanlig å blande de to uttrykkene usikkerhet og sensitivitet, der både usikkerhets- og sensitivitetsanalyser kan vurdere robustheten til studier som er basert på matematisk modellering. Men det bør igjen bemerkes at sensitivitetsanalyser ikke er det samme som usikkerhetsanalyser. Dette kommer av at sensitivitetsanalyser ikke uttrykker usikkerheter i relasjon til usikre parametre, men kun tar utgangspunkt i effekten av disse. Det er derimot mulig, via en sensitivitetsanalyse, å oppnå kunnskap om modellens inndataparametre eller antakelser som kan være avgjørende for nivået av usikkerhet i vurderingene, basert på deres betydning (Janbu, 2009). En sensitivitetsanalyse er således godt egnet som en basis for usikkerhetsanalyser.

Mens sensitivitetsanalyser identifiserer hvilke kilder til usikkerhet som vektes i konklusjoner (utdata), så er usikkerhetsanalyser den eneste teknikken som faktisk beskriver nivået av usikkerhet som er knyttet til denne konklusjonen. Ved å betrakte hvordan det i forrige kapittel ble diskutert å gå frem for å øke påliteligheten, og således redusere risikoen, er det med dette avgjørende å betrakte hvordan de to metodene, IEC 61508 og PDS, går frem for å kalkulere sikkerhetsutilgjengelighet (PFD) og beskrive tilhørende nivå av usikkerhet. Ulike metoder er ulikt egnet for å beskrive ulike kilder til usikkerhet; modell-, fullstendighets-, og inndatausikkerhet. Det er videre diskutert at usikkerhet er knyttet til hendelsen, svikt på etterspurt tid (A), og tilhørende konsekvenser (C). Hvor trolig et utfall knyttet til en spesifikk konsekvens er, vil videre kunne uttrykkes med sannlighet for svikt på etterspurt tid (PFD), fortrinnsvis med basis i gitt kunnskap (K).

5 Påliteligheten til sikkerhetssystemer i perspektiv

Det eksisterer en rekke ytelseskrav for sikkerhet, og IEC 61508 introduserer som kjent PFD for å måle sikkerhetsutilgjengelighet i forhold til hardware feil. PDS metoden introduserer videre ytelse og sikkerhetstap i en større utstrekning enn IEC 61508, ved å blant annet også å ta høyde for parametre som systematiske feil (λ_{DU-S}), Test Independent Failures (TIF) og Downtime Unavailability (DTU), der kvantifisert sikkerhetsutilgjengelighet i PDS metoden betegnes som Critical Safety Unavailability (CSU).

Formålet med dette kapittelet er å gi en kort og konkret beskrivelse av de mest relevante aspektene knyttet til kvantifisering av sikkerhetsutilgjengelighet som benyttes i de to ulike metodene. Kapittelet presenterer de to metodene for pålitelighetsberegninger i SIS på et generelt grunnlag, og vil gjennomgående forsøke å illustrere ulikhetene dem i mellom. IEC 61508 (1998), PDS håndboken (S. Hauge, Hokstad, Langseth, & Øien, 2006) og OLF 070 (2004) vil med dette bli benyttet som primærkilder i kapittelet. Mer detaljert informasjon om de to metodene vil kunne betraktes i overnevnte kilder.

5.1 Testing av sikkerhetsinstrumenterte systemer

Testing og etterfølgende feildeteksjon er avgjørende for å avdekke og eliminere skjulte feil[5] i sikkerhetssystemer (SIS), og for å komme frem til verdier for inndata til de ulike parametrene i metodene. I hovedsak foreligger det to muligheter for feildeteksjon:

- Feildeteksjon ved automatisk selvtest (inkludert operatørobservasjon)
- Feildeteksjon ved funksjonell testing (manuell testing)

5.1.1 Automatisk selvtest

I moderne SIS er ofte en logisk solver (logic solver) programmerbar, og kan utføre diagnostiske selvtester under drift. Den logiske solveren kan sende signaler til detektorer og sluttelementer (final elements), og sammenlikne responsen med forhåndsdefinerte verdier.

[5] Feil for en komponent eller et system vil i denne oppgaven betraktes som å "nå", eller å være i, en tilstand der komponenten eller systemet ikke vil kunne fullføre tiltenkt funksjon (M. Rausand & Høyland, 2004)

Den diagnostiske testingen kan avdekke feil i input og output enheter, og i økende grad, også feil i detektorer og sluttelementer. (M. Rausand & Høyland, 2004) Likevel vil det antakelig ikke være tilfelle at alle feil detekteres automatisk. Merk at den faktiske effekten på systemets ytelse, som følger av en feil som oppdages ved en selvtest, vil være avhengig av systemkonfigurasjonen og hvilke tiltak som iverksettes når feilen er oppdaget.

I tillegg til den automatiske selvtesten, kan operatører eller vedlikeholdspersonell oppdage feil mellom testene. I PDS metoden inkorporeres slike feil i den diagnostiske dekningsfaktoren for feil ved automastisk selvtest.

5.1.2 Funksjonell testing

Siden de automatiske selvtestene ikke kan avsløre alle feil blir de ulike delene av SIS derfor ofte funksjonelt testet. Funksjonelle tester utføres manuelt på forhåndsdefinerte tidsintervaller. Formålet med en funksjonell test er å avdekke skjulte feil, og å kontrollere at systemet (fortsatt) er i stand til å utføre tiltenkt funksjon om en mulig etterspørsel skulle forekomme (S. Hauge, Hokstad, et al., 2006; M. Rausand & Høyland, 2004). Innenfor pålitelighetsanalyse antas det ofte at funksjonstester er ”perfekte” i den forstand at testen klarer å generere en sann etterspørsel, og dermed detekterer alle mulige feil. I virkeligheten kan testingen derimot være imperfekt, og/eller testforholdene kan avvike fra de sanne forholdene som oppstår under etterspørsel, slik at kun enkelte deler av funksjonene testes tilstrekkelig. I PDS tilnærmingen er dette forsøkt tatt hensyn til ved å legge til sannsynligheten for uavhengige testfeil (Test independent failures) i PFD estimatet. Dette er nærmere presentert i delkapittel 5.3.3.

5.2 Parametre i IEC 61508 metoden

5.2.1 Årsaker til feil

Feil kan kategoriseres som årsak til svikt (cause of failure), der IEC 61508 skiller mellom to type av feilkategorier: *tilfeldige hardware feil* og *systematiske feil*. Standarden krever en bekreftelse på at sannsynligheten for svikt er innenfor gjeldende akseptkriterier, noe som for tilfeldige hardware feil gjøres gjennom en kvantitativ analyse. IEC 61508 metoden definerer disse feilene som følger:

Tilfeldige hardware feil er feil som følger av naturlige degraderingsmekanismer i komponenter. For slike feil antas det at systemet er designet i henhold til aktuelle driftsforhold (IEC 61508-4, 1998).

Systematiske feil er feil som kan relateres til bestemte årsaker som ikke skyldes naturlig nedbrytning (aldring). Feilene kan normalt elimineres ved en endring, enten som endring i design eller produksjonsprosessen, de operative prosedyrene eller dokumentasjon (IEC 61508-4, 1998).

I IEC 61508 er omfanget av overnevnte feilkategorier for systematiske feil ikke kvantifisert. Karakteristikken av systematiske feil er her at korrektiv handling uten modifikasjon normalt ikke vil eliminere feilårsaken, og at dette kan induseres ved å simulere feilårsaken. Disse feilene og resulterende systemutilgjengelighet er med dette ikke inkludert i PFD estimatet ved IEC 61508 metoden, men verifiseres kvalitativt ved at det må dokumenteres at de tiltakene som defineres som viktige er blitt kontrollert og tilstrekkelig gjennomgått.

5.2.1.1 Feilklassifisering

IEC 61508 metoden skiller videre mellom farlige og sikre feil, og deler alle (hardware) feil inn i :

- Dangerous (D) – farlige feil som *har* potensial til å bringe sikkerhetssystemet i farlige situasjoner dersom komponentene ikke fungerer tilstrekkelig
    - Dangerous Undetected (DU) – farlige feil som ikke oppdages ved automatiske selvtester
    - Dangerous Detected (DD) – farlige feil som oppdages ved automatiske selvtester
- Safe (S) – sikre feil som *ikke har* potensial til å bringe sikkerhetssystemet i farlige situasjoner dersom komponentene ikke fungerer tilstrekkelig
    - Safe Undetected (SU) – sikre feil som ikke oppdages ved automatiske selvtester
    - Safe Detected (SD) – sikre feil som oppdages ved automatiske selvtester

Basert på denne klassifiseringen deles feilraten, λ, inn i følgende elementer:

λ_{DU} = Raten av farlige udetekterte feil (DU)
λ_{DD} = Raten av farlige detekterte feil (DD)
λ_{D} = Raten av farlige feil (D) - λ_{DU} + λ_{DD}
λ_{SU} = Raten av sikre udetekterte feil (SU)
λ_{SD} = Raten av sikre detekterte feil (SD)
λ_{S} = Raten av sikre feil (S) - λ_{SU} + λ_{SD}

Feilrater kan videre defineres som sannsynligheten for at den faktiske levetiden (T) til en komponent vil ligge innenfor (t, t+δt). Feilraten er med dette den gjennomsnittlige tiden til feil oppstår innenfor dette tidsintervallet, der feilratefunksjonen forteller hvor sannsynlig det er at en komponent som ikke har feilet frem til tiden (t) vil feile i løpet av neste tidsintervall (OREDA, 2009).

Ettersom ulike feildata ofte foreligger i praksis, gjerne samlet som gjennomsnittlig feilrate eller lignende, er det ofte nødvendig å kalkulere og komme frem til de spesifikke feilratene som skal være inndata i metodene. Dette er nærmere illustrert i appendiks B.

5.2.2 Common cause failures (CCF)

Ved kvantifisering av påliteligheten til redundante sikkerhetssystemer, så er det videre viktig å skille mellom *uavhengige* og *avhengige* feil. Tilfeldige hardware feil som forårsakes av naturlige stressfaktorer betraktes som uavhengige feil. Det vil si at feil i en komponent ikke antas å påvirke feil i andre identiske komponenter i sikkerhetssystemet. Alle systematiske feil antas derimot å være potensielle avhengige feil, der feil i en komponent påvirker de andre komponentene. Slike feil kan resultere i simultane feil i mer enn en komponent i sikkerhetssystemet (det vil si Common Cause Failures – CCF), og vil derfor redusere effekten av redundans (S. Hauge, Hokstad, et al., 2006; M. Rausand & Høyland, 2004). CCF er med dette kun relevant for votering og konfigurasjoner bestående av flere komponenter, og vil dermed ikke være inkludert i den generelle tilnærmingsformelen for PFD for en enkelt komponent slik den er illustrert i neste delkapittel, 5.2.3.

Den mest brukte modellen for CCF i SIS er den modellen som benyttes i IEC 61508 metoden, nemlig β-faktor modellen (M. Rausand & Høyland, 2004). I β-faktor modellen antas det at en viss prosentandel av alle feil er CCF som vil medføre svikt i alle komponentene på samme tid

(eller med kort tidsintervall). Feilraten λ_{DU} med hensyn til farlige utilgjengelige feil kan dermed for en komponent skrives som:

$\lambda_{DU} = \lambda_{DU}^{(i)} + \lambda_{DU}^{(c)}$ der

$\lambda_{DU}^{(i)}$ er raten av uavhengige farlige utilgjengelige feil som påvirker en komponent, og $\lambda_{DU}^{(c)}$ er raten av common cause farlige utilgjengelige feil som vil forårsake svikt i alle systemkomponentene til samme tid. CCF faktoren er da ved å vende overnevnte formel, prosentandelen common cause kritisk utilgjengelige feil av alle farlige utilgjengelige feil i en komponent:

$$\beta_{DU} = \frac{\lambda_{DU}^{(C)}}{\lambda_{DU}}$$

I IEC 61508 metoden der β-faktor modellen benyttes, kan β for ulike systemkonfigurasjon hentes i ulike pålitelighetsdatabaser som OREDA (Offshore Reliability Data, 2009).

5.2.3 Sikkerhetsutilgjengelighet

For å til slutt kvantifisere sikkerhetsutilgjengelighet benytter IEC 61508 metoden, som tidligere nevnt, sannsynligheten for svikt på etterspurt tid (PFD) for et SIS som opererer på forespørsel, og sannsynligheten for en kritisk feil per time (PFH) for et SIS som driftes kontinuerlig. Der denne oppgaven retter fokus mot systemer som opererer på forespørsel, kalkuleres PFD på bakgrunn av feilraten (λ) til komponenten/systemet og det estimerte testintervallet (τ) til komponenten/systemet.

I IEC 61508 metoden kvantifiseres PFD (sikkerhetstapet) som følger av farlige udetekterte feil (med raten λ_{DU}) i perioder hvor det er ukjent at funksjonen er utilgjengelig. Ved å se på en enkelt komponent i systemet (1oo1) så viser utledningen i appendiks A at man da kan skrive:

$PFD \approx \frac{\lambda_{DU} \cdot \tau}{2}$ der

λ_{DU} = feilraten til kritiske uoppdagede feil for en komponent
τ = testintervallet (intervallet mellom funksjonelle tester)

PFD er videre basert på antakelsen om at komponentene har en eksponentiell levetidsfordeling[6].

Den totale systempåliteligheten (PFD) vil videre bli kalkulert ut i fra komponentenes PFD, og det vil bli tatt høyde for systemets konfigurasjon ved CCF der det foreligger redundante komponenter eller delsystemer.

5.3 Parametre i PDS metoden

5.3.1 Årsaker til feil

PDS metoden definerer og skiller på samme måte som IEC 61508 metoden mellom *tilfeldige hardware feil* og *systematiske feil*, men anvender en mer nyansert og detaljert inndeling i underkategorier av systematiske feil (S. Hauge, Hokstad, et al., 2006):

Tilfeldige hardware feil er, på samme måte som i IEC 61508 metoden, feil som følger av naturlige degraderingsmekanismer i komponenter. For slike feil antas det at systemet er designet i henhold til aktuelle driftsforhold.

Systematiske feil er, på lik linje med IEC 61508 metoden, definert som feil relatert til bestemte årsaker som ikke skyldes naturlig nedbrytning (aldring). Feilene kan normalt elimineres ved en endring, enten som endring i design eller produksjonsprosessen, de operative prosedyrene eller dokumentasjon. PDS metoden deler videre de systematiske feilene inn i tre kategorier:

- *Stress* feil oppstår ved overdreven stress, det vil si stress ut over design, blir plassert på komponenten. Overdrevet stress kan enten være forårsaket av ytre årsaker eller ved intern påvirkning. Eksempler kan være skader for prosessensorer som følger av store vibrasjoner eller ventilfeil som skyldes uforutsett sandproduksjon (S. Hauge, Hokstad, et al., 2006).
- *Design* feil blir stort sett introdusert i faser før drift, som design og planlegging. Det kan være seg feil i selve systemspesifikasjonen, en produksjonsfeil eller svikt under installasjon. Eksempler er ventilfeil som skyldes utilstrekkelig aktuator respons, sensorer som unnlater å skille mellom reelle og falske krav, og feilaktig plassering av for eksempel brann og gass detektorer.

[6] Eksponensielle fordelinger karakteriseres ved en konstant feilrate. "*En enhet som har en eksponensialfordeling, har en tilbøyelighet til å svikte som ikke er avhengig av alderen*" (Aven, 2006)

- *Interaction* feil er operasjonelle feil som er initiert av menneskelig svikt under drift eller vedlikehold/testing. Et eksempel kan være en isolasjonsventil for prosessensor som blir stående i lukket stilling.

Som en generell betraktning er det viktig å forstå at systematiske feil, som stress, design og interaksjonsfeil, kan gi opphav til feil i flere komponenter (Common Cause Failures). Tilfeldige hardware feil, kan derimot betraktes som *uavhengige* feil, og antas dermed å ikke resultere som feil i flere komponenter. Enkelte feil kan imidlertid være vanskelig å plassere i de ulike kategoriene, som for eksempel å skille på feil som følger av aldring og stress feil (S. Hauge, Hokstad, et al., 2006).

Kategorien for stress feil antas videre å være klassifisert som systematiske feil for å samsvare med definisjoner gitt i IEC (IEC 61508-4 3.6, 1998), men også fordi stressfeil har de typiske egenskapene som systematiske feil: at feil kun kan elimineres ved å fjerne overdreven stress på komponenten eller ved å endre selve komponenten (S. Hauge, Hokstad, et al., 2006).

Hensikten ved å introdusere en underkategorisering av systematiske feil, slik som i PDS metoden, er å øke fokus på typer av feil som kan introduseres gjennom designprosesser, testing og vedlikehold. Den prinsipielle bakenforliggende ideen synes å være at designere gjøres oppmerksomme på slike feil, og kan nytte dette som et verktøy for å kontrollere dem, noe som vil kunne resultere i mer pålitelig design (Häger, 2004). Det samme gjelder for testing og vedlikehold av et system. Relevansen av systematiske feil i pålitelighetskalkuleringene vil bli nærmere drøftet i delkapittel 7.1.1.

PDS metoden har med dette et stort fokus på *hele* sikkerhetsfunksjonen, og har til hensikt å gjøre rede for alle feil som vil kunne kompromittere en funksjon (føre til svikt). Noen av disse feilene er knyttet til andre grensesnitt, som for eksempel miljø, i stedet for sikkerhetssystemet alene. Det synes videre å være en del av PDS *filosofien* å inkludere slike hendelser.

5.3.1.1 Feilklassifisering

PDS metoden har en feilklassifisering som minner om den som benyttes i IEC 61508 metoden, men feilklassifiseringen her er ikke kun begrenset til tilfeldige hardware feil.

- Dangerous (D) – farlige feil som *har* potensial til å bringe sikkerhetssystemet i farlige situasjoner dersom komponentene ikke fungerer tilstrekkelig

    - Dangerous Undetected (DU) – farlige feil som ikke detekteres ved automatiske selvtester
    - Dangerous Detected (DD) – farlige feil som oppdages ved automatiske selvtester
- Safe (S) / Spurious Trip (ST) – sikre feil der komponenten opererer uten etterspørsel
    - Safe (Spurious Trip) Undetected (SU / STU) – feil som ikke oppdages ved automatiske selvtester, og dermed resulterer i falsk etterspørsel
    - Safe (Spurious Trip) Detected (SD / STD) – feil som oppdages ved automatiske selvtester, og dermed unngår falsk etterspørsel
- Noncritical (NONC) – sikre feil som ikke påvirker hovedfunksjonene i systemet, typisk en mindre oljelekkasje eller lignende som ikke påvirker sikkerhetsfunksjonene

Som illustrert ovenfor har PDS metoden valgt å benytte en noe ulik notasjon for sikre (Safe) feil, der disse feilene deles inn i Spurious Trip (feil der SIS aktiveres uten en forespørsel) og Noncritical feil (feil som ikke påvirker hovedfunksjonene av systemet).

Dangerous (D) og Spurious Trip (ST) feil blir betraktet som *farlige*, ettersom disse påvirker hovedfunksjoner (”evnen til å stenge på etterspørsel og evnen til å opprettholde produksjonen når Safe”). Spurious Trip feil blir som regel oppdaget raskt ved forekomst, mens Dangerous feil er ”sovende” og kan kun påvises ved testing eller på reell forespørsel (S. Hauge, Hokstad, et al., 2006).

Basert på denne klassifiseringen, deles feilraten, λ, inn i følgende elementer i PDS metoden:

λ_{DD} = Raten av farlige oppdagede feil
λ_{DU} = Raten av farlige uoppdagede feil
λ_{STD} = Raten av Spurious Trip oppdagede feil
λ_{STU} = Raten av Spurious Trip uoppdagede feil
λ_{NONC} = Raten av Noncritical feil

I IEC metodens notasjon utgjør raten av sikre oppdagede feil (λ_{SU}) med dette summen av λ_{STU} + λ_{NONC} i PDS notasjonen.

PDS tilnærmingen introduserer videre noen samlekategorier av overnevnte feilrater (S. Hauge, Hokstad, et al., 2006; OLF-070, 2004):

λ_{undet} = λ_{DU} + λ_{SU} som er raten av farlige feil som er uoppdaget ved automatiske selvtester (eller av personell mellom funksjonelle tester)
λ_{det} = λ_{DD} + λ_{SU} som er raten av farlige feil som er oppdaget ved automatiske

selvtester

λ_{crit} = $\lambda_D + \lambda_S$ som er raten av kritiske/farlige feil; for eksempel feil som foruten deteksjon vil kunne forårsake feil på etterspurt tid eller Spurious Trip av sikkerhetsfunksjonen

λ = $\lambda_{crit} + \lambda_{NONC}$ som er den totale feilraten

5.3.2 Common cause failures (CCF)

I PDS metoden blir det benyttet en utvidet versjon av β-faktor modellen der denne skiller mellom ulike typer av konfigurasjoner. Her avhenger CCF frekvensen av konfigurasjonen, og β-faktoren av en MooN konfigurasjon kan uttrykkes som følger:

$$\beta_{MooN} = \beta * C_{MooN}, (K < N)$$

C_{MooN} er her modifikasjonsfaktoren for de ulike systemkonfigurasjonene, og β er fortsatt common cause faktoren for konfigurasjonen slik som beskrevet i delkapittel 5.2.2. Både PDS metoden og OLF 070 inneholder spesifiserte verdier for modifikasjonsfaktoren ettersom ulike systemkonfigurasjoner benyttes. Dette betyr videre at dersom hver av de N redundante komponentene har en feilrate lik λ_{DU}, så har MooN konfigurasjonen en CCF rate for systemet som er lik:

$$C_{MooN} * \beta * \lambda_{DU}$$

Ved å benytte denne modellen så opprettholdes β som en viktig parameter der tolkningen nå er relatert til et duplisert system (S. Hauge, Hokstad, et al., 2006). Det bør videre merkes at effekten av de ulike konfigurasjonene er innført som en egen faktor, C_{MooN}, som er uavhengig av β. Dette gjør modellen relativt enkelt å benytte i praksis ettersom PDS metoden foreslår verdier for C_{MooN} faktoren ved ulike konfigurasjoner.

5.3.3 Sikkerhetsutilgjengelighet

Der IEC 61508 metoden kun benytter PFD for å betrakte sikkerhetsutilgjengelighet, benytter PDS metoden flere ulike funksjoner for å reflektere utilgjengeligheten der disse deles inn i tre hovedkategorier som utgjør Critical Safety Unavailability (CSU):

1. PFD: utilgjengelighet som følger av farlige udetekterte (DU) feil: for eksempel utilgjengelighet forårsaket av farlige feil som kun er detekterbare under funksjonell testing eller ved etterspurt tid (ikke detekterbart ved automatiske selvtester). Denne utilgjengeligheten som man gjerne refererer til som "ukjent", betraktes i PDS tilnærmingen å bestå av to elementer:
    a. Utilgjengeligheten som følger av farlige udetekterte random hardware feil (med raten λ_{DU-RH})
    b. Utilgjengeligheten som følger av farlige udetekterte systematiske feil (med raten λ_{DU-S})
2. P_{TIF}: utilgjengelighet som følger av TIF feil (Test Independent Failures): for eksempel utilgjengelighet forårsaket av skjulte farlige feil som ikke oppdages under funksjonell testing men kun som følger av etterspørsel (true demand). Disse feilene kalles Test Independent Failures (TIF), og er i denne rapporten også referert til som systematiske feil
3. DTU: utilgjengelighet som følger av kjent eller planlagt nedstengning. Dette utilgjengelighetsmålet forårsakes av at komponentene er tatt ut for reparasjon eller testing/vedlikehold. Utilgjengeligheten som følger av nedstengning kan videre deles inn i to kategorier:
    a. Kjent utilgjengelighet grunnet farlige feil (D) der komponenten må repareres. Gjennomsnittlig utilgjengelig periode som følger av disse hendelsene er lik gjennomsnittlig tid til reparasjon (Mean Time To Restoration – MTTR) – som vil si tiden fra feilen oppdages til situasjonen er gjenopprettet.
    b. Planlagt (og kjent) utilgjengelighet som følger av nede tid / hemming under funksjonstesting og / eller forebyggende vedlikehold.

Det bør videre bemerkes at det faktiske bidraget til sikkerhetstap fra kategori 3 vil være sterkt avhengig av operasjonsfilosofi, konfigurasjonen av prosessanlegget, samt konfigurasjonen av SIS (S. Hauge, Hokstad, et al., 2006). Ofte vil midlertidige kompenserende tiltak bli satt i verk når en komponent er nede for vedlikehold eller reparasjon, mens det i tilfeller med særlig kritiske komponenter kan være aktuelt å stenge ned produksjonen under restaurerings- og testperioder. Av den grunn vil det være rasjonelt å behandle utilgjengelighet som følger av nedstengning separat, og ikke i tilknytning til kategori 1 og 2. Videre, så vil det i mange tilfeller være slik at kategori 3a. og 3b. har relativt små bidrag for sikkerhetstap i forhold til kategori 1, der MTTR < τ. Dette er imidlertid ikke alltid realiteten dersom vedlikeholdsperioden for utstyr et spesielt lang. Kategori 3b. kan videre normalt betraktes som den minst kritiske, ettersom denne representerer planlagt utilgjengelighet av

sikkerhetssystemet, og reparasjon og testing som regel blir utført under planlagt nedstengning (S. Hauge, Hokstad, et al., 2006).

5.3.3.1 Sannsynligheten for svikt på etterspurt tid (PFD)

For å kvantifisere sikkerhetstap som følger av tilfeldige hardware feil, benytter IEC som kjent den gjennomsnittlige sannsynligheten for at SIS ikke er i stand til å utføre sikkerhetsfunksjonen ved etterspørsel (PFD).

I PDS metoden kvantifiseres også PFD (sikkerhetstapet) som følger av farlige udetekterte feil (med raten λ_{DU}) i perioder hvor det er ukjent at funksjonen er utilgjengelig. Gjennomsnittlig varighet for denne perioden er $\tau/2$ for en enkelkomponent. Dersom utilgjengelig nede tid (kategori 3 over) legges til, vil dette være særskilt angitt.

I PDS metoden splittes raten av farlige udetekterte feil opp i to elementer; utilgjengelighet som følger av tilfeldige hardware feil ($\lambda_{DU\text{-}RH}$) og utilgjengelighet som følger av systematiske feil ($\lambda_{DU\text{-}S}$) som er detekterbare under funksjonell testing. Med å se på en enkelt komponent i systemet (1oo1) så får en da:

$$PFD \approx \frac{\lambda_{DU} \cdot \tau}{2} = \frac{\lambda_{DU-RH} * \tau}{2} + \frac{\lambda_{DU-S} * \tau}{2}$$ der

λ_{DU} = feilraten til farlige uoppdagede tilfeldige hardware feil og systematiske feil for en komponent
τ = testintervallet (intervallet mellom funksjonelle tester)

5.3.3.2 Test Indepentent Failures (TIF)

Det antas ofte i pålitelighetsanalyser at funksjonell testing er ”perfekt”, og at man således detekterer alle feil. I virkeligheten er ikke nødvendigvis dette tilfelle der testforhold kan avvike fra reelle etterspørselsforhold, og enkelte kritiske feil kan med dette forbli i SIS etter funksjonelle tester. Det er videre et viktig og ganske unikt trekk ved PDS tilnærmingen at man forsøker å gjøre rede for disse systematiske feilene. Som diskutert ovenfor så kan de systematiske feilene enten detekteres ved funksjonelle tester (kategori 1.b over) eller under reell etterspørsel (kategori 2 over). Systematiske feil som oppdages under reell etterspørsel blir i PDS metoden referert til som Test Independent Failures (TIF), og inngår som en inndataparameter i kalkulasjoner av sikkerhetsutilgjengelighet.

I PDS tilnærmingen (S. Hauge, Hokstad, et al., 2006) defineres dette som:

P_{TIF} = *"The probability that the module/system will fail to carry out its intended function due to a (latent) systematic failure not detected by functional testing"*

Det bør videre bemerkes at dersom en ufullkommen testing foretas ved funksjonell testing, så vil dette resultere i en økt TIF sannsynlighet. For eksempel en gassdetektor som testes ved hjelp av injeksjon av testgass i huset via en spesiell port, vil ikke nødvendigvis antyde om en av flere andre porter er blokkert.

Test uavhengige feil vil ofte være systematiske av natur, som for eksempel en programmeringsfeil i applikasjonssoftwaren som ikke avdekkes siden alle årsaker og effekter ikke testes. Noen TIF'er kan likevel klassifiseres som tilfeldige hardware feil, for eksempel slitasje av en ventilstamme som forårsaker intern lekkasje, og ikke oppdages under ordinære funksjonstester.

Bidraget fra slike imperfekte tester kan på denne måten ved PDS tilnærmingen inkluderes i TIF, eller i IEC metoden slik det ofte gjøres under funksjonstester, redusere dekningsgraden til funksjonstesten fra 100 % til en lavere verdi (S. Hauge, Hokstad, et al., 2006).

5.3.3.3 Downtime Unavailability (DTU)

I PDS metoden representerer dette utilgjengelig nedetid som beskrevet i kategori 3a. og 3b ovenfor. DTU består av to elementer:

- DTU_R: utilgjengelig nedetid grunnet reparasjoner av kritiske feil med raten λ_D. Disse oppstår i en periode da det er kjent at funksjonen ikke er tilgjengelig (det vil si kategori 3a). Gjennomsnittet for denne perioden er gjennomsnittlig tid til gjenoppretting (MTTR), altså gjennomsnittlig tid fra feilen oppdages til sikkerhetsfunksjonen er reparert/gjenopprettet.
- DTU_T: planlagt nedetid som følger av aktiviteter som testing og planlagt vedlikehold (det vil si kategori 3b).

5.3.3.4 Critical Safety Unavailability (CSU)

I PDS metoden benyttes målet for Critical Safety Unavailability (CSU) for å kvantifisere samlet sikkerhetsutilgjengelighet (sikkerhetstap):

CSU = *"The probability that the component/system will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event, (and it is not known that the safety system is unavailable"* (S. Hauge, Hokstad, et al., 2006).

Således har man følgende sammenheng:

$$CSU = PFD + P_{TIF}$$

Dersom "kjent" utilgjengelig nedetid inkluderes så blir formelen:

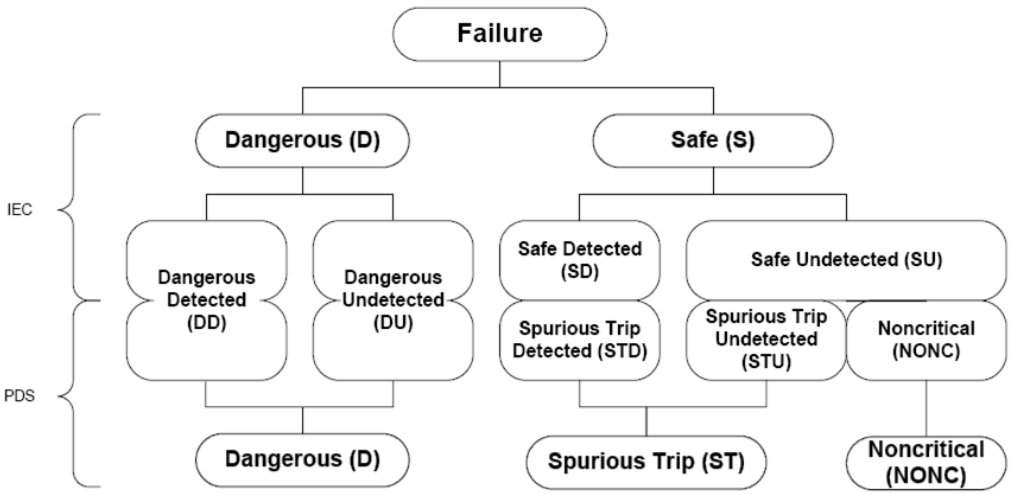
$$CSU = PFD + P_{TIF} + DTU$$

Som omtalt ovenfor så kvantifiserer IEC metoden bare utilgjengelig nedetid som skyldes komponentenes reparasjonstid som følger av kritiske feil (det vil si DTU_R), og det foreligger dermed ingen egen formel for kvantifisering av utilgjengelighet som følger av testing og inspeksjoner i IEC tilnærmingen.

5.4 Kort drøfting og illustrasjon av ulikheter i metodene

5.4.1 Notasjon og feilklassifisering

Kort oppsummert kan ulikhetene i IEC 61508 og PDS notasjon og feilklassifisering illustreres i figuren under:



Figur 5.1 - Feilklassifisering i IEC 61508 metoden og PDS metoden på komponentnivå (S. Hauge, Hokstad, et al., 2006)

Som illustrert, så har ikke IEC 61508 metoden noe eksplisitt skille mellom sikre farlige og sikre ufarlige feil. Imidlertid kan det basert på overnevnte genereres følgende tolkning; sikre oppdagede feil (SD) i IEC notasjonen er identisk med sikre Spurious Trip oppdagede (STD) i PDS metoden. Videre er sikre uoppdagede (SU) i IEC tolket som summen av sikre Spurious Trip uoppdagede (STU) og Non-critical (NONC) i PDS notasjonen (S. Hauge, Hokstad, et al., 2006).

5.4.2 Ulikheter mellom β-faktor modellene

Et problem med β-faktor tilnærmingen som benyttes i IEC 61508 metoden er at frekvensen av avhengige feil for alle M-ut-av-N (MooN) systemer[7], (M<N), er den samme (S. Hauge, Hokstad, et al., 2006). Dersom λ er feilraten for en komponent, så vil et MooN system ha en CCF bidrag lik β * λ. Således klarer ikke denne modellen å skille mellom ulike systemkonfigurasjoner (voteringer), og det samme resultatet oppnås ved for eksempel 1oo2, 1oo3 og 2oo3 systemer. En mulig løsning kan være å benytte ulike β-faktorer for ulike systemoppsett; for eksempel benytte β = 1 % for 1oo3, β = 5 % for 2oo3 og β = 10 % for 2oo3 systemer. Dette er den tilnærmingen som foreslås i IEC 61508, som inkluderer ”applikasjonsspesifikke” β-verdier (IEC61508, 1998), som til en viss utstrekning avhenger av systemkonfigurasjonen, MooN. Men frekvensen av systemets CCF avhenger kun i en liten grad av systemkonfigurasjonen (S. Hauge, Hokstad, et al., 2006). Når modellen ikke skiller mellom for eksempel 1oo2 og 2oo3, trenger ikke dette være tilstrekkelig detaljert dersom hensikten for eksempel er å sammenlikne to ulike systemkonfigurasjoner.

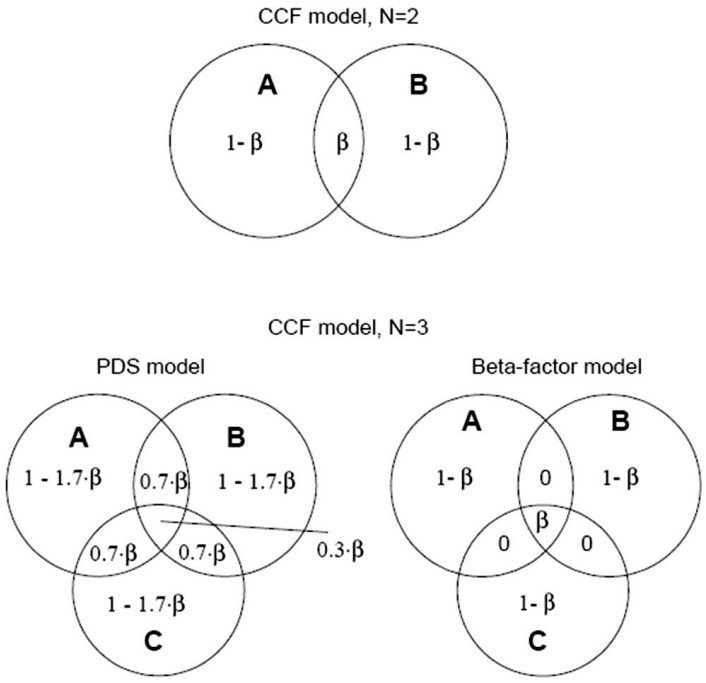
Når det kommer til fastsettelse av β-verdien ble det nevnt ovenfor at IEC 61508 benytter applikasjons- eller anleggsspesifikke β-verdier, der disse fastsettes ved å benytte sjekklister. Prinsippet om applikasjons- og anleggsspesifikke β-verdier anses også som et godt prinsipp og adopteres i PDS metoden. PDS tilnærmingen betrakter videre sjekklistene i IEC 61508 metoden som omfattende og til tider vanskelige, og foreslår dermed en forenklet tilnærming. Denne er videre utdypet delkapittel 5.4.3 og i appendiks B.

Ulikhetene mellom standard β-faktor modellen som benyttes i IEC 61508 metoden og modellen for β-faktoren i PDS metoden er videre illustrert i figur 5.2 under. En sirkel (for eksempel A) representerer her en hendelse; ”komponent A har feilet”. For et duplisert sett av redundante komponenter A og B (N=2), så er IEC 61508 og PDS tilnærmingen identisk. β

[7] MooN betyr at minst M komponenter av N redundante komponenter må fungere for at systemet skal fungere; for eksempel å gi signal om nedstengning for at nedstengning skal aktiveres

representerer her en brøkdel av feilene som påvirker både A og B slik at disse feiler simultant.

Ved tre komponenter (N=3), så antar standard β-faktor modellen at når en feil som påvirker to komponenter oppstår (for eksempel A og B), vil også den tredje komponenten (C) svikte. Dermed vil det aldri forekomme at kun to av tre komponenter feiler på grunn av en CCF. Ved å benytte PDS metoden og de oppdaterte C_{MooN} faktorene, så antas det at dersom A og B feiler som følger av en CCF, vil også C kunne svikte (men i dette eksempelet kun i 30 % av tilfellene). Det er videre noe vilkårlig å for eksempel postulere at denne fraksjonen utgjør 30 % basert på ekspertvurderinger og tilgjengelig informasjon, men i PDS metoden betraktes dette likevel som mer realistisk enn å forutsette andelen å være 100 % som i den ordinære β-faktor modellen.



Figur 5.2 - Illustrasjon av CCF modeller for N=2 og N=3 (S. Hauge, Hokstad, et al., 2006)

Fra figur 5.2 kan det også ses at C_{2oo3} faktoren i PDS metoden ville blitt 2,4. Dette kommer av at den delen av feil som påvirker 2 eller 3 komponenter er 0,3*β + 0,7*β + 0,7*β + 0,7*β = 2,4*β.

5.4.2.1 Modellering av Common Cause Failures (CCF)

En feilkategori som ikke direkte ser ut til å være overens med klassifiseringen av systematiske eller tilfeldige hardware feil i de to metodene er CCF. Per definisjon er disse feilene avhengige feil (M. Rausand & Høyland, 2004), og kan dermed ikke klassifiseres direkte som tilfeldige hardware feil. Av den grunn skulle disse feilene være klassifisert som systematiske feil, i stedet for at systematiske feil i de to metodene benyttes for å klassifisere en enkel komponentindividuell feil, mens CCF inkluderer feil fra *mer* enn en komponent (Lundteigen, 2009). De bakenforliggende årsakene til systematiske feil og CCF synes likevel å kunne betraktes som like, slik at eventuelle barriere- og forsvarstiltak mot systematiske feil dermed også vil være effektive midler for å forsvare systemet mot CCF (Lundteigen, 2009).

Når CCF inkluderes i pålitelighetsberegningene, trekkes i prinsippet en brøkdel (β) av raten for tilfeldige hardware feil som igjen klassifiseres som CCF. Dette betyr videre at CCF indirekte gis noen av de samme egenskapene som tilfeldige hardware feil, som for eksempel konstant feilrate. Dette er en noe motsigende tilnærming, men likevel den praksis som foreligger i industrien (Lundteigen, 2009).

5.4.3 Applikasjonsspesifikke kalkulasjoner

Når det er ønskelig å gjennomføre pålitelighetskalkulasjoner ved å benytte de to metodene som er presentert, må det foreligge inndata for parametrene. Inndata for disse parametrene kan finnes i datahåndbøker eller databaser, slik som OREDA og PDS datahåndboken. Disse dataene er imidlertid ofte presentert som gjennomsnittlige generiske verdier, og således er de *ikke* direkte knyttet til lokale operasjonelle forhold for det systemet det tar utgangspunkt i. For å tilpasse kalkulasjoner og system til lokale forhold ble det i delkapittel 5.4.2 nevnt at metodene kan nytte såkalte applikasjonsspesifikke parametre. IEC 61508 metoden betrakter i den anledning delvis en slik løsning når det i β-faktor modellen benyttes ulike faktorer for ulike systemoppsett; slik som for eksempel å benytte β = 1 % for 1oo3, β = 5 % for 2oo3 og β = 10 % for 2oo3 systemer. Men som tidligere nevnt så avhenger frekvensen av systemets CCF kun i liten grad av systemkonfigurasjon, der CCF i stor grad heller må betraktes å være påvirket av lokalt operasjonelle systematiske faktorer. Erfart PFD fra drift kan således i IEC 61508 metoden ikke direkte betraktes å fange opp systemets spesifikke driftsforhold i tilstrekkelig grad, ettersom det ikke foreligger kvantifisering av systematiske feil og mer inngående ekspertvurderinger og justering av faktorer for å forankre disse til systemets driftsforhold lokalt.

PDS metoden nytter videre en applikasjonsspesifikk håndtering av ulike parametre i større utstrekning enn IEC 61508 metoden, der PDS metoden håndterer CCF og systematiske feil gjennom parametrene λ_{DU-S}, β og P_{TIF}. Det antas også her, på lik linje med IEC 61508 metoden, generiske verdier for tilfeldige hardware feil. Fellesnevneren for applikasjonsspesifikke kalkulasjoner i PDS metoden synes videre å være en kombinasjon av generiske data med anleggsspesifikke betraktninger. Erfart PFD fra drift kan således i PDS metoden i større grad antas å fange opp relevante driftsforhold, og i kombinasjon med inngående bruk av ekspertvurderinger og justeringer av parametre, vil disse kunne replisere systemets operative tilstand på et godt og mer helhetlig grunnlag. Applikasjons- og anleggsspesifikk oppdatering slik det foreligger i PDS metoden anses som et godt prinsipp, og en styrke for å redusere underliggende usikkerhet i tilknytning til inndata for parametrene. Mer informasjon knyttet til kalkulasjonene for applikasjonsspesifikk oppdatering i PDS metoden foreligger i PDS metode håndboken, appendiks C (S. Hauge, Hokstad, et al., 2006), og i appendiks B i denne oppgaven. Applikasjonsspesifikke forhold vil bli nærmere drøftet i delkapittel 6.3.

5.4.4 Systematiske feil

IEC 61508 metoden kvantifiserer som tidligere nevnt ikke de systematiske feilene. Isteden anbefales bruk av teknikker og tiltak under design for å unngå systematiske feil gjennom systematisk sikkerhetsintegritet, slik det også blir gjort i PDS metoden. IEC 61508 metoden verifiserer med dette systematiske feil kun kvalitativt ved at det må dokumenteres at de tiltakene som defineres som viktige har blitt kontrollert og gjennomgått tilstrekkelig. OLF 070 støtter ikke denne tilnærmingen til håndtering av systematiske feil. Den sier at kvantifisering bør gjennomføres og inkorporeres i PFD på samme måte som i PDS metoden, der systematiske feil i PDS metoden er uttrykt ved parametrene λ_{DU-S} og P_{TIF}. Bekymringen for OLF 070 synes med dette å være at IEC 61508 metoden representerer et skritt bakover i håndteringen av pålitelighet ved å ikke kvantifisere de systematiske feilene. En kvantifisering av systematiske feil, slik som det gjøres i PDS metoden, ville kunne inngå som en PSF (Probability of Systematic Failures) faktor som følger (eller alternativt, som λ_{DU-S} og P_{TIF} faktor slik som i PDS):

$$PFD \approx \frac{\lambda_{DU} \cdot \tau}{2} + PSF$$

PSF = samlet bidrag av systematiske feil (stress, design og operasjonelle feil)

Ved å benytte denne tilnærmingen er det også mulig å vurdere det relative bidraget fra systematiske feil i PFD estimatet.

5.4.5 Farlige uoppdagede feil

Under kalkulasjoner av PFD er raten av farlige uoppdagede feil (λ_{DU}) av stor betydning, der denne inndataparameteren (sammen med testintervallet) predikerer hvor sannsynlig det er at en sikkerhetsfunksjon feiler på etterspørsel. I følge IEC 61508 så vil raten av λ_{DU} kun inkludere tilfeldige hardware feil. Likevel så vil en ved å gå gjennom historiske data kunne se at flere av de rapporterte feilene til datahåndbøker er systematiske feil (S. Hauge, Hokstad, et al., 2006). Ved å betrakte raten av farlige uoppdagede feil slik den presenteres i datahåndbøker, som blant annet OREDA og PDS håndboken, så vil disse dataene således inkludere både tilfeldige hardware feil så vel som systematiske feil. Systematiske feil vil som et resultat av dette implisitt bli inkludert i pålitelighetskalkulasjonene, også i IEC 61508 metoden. Det er på denne måten nyttig å betrakte λ_{DU} å bestå av to element; $\lambda_{DU\text{-}RH}$ som er raten av farlige uoppdagede tilfeldige hardware feil (dvs. IEC definisjonen av λ_{DU}), og $\lambda_{DU\text{-}S}$ som er raten av farlige uoppdagede systematiske feil (detekterbare under funksjonell testing). På denne måten kan den relative andelen av feil som tilhører henholdsvis tilfeldige hardware feil og systematiske feil betraktes nærmere, slik det gjøres i PDS metoden.

Det er videre verdt å merke seg at denne oppgaven betrakter IEC 61508 metoden til ikke å kvantifisere de systematiske feilene, dette til tross for at metoden implisitt i enkelte tilfeller inkluderer deler av disse feilene.

5.4.6 Faktorer for sikkerhetsutilgjengelighet

Samlet bidrag for sikkerhetsutilgjengelighet er med dette i PDS metoden uttrykt med Critical Safety Unavailability (CSU), bestående av PFD + P_{TIF} + DTU. I IEC 61508 metoden er utilgjengeligheten kun basert på sannsynligheten for svikt på etterspurt tid (PFD). Systemets utilgjengelighet med hensyn til reparasjon og testing vil ikke bli videre drøftet i denne oppgaven. Det forutsettes at testintervallene er tilstrekkelig mye lenger enn reperasjons- og nedetiden (MTTR < Testintervall (τ)). Oppgaven vil med dette se bort i fra DTU parameteren og tilhørende faktorer i IEC 61508 metoden.

Sannsynligheten for svikt på etterspurt tid er for de to metodene for en MooN konfigurasjon der M<N er (OLF-070, 2004):

$$PFD_{IEC\ 61508} \approx \frac{\tau * \lambda_{DU}}{2} + \lambda_{CommonCause\ IEC61508}$$

$$PFD_{PDS} \approx \frac{\tau * \lambda_{DU}}{2} + \lambda_{CommonCause\ PDS} + P_{TIF}$$

der

$$\lambda_{CommonCause\ IEC61508} = \lambda_{Independent} * \beta$$

$$\lambda_{CommonCause\ PDS} = \lambda_{Independent} * \beta * C_{MooN}$$

Av overnevnte formler ser en at IEC 61508 metoden nå har inkludert applikasjonsspesifikke β for CCF med utgangspunkt i β-faktor modellen, mens PDS metoden som nytter den utvidede versjonen av β-faktor modellen også skiller mellom ulike typer av voteringer og konfigurasjoner ved C_{MooN}. PDS metoden har videre også inkludert samlet bidrag fra systematiske feil (λ_{DU-S}) i raten av farlige uoppdagede feil, samtidig som sannsynligheten for systematiske testuavhengige feil (P_{TIF}) er inkludert.

5.4.7 Oppsummerende betraktninger

Overnevnte fremgangsmåte for kvantifisering av sikkerhetsutilgjengelighet, herunder PFD, betraktes i metodene å være verifikasjonsprosessen som sørger for at systemet er innenfor de kvantitative SIL kravene. I en livssyklusfase ble det i delkapittel 3.2.2.3 diskutert at prosessen for å sørge for at SIS i alle livsfaser møter de spesifiserte kravene skal følge gjentakende evalueringer i drift. I IEC 61508 metoden foreligger det ikke noen annen fremgangsmåte enn overnevnte metode for oppdatering av inndataparametre for SIS. Metoden antas derimot i en underliggende implisitt betraktning å uttrykke at feilratene bør oppdateres etter hvert som nye generiske operasjonelle data foreligger. Ut i fra en realistfortolkning betraktes dette å redusere tilhørende (aleatorisk) usikkerhet. Mens det ut i fra et prediktivt perspektiv ikke vil redusere (den epistemiske) usikkerheten med mindre det

nyttes ekspertvurderinger til å predikere frekvenser av fremtidige hendelser, og at disse anvendes i kalkulasjonene.

I PDS metoden foreligger det derimot en metodisk fremgangsmåte for oppfølging av SIS i driftsfaser, blant annet ved applikasjons- og anleggsspesifikk oppdatering av inndataparametre for CCF og systematiske feil. I den grad oppdateringen anvender utstrakt bruk av ekspertvurderinger, så vil dette kunne betraktes som et godt prinsipp for å redusere tilhørende epistemisk usikkerhet.

For å evaluere styrker og svakheter ved håndtering av usikkerhet under komparasjon av de to metodene, er en systemanalyse av en case blitt gjennomført som et eksempel.

6 Resultater – Systemanalyse av case

Som nevnt i innledende betraktninger har en systemanalyse av en case blitt gjennomført for å opparbeide førstehånds erfaring med de to ulike metodene, samt for å forsøke å illustrere ulikhetene dem i mellom. Kalkulasjonene har blitt dokumentert i et separat appendiks i et forsøk på å gjøre oppgaven mer leservennlig. Full oversikt over informasjonen som presenteres i dette kapittelet fås dermed ved å ta for seg kalkuleringene i appendiks B før dette kapittelet leses.

Det er videre viktig og igjen minne om at kalkulasjonene i systemanalysen av caset kun tar for seg de kvantitative kalkulasjoner av PFD som benyttes for å verifisere SIL, og at denne oppgaven ikke direkte har til hensikt å gi svar på om pålideligheten til systemet samsvarer med underliggende SIL krav. Utviklingen av design, installasjoner, testintervaller og operasjons- og vedlikeholdsprosedyrer er ikke inkludert i analysen. Kapittelet presenterer med dette resultatene fra systemanalysen av caset, og diskuterer erfaringene ved å benytte de ulike metodene for å håndtere usikkerhet og kvantifisere PFD i henhold til SIL verifisering.

6.1 Generelle observasjoner

I oppgaven har det vært nødvendig å vurdere faktorer og terminologien som benyttes i de to metodene, der disse ikke er helt like og overens med det som synes å være etablert i databaser og andre kilder. Et eksempel på dette kan være feilratene og feilkategoriseringen som benyttes i IEC 61508 metoden. Definisjonen av farlige uoppdagede og oppdagede samsvarer ikke med feilkategoriseringen i for eksempel PDS metoden og OREDA som er en av de mest brukte feildatabasene. Tilsvarende, så har PDS metoden enkelte faktorer som ikke er å finne i OREDA databasen, som for eksempel sannsynligheter for systematiske testuavhengige feil.

Uenighet mellom PDS metoden og IEC 61508 metoden om kvantifisering av systematiske feil indikerer videre at det foreligger ulike meninger, men også her ulik terminologi. Den kvalitative tilnærming for systematisk sikkerhetsintegritet, der SIS skal kontrollere og unngå systematiske feil, har ikke blitt videre betraktet siden metodene ikke eksplisitt kvantifiserer disse feilene for verifikasjon i henhold til hardware sikkerhetsintegritet. Når det i denne oppgaven kun har blitt tatt hensyn til den kvantitative delen av de systematiske feilene, så er det videre å betrakte som uheldig at disse ikke håndteres av IEC 61508 metoden.

Tilnærmingen til håndtering av systematiske feil, slik disse betraktes i PDS metoden, støttes videre av OLF 070 (2004). For eksempel så vil det å ikke betrakte, samt ta høyde for, kvantitative systematiske feil tidlig i designprosess kunne resultere i uønsket og mindre robust effekt av systemer (Häger, 2004). Det å ikke betrakte systematiske feil kvantitativt vil bli nærmere drøftet i delkapittel 7.1.1.

Det kvantitative PFD kravet som anvendes for SIL verifikasjon er basert på en velkjent modell for å estimere systemtilgjengelighet (Mean Time Between Failures) (Häger, 2004). Det som i tillegg anvendes i disse metodene for å kvantifisere PFD er å identifisere og klassifisere feil i kategoriene for farlige oppdagede og farlige uoppdagede feil. Det vil si feil som resulterer i tap av sikkerhetssystemet (SIS), og som dermed gjør sikkerhetsfunksjonen (SIF) ute av stand til å utføre tiltenkt funksjon. Det er i begge metodene viktig at klassifiseringen av feil blir gjort riktig for å komme frem til en mest mulig realistisk prediksjon av PFD, der nøyaktighet av inndata har mye å si for prediksjonens statistiske kvalitet. For å sikre riktig feilklassifisering så benyttes det i industrien til tider såkalte FMEDA/FMECA (Failure Modes Effects and Diagnostic/Criticality Analysis) for å evaluere hvilke typer feil en komponent kan ha. Denne metodikken har således betydning for PFD ettersom det her vurderes hvilke typer av feil som skal kategoriseres som farlige uoppdagede feil. Når en FMEDA/FMECA gjennomføres skal denne baseres på ekspertvurderinger, noe som betraktes som et godt prinsipp og som ved bruk i tilknytning til de to metodene kan forhindre feilklassifisering av feil. Et eksempel på en utfordring og en potensiell fallgruve kan være klassifiseringen av feil i farlige oppdagede og uoppdagede. Dersom disse feilene kategoriseres ukritisk i de to metodene, vil dette kunne føre til ukorrekte feilrater med tilhørende stor usikkerhet. Dette skyldes at feil kan være av en slik art at disse ikke lar seg reparere innefor et kort tidsintervall, som for eksempel dersom komponenten/systemet er vanskelig tilgjengelig. Det kan med dette i enkelte tilfeller være mer rasjonelt å klassifisere farlige oppdagede feil som farlige uoppdagede feil umiddelbart, dersom disse ikke kan repareres innen kort tid. Her vil lokale rutiner og operasjonsfilosofi, samt menneskelige og organisatoriske forhold, kunne betraktes å ha stor betydning. Det synes med dette å være avgjørende at feilrater baseres på ekspertvurderinger for å håndtere den iboende usikkerheten knyttet til klassifisering av feil, der usikkerheten vil være betinget på tilgjengelig kunnskap på det tidspunktet feilraten ble kategorisert.

Et av de mest kritiske elementene ved fastsettelse av PFD er med dette de tilgjengelige inndata og tilgjengelig informasjon for fastsettelse av feilrater. Det er nødvendig, enten ved testing eller operasjonell erfaring, å komme frem til mest mulig reelle feilrater for det systemet som betraktes. I dette systemcaset har dette ikke vært av signifikant betydning siden analysen ikke vil bli brukt i annen utstrekning enn denne oppgaven, og fordi de angitte

feilratene ikke nødvendigvis måtte gjenspeile de faktiske feilratene for å illustrere ulikheter mellom metodene.

Det bør videre bemerkes at begge metodene er basert på statistisk atferd av systemer, og dermed tar utgangspunkt i, og betrakter, statistiske sammenhenger der usikkerhet reduseres ved å samle inn mer driftsdata. Det bør likevel igjen nevnes at PDS metoden legger til rette for oppdatering av parametre for å tilpasse dette til applikasjons- og anleggsspesifikke forhold. Således har metoden til dels utviklet en fremgangsmåte for å redusere statistisk (aleatorisk) usikkerhet ved å oppdatere feilrater etter hvert som nye operasjonelle data foreligger, og samtidig gjøre bruk av kvalitative vurderinger som kan bidra til å redusere (epistemisk) usikkerhet ved fastsettelse av nye parameterverdier. Det ble tidligere i oppgaven diskutert at usikkerhet også må relateres til den kunnskapen som foreligger for å betrakte og uttrykke sannsynligheter for svikt. I den sammenheng bør det nevnes at ingen av metodene eksplisitt inneholder noen form for usikkerhetsvurderinger som strekker seg ut over kategorisering av hardware feil. PDS metodens håndtering av systematiske feil og testuavhengige feil kan likevel betraktes å delvis være underlagt ekspertvurderinger om underliggende sammenhenger, der grad av lokal forankring til dels blir uttrykt i applikasjonsspesifikke verdier. I anledning at oppgaven tidligere har diskutert behovet for å kunne uttrykke usikkerhet, fortrinnsvis med basis i gitt kunnskap (K), synes ikke kunnskaps- eller usikkerhetsdimensjonen å bli tilstrekkelig håndtert eller reflektert i de to metodene i tilknytning til PFD (P). Det vil si at ingen av metodene ser ut til å eksplisitt uttrykke at det bør gjennomføres en systematisk fremgangsmåte for å akkumulere informasjon i tilknytning til systemets lokale operative driftsforhold, men også at det i metodene ikke foreligger en fremhevet vurdering av den usikkerheten som er forbundet med angitt PFD prediksjon. Dette synes å være vesentlig for å kunne redusere tilhørende epistemiske usikkerhet og samtidig gi beslutningstaker informasjon om prediksjonens kvalitet, og vil bli nærmere drøftet i senere kapitler av oppgaven.

6.2 Anvendelse av metodene

Med utgangspunkt i grunndataene fra systemanalysen av caset er sikkerhetsutilgjengelighet, herunder total sannsynlighet for svikt på etterspurt tid (PFD), ved de to metodene kalkulert til:

$PFD_{IEC\ 61508\ metoden} \approx 3{,}27E\text{-}06$

$PFD_{PDS\ metoden} \approx 3{,}04E\text{-}06$

Av overnevnte kan det antydes at PDS metoden totalt sett gir ett mer konservativt uttrykk for sikkerhetsutilgjengelighet enn IEC 61508 metoden. Dette vil fortrinnsvis skyldes at PDS metoden benytter en modifikasjonsfaktor (C_{MooN}) for å uttrykke redundant konfigurasjon (votering), og tar høyde for sannsynligheten for testuavhengige feil (P_{TIF}). Det er videre liten ulikhet i prediksjonene, ettersom begge metodene tar utgangspunkt i gjennomsnittsraten av farlige uoppdagede feil (λ_{DU}). Da vil, som tidligere nevnt, også IEC 61508 metoden implisitt inkludere deler av de systematiske feilene, og uten oppdatering av applikasjons- og anleggsspesifikk rate for $\lambda_{DU\text{-}S}$, så vil begge metodene med dette anvende den samme gjennomsnittsraten av farlige uoppdagede feil.

En del faktorer slik som redundans og konfigurasjon (votering) kan i drift, så vel som i denne systemanalysen, antas å primært være påvirket av beslutninger som blir tatt under design (Lundteigen, 2010). Feilratene er derimot en ukjent størrelse som i driftsfasen må besluttes, der feilraten av farlige (uoppdagede) feil ikke nødvendigvis er slik de var under design og slik pålitelighetsdata fra leverandører eller databaser skulle tilsi. Særlig avgjørende er det at metodene er i stand til å gjenspeile systematiske forhold som kan påvirke det aktuelle system, for eksempel forhold som systematisk vil ha innvirkning på feilrater som følger av lokale operative driftsforhold. Feilrater og testintervaller er med dette parametre som ved kvantifisering av PFD i driftsfasen potensielt kan antas å påvirke mulighetene for verifikasjon i henhold til underliggende SIL krav, altså der operasjonelle forhold, drift og slitasje vil kunne påvirke sannsynligheten for svikt på etterspurt tid. Det er med dette av særlig interesse at de to metodene i driftsfaser klarer å gjenspeile feilrater for reelle operasjonelle driftsforhold, og at testintervallene gjennomføres med gode rutiner og oppdaterte tidsintervaller.

I industrier er det i stor grad slik at testintervaller gjennomføres etter fastlagte rutiner og med faste tidsintervaller. Eventuell oppdatering av tidsintervall for testing vil dermed følge et kost-nytte forhold, og anses som et punkt som strekker seg ut over primærfokus i denne oppgaven. I kombinasjon med oppgavens begrensninger som følger av avsatt tid, vil testintervall og oppdatering av dette som sådan ikke bli nærmere håndtert. Dette henger også sammen med at denne oppgaven ikke vil ha fokus på om de kalkulerte PFD prediksjonene kan verifiseres i henhold til underliggende SIL krav, men at primærfokus vil være styrker og svakheter i håndteringen av usikkerhet i prediksjonene.

6.3 Oppdatering av inndataparametre

Når systemer settes i drift utsettes gjerne disse for nye operasjonelle forhold og faktorer, samtidig som alle relevante betraktninger ikke nødvendigvis er tatt høyde for i design. Det er med dette avgjørende å kunne si noe om den erfarte PFD fra drift i forhold til den beregnede PFD'en fra design. Ingen av metodene ser i dag ut til å direkte nytte Bayesiansk oppdatering, til tross for at de underliggende betrakter at dette vil være viktig. Det foreligger likevel en kvasi Bayesiansk oppdatering, som delvis kombinerer generiske data og ekspertvurderinger av feilrater og testintervaller i PDS metodens anbefaling for oppfølging av SIS i driftsfaser. Det er i dette tilfellet viktig å få frem at denne oppdateringen ikke ser ut til å inkludere andre systematiske metoder og/eller betraktninger for å akkumulere kunnskap om systemet det tas utgangspunkt i. For nye systemer som settes i drift, og ved ny teknologi, er det særlig avgjørende å benytte systematiske vurderingsmetoder og ekspertkunnskap for å redusere den epistemiske usikkerheten. Den epistemiske usikkerheten kan derimot til en viss grad anses å være dekket av de generiske dataene (feilratene) etter hvert som systemet oppnår lang driftserfaring.

De anleggsspesifikke betraktningene for parametrene λ_{DU-S} i PDS metoden er delvis knyttet til ekspertvurderinger som vurderer godheten av rater for stress-, design- og interaksjonsfeil. Det vil si at metoden kun justerer for årsaker til feil som er knyttet til forannevnte feilkategorier, og dermed ikke fanger opp alle systemspesifikke forhold som berører årsaker til systematiske feil (S. Hauge, Hokstad, et al., 2006). Dette kan for eksempel være anleggsspesifikke lokale værforhold, luftfuktighet og lignende. Det vil med dette være opp til den enkelte pålitelighetsanalytikeren å justere for eventuelle øvrige forhold, der det i overnevnte ikke foreligger noen metodisk fremgangsmåte for å vurdere fullstendighet/ufullstendighet og således usikkerheten knyttet til alle relevante forhold. Det kan tenkes at en metodisk fremgangsmåte for å avdekke og håndtere slike forhold, kunne vært basert på en systematisk tilnærming for å identifisere scenarier som kan medføre fare eller operasjonelle problemer knyttet til det aktuelle system.

For P_{TIF} parameteren presenteres gjennomsnittsverdier som tverrsnittet av ulike systemer i PDS datahåndboken (S. Hauge, Hokstad, et al., 2006). Ved å benytte applikasjons- eller anleggsspesifikke verdier så vil man også ved denne faktoren kunne gi mer representative kalkulasjoner. De anleggsspesifikke betraktningene er relatert til kvalitative vurderinger av fullstendigheten ved en funksjonstest som kategoriseres etter testenes godhet (Fullstendig test, Utvidet test, Normal test, Forenklet test). Parameteren multipliseres her med en konstant som er knyttet til ulike kategoriene av testenes fullstendighet, der

oppdateringsmetoden som presenteres ikke kan betraktes som komplett dekkende for alle forhold som påvirker P_{TIF} (S. Hauge, Hokstad, et al., 2006). Det er også ved oppdatering av denne parameteren opp til pålitelighetsanalytikeren(e) eller en ekspertgruppe å justere for eventuelle øvrige forhold, samt å betrakte fullstendigheten av nåværende og tidligere utførte tester.

Dataene for β er i PDS metoden, så vel som i IEC 61508 metoden, basert på gjennomsnittsverdier for industrien (S. Hauge, Hokstad, et al., 2006). De anleggsspesifikke betraktningene som er relatert til den utvidede versjonen av β-faktor modellen som benyttes i PDS metoden, er videre knyttet til "grad av beskytelse" mot CCF. Det er med dette opp til pålitelighetsanalytikeren(e) å gjøre en vurdering av systemets beskyttelse mot CCF (Veldig god, Utvidet, Normal, Redusert), der β-verdien deretter multipliseres med forhåndsbestemte konstanter som er knyttet til de ulike gradene av beskyttelse. Slik det var tilfelle for PDS metodens applikasjonsspesifikke vurdering av λ_{DU-S} og P_{TIF}, så er også metoden som presenteres for applikasjonsspesifikke β-verdier knyttet til ufullstendighet rundt påvirkningsfaktorene (S. Hauge, Hokstad, et al., 2006). På denne måten legges "dokumentasjonsbyrden" på produsenter og brukere av SIS for å dokumentere de tiltak som iverksettes for unngåelse av CCF, der det kan tenkes situasjoner hvor slik dokumentasjon kan være mangelfull og/eller ikke tilstedeværende. Slike eventuelle implikasjoner kunne vært redusert, samtidig som det ville kunne foreligge et sterkere prediksjonsgrunnlag, dersom det hadde vært benyttet en systematisk tilnærming for å identifisere eventuelle barrierefunksjoner for å unngå farer og operasjonelle problemer knyttet til det aktuelle system.

IEC 61508 metoden anvender såkalte sjekklister for å tilpasse β til lokale operasjonelle driftsforhold. Denne tilnærmingen anses som omfattende og godt dekkende for å redusere tilhørende (epistemisk) usikkerhet i β-faktoren og omkringliggende fullstendighet i predikert parameterverdi. Sjekklistene anses å være godt egnet som grunnlag for en systematisk vurdering og identifisering av β, men det legges til grunn at disse ikke har blitt gjennomgående og systematisk betraktet i denne oppgaven. Det forutsettes derimot at sjekklistene må gjennomgås tilstrekkelig, og at det legges til grunn ekspertvurderinger for å vurdere effekten av eventuelle påvirkningsfaktorer og barrierer på det aktuelle system.

Tilnærmingene for applikasjons- og anleggsspesifikk oppdatering, særlig i utstrakt kombinasjon med ekspertvurderinger, anses i denne oppgaven å redusere usikkerhet i tilknytning til inndataparametrene og vurderinger av PFD prediksjonenes fullstendighet. Dette anses som gode prinsipper som i industrien bør vektlegges, til tross for at dette kan oppfattes som omfattende og ressurskrevende.

6.3.1 Resultater fra oppdatering av grunndata i systemanalysen av caset

For å illustrere hvordan IEC 61508 og PDS metoden tar høyde for variasjon knyttet til fullstendighet og inndataparametrene, har det blitt foretatt en applikasjons- og anleggsspesifikk oppdatering for å tilpasse systemet til et tenkt scenario. Dette kan også forstås som en enkel sensitivitetsbetraktning der det på bakgrunn av oppdatering av inndataparametre er mulige å betrakte variasjon i resultatet, altså predikert PFD. Utgangspunktet for oppdateringen er gjennomsnittsverdiene for inndataparametrene som er angitt som grunndata for analysen. Mer informasjon knyttet til selve oppdateringen og bakenforliggende antakelser foreligger i appendiks B.

Med utgangspunkt i oppdaterte inndataparametre i systemanalysen av caset så er sikkerhetsutilgjengelighet, herunder total sannsynlighet for svikt på etterspurt tid (PFD), ved de to metodene nå kalkulert til:

$PFD_{\text{IEC 61508 metoden}} \approx 2{,}99\text{E-}06$

$PFD_{\text{PDS metoden}} \approx 1{,}08\text{E-}05$

Av overnevnte kan det observeres at det etter applikasjons- og anleggsspesifikk oppdatering fortsatt er IEC 61508 metoden som gir den mest optimistiske prediksjonen av PFD, slik det var i kalkuleringene med utgangspunkt i grunndata. PDS metoden gir videre et mer konservativt uttrykk for predikert PFD etter oppdateringen, mens IEC 61508 gir et mer optimistisk uttrykk for predikert PFD etter oppdateringen.

Det mer optimistiske uttrykket for kalkulert PFD i IEC 61508 metoden, skyldes fortrinnsvis antakelsen om at en ekspertgruppe basert på sjekklisten har kommet frem til en β-verdi for angitt system tilsvarende 30 % av hva gjennomsnittsverdien er i grunndataene. Dette betyr at 70 % feilene som foreligger under ”normale” forhold nå vil forhindres, noe som vil gi grunn til å anslå en mer optimistisk prediksjon for sannsynligheten for svikt på etterspurt tid (PFD).

Det mer konservative uttrykket for kalkulert PFD i PDS metoden, skyldes fortrinnsvis antakelsen om at implementering av systemspesifikke tiltak for systematiske interaksjonsfeil er anslått å være mindre enn tilstrekkelig. Dersom en ekspertgruppe, slik som i dette tilfelle, således hadde anslått effekten av tiltak mot systematiske interaksjonsfeil å være fraværende, så ville de kunne predikert en mulig frekvens av slike feil. I dette tilfellet ble det antatt at ekspertgruppen anså denne frekvensen å være høy, og at sannsynligheten for interaksjonsfeil således var betydelig. Dette ble deretter vektet mot øvrige faktorer av

påvirkning på raten av farlige uoppdagede systematiske feil (λ_{DU-S}). Som et resultat av dette kunne det observeres at frekvensen av λ_{DU-S} økte med en faktor på 2,058 for hver enkelt komponent, og at den totale raten av farlige uoppdagede feil (λ_{DU}) resulterte i en mer konservativ frekvens.

Applikasjons- og anleggsspesifikk oppdatering av inndataparametrene P_{TIF} og β, vil isolert sett i den oppdaterte systemanalysen av caset resultere i en mer optimistisk prediksjon av PFD. Dette kommer av antakelsene der en ekspertgruppe antas å ha dokumentert og anslått utvidede testprosedyrer for de funksjonelle testene, og at omkring 70 % av eventuelle feil som avdekkes under "normale" gjennomsnittlige funksjonstester i grunndataene nå vil avdekkes i den utvidede testen. I tillegg ligger det til grunn en antatt dokumentasjon der det er implementert og foreligger et utvidet nivå av beskyttelse mot CCF i systemet. En ekspertgruppe har således kommet frem til at frekvensen av CCF er redusert, og dette vil tilsvare omkring 50 % av CCF av grunndataene. Likevel kan det ut i fra kalkulasjonene i PDS metoden observeres at den totale PFD prediksjonen nå er mer konservativ, som følger av vurderinger som legger til grunn og den økte rate av systematiske feil. Dette vil også kunne betraktes som en indikasjon på at systemet er sensitivt for variasjon i systematiske feil, og at usikkerhetsvurderinger omkring disse parameterverdiene i særlig stor grad bør vektlegges.

Som det tidligere i oppgaven har blitt diskutert, bør grad av usikkerhet (U) i tilknytning til den informasjon og kunnskap (K) som ligger til grunn for sannsynlighetsprediksjonen (P) uttrykkes. I ekspertvurderingene som ligger til grunn for applikasjons- og anleggsspesifikk oppdatering, ser ingen av metodene ut til eksplisitt å uttrykke betydningen av usikkerhetsvurderinger. Dette vil bli nærmere belyst i senere kapitler av oppgaven.

7 Drøfting

Sikkerhets- og pålitelighetsvurderinger bygger på en rekke antakelser om systemer og hvilke forhold disse driftes under. Dersom beslutningstakere ikke er klar over graden av usikkerhet knyttet til disse forutsetningene og betingelsene, kan resultatene feiltolkes og verken gi eller beskrive et operasjonelt risikobilde for SIS (Lundteigen, 2009).

De to metodene, IEC 61508 og PDS, er begge i tråd med hovedprinsippene i IEC-standardene, og er begge nyttige verktøy for implementering og verifisering av kvantitative (SIL) krav som beskrevet i IEC 61508 og OLF 070. For enkelte områder som feilklassifisering, modellering av feilårsaker (CCF) og ved håndtering av systematiske feil (DU-S og TIF), skiller metodene til tross for dette på fremgangsmåte og hva som inkluderes i prediksjonene.

I det følgende vil det utdypes hvordan de underliggende faktorene og ulikhetene kan påvirke nivået av usikkerhet i metodenes utilgjengelighetskalkulasjoner, herunder PFD prediksjoner. Dette vil bli gjort med utgangspunkt i operasjonaliseringen av usikkerhet som ble presentert i delkapittel 2.2, hvor disse faktorene vil bli drøftet for å kunne gi svar på oppgavens underliggende problemstilling.

7.1 Usikkerhet som følger av ufullstendighet

Som tidligere beskrevet bør manglende kunnskap eller erfaring med systemet det tas utgangspunkt i, betraktes når det skal utføres pålitelighetsanalyser hvor dette kan lede til at relevante feil ikke blir identifisert og/eller riktig kategorisert. Siden inndata til analysene i stor grad er generiske data, er det vanskelig å spore om alle relevante feilmodi er inkludert. Det bør videre bemerkes at OREDA i enkelte tilfeller inneholder en feilkategori som kalles ”ukjent”. Dette kan gi grunn til å tro at farlige feil til tider ikke blir tatt hensyn til i pålitelighetsanalysene, og at dette således kan øke usikkerheten i begge metodene. Det er videre vanskelig å anslå den ukjente delen av ufullstendighetsusikkerhet, som for eksempel ukjente feil. I stor grad må det dermed festes tillit til at vurderingene omfatter de viktigste og mest betydningsfulle aspektene av systemene, der eventuelle konservative anslag synes å bli nyttet for å kompensere for eventuelle glemte eller ukjente elementer. Det bemerkes videre at de to metodene kunne anvendt ekspertvurderinger i tilknytning til FMEDA/FMECA analyser, for å vurdere i hvilken grad analysene inkluderer alle relevante feilmodi.

IEC 61508 metoden synes videre å ikke behandle effekten av menneskelig interaksjon, noe som kan betraktes som en ukjent ufullstendighetsusikkerhet som kan være av betydning. Grad av kjennskap til denne effekten kan diskuteres, men det synes videre som om PDS metoden forsøker å justere for slik interaksjon i form av systematiske feil (λ_{DU-S}) og sannsynligheten for testuavhengige feil (P_{TIF}). Menneskelig interaksjon skjer normalt under vedlikehold, testing og modifikasjon, og bør inkluderes i pålitelighetsanalysene. Mange leverandører hevder videre at de leverer systemer med gjennomsnittlig tid til feil (MTTF) som i enkelte tilfeller strekker seg til mange tusen år. Likevel, så opplever mange operatører kritiske feil i systemer (Janbu, 2009). Således er det åpenbart at det er noen aspekt som påvirker påliteligheten til SIS, og som bør videre utredes. Menneskelig interaksjon synes videre å være en av dem.

7.1.1 Bør systematiske feil kvantifiseres?

Når det gjelder kvantifisering av λ_{DU-S} og P_{TIF} bør det noteres at (OLF-070, 2004):

1. systematiske feil synes å være nært linket til aktuelle applikasjoner og installasjoner
2. objektive data for systematiske feil foreligger ikke, og sammen med lite historisk datamateriale, vil tallfesting i større grad måtte være basert på subjektive data og ekspertvurderinger

(1) verdier for systematiske feil som er nært linket til aktuelle applikasjoner og installasjoner kan blant annet betraktes å være en funksjon av lokal produksjonsprosess, de operative prosedyrene og sikkerhetsfilosofi. Dette relateres til ulike typer av systematiske feil, der disse blant annet kan oppstå som følger av stress og belastning ut over design, operasjonelle feil som er initiert av menneskelig svikt under drift eller vedlikehold/testing og lignende, og på denne måten vil kunne påvirke feilrater (DU-S) og lokale P_{TIF} verdier. Noen av disse feilene er som tidligere nevnt knyttet til andre grensesnitt, som for eksempel miljø og andre lokale aspekt, men vil likevel systematisk kunne påvirke sikkerhetstapet og være nært knyttet til aktuelle applikasjoner og installasjoner. Det anses videre å være svært viktig at lokale operative forhold gjenspeiles i pålitelighetsanalysene, og således vil λ_{DU-S} og P_{TIF} prediksjoner kunne bidra til å styrke pålitelighetskalkuleringene.

(2) I følge klassisk relativ frekvens paradigmet (realistfortolkningen), kan sannsynligheten for systematiske feil tolkes som den relative andelen av ganger systematiske feil oppstår dersom systemet opererer under de samme betingelsene over en uendelig periode. Men den underliggende sannsynligheten er ukjent, og estimeres i pålitelighetskalkulasjoner. Dersom

denne sannsynlighetsfortolkningen benyttes, vil det måtte tas hensyn til at anslått pålitelighet kan være unøyaktig i forhold til en tenkt underliggende *sann* pålitelighet. Usikkerheten i estimatene vil med dette være vesentlig, og vanskelig kunne uttrykkes på siden av sannsynlighetsestimatet. Den alternative subjektive fortolkningen betrakter derimot sannsynligheten som et mål på usikkerhet omkring andelen av systematiske feil, sett gjennom pålitelighetsanalytikerens tilgjengelige bakgrunnsinformasjon og kunnskap.

Etter den subjektive (prediktiv epistemisk) fortolkningen, tildeles en sannsynlighet etter gjennomførte usikkerhetsvurderinger og usikkerhetsbetraktninger, og det foreligger ingen referanse til sanne og absolutte sannsynligheter. En sannsynlighet for systematiske feil vil uansett være betinget på bakgrunnsinformasjon, og gitt denne bakgrunnsinformasjonen er det ingen usikkerhet relatert til den satte sannsynligheten siden denne er et uttrykk for usikkerheten (Aven, 2008a). Imidlertid er ikke en sannsynlighet alene et perfekt verktøy til alle slike formål. De tildelte sannsynlighetene er betinget av en bestemt bakgrunnsinformasjon, og vil kunne gi ufullstendige prediksjoner om fremtidige hendelser. Overraskelser i forhold til satt sannsynlighet kan forekomme, og ved å sette en sannsynlighet kan slike overraskelser bli oversett (Aven, 2008a).

Så, kan sannsynligheter med dette betraktes som ”objektive”? Ved betraktning av systematiske feil kan ikke slike feil relateres til gjentatte konstruerte eksperiment under like betingelser. Antatt like feildata innhentes, men på mikronivå vil disse kunne være spesielt knyttet til spesifikke installasjoner, ulike testforhold, ulike operasjonelle prosedyrer og så videre. Sett ut i fra overnevnte, er det ikke åpenbart hvordan man skal gjennomføre uendelig testing under like forhold, og dermed er det ikke mulig å betrakte pålitelighetstendenser ut i fra den tro at det foreligger ”objektive” sannsynligheter. Sannsynligheter må i pålitelighetsanalyser altså betraktes ut i fra det prediktive perspektivet, der det ikke er noen usikkerhet relatert til pålitelighetsanalysen, men usikkerhet knyttet til bakgrunnsinformasjonen og vurderingene som foreligger når denne blir betraktet. Det er med dette avgjørende å reflektere lokale operative forhold for å redusere usikkerheten knyttet til pålitelighetsanalysene.

I PDS har det blitt dokumentert at *”sikkerhetsfunksjoners utilgjengelighet ofte er forårsaket av systematiske feil”* (OLF-070, 2004), som for eksempel:

- Detektorsvikt på grunn av feilplassering
- Detektorer som ikke er i stand til å skille mellom ekte og falske alarmer
- Utilstrekkelige funksjonelle testprosedyrer

- Menneskelige feil under funksjonell testing, som f. eks. gal kalibrering av transmitter
- Feil i nedstengningsventil hvis operatører f. eks. har etterlatt isolasjonsventil avstengt i lukket stilling
- Unnlate å utføre sikkerhetsfunksjon som følger av software feil

Dette er elementer som i PDS metoden er underlagt systematiske feil. I PDS metoden hevdes det at det ikke er fornuftig å kun tallfeste bidraget fra hardware feil, og etterlate seg et så stort bidrag til sikkerhetstap. Det foreligger videre en enighet om at det kan være vanskeligere å kvantifisere systematiske feil. PDS metoden lykkes likevel i å gi typiske generiske verdier for λ_{DU-S} og P_{TIF}, samt å ha utviklet en tilnærming for å opprettholde anleggsspesifikke λ_{DU-S} og P_{TIF} verdier (S. Hauge, Hokstad, et al., 2006; OLF-070, 2004). Det burde også være mulig å komme frem til enklere tilnærminger, for eksempel i tråd med å opprettholde anleggsspesifikke β'er slik som det er presentert i IEC 61508-6, D (1998) (OLF-070, 2004).

Det bør som tidligere nevnt noteres at IEC 61508 metoden implisitt kvantifiserer deler av de systematiske feilene gjennom foreslått metode for kvantifisering av tilfeldige hardware feil og hardware relaterte common cause failures (CCF) (IEC 61508-6, D, 1998). Tilnærmingen som er valgt av IEC er forståelig ettersom feilrater for systematiske feil ofte er vanskelige å predikere, og vil avhenge av hvert enkelt prosessanlegg. På en annen side foreligger det en rekke grunner til at man også burde forsøke å kvantifisere bidraget fra systematiske feil, slik som i PDS metoden. Et av hovedformålene ved gjennomføring av pålitelighetsanalyser, er blant annet å predikere hvordan systemet faktisk vil operere under normale driftsforhold (som motsetningen til laboratorium forhold) på spesifikke prosessanlegg. Tilsvarende, ved å benytte feilestimater i kvantitative risikoanalyser (QRA) og andre analyser, vil det med dette være viktig å benytte mest mulig realistiske rater for å reflektere den faktiske risikoen som er relatert til driften (S. Hauge, Hokstad, et al., 2006).

Systematiske feil kan videre være et stort og dominerende bidrag til den totale sannsynligheten for feil. Dette kan for eksempel ses ved at det foreligger store avvik mellom sertifikat-/produsentdata (der disse som oftest kun er relatert til tilfeldige hardware feil), og data fra faktisk ytelse i drift (noe som også vil omfatte systematiske feil) (S. Hauge, Hokstad, et al., 2006; S. Hauge, Langseth, & Onshus, 2006). Ulikehetene i relasjon til de to metodenes PFD kalkulasjoner fra systemanalysen av caset skyldes i hovedsak også oppdatering av systematiske feil med antatt ytelse fra drift. Det kan av overnevnte dermed betraktes som noe ulogisk og ufullstendig å kun inkludere deler av feilratene i pålitelighetskalkuleringene.

7.2 Usikkerhet i modellene

Både IEC 61508 metoden og PDS metoden antar som tidligere nevnt statistisk atferd for de systemer det tar utgangspunkt i. Begge metodene er i stor grad knyttet til forhåndsdefinerte feilrater fra pålitelighetsdatabaser, samt feil som eventuelt oppdages under testing eller rutinemessig kontroll. Sett ut i fra et klassisk sannsynlighetsperspektiv så vil metodene kunne betraktes som dekkene i den grad de representerer et tilstrekkelig stort datagrunnlag for det system (eller tilsvarende systemer) som det tas utgangspunkt i, der usikkerhet i modellen således vil være knyttet til om man står ovenfor "rett" modell for å reflektere virkeligheten. Under betraktninger om bruk av riktig modell, som gjerne er eksakt og som representerer den riktige modellen for et fenomen, refereres det til en korrekt sannsynlighetsfordeling. Således er det relevant å diskutere modellusikkerhet, altså avviket mellom "korrekt" modell og den som benyttes (klassisk relativ frekvens perspektiv). Ut i fra et prediktivt sannsynlighetsperspektiv, betraktes derimot modellene som kun inkluderer statistisk atferd å være betinget med stor grad av usikkerhet. Modellene tar ikke høyde for eventuelle betraktninger knyttet til lokale forhold, og således representerer disse stor epistemisk usikkerhet. Ut i fra et prediktivt perspektiv, vil det videre ikke være like avgjørende å betrakte modellusikkerhet. Dette kommer av at man ut i fra en prediktiv tenkning ikke vil betrakte usikkerheten i modellen, ettersom denne kun kan forstås som en forenkling av virkeligheten. Siden det i denne oppgaven ikke er nærliggende å fokusere på om det foreligger en rett verdi, vil videre drøfting omkring operasjonalisering av modellusikkerhet således ikke anses som relevant i denne kontekst.

7.3 Usikkerhet i inndata

Som tidligere nevnt vil de miljømessige forholdene for systemer variere, og dermed vil pålitelighetsdata være avhengig av det spesifikke systemet som analyseres. Stor grad av usikkerhet foreligger derfor ved kun å feste tillit til generisk informasjon i form av leverandørdata og testdata fra andre systemer.

Pålitelighetskalkuleringene med utgangspunkt i grunndataene for systemanalysen av caset som angis i appendiks B, har kun benyttet generiske data fra databaser. Mange rapporter for SIL verifikasjon benytter videre leverandørdata for systemer, som normalt presenterer en lavere feilrate enn hva de generiske dataene gjør (Janbu, 2009). Dette kan som tidligere diskutert skyldes flere forhold. Leverandørdata samles ofte inn fra systemer som er tilknyttet

nyere teknologi enn hva de generiske dataene er basert på, og påliteligheten til like systemer kan således variere. Leverandørdata blir også ofte betraktet å bestå av lite felterfaring, samt være samlet inn under laboratorieforsøk og andre testforhold som gjerne ikke svarer til systemets reelle etterspørsel. Hvis dette skulle være tilfelle ville viktige faktorer som menneskelig interaksjon, systemenes operasjonelle driftsmiljø, og så videre ikke være reflektert. Feilratene vil i så tilfelle kunne betraktes som optimistiske ettersom disse vil kunne være underestimerte. Store ulikheter mellom leverandør og generiske data øker dermed usikkerheten knyttet til prediksjonene, både fra et klassisk relativ frekvens perspektiv så vel som et subjektivt Bayesiansk perspektiv. Usikkerheten ville i så tilfelle kunne reduseres ved å hente inn mer driftsdata ut i fra det klassiske perspektivet, mens det prediktivt subjektive perspektivet ville redusert usikkerheten ved å øke kunnskapen (redusere epistemisk usikkerhet) om lokale operasjonelle forhold ved for eksempel ekspertvurderinger.

Ikke bare foreligger det ulikheter mellom leverandørdata og generiske data, men også ulikheter mellom de generiske dataene som presenteres i ulike pålitelighetsdatabaser vil kunne forekomme. En sensitivitetsstudie som er presentert i Janbu (2009) viser at to ulike feilrater for samme komponent fra henholdsvis OREDA og OLF 070, resulterte i signifikant ulike prediksjon av sikkerhetsutilgjengeligheten. Dette indikerer at nivået av datausikkerhet er relativt høyt, og kan være avgjørende for om systemet møter de spesifiserte akseptkriteriene (SIL kravene) eller ikke. Videre så ville det ikke foreligge noe nivå av datausikkerhet ut i fra et prediktivt epistemisk perspektiv, der prediksjonen av sikkerhetsutilgjengelighet nettopp ville kunne anses som et mål på usikkerheten, betinget på tilgjengelig bakgrunnsinformasjon. Det er likevel viktig å ikke forstå dette som om at all usikkerhet er eliminert, da det kan foreligge stor grad av usikkerhet knyttet til den kunnskapen som foreligger. Usikkerheten knyttet til den informasjonen og kunnskapen som foreligger, er blant annet avhengig av grundighet i analyser og forhold som benyttes for å øke systemforståelsen og kunnskapen omkring systemet som analyseres.

7.3.1 Applikasjons- og anleggsspesifikk oppdatering

For å raskt oppsummere forhold knyttet til applikasjons- og anleggsspesifikk oppdatering knyttet til de to metodene, så synes IEC 61508 metoden å representere relativt stor grad av epistemisk usikkerhet knyttet til ufullstendighet og parameterverdier i forhold til PDS metoden. Dette kan begrunnes i at IEC 61508 metoden ikke legger til grunn ekspertvurderinger for å oppdatere parametrene ut over sjekklisten som benyttes for β-

faktorer, og på denne måten ikke forsøker å identifisere og inkludere alle relevante faktorer og farer i kalkulasjonene. PDS metoden tar videre høyde for kombinasjonen av generiske data og anleggsspesifikke betraktninger. Det medfører likevel begrensninger at betraktningene skal være knyttet til forhåndsdefinerte kvalitative kategorier, som igjen inkluderes ved å multiplisere med en forhåndsdefinert konstant. Det antas at PDS metoden har etablert forhåndsdefinerte kategorier og konstanter for å forenkle, samt gjøre metoden lettere anvendelig. Tatt i betraktning at applikasjons- og anleggsspesifikk oppdatering hadde vært myntet på ekspertvurderinger av personer med god bekjentskap til systemet, ville de forhåndsdefinerte kategorier betraktes som unødvendig i den grad ekspertene ville vært best egnet til å predikere godhet, usikkerhet og fullstendighet i inndataparametrene. Så sant de forhåndsdefinerte kategoriene og konstantene ikke betraktes som endelige og ufravikelige, så anses dette likevel som en god tilnærming.

Som beskrevet dekker ikke de ulike inndataparametrene i noen av metodene alle forhold av påvirkning. Dette kan være seg i hvilken grad de gjenspeiler systemers operasjonelle driftsforhold knyttet til vær og vind, og/eller andre forhold som kan betraktes som ufullstendig dekket. Det kan tenkes at tilstrekkelig akkumulasjon av relevant informasjon, som igjen knyttes til og betraktes ut i fra ekspertvurderinger, ville kunne resultert i redusert usikkerhet i tilknytning til både inndataparametrene og fullstendigheten av prediksjonene. En systematisk tilnærming for å identifisere scenarioer som kan medføre fare eller operasjonelle problemer knyttet til det aktuelle system, kunne således vært nyttet for å redusere tilhørende epistemisk usikkerhet knyttet til begge metodene. En slik systematisk tilnærming er inkludert og nærmere beskrevet i kapittel 8.

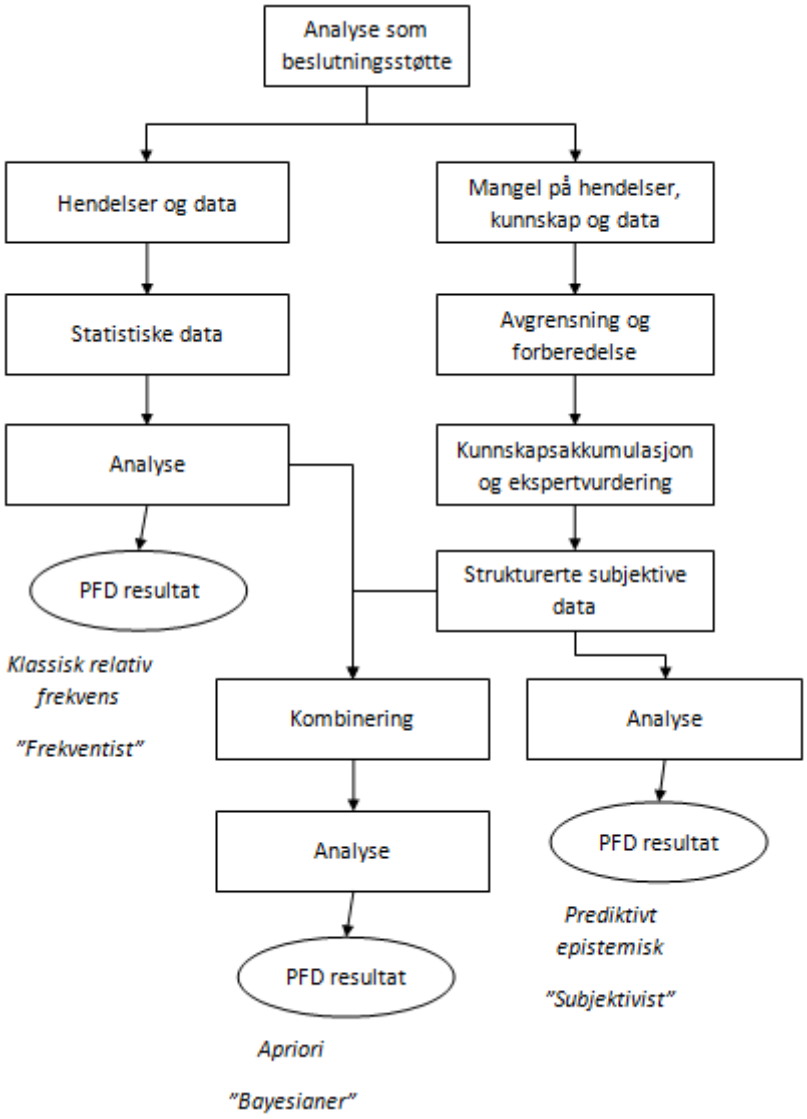
7.4 Ulike tilnærminger fra datainnsamling til PFD prediksjon

Basert på IEC 61508 metodens fokus på statistiske inndata, samt tilhørende håndtering og analyse, kan dette betraktes som en fremgangsmåte som er knyttet til klassisk relativ frekvens perspektiv (frekventist). Dette kommer av at metoden relaterer farlige feil til dens relative frekvens, der sannsynligheten for svikt på etterspurt tid er et direkte uttrykk for andelen av ganger en hendelse inntreffer i en tenkt uendelig populasjon av observasjoner gjort under identiske forhold. Ut i fra tidligere drøftinger der det har kommet frem at det ikke foreligger homogene feilrater for systemer, vil denne metoden i praksis være betinget med stor grad av epistemisk usikkerhet uavhengig av om datamaterialet fra systemet (eller tilsvarende systemer) er stort. Ut i fra oppgavens underliggende usikkerhetsperspektiv, representerer IEC 61508 metodens fremgangsmåte for analyse som beslutningsstøtte stor

grad av usikkerhet knyttet til både inndata og fullstendighet. Det foreligger altså ingen direkte underliggende vurdering av om alle relevante feilmodi er inkludert i den grad disse ikke kun er hentet fra databaser, samtidig som metoden ikke tar høyde for et stort og viktig bidrag for sikkerhetsutilgjengelighet ved å ikke kvantifisere de systematiske feilene (λ_{DU-S} og P_{TIF}, eller eventuelt PSF). Metoden ser med dette ut til å anvende en "frekventistisk" tilnærming til håndtering av sikkerhetsutilgjengelighet i den grad inndata kun er hentet fra databaser, og det ikke foreligger noen kategorisering (FMEDA/FMECA etter test) og ekspertvurdering av feilrater. Dette er nærmere illustrert i figur 7.1 under.

PDS metoden forsøker som nevnt ovenfor å oppdatere de generiske feilratene, og vil dermed i en analyse for beslutningsgrunnlag hente inn lokale operasjonelle driftsdata for å oppdatere de statistiske dataene. Disse kan dels betraktes som strukturerte subjektive data, og i kombinasjon med anvendelse av tidligere feilrater fra angitt system (og tilsvarende systemer), kan PDS metoden betraktes å nytte a priori kunnskap som representerer grensen mellom en frekventisk og den prediktivt Bayesianske tilnærmingen til statistikk. PDS metoden kan delvis betraktes som subjektiv i den grad evalueringen og oppdateringen av feilrater er basert på betraktninger om tidligere observasjoner. Dersom inndataparametrene kun hadde vært basert på ekspertvurderinger av lokalt operasjonelle driftsforhold, ville metoden vært subjektivistisk forankret. Det legges videre til grunn at PDS metoden ikke benytter ekspertvurderinger for å generere (akkumulere) ny- og oppdatert kunnskap om et system, men at de vurderinger som foreligger er basert på betraktninger om tidligere observasjoner, og derfor kun til dels kan betraktes som et prediktivt Bayesiansk perspektiv. Oppgaven vil nærmere bestemt forstå PDS metoden å representere et a priori perspektiv i tilnærming til håndtering av sikkerhetsutilgjengelighet.

Usikkerhet i relasjon til PDS metoden synes i tilknytning til inndata å være noe mindre enn i IEC 61508 metoden, ettersom det foreligger et a priori perspektiv der tidligere feilrater vil kunne vurderes ut i fra applikasjons- og anleggsspesifikke betraktninger. PDS metoden ser også ut til å være mer fullstendig, og dermed representere mindre grad av usikkerhet knyttet til ufullstendighet enn IEC 61508 metoden. Dette kan begrunnes i at det blir forsøkt justert for systematiske feil og test uavhengige (systematiske) feil, noe som i denne oppgaven anses som en vesentlig styrke for PDS metoden kontra IEC 61508 metoden (jf. delkapittel 7.1.1). Til tross for dette så betrakter heller ikke PDS metoden kunnskapsdimensjonen og usikkerhet i en større utstrekning, som for eksempel i relasjon til innhenting av informasjon til ekspertvurderinger og fremtidige prediksjoner. På denne måten kan også PDS metoden representere relativ høy grad av epistemisk usikkerhet, til tross for at pålitelighetsanalytikerens grad av tro til dels blir oppdatert ved applikasjons- og anleggsspesifikk oppdatering.



Figur 7.1 - Ulike tilnærminger fra datainnsamling til PFD resultat. Inspirert av Øien mfl. (1996)

7.5 Oppsummerende betraktninger

Etterlevelse av IEC-standardene har etter hvert blitt et kvalitetsstempel innenfor mange industrier. Standardene håndterer ikke eksplisitt usikkerhet i tilknytning til kvantitative pålitelighetsanalyser av SIS, men indikerer likevel tvil omkring validiteten i resultatene (Janbu, 2009). Som tidligere nevnt har bruk av frekvens for å måle sannsynlighet blitt kritisert på det grunnlag at det kan betraktes som hasardiøst å feste tillit til tidligere frekvenser, når man skal forsøke å predikere fremtidig adferd. IEC 61508, og til dels PDS

metoden, ser likevel ut til å følge denne tilnærmingen der det kun delvis betraktes at frekvensene skal oppdateres på bakgrunn av oppdaterte feilrater fra lokale operasjonelle driftsforhold.

Argumenter for realistfortolkningen og tilhørende perspektiver kan uttrykkes ved å betrakte hvordan Monk (2010) beskriver sammenhengene mellom sannsynlighet og usikkerhet:

"Outcomes of repeated experiments form an envelope of possibilities that can be calculated to an astonishing degree of precision and lend credibility to the use of probability to describe uncertainty".

Likevel så vil overnevnte fortolkning kun være gjeldende for problemstillinger som er knyttet til at samme hendelse (A) repeteres gang etter gang, eller at et stort antall uniforme elementer er involvert til samme tid (G. Rausand, 2005). I virkeligheten er det ikke mulig å finne en gruppe komplett homogene systemer, noe som anses som en av de viktigste kritikkene mot klassisk relativ frekvens sannsynlighetstilnærming. Basert på vår kunnskap (K), så vet man at det foreligger usikkerhet (U) knyttet til hendelse (A) og tilhørende konsekvenser (C). Et valid poeng er dermed å inkludere kunnskap og usikkerhet i våre sannsynlighetsprediksjoner (P). I tilnærming til å ta opp en fullbyrdes risikobasert tilnærming, virker det noe ulogisk og motstridende å ikke ta hensyn til alle dimensjoner av usikkerhet.

PDS metoden tar videre hensyn til systematiske feil, men anvender fastsatte rater samtidig som oppdateringen av disse ikke fanger opp alle systemspesifikke forhold som berører årsaker til disse feilene (S. Hauge, Hokstad, et al., 2006). Dette anses som en svakhet ettersom alle lokale operasjonelle forhold også vil være av stor betydning og bør gjenspeiles, men likevel som en styrke i forhold til IEC 61508 som ikke kvantifiserer disse feilene. Feilrater fra systemer som er i drift kan videre anses å bestå av både sikre og usikre, så vel som tilfeldige hardwarebaserte og systematiske feil, ettersom det er usikkerhet knyttet til kategorisering av feilrater (ikke alle benytter FMEDA/FMECA). Ekspertvurderinger for å kategorisere de ulike typene av feil kan her anvendes for å forsøke å ta høyde for menneskelig interaksjon, noe som per dags dato ikke synes å være tilstrekkelig i hensyn tatt i begge de ulike metodene.

Som tidligere drøftet vil de bakenforliggende årsakene til systematiske feil og CCF i enkelte tilfeller kunne betraktes som like, slik at eventuelle barriere- og forsvarstiltak mot systematiske feil dermed også vil være effektive midler for å forsvare systemet for CCF. Således vil det også være viktig å inkludere ekspertvurderinger for å evaluere i hvilken grad

slike feil synes å overlappe, og eventuelt i hvilken grad alle faktorer og kilder til påvirkning for både systematiske feil og CCF er inkludert i vurderingene.

I de tidligere kapitlene av denne oppgaven har ulike fortolkninger av usikkerhet blitt diskutert. Mye av drøftingen er dermed relatert til om usikkerhet enten kan betraktes som kunnskapsbasert og/eller også som tilfeldig stokastisk basert. Usikkerhet har i denne oppgaven blitt definert som grad av tro, og desto mindre en vet om det system det tas utgangspunkt i, desto mer usikkerhet vil det foreligge i våre prediksjoner. For å gjøre en god prediksjon av sikkerhetsutilgjengelighet, er det derfor avgjørende at usikkerhet på forhånd er betraktet. Dette kan relateres til at det bør gjennomføres en usikkerhetsvurdering for å samle og formidle den kunnskap som foreligger omkring systemet og de forhold dette driftes under. Med den usikkerhet som foreligger i pålitelighetsvurderinger, særlig i forbindelse med nytt utstyr, så bør håndtering av usikkerheten i pålitelighetsvurderingene gjennomføres ved akkumulasjon av kunnskap omkring det systemet det tas utgangspunkt i. Kunnskap og informasjon fra kvalitative vurderinger kan således kvantifiseres og benyttes som solide bidrag slik at det ikke foreligger noen usikkerhet i tilknytning til predikert PFD. Usikkerheten i prediksjonen er derimot forbundet med den kunnskapen (K) som benyttes for å predikere PFD. En vil med dette forstå at PFD sannsynligheten ikke alene er tilstrekkelig for å beskrive risikoen forbundet med systemet, der det også må refereres til grad av usikkerhet forbundet med kunnskapen som ligger til grunn for prediksjonen (jf. delkapittel 3.2.3). Dette for å gi beslutningstaker tilstrekkelig og god informasjon om kvaliteten på den fremstilte prediksjonen. Andre tilhørende kvalitative og semi-kvantitative krav til sikkerhetsintegritet vil til dels kunne betraktes å kompensere for manglende håndtering av usikkerhet og fremstilling av dette i tilknytning til PFD i begge metodene. Likevel så anses ikke dette som tilstrekkelig, der grad av usikkerhet som er forbundet med kunnskapen som benyttes for å predikere PFD særskilt bør uttrykkes i tilknytning til PFD i verifikasjonsrapporter.

Direkte etterlevelse ved konsekvent bruk av de to metodene for gjennomføring av en SIL vurdering, vil med dette kunne representere usikkerhet i tilknytning til inndata og ufullstendighet. Dette oppstår dersom pålitelighetsanalytikeren følger fremgangsmåten for de to metodene, uten å i tillegg generere inngående kunnskap og betrakte tilhørende usikkerhet omkring angitt system. Neste kapittel presenterer en mulig metodisk fremgangsmåte for å inkludere kunnskapsakkumulasjon og usikkerhetsvurderinger i tilknytning til pålitelighetsvurderingene som foretas, for å verifisere et system i henhold til underliggende SIL krav.

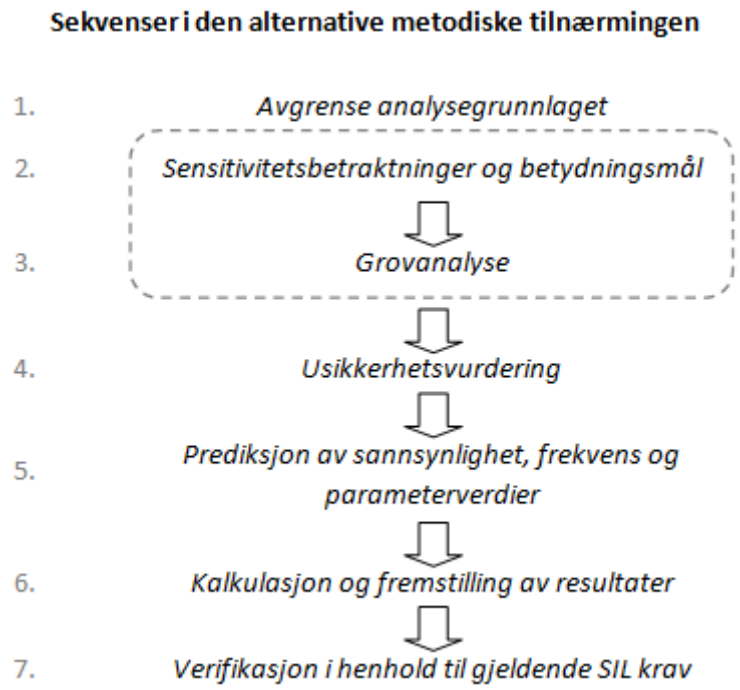
8 Alternativ metodisk tilnærming for å implementere usikkerhet i SIL verifikasjon

Det foreligger som tidligere diskutert formål og krav knyttet til de ulike fasene i livssyklusen til SIS. Det ble nevnt at det under analyser i tidlige faser skulle utarbeides fare- og risikoanalyser for å identifisere nødvendige sikkerhetsfunksjoner for å ivareta og kontrollere risikoen knyttet til EUC. I denne alternative metodiske tilnærmingen tas nettopp dette forhold med i videre analyser under realisering og drift, der det legges opp til en systematisk strategi for også å identifisere potensielle farer og forhold som er knyttet til SIS og eventuelle operasjonelle driftsimplikasjoner.

Hovedforskjellen mellom kalkulasjonene av PFD ved hjelp av de metodiske fremgangsmåtene som benyttes i IEC 61508 og PDS metoden, og denne alternative metodiske tilnærmingen for å kalkulere PFD, er knyttet til usikkerhetsvurderinger. I denne alternative metodiske tilnærmingen gjennomføres det nettopp en usikkerhetsvurdering som er ment å redusere epistemisk usikkerhet knyttet til informasjon som uttrykkes i PFD. Til tross for hovedfokus på PFD, så vil ikke all usikkerhet kunne reflekteres i denne sannsynligheten (P), uansett hvilken metode som benyttes. Dette kommer av at sannsynlighetene er betinget på en bestemt bakgrunnsinformasjon, og vil kunne gi ufullstendige prediksjoner ettersom overraskelser i forhold til satt sannsynlighet kan forekomme (jf. øvrige betraktninger i oppgaven som f. eks. delkapittel 7.1.1). Det er med dette viktig at usikkerhetsvurderingene også blir fremstilt før verifikasjon, og at det er opp til beslutningstaker å vurdere grad av usikkerhet (U) før PFD vurderes opp i mot fastsatte akseptkriterier (SIL nivå).

Det er videre viktig å bemerke at den foreslåtte fremgangsmåten som foreligger i dette kapittelet ikke erstatter kravene knyttet til IEC-standardene, og foreslås som en utvidelse som må nyttes i kombinasjon med en av metodene for kvantitativ kalkulering av sikkerhetsutilgjengelighet. Det er basert på overnevnte drøfting besluttet å ta utgangspunkt i PDS metodens feilklassifisering, modellering av feilårsaker (CCF) og kalkulasjon av systematiske feil. Hvilke handlinger som må utføres, samt omfanget av disse handlingene, vil variere med type og kompleksitet i systemet og dets relaterte prosesser. Under utvikling av de ulike sekvensene som blir presentert så har det her blitt tatt utgangspunkt i landbaserte gass- og prosessterminaler.

Pålitelighetskalkulasjoner som gjennomføres med utgangspunkt i gjennomsnittlige verdier for inndataparametre, kan betraktes å ikke være tilstrekkelig tilpasset applikasjons- og anleggsspesifikke forhold for et gitt system. For å fungere som beslutningsstøtte, må også kalkulasjonene oppdateres etter hvert som mer informasjon blir gjort tilgjengelig. Dette i tillegg til de applikasjons- og anleggsspesifikke oppdateringene som foretas når systemet settes i drift. For å sikre at pålitelighetsanalyser til enhver tid gjenspeiler tilgjengelig kunnskap, og at beslutninger blir fattet på et tilstrekkelig sterkt grunnlag, bør pålitelighetsanalysene med dette oppdateres slik at verdifull informasjon som kan bidra til å redusere usikkerheten omkring viktige parametre under drift blir tatt hensyn til. Slik oppdatering krever prosedyrer for periodevis eller fortløpende manuell oppdatering. Kapittelet presenterer med dette en manuell oppdateringsprosedyre for vurdering av sikkerhetsutilgjengeligheten til SIS knyttet til lokale operasjonelle driftsforhold. Prosedyren er basert på vurdering av usikkerhet om mengder som kan gis fysiske tolkninger, noe som er godt overens med ønskede betraktninger ut i fra et prediktivt epistemisk perspektiv.



Figur 8.1 - Sekvenser i den alternative metodiske tilnærmingen

Figur 8.1 illustrerer og tydeliggjør de ulike sekvensene i den alternative metodiske tilnærmingen. Det bemerkes at betraktninger av usikkerhet gjennomføres parallelt gjennom

hele prosessen, men at det blir lagt særlig vekt på usikkerhetsvurderinger i tilknytning til resultater fra sensitivitetsbetraktninger, betydningsmål og grovanalyser.

8.1 Analysegrunnlaget

Det er av stor betydning at det konkretiseres et analysegrunnlag som avgrenses, og dersom dette er av stor utstrekning, deles opp i ulike analyseobjekter som i sum utgjør analysegrunnlaget for vurderingene. Oppgaven vil her betrakte HIPPS systemet som er illustrert i systemanalysen av caset i appendiks B for å kunne relatere de ulike sekvensene til et system. Analysen begrenses til kun å ta utgangspunkt i de tre trykkbryterne; PSH(A), PSH(B) og PSHH. Det vil si at inndataparametrene for de andre komponentene i HIPPS systemet antas å være ”kjente” verdier, og at det dermed ikke er usikkerhet knyttet til verdier for disse komponentene. Dette er en sterk begrensning som lite trolig vil kunne forekomme i industrien, der eventuelle kjente verdier ikke kan antas å foreligge i en så stor utstrekning. Dette betraktes likevel ikke som avgjørende i denne sammenheng, siden det kun er ønskelig å illustrere de ulike sekvensene i en alternativ metodisk tilnærming. Relevante data for å illustrere sekvensene i denne alternative metodiske tilnærmingen vil bli hentet fra de oppdaterte applikasjons- og anleggsspesifikke dataene i PDS metoden – det vil si delkapittel B.6.2 i appendiks B.

Avhengig av hvilken livssyklusfase systemet er i, tilgang på relevant informasjon, systemets kompleksitet, med mer, så er det ved periodevis oppdatering hensiktsmessig å anvende en systematisk fremgangsmåte for å akkumulere kunnskap og samle inn informasjon i systemet. Dersom all informasjon til enhver tid blir oppdatert etter hvert som det foreligger, og samtidig inkludert i fortløpende analyser, så vil ikke en systematisk fremgangsmåte for å samle inn mer informasjon være hensiktsmessig ettersom all relevant informasjon da til enhver tid er representert i analysen. En systematisk fremgangsmåte, slik den er illustrert i delkapittel 8.2, er hensiktsmessig når systemer er i designfaser, når systemer skal settes i drift, eller når tilgangen på relevant informasjon om systemet og dets lokale operasjonelle driftsforhold fra drift betraktes å være liten og/eller ikke oppdatert.

8.2 Tilnærming

Svikt på etterspurt tid betraktes som den uønskede hendelsen A. Den systematiske fremgangsmåten som presenteres her er ment å identifisere farer og akkumulere informasjon for å kartlegge og senere kunne beskrive påliteligheten til systemet og tilhørende usikkerhet forbundet med prediksjonen. Rent praktisk så vurderes kombinasjonen av mulige konsekvenser og usikkerhet (sannsynlighet) opp i mot systemets barrierer. Usikkerhet knyttet til de uønskede hendelsene kan for eksempel beskrives ved (Aven, 2007):

- Sannsynligheten for at en uønsket hendelse skal oppstå
- Forventet antall uønskede hendelser for en gitt tidsperiode

For å belyse overnevnte så legges det til grunn at det gjennomføres en sensitivitetsanalyse (inkludert betydningsmål) i kombinasjon med en grovanalyse. Selve gjennomføringen av grovanalysen tar utgangspunkt i en systematisk og strukturert fareidentifikasjonsprosess (HAZID/HAZOP), og kombinerer sjekklister med ekspertgruppens erfaringer og kompetanse om analysegrunnlaget. Disse vurderingsmetodene blir således benyttet i tilknytning til systemet, for å hente inn informasjon som vil kunne øke og/eller oppdatere kunnskapen.

8.2.1 Usikkerhets- og sensitivitetsbetraktninger

En sensitivitetsanalyse er viktig for å gjøre en samlet vurdering av betydningen til komponentene og inndataparametrene som betraktes å være usikre. Ulike komponenter og parametre vurderes, for deretter å videre kunne ta hensyn til de komponentene og parametrene som representerer høy usikkerhet og høy sensitivitet i senere betraktninger. For å vurdere sensitiviteten har oppgaven allerede illustrert at systematiske feil kan betraktes å være et stort og viktig bidrag for PFD, og at PFD således kan forstås som sensitiv ovenfor parametre som omhandler de systematiske feilene ($\lambda_{DU\text{-}S}$ og P_{TIF}). Sensitivitet i forhold til hvilke parametre som inkluderes i analysen anses ikke her å være avgjørende, der fokus raskt vil foreligge omkring hvilke parametre som skal inkluderes i modellen for å representere en underliggende "korrekt" metode for PFD kalkulasjoner. Ut i fra et prediktivt perspektiv er det i større grad viktig å fokusere på om all relevant informasjon om faktorer og forhold er representert i de ulike parametrene, noe som vil bli nærmere belyst under fareidentifikasjonsprosessen i neste delkapittel. Sensitivitetsbetraktninger i form av metoder for å identifisere den (de) dominante bidragene til feil i et system, altså en vurdering av de

ulike komponentenes betydning (sensitivitet), betraktes derimot som viktig. Ved å vurdere betydningen til de ulike komponentene kan man på denne måten avgrense den videre analysen ved å rette fokus mot de komponentene som etter måten medfører en stor endring i systempåliteligheten, og/eller som er mest vesentlig for å forbedre den totale systempåliteligheten. Hvilket betydningsmål som bør benyttes i et bestemt tilfelle, avhenger av hvilke karakteristikker det ønskes at målet skal reflektere. Siden begge betydningsmålene kan gi verdifull informasjon om hvilke komponenter som bør tilegnes ekstra oppmerksomhet i videre vurderinger, velger denne oppgaven å avgrense dette til hvilken fase i livssyklusen systemet befinner seg (slik det også i mange tilfeller gjøres i annen litteratur). I designfasen kan mål for forbedringspotensial (Improvement potential) være mest informativt, mens Birnbaums mål kan være mest informativt for et system med frossen design (Aven, 2006). Dette kommer av at det i design i større grad er mulig å påvirke systemet, og dermed planlegge eventuelle endringer og forbedringer på en mer kostnadseffektiv måte. I drift betraktes derimot utskiftning og forbedring av komponenter som veldig kostbart. I drift vil det heller ikke kunne antas en perfekt komponent slik det gjøres under mål for forbedringspotensial, der en slik antakelse vil være urimelig (ikke gi mening). I drift er det derimot mer hensiktsmessig å kunne referere til at det kan forekomme en liten endring, noe som er i tråd med Birnbaums mål. I vårt tilfelle kan systemet betraktes å være frossent, og oppgaven tar med dette utgangspunkt i Birnbaums mål for å kunne reflektere hvordan små forbedringer av komponentpålitelighetene påvirker systempåliteligheten i videre analyser.

Den (de) komponenten(e) som representerer størst risiko ved å være av størst betydning for sikkerhetssystemer, vil på denne måten bli særlig nøye vurdert av ekspertgruppen i videre usikkerhetsvurderinger og ved fastsettelse av komponentenes ulike parameterverdier. Eventuelt så kan ekspertgruppen avgjøre om det skal gjennomføres nærmere analyser, og eller om enkeltkomponenter skal skriftes ut / forbedres.

Tabell 8.1 - Betydningsmål

Komponent	Forbedringspotensial (I_i^A)	Birnbaums mål (I_i^B)
PSH(A)	7,13E-06	7,21E-06
PSH(B)	7,13E-06	7,21E-06
PSHH	9,20E-07	9,29E-07

Birnbaums betydningsmål rangerer komponentene etter hvor følsomt systemet er for endringer i komponentenes pålitelighet, hvor målet avhenger av komponentenes feilrater og

komponentenes plassering i systemet. Dette innebærer at komponentene og de grunnleggende hendelsene som systemet er sårbart ovenfor, som for eksempel CCF, vil ha en høy rangering. Komponenter i parallelle strukturer vil dermed avhenge av hverandres feilrater. Den grenen i en parallell struktur som har lavest pålitelighet vil derfor lede til den høyeste rangeringen for den motsatte grenen på grunn av det høyeste gapet ($h(1_i, p)$-$h(0_i, p)$). Ut i fra overnevnte kan man se at en liten endring i PSH(A) og PSH(B) pålitelighet medfører en etter måten stor endring i systempåliteligheten. Systemets pålitelighet kan da betraktes å være mer sensitivt for endringer i disse komponentenes pålitelighet enn en tilsvarende endring i PSHH pålitelighet. Ut i fra overnevnte betraktes disse komponentene som særlig viktige i den kommende fareidentifikasjonsprosessen, og eventuell usikkerhet knyttet til inndataparametrene må her belyses og tilegnes særlig vekt.

8.2.2 Grovanalyse

En grovanalyse er en sikkerhetsanalyse som i dette tilfellet har til hensikt å avdekke potensielle farer. Dette gjøres ved å ta utgangspunkt i sjekklister og ledeord for å gjennomføre en systematisk og strukturert fareidentifikasjonsprosess for å få frem eventuell ny og oppdatert informasjon om systemet. Som en systematisk og strukturert prosess for fareidentifikasjon, foreslås det i denne oppgaven å benytte en HAZOP-analyse (Hazard and Operability). En HAZOP-analyse er en systematisk og strukturert analyse der stikkord benyttes for å identifisere scenarioer som kan medføre farer eller operasjonelle problemer knyttet til et system. Mer informasjon knyttet til selve HAZOP-analysen kan betraktes i Aven mfl. (2008) s. 89-91.

Som det ble nevnt i forrige delkapittel, blir det i grovanalysen lagt vekt på eventuelle farer og prosesser knyttet til de komponenter som er av størst betydning for systemet. Det vi si de komponentene som etter usikkerhets- og sensitivitetsbetraktningene representerte størst grad av betydning og usikkerhet for det aktuelle system. Resultatet fra vår analyse viser at PSH(A) og PSH(B) skal tilegnes særlig mye oppmerksomhet. Etter gjennomført HAZOP-analyse har ekspertgruppen da identifisert farer og potensielle hendelser som kan medføre problemer, med særlig vekt på de mest usikre og betydningsfulle komponentene i systemet. Dette antas å ha ledet til oppdatert, eventuelt ny, informasjon om systemets lokale operasjonelle driftsforhold.

Basert på erfaringer og tilgjengelig informasjon om systemet, beskriver ekspertgruppen deretter usikkerheten knyttet til de uønskede hendelsene i kombinasjon med mulige årsaker

og effekter for hver fare som er identifisert. Usikkerheten knyttet til de uønskede hendelsene kan, som tidligere nevnt, beskrives ved å angi sannsynligheten for at en uønsket hendelse skal oppstå og forventet antall uønskede hendelser for en gitt tidsperiode. På denne måten vurderer ekspertgruppen usikkerheten knyttet til hver enkelt komponent i systemet ut i fra:

- Historiske data: det vil si at ekspertgruppen vurderer i hvilken grad tidligere data er relevante for analysen, og om det således kan inkluderes erfaringer fra tidligere hendelser
- Ny og oppdatert informasjon: dette kan være seg nye rutiner eller barrierer som er etablert, og identifiserte farer eller mulige hendelser som kan påvirke sannsynlighetene

Anta at ekspertgruppen på følgende måte har kommet frem til sannsynligheter og tilhørende frekvens av farlige feil (λ_{DU}) for de ulike komponentene:

Tabell 8.2 - Farlige uoppdagede feil for PSH(A)

Farlige uoppdagede hardware feil (λ_{DU-RH})		**Farlige uoppdagede systematiske feil (λ_{DU-S})**	
Sannsynlighet	**Frekvens**	**Sannsynlighet**	**Frekvens**
0,1	2,00E-06	0,2	8,00E-05
0,2	4,00E-06	0,2	1,00E-06
0,2	6,00E-06	0,2	6,00E-06
0,1	8,00E-06	0,1	9,00E-06

Forventet antall farlige uoppdagede feil for PSH(A) er da:

$$E(\lambda_{DU-RH}) = \frac{\sum p_i x_i}{n} = 3{,}00E-06$$

$$E(\lambda_{DU-S}) = \frac{\sum p_i x_i}{n} = 1{,}83E-05$$

der *p* er predikert sannsynlighet for utfall *i*, og *x* er predikert frekvens av utfall *i*.

Det kan med bakgrunn i overnevnte tabell betraktes at dette ikke summerer til 1, noe som kan indikere at ekspertgruppen har tatt høyde for at feil ikke trenger å oppstå i neste

tidsperiode. Samtidig indikerer dette at dersom farlige feil skulle inntreffe, så er det forventet å ligge innenfor overnevnte frekvens.

Oppgaven antar også at ekspertgruppen på tilsvarende måten har kommet frem til følgende forventet antall farlige uoppdagede feil for PSH(B) og PSHH:

PSH(B): $E(\lambda_{DU\text{-}RH}) = 5{,}20E\text{-}06$ og $E(\lambda_{DU\text{-}S}) = 1{,}86E\text{-}05$

PSHH: $E(\lambda_{DU\text{-}RH}) = 6{,}80E\text{-}06$ og $E(\lambda_{DU\text{-}S}) = 4{,}65E\text{-}05$

Basert på akkumulert informasjon fra grovanalysen og anvendelse av relevante data, har ekspertgruppen videre kommet frem til følgende (predikerte) verdier for de øvrige parametrene for komponentene:

Tabell 8.3 - Pålitelighetsparametre for PSH(A), PSH(B) og PSHH

Inndataparameter	PSH(A)	PSH(B)	PSHH
β	0,03	0,03	0,02
P_{TIF}	2,50E-03	2,50E-03	1,50E-03
r	0,5	0,5	0,4

Det antas at testintervallet holdes konstant, 8760 (timer).

Den alternative metodiske tilnærmingen har med dette gjennomført en usikkerhetsvurdering som er ment å redusere epistemisk usikkerhet knyttet til informasjon om de ulike parametrene, og som ved videre kalkulasjoner vil bli inkludert i PFD prediksjonen. På denne måten vil PFD prediksjonen være et uttrykk for ekspertgruppens usikkerhet i tilknytning til systemets sikkerhetsutilgjengelighet. Likevel så vil det foreligge usikkerhet knyttet til den kunnskap som foreligger, der denne er betinget på tilgjengelig informasjon på det tidspunktet analysen ble foretatt. Den alternative metodiske tilnærmingen legger derfor til grunn at ekspertgruppen må gjøre en vurdering av usikkerhet i tilknytning til de inndata og den fullstendighet som foreligger i de fastsatte prediksjonene. Grad av usikkerhet (U) uttrykkes da som henholdsvis *lav*, *moderat* eller *høy* usikkerhet i tilknytning til kalkulert PFD prediksjon. Dette vil bli nærmere illustrert i neste delkapittel, hvor resultatet av predikert PFD vil bli uttrykt med ny og oppdatert informasjon i tilknytning til lokale operasjonelle driftsforhold for HIPPS-systemet.

8.3 Kalkulasjon og fremstilling av resultater

Kalkulasjonene er gjennomført i tilknytning til formlene og parametrene som foreligger i PDS metoden, og er nærmere illustrert i appendiks C.

Pålitelighetsanalysen skal gi en detaljert beskrivelse av risiko. Det vil si en beskrivelse som dekker (C, C*, U, P, K) i henhold til beskrivelsen i delkapittel 3.3. Ekspertgruppen skal med dette ha forsøkt å identifisere mulige uønskede hendelser og feil som kan oppstå i systemet (A), gjøre en prediksjon av sikkerhetstapet/feilfrekvenser (C*), uttrykke usikkerheten (U) og angi sannsynligheter (P) gitt bakgrunnskunnskapen (K). En mer detaljert beskrivelse av disse faktorene skal foreligge som resultater fra grovanalysen. Det endelige resultatet av analysen er presentert i tabellen under, og er et uttrykk for predikert PFD:

Tabell 8.4 - Resultat fra den alternative metodiske tilnærmingen

Sikkerhetutilgjengelighet	Prediksjon
PFD_{System}	3,46E-03
Grad av usikkerhet	Lav

Av resultatet ser man at den alternative metodiske tilnærmingen uttrykket sannsynligheten for svikt på etterspurt tid (PFD) å være 3,46E-03. Informasjonen og kunnskapen som ligger til grunn for vurderingen betraktes å være godt dekkende, og usikkerheten forbundet med prediksjonen er således lav. Resultatet som indikerer lav grad av usikkerhet og godt dekkende informasjon og kunnskap, vil være forankret i ekspertgruppens resultater og detaljert beskrivelse av faktorene etter gjennomføring av sensitivitets-, grov- og usikkerhetsanalyse for HIPPS systemet. Foreløpige begrensninger knyttet til denne delen av analysen er for øvrig nærmere belyst i delkapittel 8.4, i kombinasjon med en nærmere foreslått fortolkning av resultater fra den alternative metodiske tilnærmingen.

Det betraktes ikke å være avgjørende å drøfte kalkulert PFD prediksjonen fra den alternative metodiske tilnærmingen i tilknytning til resultatene fra IEC 61508 metoden og PDS metoden, da disse er betinget på antatte ekspertvurderinger. Det legges likevel vekt på at den alternative metodiske tilnærmingen har benyttet en systematisk og strukturert analyse for å inkludere all tilgjengelig informasjon og kunnskap som foreligger om HIPPS systemet. Det foreligger dermed ikke noen usikkerhet i tilknytning til denne prediksjonen, slik det vil gjøre ved å benytte de to andre metodene. Usikkerheten i tilknytning til angitt prediksjon i den

alternative metodiske tilnærmingen, er uttrykt som grad av usikkerhet knyttet til den informasjonen og kunnskapen som foreligger på det tidspunkt analysen ble gjennomført. På denne måten kan beslutningstaker nå også vurdere godheten av informasjonen som ligger til grunn for PFD prediksjonen før verifisering i tilknytning til gjeldende SIL krav.

8.4 Utviklingspotensial og foreløpige begrensninger

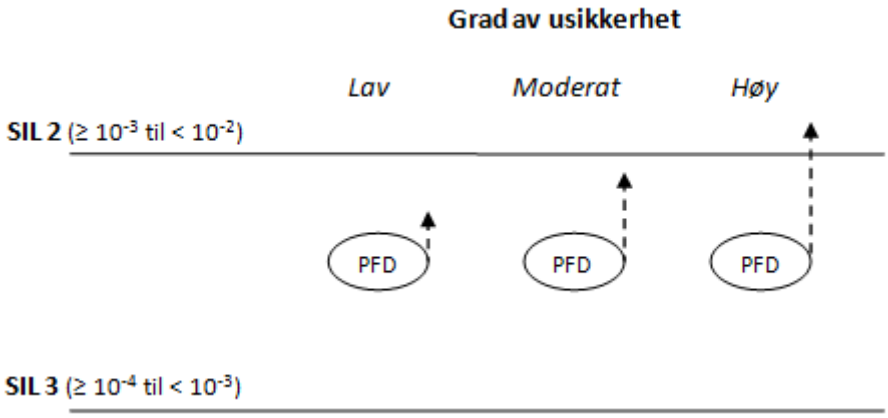
Slik den alternative metodiske tilnærmingen på nåværende tidspunkt er presentert, er fremgangsmåten for kategorisering av usikkerhetsgrad ikke tilstrekkelig belyst i prosedyren. Dette kan være spørsmål om hva som betraktes som godt dekkende, og hva som kan betraktes som ikke tilstrekkelig godt dekkende. På denne måten kan det stilles spørsmål med hva som skal danne grunnlaget for å angi henholdsvis lav, moderat eller høy usikkerhet i tilknytning til kalkulert PFD prediksjon. Relevant informasjon og kunnskap om systemet akkumuleres på en systematisk og strukturert måte, og det gjennomføres usikkerhets- og sensitivitetsbetraktninger fra en ekspertgruppe der dette er ment å lede til prediksjon av usikkerhetsgrad. Prosedyren utrykker likevel liten informasjon knyttet til en enhetlig kategorisering av usikkerhetsgrad, og dermed hvordan overgangen mellom analyse og konklusjon skal betraktes. En erfaren og høyt kompetent ekspertgruppe vil muligens kunne klare å argumentere seg frem til grad av usikkerhet. Likevel er den alternative metodiske tilnærmingen ment å kunne fungere for enhver kompetent ekspertgruppe, der prosedyren også må inkludere en enhetlig tilnærming for å komme frem til grad av usikkerhet knyttet til prediksjonen. En mulig løsning vil kunne være å presentere en detaljert sjekkliste knyttet til prosessen med å akkumulere og analysere informasjon og kunnskap i ekspertgruppen. Hva som skal ligge til grunn for å kategorisere grad av usikkerhet som henholdsvis lav, moderat eller høy usikkerhet må videre belyses. Dette synes å være en viktig faktor som ikke er tilstrekkelig belyst, og den alternative metodiske tilnærmingen er for øyeblikket ikke fullstendig.

Det bør også tas stilling til hvordan fortolkningen av resultatene, henholdsvis sannsynligheten (PFD) og usikkerheten (grad av usikkerhet), skal vurderes opp i mot de fastsatte SIL kriteriene. Det vises med dette til betraktninger om usikkerhet i relasjon til detaljkrav og akseptkriterier i delkapittel 3.2.3. Der blir det blant annet uttrykt at et system kan ligge innenfor akseptkriteriene, men likevel være forbundet med høy grad av usikkerhet, og da ikke nødvendigvis bør aksepteres uten videre vurderinger. Denne oppgaven har tidligere bemerket at aksept i henhold til SIL kravene ikke vil bli diskutert, men det betraktes likevel som viktig å nevne hvordan grad av usikkerhet rent praktisk kan fortolkes i den

alternative metodiske tilnærmingen. Uten å foregripe hvorledes usikkerhet bør betraktes i forhold til SIL nivåene på et generelt grunnlag, kan det tenkes at et mulig krav til usikkerhet kan etableres i IEC-standardene eller som interne prosedyrer i industrien. En mulig løsning som kan vurderes er å betrakte forhåndsdefinerte prosentkrav til usikkerhetsgrad. Anta at følgende krav til grad av usikkerhet foreligger med følgende prosentvise margin: lav usikkerhet = 5 %, moderat usikkerhet = 20 % og høy usikkerhet = 40 %. Som illustrert i figur 8.2, antas det at kalkulert PFD prediksjonen ligger mellom SIL 2 og SIL 3. Avstanden mellom SIL 2 og SIL 3 beregnes, der de prosentvise marginene kalkuleres som en grense på for eksempel 5 % av denne avstanden, som adderes med kalkulert PFD prediksjon. Dette kan illustreres følgende formel:

$$\left((SIL_n - SIL_{n+1}) * M_i\right) + PFD$$

Der SIL_n i vårt tilfelle refererer til SIL 2, SIL_{n+1} refererer til SIL 3, og M_i er lik den prosentvise marginen for henholdsvis lav, moderat eller høy usikkerhet. Grad av usikkerhet vil i dette tilfellet kunne påvirke aksept/ikke aksept i forhold antatt SIL nivå, ettersom hvilken grad av usikkerhet som er forbundet med prediksjonen.



Figur 8.2 - Mulig fortolkning knyttet til predikert grad av usikkerhet

Dersom grad av usikkerhet i en tenkt kalkulasjon hadde vært lav med en kalkulert PFD slik den er illustrert i figur 8.2, så ser man at en 5 % addert margin for kalkulert PFD fortsatt er godt innenfor SIL 3 grensen. Predikert PFD med lav grad av usikkerhet kan derfor aksepteres. Ved moderat grad av usikkerhet, altså 20 % usikkerhetsmargin, vil predikert PFD også kunne aksepteres ettersom kalkulasjonen ligger innenfor SIL 3 grensen. Dersom grad av usikkerhet hadde vært høy, altså en 40 % usikkerhetsmargin, ville derimot predikert PFD ikke blitt

akseptert ettersom det er stor usikkerhet forbundet med prediksjonen. Ved å ta høyde for usikkerhetsmarginen, er det høy usikkerhet forbundet med prediksjonen, og PFD har potensial til å ligge utenfor grensen til SIL 3. Informasjon og kunnskap som ligger til grunn for vurderingen vurderes i et slikt tilfelle ikke å være godt dekkende, og usikkerheten rundt prediksjonen er således høy. Illustrasjonen av størrelsesforholdene og marginene i figur 8.2 er ikke gjengitt i korrekte oppgitte størrelser. Dette betraktes derimot ikke som avgjørende, ettersom det er bakenforliggende tanker og en mulig fortolkning av grad av usikkerhet som blir forsøkt formidlet. Hvor stor usikkerhetsmargin som bør ligge til grunn for de ulike usikkerhetskategoriene, og en rekke andre forhold i tilknytning til aksept/ikke aksept, må vurderes nærmere. Aksept i forhold til grad av usikkerhet må derfor forstås som et utgangspunkt for videre arbeid.

8.5 Oppsummerende betraktninger

I den alternative metodiske tilnærmingen er det samlet inn såkalte subjektive data på en systematisk og strukturert måte. En subjektivist vil nytte disse til å predikere en sannsynlighet for svikt i systemet. Dersom det i tillegg til å benytte overnevnte subjektive betraktninger nyttes statistiske data, kan dette betraktes som Bayesianerens alternativ (jf. figur 7.1). For å skissere en fullbyrdes prediktiv epistemisk tilnærming så relateres sannsynligheter til mål på usikkerhet knyttet til prediksjoner av observerbare størrelser, slik som feil innenfor en gitt tidsperiode. Usikkerheten er da rent epistemisk, det vil si kun som et resultat av manglende kunnskap (informasjon). Både ekspertvurderinger og relevante historiske ”harde data” benyttes dermed for å kvantifisere denne usikkerheten. Dette ble også til dels utført under applikasjons og anleggsspesifikk oppdatering ved PDS metoden (og ved CCF i IEC 61508), men perspektivet og metoden som her fremstilles er igjen relatert til andre fundamentale spørsmål om hvordan risiko og usikkerhet uttrykkes, hvordan modeller skal fortolkes, og hvordan man skal forstå bruk av parametriske fordelinger og parametre i en pålitelighetsanalytisk kontekst (Apeland, Aven, & Nilsen, 2002).

Ut i fra forestående drøftinger i oppgaven kan to dimensjoner betraktes å være viktige for en usikkerhetsanalyse i tilknytning til kalkulasjon av PFD:

- Få frem usikkerhet kvalitativt: diskutere og beskrive usikkerhetsfaktorer, deres årsaker og hvordan disse antas å påvirke systemet. Den kvalitative delen er således viktig for oversikt og bevisstgjøring, og som grunnlag for kvantifisering

- Få frem usikkerhet kvantitativt: sette tall på sannsynligheter, utfall og eventuelle påvirkningsvariabler

Et av de viktigste elementene med den alternative fremgangsmåten for gjennomføring av kvantitativ SIL verifikasjon, er å påvise svakheter og farer i et system som betraktes som mulige usikkerhetsfaktorer. Dette gjøres ved å fokusere på relevant informasjon, men er også ment å kunne lede til ny og utvidet informasjon om mulige sensitive parametre ut over statistisk målbare hardware feil i gjennom fareidentifikasjonsprosessen. Slike betraktninger er likevel i praksis ikke alltid særlig enkelt ettersom systemer og driftsforhold i stadig større grad blir mer avanserte og komplisert. Kompliserte systemer kan medføre at hendelser og reaksjoner, som isolert sett virker ufarlige, virker sammen og gir virkninger som langt overstiger det systemet er konstruert for. I tillegg vil et komplisert system også gjøre det vanskelig å se alle muligheter for farlige hendelser som kan oppstå. Utfordringen er derfor å presentere usikkerheter på en hensiktsmessig måte for å gi beslutningstaker et godt grunnlag for å fatte beslutninger (Aven, 2007). Den struktur og beskrivelse som er gjort i den alternative metodiske tilnærmingen er et utgangspunkt for nettopp å møte denne utfordringen.

Det bemerkes at det knyttet til oppgavens begrensninger ikke har vært mulig å gå nærmere inn på ledeord og sjekklister for bruk i denne alternative metoden. Ledeord og sjekklister for HAZOP antas å være basert på detaljert betraktninger, herunder tekniske, utstyrsspesifikke og menneskelige aspekt, og at denne detaljerte analysen er i stand til å betrakte risiko ved ulike beslutninger om kvalitet og funksjoner i sikkerhetssystemet. Ut i fra tidligere drøfting i oppgaven er det diskutert at det foreligger flere forhold som i IEC 61508 metoden og PDS metoden ikke inkluderes i kvantifiseringen av PFD. Gjennomføringen av en grovanalyse er med dette ment å kunne påvise hendelser og potensielle farer knyttet til systemet, og at man således basert på en kvalitativ vurdering reduserer tilhørende epistemisk usikkerhet knyttet til systemet. Denne informasjonen er deretter kategorisert av en ekspertgruppe, som kan benytte ny og oppdatert kunnskap til å betinge ulike inndataparametre for å kvantifisere PFD.

Det er videre viktig at det i denne typen analyser reflekteres rundt analyse- og ekspertgruppen. I stor grad vil det være slik at gjennomføring av analysen en dag vil kunne gi en prediksjon, mens en annen ekspertgruppe vil kunne gi en annerledes prediksjon ved en annen anledning. En ”god” ekspertgruppe er en analysegruppe bestående av aktører med kompetanse innenfor ulike felt i tilknytning til systemet. I så tilfelle, vil subjektive vurderinger i forhold til en grov- og usikkerhetsanalyse i form av diskusjoner kunne antas å representere eg godt reflektert syn dersom det er foretatt av en ”god” ekspertgruppe. En annen

ekspertgruppe, bestående av aktører med lik bakgrunn, vil antas å kunne komme frem til noenlunde like betraktninger. Dette avhenger også av dokumentasjon, relevante data, hvilke forutsetninger som gjøres med videre. Basert på den informasjon og kunnskap ekspertgruppen hadde for hånd etter gjennomført HAZOP, betraktes dette å kunne gi gode prediksjoner om fremtidige uønskede hendelser. Det vil ikke si at det i fremtiden ikke vil kunne fremkomme ny informasjon som vil kunne resultere i en annen prediksjon. Det bemerkes igjen som avgjørende at det reflekteres rundt ekspertgruppen, og at det settes ned en kompetent og "god" gruppe for å gjennomføre analysene.

Denne fremgangsmåten for å gjennomføre en SIL verifisering har således fokus på å belyse den kunnskap og de forhold som måtte være fraværende, og ikke minst inkludere disse i kalkuleringene av PFD i analyseobjektet. Formålet med den alternative metodiske tilnærmingen for å implementere usikkerhet i SIL verifikasjon kan kort oppsummeres i følgende punkter:

- Sikre størst mulig grad av fullstendighet og mest mulig representative inndataparametre ved å gjennomføre usikkerhetsvurderinger
- Gjennomføre en bedre prediksjon om fremtidens behov og krav i systemer
- Være en del av beslutningsgrunnlaget relatert til underliggende akseptkrav
- Få frem mulige forhold i systemet som krever forhåndstiltak for å avverge eller begrense risiko

9 Konklusjon

Hovedformålet med denne oppgaven var å undersøke i hvilken grad metoder for kvantifisering av sikkerhetsutilgjengelighet i SIS justerer, håndterer og tar høyde for usikkerhet knyttet til SIL verifisering. Hovedformålet ble deretter delt inn i fem ulike delmål, som har blitt gjennomført og forsøkt adekvat belyst.

Ut i fra et prediktivt epistemisk perspektiv synes IEC 61508 metoden å representere relativt høy grad av usikkerhet knyttet til ufullstendighet og inndata i forhold til PDS metoden. IEC metoden legger ikke til grunn ekspertvurderinger for å oppdatere parametrene ut over sjekklisten som benyttes for β-faktorer, og på denne måten forsøker ikke metoden å identifisere og inkludere alle relevante faktorer og farer i kalkulasjonene. Systematiske feil, som kan betraktes som et stort og viktig bidrag til sikkerhetsutilgjengelighet, kvantifiseres og inkluderes heller ikke i metodens PFD prediksjoner. Det kan derfor betraktes som ufullstendig å kun inkludere deler av feilratene i pålitelighetskalkulasjonene, og på denne måten utelate effekten av menneskelig interaksjon og andre viktige faktorer. Dette så fremt pålitelighetsanalytikeren(e) selv ikke justerer parametrene i en prosess ut over det som dekkes ved konsekvent anvendelse av metoden.

PDS metoden tar videre høyde for kombinasjonen av generiske data og anleggsspesifikke betraktninger. Metoden inkluderer også parametre som systematiske feil og utilgjengelighet som følge av nedstengning i kalkulasjoner av sikkerhetsutilgjengelighet, og synes på denne måten å være mer omfattende og fullstendig enn IEC 61508 metoden. Verdier for inndataparametrene som anvendes i PDS metoden synes å være forbundet med mindre usikkerhet enn verdier for inndataparametre i IEC 61508 metoden. Dette skyldes fortrinnsvis at PDS metodens applikasjons- og anleggsspesifikke oppdatering er mer omfattende, og nyttes i tilknytning til flere parametre enn i IEC 61508 metoden. Ved utstrakt bruk av ekspertvurderinger under applikasjons- og anleggsspesifikk oppdatering, er PDS metoden bedre egnet til å reflektere systemers lokale operasjonelle driftsforhold. PDS metoden ser på denne måten ut til å justere, håndtere og ta høyde for usikkerhet knyttet til SIL verifisering på et bredere og mer omfattende grunnlag enn IEC 61508 metoden.

Likevel dekker ikke de ulike inndataparametrene i noen av metodene alle forhold av betydning. Dette kan vise seg i hvilken grad de gjenspeiler alle relevante operasjonelle forhold knyttet til for eksempel vær og vind, og/eller andre forhold som kan betraktes som ufullstendig dekket. Resultatene fra analysen indikerer dermed at konsekvent bruk av begge metodene for kvantifisering av predikert PFD vil kunne representere usikkerhet, der grad av

usikkerhet betraktes å være størst ved anvendelse av IEC 61508 metoden. Usikkerhet knyttet til fullstendighet og inndata i de to metodene, oppstår dermed som følger av metodenes begrensninger knyttet til å inkludere alle relevante forhold av betydning.

I anledning at oppgaven har drøftet behovet for å kunne uttrykke usikkerhet, fortrinnsvis med basis i gitt kunnskap, synes ikke kunnskaps- eller usikkerhetsdimensjonen å bli tilstrekkelig håndtert eller reflektert i de to metodenes kalkulasjoner av PFD. Oppgaven har derfor utviklet en alternativ metodisk tilnærming for å inkludere kunnskapsakkumulasjon med usikkerhets- og ekspertvurderinger. Den alternative metodiske tilnærmingen uttrykker på denne måten behovet for en systematisk og strukturert fareidentifikasjonsprosess, for å inkludere alle scenarioer som kan medføre farer eller operasjonelle problemer knyttet til det aktuelle system. I lys av ny og/eller oppdatert informasjon og kunnskap, betraktes den alternative metodiske tilnærmingen dermed å kunne reflektere systemer i det virkelige liv og dets omgivelser på et godt grunnlag. Metoden uttrykker på denne måten den sterkeste prediksjonen av PFD, der den justerer, håndterer og tar høyde for usikkerhet knyttet til SIL verifisering på et helhetlig grunnlag som strekkes seg ut over begrensninger knyttet til IEC 61508 metoden og PDS metoden.

9.1 Forelått videre arbeid

Denne oppgaven har blitt gjennomført innenfor et begrenset tidsrom og med begrensede ressurser. Temaene i oppgaven er omfattende og komplekse, og vil derfor kunne bli vurdert videre i grundigere analyser. I kombinasjon med tema som strekker seg ut over oppgavens avgrensning, anbefales det at følgende områder fra denne oppgaven vektlegges med hensyn til videre arbeid:

- Oppgaven er begrenset til å ta utgangspunkt i kvantitative krav i relasjon til sikkerhetsintegritet, herunder kvantifisering av PFD. Det bør også vurderes i hvilken grad øvrige krav til sikkerhetsintegritet, herunder semi-kvantitative og kvalitative krav, kan påvirke nivået av usikkerhet knyttet til SIL verifisering. Eventuelt om, og hvordan, dette ville kunne påvirket konklusjonen fra denne oppgaven.
- Det er i oppgaven bemerket at PDS metoden ikke tar høyde for alle relevante faktorer under applikasjons- og anleggsspesifikk oppdatering. Hvilke faktorer metoden tar høyde for, og som inkluderes i de ulike parametrene, i kombinasjon med hvilke faktorer metoden ikke tar høyde for bør belyses nærmere.

- I den alternative metodiske tilnærmingen bør det som nevnt arbeides i retning av å etablere en enhetlig og konkret prosedyre for å komme frem til kategorisering av usikkerhetsgrad (lav, moderat eller høy), og dermed hvordan overgangen mellom analyse og konklusjon skal forankres (jf. første avsnitt i delkapittel 8.4).
- I tilknytning til den alternative metodiske tilnærmingen bør det også nærmere vurderes hvordan fortolkning av resultatene (PFD og grad av usikkerhet) skal vurderes opp i mot de allerede fastsatte SIL kriteriene (jf. andre avsnitt i delkapittel 8.4).

10 Referanser

Abrahamsen, E. B. (2009). Forelesning MOS 190 - Pålitelighetsanalyse. Stavanger: E. B. Abrahamsen.

Apeland, S., Aven, T., & Nilsen, T. (2002). Quantifying uncertainty under a predictive, epistemic approach to risk analysis. *Reliability Engineering & System Safety, 75*, 93-102.

Aven, T. (2003). *Foundations of risk analysis: a knowledge and decision-oriented perspective*. Chichester: Wiley.

Aven, T. (2006). *Pålitelighets- og risikoanalyse*. Oslo: Universitetsforlaget.

Aven, T. (2007). *Risikostyring: grunnleggende prinsipper og ideer*. Oslo: Universitetsforlaget.

Aven, T. (2008a). *Risk analysis and risk management. Basic concepts and principles*. Paper presented at the Summer Safety and Reliability Seminars.

Aven, T. (2008b). *Risk analysis: assessing uncertainties beyond expected values and probabilites*. Chichester: John Wiley.

Aven, T., Røed, W., & Wiencke, H. S. (2008). *Risikoanalyse: prinsipper og metoder, med anvendelser*. Oslo: Universitetsforlaget.

Bedford, T., & Cooke, R. (2001). *Probabilistic Risk Analysis - Foundations and Methods*. Cambridge: Cambridge University Press.

Drouin, M., Parry, G., Lehner, J., Martinez-Guridi, G., Wheeler, J., & LaChance, T. (2009). *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making*. United States: Office of Nuclear Regulatory Research.

Hauge, S., Hokstad, P., Langseth, H., & Øien, K. (2006). *Reliability Prediction Methods for Safety Instrumented Systems, PDS Method Handbook, 2006 edition*. Trondheim, Norway: SINTEF.

Hauge, S., Langseth, H., & Onshus, T. (2006). *Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2006 edition*. Trondheim, Norway: SINTEF.

Hauge, S., Lundteigen, M. A., Hokstad, P. R., & Håbrekke, S. (2010). *Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook, 2010 Edition*. Trondheim: SINTEF.

Hokstad, P. R., Hauge, S., & Onshus, T. (2001). *Bruk av HIPPS for utstyrsbeskyttelse*.

Häger, D. (2004). *Implementation of SIL requirements in the Norwegian offshore industry.* D. Häger, Stavanger.

IEC61508 (1998). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. Geneva: International Electrotechnical Commission.

IEC61511 (2003). *Functional Safety - Safety Instrumented Systems for the Process Industry*. Geneva: International Electrotechnical Commission.

ISO8402 (1986). *Quality Vocabulary*. Geneva: International Organization for Standardization.

ISO10418 (2003). *Petroleum and natural gas industries - Offshore production instrallations, basic surface process safety systems*: International Standard Organization.

ISO13702 (1999). *Petroleum and natural gas industries - Control and mitigation of fires and explosions on offshore production installations - Requirements and guidelines*. Geneva: International Standard Organization.

Janbu, A. F. (2009). *Treatment of Uncertainties in Reliability Assessment of Safety Instrumented Systems.* A. F. Janbu, Trondheim.

Lundteigen, M. A. (2009). *Safety instrumented systems in the oil and gas industry: concepts and methods for safety and reliability assessments in design and operation.* Norges teknisk-naturvitenskapelige universitet, Trondheim.

Lundteigen, M. A. (2010). *Implementering av IEC 61508 og IEC 61511: Oppfølging av pålitelighet i driftsfasen*. Paper presented at the ESRA.

Lundteigen, M. A., & Hauge, S. (2008). *Utfordringer knyttet til oppfølging av instrumenterte sikkerhetssystemer (SIS) i drift*. Paper presented at the Prosessikkerhet 2008, 25-26 nov.,

Monk, J. (2010). Risk: a fiction. Retrieved from http://www.ifz.tugraz.at/index_en.php/filemanager/download/120/monk.pdf

Mosleh, A., Siu, N., Smidts, C., & Lui, C. (1995). *Model Uncertainty: Its Characterization and Quantification*. Maryland: Center for Reliability Engineering, University of Maryland.

NASA (2002). *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Parctitioners*. Washington: NASA Office of Safety and Mission Assurance.

OLF-070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry*. Stavanger, Norway: The Norwegian Oil Industry Association.

OREDA (2009). *Offshore Reliability Data Handbook*. Høvik: Distributed by: Det norske veritas.

Parry, G. W. (1996). The characterization of uncertainty in Probabilistic Risk Assessments of complex systems. *Reliability Engineering & System Safety*, 119-126.

Ptil § 18 Styringsforskriften - Innsamling, bearbeiding og bruk av data (2001 (a)).

Ptil § 44 Aktivitetsforskriften - Vedlikeholdsprogram (2001 (b)).

Ptil § 7 Sikkerhetsfunksjoner - OLFs retningslinje for bruk av IEC 61508 (2003).

Rausand, G. (2005). *Uncertainty Management in Reliability Analysis.* G. Rausand, Trondheim.

Rausand, M., & Høyland, A. (2004). *System reliability theory: models, statistical methods, and applications*. Hoboken, N.J.: Wiley-Interscience.

Safetec (2010). SIL-analyser og PFD beregning Retrieved Januar 21, 2010, from http://www.safetec.no/article.php?id=19

SINTEF (2010). IEC 61508: Hovedprinsipper og veiledning, from http://www.sintef.no/project/PDS/Presentations/IEC%2061508%20prinsipper%20og%20veiledning%20-%20endelig.pdf

Smith, D. J., & Simpson, K. G. L. (2004). *Functional safety: a straightforward guide to applying IEC 61508 and relatedstandards*. Amsterdam: Elsevier.

Watson, S. R. (1993). The meaning of probability in probabilistic safety analysis. *Reliability Engineering & System Safety*, 261-269.

APPENDIKS A: Utledning av PFD / MFDT

A.1 Introduksjon

Dette appendikset presenterer utledning av PFD_{AVG}/MFDT (Abrahamsen, 2009). PFD kalkuleringer tar på generelt grunnlag utgangspunkt i en velkjent modell for kvantifisering av systemtilgjengelighet. I denne modellen er PFD essensielt sett det samme som parametere Mean Fractional Dead Time (MFDT) (Häger, 2004). MFDT benyttes vanligvis når man analyserer kvaliteten i et system, og mer detaljer om MFDT modellen kan innhentes i Rausand & Høyland (2004). De to metodene, IEC 61508 og PDS metoden, illustrerer en noe ulik fremgangsmåte for kalkulering av PFD, men modellene er essensielt sett de samme.

A.2 Utledning

PFD_{AVG} = The Average Probability of Failure on Demand
F(t) = Levetidsfordelingen
τ = Tidsintervall mellom test

PFD_{AVG} kan uttrykkes som $\frac{\int_0^\tau F(t)dt}{\tau}$ under følgende forutsetninger:

- Komponentene settes i drift i tid 0
- Systemets tilstand kan kun identifiseres ved en test
- Systemet testes og repareres regelmessig etter faste tidsintervaller med lengden τ
- Etter en test eller reparasjon antas systemet å være ”så godt som nytt”
- Tid for test og reparasjon antas å være neglisjerbar

Utilgjengeligheten i tid, $\bar{A}_i(t)$, uttrykker sannsynligheten for at systemet vil feile i å respondere på etterspurt tid.

Man har da at:

$\bar{A}_i(t)$ = P(en feil har oppstått i eller før tiden t) = P(T≤t) = F(t) = PFD (t)

Men i de fleste sammenhenger er man ikke direkte interessert i utilgjengeligheten ($\bar{A}_i(t)$ = PFD (t)) som en funksjon av tid, men som gjennomsnittet i det lange løp.

Når man da vet at komponenten er så god som ny etter test og reparasjon, så vil gjennomsnittet i det lange løp være lik gjennomsnittet i første tidsintervall (0, τ).

Det forutsettes eksponential fordeling, og man får:

$F(t) \approx \sum_{j=1}^{M} \prod_{i \in kj} q_i(t)$ og $q_i(t) \approx 1 - e^{-\lambda t}$

der man ved $\lambda_\tau < 0{,}1$ kan skrive $F(t) \approx \sum_{j=1}^{M} \prod_{i \in kj} (\lambda_i t) dt$

Man har da at:

$$PFD_{AVG} \approx \frac{\int_0^\tau \sum \prod (\lambda_i t) dt}{\tau} = \frac{\int_0^\tau \sum (\prod \lambda_i) t^{|kj|}\, dt}{\tau} = \frac{\sum (\prod \lambda_i) \int_0^\tau t_i^{|kj|}\, dt}{\tau} = \frac{\sum (\prod \lambda_i) \left[\frac{t^{|kj|+1}}{|kj|+1}\right]_0^\tau}{\tau}$$

$$= \frac{\sum \frac{1}{|kj|+1} \prod (\lambda_i) t^{|kj|+1}}{\tau} = \sum_{j=1}^{M} \frac{1}{|kj|+1} \prod_{i \in kj} (\lambda_i \tau)$$

$$PFD_{AVG} \approx MFDT \approx \sum_{j=1}^{M} \frac{1}{|kj|+1} \prod_{i \in kj} (\lambda_i \tau)$$

A.3 Referanser

Abrahamsen, E. B. (2009). Forelesning MOS 190 - Pålitelighetsanalyse. Stavanger: E. B. Abrahamsen.

Häger, D. (2004). *Implementation of SIL requirements in the Norwegian offshore industry.* D. Häger, Stavanger.

Rausand, M., & Høyland, A. (2004). *System reliability theory: models, statistical methods, and applications*. Hoboken, N.J.: Wiley-Interscience.

APPENDIKS B: Casestudie av HIPPS-system

B.1 Introduksjon

Dette dokumentet utgjør en casestudie av et HIPPS-system, og består av de nødvendige kalkulasjonene og analysene som må foreligger for å betrakte sikkerhetsutilgjengelighet, herunder PFD, ved å benytte IEC 61508 metoden og PDS metoden.

Men hensyn til konfidensialitet så kan ikke feildata for systemet, samt en detaljert system- og funksjonsbeskrivelse angis. Til tross for at rapporten kan klassifiseres som konfidensiell av Universitetet i Stavanger i løpet av en fem års periode, vil informasjonen betraktes som konfidensiell selv etter den tid. Feildataene og nærmere systembeskrivelse er med dette anonymisert, og representerer på ingen måte feildata eller systemer i direkte tilknytning til Gassco eller andre bidragsytere i oppgaven.

Dokumentet er ikke utarbeidet for SIL verifisering eller underlagt begrensninger i forhold til annen leveringsplikt i industrien/prosjekter. Dokumentet inneholder kun resultater for kvantifisering av PFD som en caseillustrasjon for bruk i denne masteravhandlingen.

I fortsettelsen vil kun de to ulike metodenes fremgangsmåter for kvantitative kalkulasjoner av PFD og systematiske feil bli betraktet, der formålet har vært å illustrere ulikhetene mellom de to metodene.

B.2 Tilnærming

Inndata til beregningene har i hovedsak blitt hentet fra OREDA (2009) og PDS data håndbok (S. Hauge, Langseth, et al., 2006) for HIPPS komponenter.

Inndataparametrene som benyttes i kalkuleringene er:

- λ_{DU} = Raten av farlige uoppdagede feil. Hentet fra OREDA og PDS data håndbok. Feilratene som blir presentert i dette appendikset er anonymisert
- τ = Testintervallet. Hentet ut i forhold til ordinær operasjonsfilosofi for komponentene. Dersom det er usikkerhet knyttet til testintervallet, så bør det her benyttes et pessimistisk anslag

- β = Andel feil som kan medføre svikt i alle komponentene på samme tid (eller med kort tidsintervall). Det er kun tatt høyde for CCF der dette er relevant. β er hentet fra OREDA, mens verdier for C_{MooN} er hentet i OLF 070 (2004)
- P_{TIF} = Sannsynligheten for testuavhengige (systematiske) feil, altså feil som ikke oppdages under funksjonell testing, men som avdekkes under reell etterspørsel (Stein Hauge, et al., 2010). Hentet fra PDS data håndboken
- r = brøkdelen av λ_{DU} som stammer fra tilfeldige hardware feil: $r = \lambda_{DU-RH}/\lambda_{DU}$. Benyttes for å separere tilfeldige hardware feil og systematiske feil i raten av farlige uoppdagede feil. Hentet fra PDS data håndboken

Under kalkulasjoner av PFD er raten av farlige uoppdagede feil (λ_{DU}) av stor betydning, der denne inndataparameteren (sammen med testintervallet) predikerer hvor sannsynlig det er at en sikkerhetsfunksjon feiler på etterspørsel. I følge IEC 61508 så vil raten av λ_{DU} kun inkludere tilfeldige hardware feil. Likevel, vil en som nevnt i hovedrapporten til dette appendikset, se at flere av de rapporterte feilene i data håndbøker er systematiske feil (S. Hauge, Hokstad, et al., 2006). Systematiske feil vil som et resultat av dette til dels bli inkludert implisitt, og således betraktet i kalkulasjonene.

I denne systemanalysen av caset vil oppgaven i første omgang betrakte raten av farlige uoppdagede feil slik den blir presentert i data håndbøker, det vil si at feilraten ikke vil være oppdatert for å samsvare med eventuelle applikasjons- og anleggsspesifikke forhold. Disse dataene blir betraktet som grunndata og grunnkalkulasjoner for caset. I en andre kalkulasjon, vil oppgaven illustrere ulikheten mellom metodene dersom det benyttes oppdatering av inndataparameterne ut i fra et tenkt applikasjons- og anleggsspesifikt scenario. Dette er illustrert i kapittel B.6 av appendikset.

Når det gjelder CCF så avvises β-faktor modellen i PDS metoden. For å gjøre en sammenlikning mellom for eksempel 1oo2, 1oo3 og 2oo3 votering, så betrakter PDS metoden at det bør foreligge ulike β'er for ulike voteringskonfigurasjoner. Denne faktoren er ikke inkludert i standard β-faktor modellen slik den beskrives i IEC 61508 metoden. PDS metoden introduserer med dette C_{MooN} faktoren, der man for en MooN votering (M<N) har:

$$\beta_{MooN} = C_{MooN} * \beta$$

Modifikasjonsfaktoren C_{MooN} reflekterer her systemets konfigurasjon (votering) med følgende verdier:

Tabell B.1 – Numeriske verdier for modifikasjonsfaktoren ved MooN votering (S. Hauge, Langseth, et al., 2006; OLF-070, 2004)

Votering	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
C_{MooN}	1,0	0,3	2,4	0,15	0,8	4,0

Raten av CCF er med dette kalkulert ut fra raten av farlige oppdagede (uavhengige) feil og β-faktorene:

$$\lambda_{CommonCause\ IEC61508} = \lambda_{Independent} * \beta$$

$$\lambda_{CommonCause\ PDS} = \lambda_{Independent} * \beta_{MooN}$$

Der hvor sannsynligheten for systematiske feil er inkludert i beregningene, vil disse bli lagt til som raten λ_{DU-S} og en P_{TIF} faktor. Merk at raten λ_{DU-S} uten å oppdatere eller å justere vil inngå i λ_{DU} på lik linje i de to metodene under grunnkalkulasjonen – ulikheten kommer først til syne når oppgaven tar for seg det anleggsspesifikke scenarioet med oppdatering av ratene.

$$\lambda_{DU} = \lambda_{DU-RH} + \lambda_{DU-S}$$

der $\lambda_{DU-S} = (1 - r) * \lambda_{DU}$

Sannsynligheten for svikt på etterspurt tid er for de to metodene kalkulert med utgangspunkt i grunnformelen for en MooN konfigurasjon der M<N (OLF-070, 2004):

$$PFD_{IEC\ 61508} \approx \frac{\lambda_{DU} * \tau}{2} + \lambda_{CommonCause\ IEC61508}$$

$$PFD_{PDS} \approx \frac{\lambda_{DU} * \tau}{2} + \lambda_{CommonCause\ PDS} + P_{TIF}$$

der man for PDS metoden har:

$$\frac{\lambda_{DU} * \tau}{2} = \frac{\lambda_{DU-RH} * \tau}{2} + \frac{\lambda_{DU-S} * \tau}{2}$$

$$P_{TIF} \approx P_{TIF\ (MooN)} * \beta_{MooN} \quad \text{(M<N)}$$

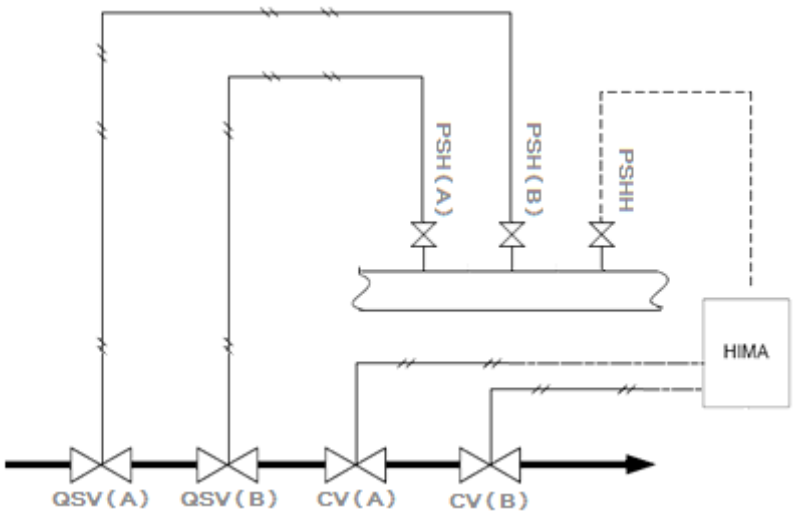
Den totale systempåliteligheten (PFD) vil videre bli kalkulert ut i fra komponentenes PFD. Det vil bli tatt høyde for systemets konfigurasjon (votering) ved CCF der det foreligger redundante komponenter eller delsystemer. Systemets utilgjengelighet med hensyn til reparasjon og testing er ikke inkludert i kalkuleringene. Testintervallene anses å være tilstrekkelig mye lenger enn reparasjons- og nedetiden (MTTR < Testintervall (τ)), og at man dermed kan se bort fra eventuell tid knyttet til reparasjon.

B.3 Casebeskrivelse – HIPPS system

HIPPS (High Integrity Pressure Protection System) er et frittstående sikkerhetssystem som i dette caset er utformet for å kunne håndtere uønskede hendelser som skyldes begrenset fakkelkapasitet. Filosofien er å stenge tilførselen av hydrokarboner til et system eller en seksjon dersom trykket er høyere enn det som er forhåndsinnstilt. Innstillingsverdien for HIPPS-trykket er lavere enn innstillingsverdien for PSV'er (Pressure Safety Valves), der disse beskytter systemet eller seksjonen.

En standard HIPPS løsning består av en trykksensor som via en logikk stenger en eller flere (hurtigvirkende) ventiler når det målte trykket i mediet kommer over en fastsatt verdi (Hokstad, Hauge, & Onshus, 2001).

I caset for systemanalysen benytter HIPPS et primært og et sekundært system. Det primære systemet består av to hurtigavstengningsventiler (QSV - Quick Shut-off Valve) som aktiveres av trykktransmitter eller trykkbrytere gjennom et pneumatisk kontrollsystem. Det sekundære systemet består av to uavhengige kontrollventiler (CV - Control Valve) som er plassert i serier med det primære systemets QSV'er for å kunne møte angitte PFD krav. Det sekundære systemet har et elektrisk kontrollsystem som aktiveres av trykkbrytere, og i enkelte tilfeller trykksendere. PFD for HIPPS funksjonen påvirker sannsynligheten for at fakkelsystemet overbelastes. Kontrollventilen som er i serie med en QSV stenges av ved samme trykk som QSV'en. Kontrollventilen er dermed et uavhengig, sekundært trykksikkerhetselement. Denne funksjonen gjør kontrollventilen til en del av HIPPS systemet.

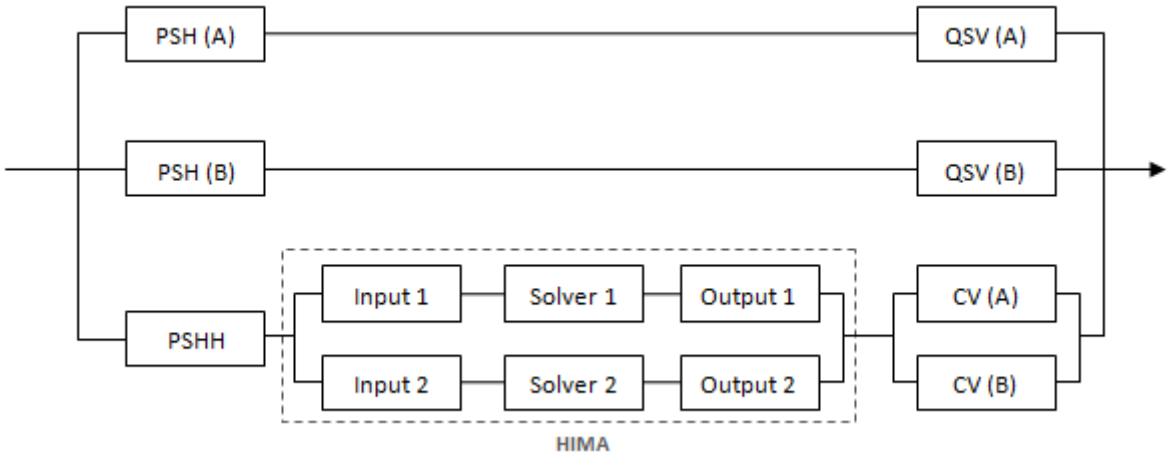


Figur B.1 - HIPPS systemet for analysen

Den avgrensede HIPPS-systemet som benyttes i caset for systemanalysen er illustrert i figur B.1, og består av:

- Fire ventiler i serie hvor to (primær HIPPS) er hurtigavstengningsventiler (QSV) og de to andre (sekundær HIPPS) er kontrollventiler (CV)
- En trykktransmitter eller trykkbryter, samt en signaloverføring som er dedikert til QSV, drives pneumatisk med en rørkobling til en ventilaktuator, mens kontrollventilene stenges med et signal fra en elektrisk bryter som rutes via en HIMA (logisk solver)

Basert på systemets oppbygning kan det illustreres og settes opp et logisk pålitelighets blokk diagram (Reliability Block Diagram - RBD) slik som illustrert i figur B.2.



Figur B.2 - Pålitelighet blokk diagram for HIPPS systemet i analysen

Systemet består av tre moduler (sløyfer) som deles inn i primær (A og B) og sekundær (C) HIPPS; seriemodul A med PSH (A) og QSV (A), seriemodul B med PSH (B) og QSV (B), og modul C med PSHH, HIMA, CV (A) og CV (B). Systemet som helhet har en 1oo3 votering, mens HIMA funksjonen og kontrollventilene igjen er votert med en 1oo2 konfigurasjon.

B.4 Inndata for PFD kalkulering

Som tidligere nevnt er de dataene som blir presentert i dette caset anonymisert for å ivareta konfidensialitetsbegrensningene. De dataene som presenteres kan med dette være noe begrenset i forhold til eventuell faktisk dokumentasjonen av inndata til analyser, og representerer *ikke* observerte data fra angitt system. Det legges videre til grunn at faktiske operasjonelle driftsdata fra et system ikke er en forutsetning for å illustrere ulikhetene mellom kalkulasjonene. I tabellen under følger grunndata for systemanalysen av caset:

Tabell B.2 – Grunndata for angitt system

Komponent	Feilrate (λ_{DU})	β-faktor	Testintervall τ (timer)	P_{TIF}	r
PSH (A)	1,60E-06	0,05	8760	5,0E-03	0,5
PSH (B)	1,60E-06	0,05	8760	5,0E-03	0,5
PSHH (C)	1,40E-06	0,03	8760	5,0E-03	0,5
HIMA Input	1,20E-06	0,03	8760	1,0E-03	0,5
Logic Solver (HIMA)	1,10E-06	0,03	8760	1,0E-03	0,5
HIMA Output	1,20E-06	0,03	8760	1,0E-03	0,5
QSV (A)	3,20E-06	0,05	8760	1,0E-03	0,5
QSV (B)	3,20E-06	0,05	8760	1,0E-03	0,5
CV (A)	2,70E-06	0,03	8760	1,0E-03	0,5
CV (B)	2,70E-06	0,03	8760	1,0E-03	0,5

Dataene er estimert på bakgrunn av en operasjonsfilosofi der systemet vil bli testet en gang i året (τ er da 12 måneder/8760 timer). Det har blitt lagt til grunn en β-faktor på 5 % for pneumatiske og hydrauliske komponenter, og 3 % for elektroniske komponenter.

B.5 PFD kalkulering

Denne delen av appendikset kalkuleres PFD for det sikkerhetsinstrumenterte HIPPS systemet for å komme frem til kvantifisert sikkerhetsutilgjengelighet. Den uønskede hendelsen er at *"HIPPS systemet svikter i å lukke minst en av ventilene i tilfeller ved høyt trykk"*. Kapitlet presenterer med dette alle resultatene fra kalkulasjonene som må foreligger for å komme frem til systemets PFD slik det er presentert i rapporten.

Tabell B.3 – Kalkulasjoner for komponentene

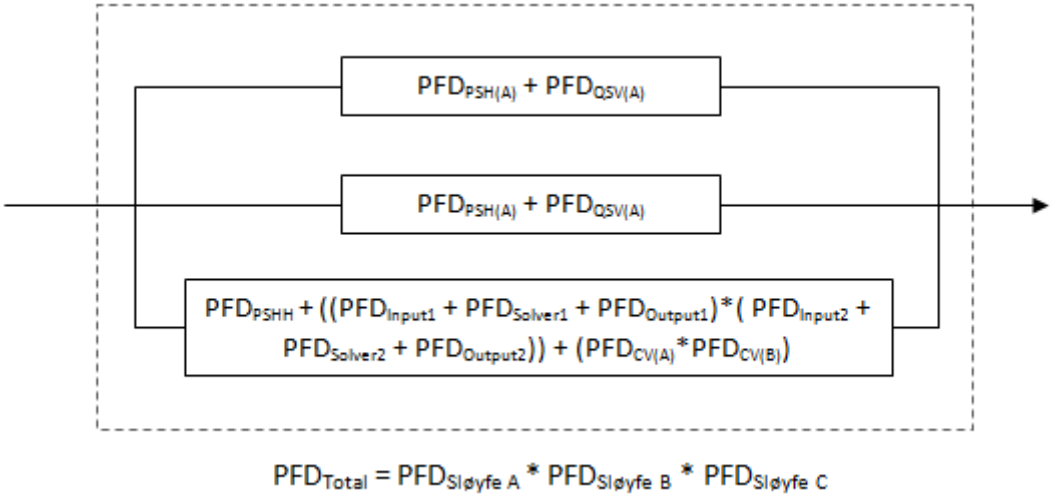
Komponent	Hardware feil (λ_{DU-RH}) - PDS	Systematiske feil (λ_{DU-S}) - PDS	IEC: $\lambda_{DU}*\tau/2$ (komponent)	PDS: $\lambda_{DU}*\tau/2$ (komponent)
PSH (A)	8,00E-07	8,00E-07	7,01E-03	7,01E-03
PSH (B)	8,00E-07	8,00E-07	7,01E-03	7,01E-03
PSHH (C)	7,00E-07	7,00E-07	6,13E-03	6,13E-03
HIMA Input	6,00E-07	6,00E-07	5,26E-03	5,26E-03
Logic Solver (HIMA)	5,50E-07	5,50E-07	4,82E-03	4,82E-03
HIMA Output	6,00E-07	6,00E-07	5,26E-03	5,26E-03
QSV (A)	1,60E-06	1,60E-06	1,40E-02	1,40E-02
QSV (B)	1,60E-06	1,60E-06	1,40E-02	1,40E-02
CV (A)	1,35E-06	1,35E-06	1,18E-02	1,18E-02
CV (B)	1,35E-06	1,35E-06	1,18E-02	1,18E-02

Tabell B.4 - Kalkulasjoner for komponentene (II)

Komponent	CCF (IEC)	CCF (PDS)	CCF (P_{TIF})	PFD (IEC)	PFD (PDS)
PSH (A)	3,50E-04	1,05E-04	7,50E-05	7,36E-03	7,19E-03
PSH (B)	3,50E-04	1,05E-04	7,50E-05	7,36E-03	7,19E-03
PSHH (C)	1,84E-04	5,52E-05	4,50E-05	6,32E-03	6,23E-03
HIMA Input	1,58E-04	4,73E-05	9,00E-06	5,41E-03	5,31E-03
Logic Solver (HIMA)	1,45E-04	4,34E-05	9,00E-06	4,96E-03	4,87E-03
HIMA Output	1,58E-04	4,73E-05	9,00E-06	5,41E-03	5,31E-03
QSV (A)	7,01E-04	2,10E-04	1,50E-05	1,47E-02	1,42E-02
QSV (B)	7,01E-04	2,10E-04	1,50E-05	1,47E-02	1,42E-02
CV (A)	3,55E-04	1,06E-04	9,00E-06	1,22E-02	1,19E-02
CV (B)	3,55E-04	1,06E-04	9,00E-06	1,22E-02	1,19E-02

Man kan på bakgrunn av informasjonen i tabellene B.3 og B.4 således kalkulere den totale systempåliteligheten i de ulike metodene. Figur B.3 under er ment som en informativ

illustrasjon av kalkulasjoner for systemets totale PFD. Illustrasjonen er en forenklet pålitelighet blokk diagram (RBD) basert på HIPPS systemet i caset. Beregningene som presenteres er videre basert på komponentenes PFD'er slik disse er presentert i tabell B.4 over.



Figur B.3 - Illustrasjon av PFD kalkulasjoner

Tabell B.5 - Systemets PFD ved IEC 61508 metoden og PDS metoden (grunndata)

Sikkerhetutilgjengelighet	IEC 61508 metoden	PFD metoden
PFD_{System}	3,27E-06	3,04E-06

Dersom det antas at HIPPS systemet i gjennomsnitt blir utløst to ganger i året, vil sannsynligheten for å observere svikt i HIPPS systemet på etterspørsel i et spesifikt år være:

$IEC\ 61508: (3{,}27 * 10^{-6}) * 2 = 6{,}54 * 10^{-6}$

Gjennomsnittstiden til en slik feil er da: $10^6/6{,}54\,år \approx 152\ 000\ år$

$PDS: (3{,}04 * 10^{-6}) * 2 = 6{,}08 * 10^{-6}$

Gjennomsnittstiden til en slik feil er da: $10^6/6{,}08\,år \approx 164\ 000\ år$

B.6 Applikasjons- og anleggsspesifikk oppdatering

For å illustrere hvordan metodene tar høyde for usikkerhet (variasjon) knyttet til fullstendighet og inndata, har en enkel sensitivitetsbetraktning basert på oppdatering av inndata blitt foretatt for å betrakte variasjon i utdata. Det vil si at man oppdaterer inndataparametre som er av betydning for å anta samsvar med eventuelle applikasjons- og anleggsspesifikke forhold, og således vil kunne nytte dette til å vurdere den relative endringen i utdata som følger av endring i inndata. Det legges videre til grunn at det i denne oppdateringen vil tas utgangspunkt i forhold som antas å være direkte knyttet til lokale operasjonelle forhold - det vil si at man vektlegger endring i parameterverdier knyttet til systematiske feil og CCF. De applikasjonsspesifikke kalkulasjonene som her nyttes er mer inngående beskrevet i PDS metode håndboken, appendiks C (S. Hauge, Hokstad, et al., 2006).

B.6.1 Oppdatering

B.6.1.1 Raten av systematiske feil – $\lambda_{DU\text{-}S}$

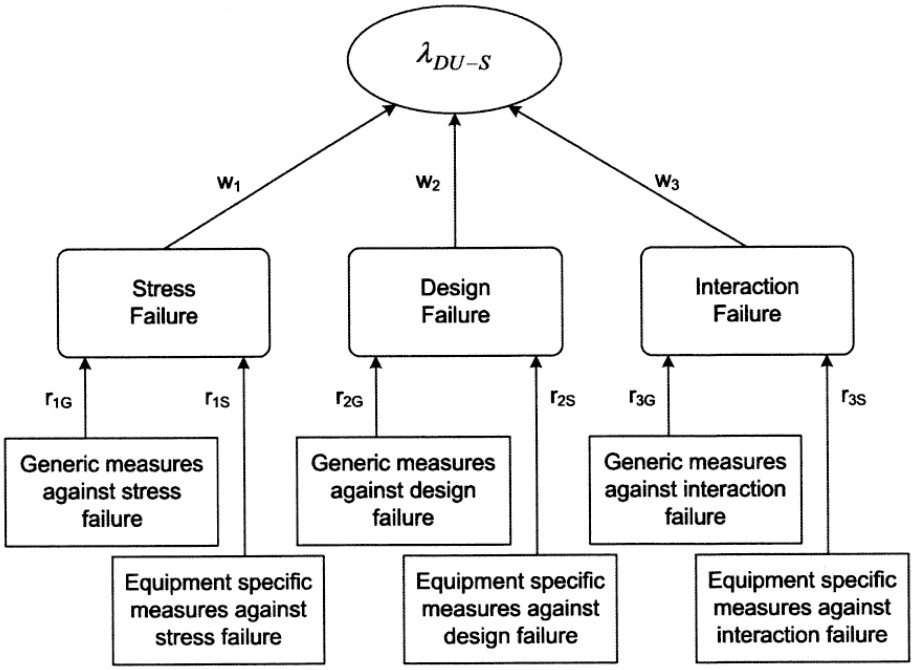
I PDS metoden legges det til grunn en tilnærming for å tilpasse den gjennomsnittlige raten av farlige uoppdagede systematiske feil ($\lambda_{DU\text{-}S}$) til applikasjonsspesifikke verdier ved kvalitativt å vurdere:

- unngåelse og kontroll av systematiske feil for generiske data
- unngåelse og kontroll av systematiske feil knyttet til applikasjonsspesifikke forhold

Disse blir deretter "vektet" etter "grad av kvalitet" for generiske så vel som utstyrsspesifikke applikasjonsforhold. Oppgaven benytter $\hat{\lambda}_{DU-S}$ for å illustrere den oppdaterte applikasjonsspesifikke verdien som kalkuleres i følgende formel (S. Hauge, Hokstad, et al., 2006):

$$\hat{\lambda}_{DU-S} = \lambda_{DU-S}(w_1 * r_{1G} * r_{1S} + w_2 * r_{2G} * r_{2S} + w_3 * r_{3G} * r_{3S})$$

der de ulike parametrene er nærmere beskrevet i figur B.4:



Figur B.4 - Applikasjonsspesifikk modell for λ_{DU-S} (S. Hauge, Hokstad, et al., 2006)

Det antas at det kan dokumenteres at de kvalitative kravene knyttet til unngåelse og kontroll av systematiske feil for de generiske dataene er ivaretatt som følger:

- Stressfeil: nødvendige tiltak er ivaretatt
- Designfeil: alle nødvendige og anbefalte tiltak er ivaretatt
- Interaksjonsfeil: noen nødvendige og høyst anbefalte tiltak blir ivaretatt

Ut i fra tabeller i PDS metode håndboken (S. Hauge, Hokstad, et al., 2006, s. 53-54), ser man at nødvendige tiltak for samsvar med krav for å unngå og kontrollere systematiske stressfeil tilsvarer r_{1G} = 1. Videre så er alle nødvendige og anbefalte tiltak iverksatt for å unngå og kontrollere systematiske designfeil tilsvarer r_{2G} = 0,1, og at noen nødvendige og høyst anbefalte tiltak ivaretatt for systematiske interaksjonsfeil korresponderer med r_{3G} mellom 0,1 og 1,0. Om man da antar at effekten av implementerte tiltak har blitt vurdert av en ekspertgruppe, og at de systematiske interaksjonsfeilene samsvarer med omkring 50 % av hva som er nødvendig for å unngå og kontrollere alle systematiske interaksjonsfeil, så benyttes r_{3G} = 0,5.

Oppgaven antar videre at det kan dokumenteres at de kvalitative kravene knyttet til unngåelse og kontroll av systematiske feil for systemet i caset under drift er ivaretatt som følger:

- Stressfeil: alle kjente konkrete tiltak og gode barrierer er implementert
- Designfeil: noen spesifikke tiltak og gode barrierer er implementert
- Interaksjonsfeil: kjente tiltak og barrierer er mindre enn tilstrekkelig

Ut i fra tabeller i PDS metode håndboken ser man at når alle kjente konkrete tiltak og gode barrierer er implementert mot systematiske stressfeil korresponderer med r_{1S} = 0,1. Videre er noen spesifikke tiltak og barrierer implementert mot systematiske designfeil, noe som samsvarer med r_{2S} mellom 0,3 og 1,0. Om det antas at effekten av implementerte tiltak har blitt vurdert at en ekspertgruppe som anslår at disse svarer til 20 % av "normal praksis", så anvendes r_{2S} = 0,8. Implementering av systemspesifikke tiltak mot systematiske interaksjonsfeil er anslått å være mindre enn tilstrekkelig, og r_{3S} er da mellom 1,0 og 10 i PDS metoden. Basert på en ekspertgruppes vurdering anslås effekten av slike tiltak å være fraværende, og ekspertgruppen anslår at r_{3S} = 10.

Til slutt har ekspertgruppen basert på en analyse av feildataene kommer frem til følgende vekting av systematiske feil: stressfeil (50%), designfeil (10%) og interaksjonsfeil (40%).

Overnevnte kvalitative vurderinger kan da oppsummeres der eksperter/risikoanalytikeren(e) har tilegnet følgende parameterverdier:

Stressfeil	w_1 = 0,5	r_{1G} = 1,0	r_{1S} = 0,1
Designfeil	w_2 = 0,1	r_{2G} = 0,1	r_{2S} = 0,8
Interaksjonsfeil	w_3 = 0,4	r_{3G} = 0,5	r_{3S} = 10

Faktoren for påvirkning av de systematiske feilene kalkuleres da til å være 2,058. Da får man følgende forhold: $\hat{\lambda}_{DU-S} = \lambda_{DU-S}(2{,}058)$

Applikasjons- og anleggsspesifikk feilrate for de systematiske feilene kan da oppdateres, og man får en ny og oppdatert rate for de systematiske feilene ($\hat{\lambda}_{DU-S}$) for hver komponent. Merk at overnevnte oppdatering kun vil inngå som en faktor i PDS metoden, altså ikke i IEC 61508 metoden som ikke kvantifiserer de systematiske feilene.

B.6.1.2 Sannsynligheten for testuavhengige feil – P_{TIF}

Slik som for raten av systematiske feil, er sannsynligheten for testuavhengige feil (P_{TIF}) også angitt som gjennomsnittsverdier for ulike systemer. Oppgaven vil benytte notasjonen $\hat{P}_{TIF}$ for den oppdaterte applikasjons- og anleggsspesifikke sannsynligheten. I den anledning introduserer PDS metoden følgende modell:

$$\hat{P}_{TIF} = k_T * P_{TIF}$$

Parameteren k_T beskriver her fullstendigheten til de funksjonelle testene på angitt system, altså evnen til å avdekke feil. P_{TIF} er videre gjennomsnittsverdien som betraktes under "normale" funksjonelle tester.

Anta at en ekspertgruppe har dokumentert at en utvidet prosedyre for de funksjonelle testene foreligger og skal benyttes for systemet som betraktes. Fra PDS metode håndboken ser man at en utvidet test kan tilsvare k_T = 0,3, noe som betyr at omkring 70 % av feilene som ikke avdekkes under "normale" gjennomsnittlige funksjonstester vil avdekkes i den utvidete testen. Med dokumentert utvidete testprosedyrer får man da følgende applikasjons- og anleggsspesifikke faktor for systemanalysen i caset: $\hat{P}_{TIF} = 0{,}3 * P_{TIF}$

B.6.1.3 Beskyttelse mot CCF – β

Til slutt ønsker oppgaven også å betrakte β for de ulike komponentene i systemet. Verdiene som er angitt for β er også gjennomsnittsverdier fra industrien. Oppgaven vil benytte notasjonen $\hat{\beta}$ for den applikasjonsspesifikke verdien. I den anledning presenterer PDS metoden følgende modell:

$$\hat{\beta}_{PDS} = k_\beta * \beta$$

Parameteren k_β beskriver her systemets grad av beskyttelse mot CCF, mens β er den generiske verdien hvor det antas "gjennomsnittlig" beskyttelse.

Anta at en ekspertgruppe har dokumentert at et utvidet nivå av beskyttelse mot CCF er implementert i angitt system. Fra PDS metode håndboken finner man da at et utvidet nivå av beskyttelse svarer til k_β = 0,5, som betyr at 50 % av feilene som foreligger under "normal beskyttelse" nå vil forhindres. Med utvidet beskyttelse mot CCF så får man da følgende applikasjons- og anleggsspesifikke faktor for systemanalysen i caset: $\hat{\beta}_{PDS} = 0{,}5 * \beta$

IEC 61508-6, Appendiks D beskriver videre en sjekklistebasert metode for å kalkulere applikasjons- og anleggsspesifikk β-verdi. Denne metoden innebærer å svare på en rekke spørsmål under følgende overskrifter:

1. Separasjon / segregering
2. Redundans
3. Design, kompleksitet og erfaring
4. Vurdering av data
5. Menneskelig interaksjon og prosedyrer
6. Opplæring, kompetanse og sikkerhetskultur
7. Omgivelseskontroll
8. Omgivelsestesting

Overnevnte anses som et godt prinsipp, og vil ved ekspertvurderinger kunne fungere som en god tilnærming for å komme frem til applikasjons- og anleggsspesifikke β-verdier.

I denne systemanalysen av caset antas det videre at en ekspertgruppe basert på sjekklisten i IEC metoden kommer frem til at applikasjons- og anleggsspesifikk β-verdi for angitt system er tilsvarende 30 % av hva gjennomsnittsverdien for industrien er. Dette betyr at 70 % feilene som foreligger under "normale" forhold nå vil forhindres. Man får da $\hat{\beta}_{IEC} = 0{,}3 * \beta$

B.6.2 Oppdatert PFD kalkulering

Basert på oppdaterte parametre som er tilpasset et tenkt lokalt operasjonelt driftsforhold kan en nå oppdatere kalkulasjonene av PFD. Kalkulasjonene vil ta utgangspunkt i grunndataene fra systemanalysen av caset, og oppdatere med følgende parametre:

IEC 61508: $\hat{\beta}_{IEC}$

PDS: $\hat{\lambda}_{DU-S}$, $\hat{P}_{TIF}$ og $\hat{\beta}_{PDS}$

Tabell B.6 - Oppdaterte kalkulasjoner for komponentene

Komponent	Hardware (λ_{DU-RH}) (PDS)	Systemat. ($\hat{\lambda}_{DU-S}$) (PDS)	Farlige feil ($\hat{\lambda}_{DU}$) (PDS)	$\hat{\beta}$-faktor (IEC)	$\hat{\beta}$-faktor (PDS)	$\hat{P}_{TIF}$ (PDS)
PSH (A)	8,00E-07	1,65E-06	2,45E-06	0,015	0,025	1,5E-03
PSH (B)	8,00E-07	1,65E-06	2,45E-06	0,015	0,025	1,5E-03
PSHH (C)	7,00E-07	1,44E-06	2,14E-06	0,009	0,015	1,5E-03
HIMA Input	6,00E-07	1,23E-06	1,83E-06	0,009	0,015	3,0E-04
Logic Solver (HIMA)	5,50E-07	1,13E-06	1,68E-06	0,009	0,015	3,0E-04
HIMA Output	6,00E-07	1,23E-06	1,83E-06	0,009	0,015	3,0E-04
QSV (A)	1,60E-06	3,29E-06	4,89E-06	0,015	0,025	3,0E-04
QSV (B)	1,60E-06	3,29E-06	4,89E-06	0,015	0,025	3,0E-04
CV (A)	1,35E-06	2,78E-06	4,13E-06	0,009	0,015	3,0E-04
CV (B)	1,35E-06	2,78E-06	4,13E-06	0,009	0,015	3,0E-04

Tabell B.7 - Oppdaterte kalkulasjoner for komponentene (II)

Komponent	λ_{DU}*τ/2 (IEC)	λ_{DU}*τ/2 (PDS)	CCF (IEC)	CCF (PDS)	CCF - $\hat{P}_{TIF}$ (PDS)
PSH (A)	7,01E-03	1,07E-02	1,05E-04	8,04E-05	1,13E-05
PSH (B)	7,01E-03	1,07E-02	1,05E-04	8,04E-05	1,13E-05
PSHH (C)	6,13E-03	9,38E-03	5,52E-05	4,22E-05	6,75E-06
HIMA Input	5,26E-03	8,04E-03	4,73E-05	3,62E-05	1,35E-06
Logic Solver (HIMA)	4,82E-03	7,37E-03	4,34E-05	3,32E-05	1,35E-06
HIMA Output	5,26E-03	8,04E-03	4,73E-05	3,62E-05	1,35E-06
QSV (A)	1,40E-02	2,14E-02	2,10E-04	1,61E-04	2,25E-06
QSV (B)	1,40E-02	2,14E-02	2,10E-04	1,61E-04	2,25E-06
CV (A)	1,18E-02	1,81E-02	1,06E-04	8,14E-05	1,35E-06
CV (B)	1,18E-02	1,81E-02	1,06E-04	8,14E-05	1,35E-06

Tabell B.8 - Oppdaterte PFD kalkulasjoner for komponentene

Komponent	PFD (IEC)	PFD (PDS)
PSH (A)	7,11E-03	1,08E-02
PSH (B)	7,11E-03	1,08E-02
PSHH (C)	6,19E-03	9,42E-03
HIMA Input	5,30E-03	8,07E-03
Logic Solver (HIMA)	4,86E-03	7,40E-03
HIMA Output	5,30E-03	8,07E-03
QSV (A)	1,42E-02	2,16E-02
QSV (B)	1,42E-02	2,16E-02
CV (A)	1,19E-02	1,82E-02
CV (B)	1,19E-02	1,82E-02

Tabell B.9 - Systemets PFD ved IEC 61508 metoden og PDS metoden (oppdaterte data)

Sikkerhetutilgjengelighet	IEC 61508 metoden	PFD metoden
PFD_{System}	2,99E-06	1,08E-05

Dersom det antas at HIPPS systemet i gjennomsnitt blir utløst to ganger i året, vil sannsynligheten for å observere svikt i HIPPS systemet på etterspørsel i et spesifikt år være:

$IEC\ 61508: (2{,}99 * 10^{-6}) * 2 = 5{,}98 * 10^{-6}$

Gjennomsnittstiden til en slik feil er da: $10^6 / 5{,}98\,år \approx 167\,000\,år$

$PDS: (1{,}08 * 10^{-5}) * 2 = 2{,}16 * 10^{-5}$

Gjennomsnittstiden til en slik feil er da: $10^5 / 2{,}16\,år \approx 46\,000\,år$

B.7 Referanser

Hauge, S., Hokstad, P., Langseth, H., & Øien, K. (2006). *Reliability Prediction Methods for Safety Instrumented Systems, PDS Method Handbook, 2006 edition*. Trondheim, Norway: SINTEF.

Hauge, S., Langseth, H., & Onshus, T. (2006). *Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2006 edition*. Trondheim, Norway: SINTEF.

Hauge, S., Lundteigen, M. A., Hokstad, P. R., & Håbrekke, S. (2010). *Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook, 2010 Edition*. Trondheim: SINTEF.

Hokstad, P. R., Hauge, S., & Onshus, T. (2001). *Bruk av HIPPS for utstyrsbeskyttelse*.

Häger, D. (2004). *Implementation of SIL requirements in the Norwegian offshore industry.* D. Häger, Stavanger.

IEC61508 (1998). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. Geneva: International Electrotechnical Commission.

OLF-070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry*. Stavanger, Norway: The Norwegian Oil Industry Association.

OREDA (2009). *Offshore Reliability Data Handbook*. Høvik: Distributed by: Det norske veritas.

APPENDIKS C: Kalkulasjoner med alternativ metodisk tilnærming

C.1 Introduksjon

Dette appendikset inneholder kalkulasjoner av PFD for det sikkerhetsinstrumenterte HIPPS systemet ut i fra den foreslåtte alternative metodiske tilnærmingen for å implementere usikkerhet i SIL verifikasjon. Kalkulasjonene er gjennomført etter PDS metodens kalkuleringsformler, slik de er presentert i hovedrapporten og nærmere beskrevet i appendiks B (B.2).

C.2 Kalkulasjoner

Tabell C.1 - Kalkulasjoner for komponentene ved alternativ metodisk tilnærming

Komponent	Hardware ($\hat{\lambda}_{DU-RH}$)	Systemat. ($\hat{\lambda}_{DU-S}$)	Farlige feil ($\hat{\lambda}_{DU}$)	$\hat{\beta}$-faktor	$\hat{P}_{TIF}$	r
PSH (A)*	3,00E-06	1,83E-05	2,13E-05	0,03	2,5E-03	0,5
PSH (B)*	5,20E-06	1,86E-05	2,38E-05	0,03	2,5E-03	0,5
PSHH (C)*	6,80E-06	4,65E-05	5,33E-05	0,02	1,5E-03	0,4
HIMA Input	6,00E-07	1,23E-06	1,83E-06	0,015	3,0E-04	0,5
Logic Solver (HIMA)	5,50E-07	1,13E-06	1,68E-06	0,015	3,0E-04	0,5
HIMA Output	6,00E-07	1,23E-06	1,83E-06	0,015	3,0E-04	0,5
QSV (A)	1,60E-06	3,29E-06	4,89E-06	0,025	3,0E-04	0,5
QSV (B)	1,60E-06	3,29E-06	4,89E-06	0,025	3,0E-04	0,5
CV (A)	1,35E-06	2,78E-06	4,13E-06	0,015	3,0E-04	0,5
CV (B)	1,35E-06	2,78E-06	4,13E-06	0,015	3,0E-04	0,5

Tabell C.2 - Kalkulasjoner for komponentene ved alternativ metodisk tilnærming (II)

Komponent	$\lambda_{DU}*\tau/2$	CCF	CCF - $\widehat{P}_{TIF}$	PFD (PDS)
PSH (A)	9,33E-02	8,40E-04	2,25E-05	9,42E-02
PSH (B)	1,04E-01	9,38E-04	2,25E-05	1,05E-01
PSHH (C)	2,33E-01	1,40E-03	9,00E-06	2,35E-01
HIMA Input	8,04E-03	3,62E-05	1,35E-06	8,07E-03
Logic Solver (HIMA)	7,37E-03	3,32E-05	1,35E-06	7,40E-03
HIMA Output	8,04E-03	3,62E-05	1,35E-06	8,07E-03
QSV (A)	2,14E-02	1,61E-04	2,25E-06	2,16E-02
QSV (B)	2,14E-02	1,61E-04	2,25E-06	2,16E-02
CV (A)	1,81E-02	8,14E-05	1,35E-06	1,82E-02
CV (B)	1,81E-02	8,14E-05	1,35E-06	1,82E-02

Tabell C.3 - Systemets PFD ved alternativ metodisk tilnærming

Sikkerhetutilgjengelighet	Prediksjon
PFD_{System}	3,46E-03
Grad av usikkerhet	Lav

Dersom det antas at HIPPS systemet i gjennomsnitt blir utløst to ganger i året, vil sannsynligheten for å observere svikt i HIPPS systemet på etterspørsel i et spesifikt år være:

$$Alternativ\ metodisk\ tilnærming: (3{,}46 * 10^{-3}) * 2 = 6{,}92 * 10^{-3}$$

Gjennomsnittstiden til en slik feil er da: $10^3/6{,}92\ år \approx 150\ år$