Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

BACHELOROPPGAVE

Studieprogram/spesialisering: Bachelor i ingeniørfag / Automatisering og elektronikkdesign	Vårsemesteret 2021 Åpen
Forfatter(e): Kent-Stian H. Larsen, Karsten Bruun	
Fagansvarlig: Arnfinn Aas Eielsen Veileder(e): Arnfinn Aas Eielsen	
Tittel på bacheloroppgaven: Prosess for optimalisering av SIS-systemer i drift og vedlikeholdsfasen Engelsk tittel: Process for optimization of SIS-Systems in overall operation	
Studiepoeng: 20	
Emneord: SIS, PFD, SIL, IEC 61508, IEC 61511, NOG 070, Pålitelighetsanalyse, λ_{DU}	Sidetall:90 + vedlegg/annet:10 Stavanger 15. mai 2021

Forord

Denne bacheloroppgaven er skrevet ved Institutt for data- og elektroteknologi ved Det teknisk- naturvitenskapelige fakultet Universitetet i Stavanger (UiS) under vårsemesteret 2021. Oppgaven er en del av bachelorprogrammet for Automatisering og elektronikkdesign.

Interesse innen sikkerhetssystemer har vært inspirasjonen til å utføre denne oppgaven og i løpet av vår semesteret har det blitt utviklet et forslag til hvordan en kan lette arbeidet med å opprettholde et sikkert SIS system med fokus på å kategorisere utstyr i grupper, feilregistrering og klassifisering for å ha kontroll over et sikkerhetssystem innen olje- og energibransjen.

Forfatterne av denne oppgaven er Kent-Stian H. Larsen og Karsten Bruun som studerer Bachelor i Automatisering og elektronikkdesign ved Institutt for Data- og Elektroteknikk (IDE), Universitetet i Stavanger. Kent-Stian H. Larsen innehar fagbrev som elektriker og automatiker samt videreutdannelse innen automatisering ved Stavanger offshore tekniske skole. Han startet karrieren med å ta fagbrev som elektriker innen hus, kontorbygg og landbasert industri for så å gå over til offshore bransjen hvor han tok fagbrev som automatiker.Med et Ønske om å videreutvikle seg fullførte han teknisk fagskole for så å begynne ved Universitetet i Stavanger.
Karsten Bruun innehar fagbrev som elektriker. Han utdannet seg som skipselektriker og jobbet på supplybåter i nordsjøen før han tok videreutdannelse innen automasjon på teknisk fagskole for å fordype seg i faget. Deretter fortsatte Karsten på universitetet samtidig som han jobber offshore på borerigg.

Forfatterne av denne rapporten vil rette en takk til Solfrid Håbkrekke ved Sintef og Mary Ann Lundteigen ved NTNU for teknisk veiledning under arbeidet på denne oppgaven.

Stavanger, 15. Mai 2021

Kent-Stian H. Larsen
Karsten Bruun

Sammendrag

Gjennom Petroleumstilsynets forskrifter skal alle innretninger på norsk sokkel ha kontroll over barrierene og sikkerhetsfunksjonene sine. IEC 61508/511 skal da benyttes for utforming av systemene. IEC 61508 er en generisk standard som gjelder flere bransjer, mens IEC 61511 er en prosess sektor standard som er basert på utprøvde eller sertifiserte produkter. NOG 070 er en standard som er utarbeidet av bransjen i samarbeid med aktører innen olje- og energisektoren som er mer rettet for petroleumsinstallasjoner.

Denne bacheloroppgaven tar for seg fasene i livssyklusen til sikkerhetsinstrumenterte systems livssyklus som omhandler drift, vedlikehold og modifikasjon. I denne fasen må en vurdere styring for oppfølging av sikkerhetssystemer. Oppgaven har foreslått et rammeverk for å strukturere utstyr i grupper (utstyrs taksonomier) for å forbedre kvaliteten ved rapportering av feil og slik at en kan slå sammen feilfrekvensene for utstyrsgruppene. Ved å strukturere utstyrsgrupper muliggjør dette at en enkelt kan kvantifisere farlige udekterte feil i et anlegg.
Gjennom å ha utarbeidet et forslag på hvordan en kan utføre pålitelighetsanalyse gjennom SIL-oppfølging av sikkerhetsinstrumenterte system kan en demonstrere at sikkerheten er ivaretatt.

Hovedbidragene i rapporten er:

- Forskjellige metoder for kalkulasjon for å oppdatere funksjonstestintervall av utstyr av en sikkerhet instrumentert funksjon (SIF).
- Forskjellige tilnærminger for estimering av farlige udetekterte feil.
- Bruk av partiell operasjon for å bidra til full operasjon av ventiler gjennom funksjonstest.
- Estimering av PFD ved votering av flere elementer i en SIF
- Forslag til valg av utstyres taksonomier.

Innhold

Tabeller

Figurer

Formler

Forkortelser

BDV	Blowdown valve
CCF	Common cause failure
DD	Dangerous Detected failures
DU	Dangerous Undetected failures
E/E/PE	Elektrisk, Elektronisk eller Programmerbart Elektronisk utstyr (Electrical/Electronic/programmable Electronic)
ESD	Nødavstegningssystem (Emergency Shutdown)
ESV	Emergency Shutdown Valve
EUC	Utstyr under kontroll (Equipment under Control)
FMEA	Failure Mode and Effect Analysis
FST	Full Stroke Test
IEC	International Electrotechnical Commissioning
I/O	Input/output
ISO	International Organization for Standardization
LOPA	Layer Of Protection Analysis
MoC	Management of Change
MooN	M out of N
NOG 070	070 Norwegian oil and gas, Applikasjon av IEC 61508 og IEC 61511 i den norske petroleumsindustrien. (Anbefalte SIL krav)
PFD	Probability of Failure on Demand
PFH	Probability of a dangerous Failure per Hour
PSD	Process Shutdown
PST	Partial Stroke Test
RNNP	Risikonivå i norsk petroleumsvirksomhet
SAS	Safety Automated System

SCE	Safety Critical Element
SCV	Safety Critical Valve
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirement Specification
XSV	Process Shutdown Valve

Definisjoner

Common cause failure (CCF)	Systematiske feil på to eller flere lignende komponenter (f.eks. Samme utstyrstype, sted, samme leverandør osv.) på grunn av samme årsak og innenfor et testintervall. [6]
Degradert feil	Feil eller svikt som ikke setter de grunnleggende funksjonene ut av operativ tilstand. [4]
Equipment under control (EUC)	Utstyr, maskiner, apparater eller anlegg som blir brukt til produksjon og prosess
Generiske data	Data innsamlet av en organisasjon og publisert i håndbøker eksempel PDS håndbok. De innsamlede data kan være for bestemte komponenttyper (ikke spesifikt relatert til merker), og kan være en kombinasjon av driftserfaring, produsentdata som gjelder for en spesifikk bransjesektor eller spesifikke bruksforhold (f.eks. olje- og gassindustri fra land).
Globale sikkerhetsfunksjoner	Funksjoner som vanligvis gir beskyttelse for ett eller flere brannområder. Eksempler er nødstopp, isolasjon av tennskilder og ESD
Ikke kritisk feil	Feil eller svikt i en utstyrsenhet som ikke forårsaker en umiddelbar opphør av evnen til å utføre den nødvendige funksjonen. [4]
Kritisk feil	Feil eller svikt med potensial for å sette det sikkerhetsinstrumenterte systemet i en farlig eller ut av operativ tilstand.[4]
Lokale sikkerhetsfunksjoner	Funksjoner begrenset til beskyttelse av en bestemt prosessutstyrsenhet. Et typisk eksempel er beskyttelse mot høyt nivå i en separator gjennom PSD-systemet
MooN	Leses «M out of N». System bestående av «N» uavhengige kanaler som er koblet på en slik måte at «M» kanaler er tilstrekkelig for å oppfylle sikkerhetsfunksjonen i hvert tilfelle.

PFD	Definert som gjennomsnittlig sannsynlighet for at et sikkerhetssystem ikke er i stand til å utføre sin sikkerhetsfunksjon etter behov.
Proof test	Planlagt operasjon utført med konstant tidsintervall for å oppdage potensielle skjulte feil som kan ha oppstått i mellomtiden. [4]
Repeterende feil	To eller flere DU-feil (systematiske feil) av samme komponent på grunn av samme årsak. [6]
Sikkerhetskritisk system	Et system hvis svikt som kan føre til skade på mennesker, lide store økonomiske tap og/eller miljøskader. [4]
Taksonomi	Systematisk klassifisering av utstyr i generiske grupper basert på faktorer som er mulig felles for flere av elementene. [4]
λ	Sviktintensitet (feil/time)
λ_D	Dangerous failure (farlige feil), λ_D=λ_{DU}+λ_{DD}
λ_{DD}	Dangerous Detected failure (Farlige detekterte feil). Feil som detekteres/oppdages ved automatisk selv test.
λ_{DU}	Dangerous Undetected failure (Farlige udetekterte feil). Feilen som ikke oppdages ved automatisk selvtest.
λ_{SD}	Safe Undetected failure (Sikker detekterte feil). Sikker feil som oppdages ved automatisk selvtest.
λ_{SU}	Safe Detected failure (Sikker detekterte feil). Sikker feil som ikke oppdages ved automatisk selvtest.

Kapittel 1

Introduksjon

1.1 Mål

Oppgaven med å opprettholde den påkrevde ytelsen til et sikkerhetssystem (SIS) kan være vanskelig å følge opp da det ikke foreligger noen spesifikk metode å utføre dette på, og de ulike metodene kan gi usikkerhet ved kvantifisering av systempålitelighet. Da er det viktig å ha en felles struktur for å gruppere likt utstyr, feilregistrering, klassifisering og rapportering av sikkerhetskritisk utstyr.

Denne oppgaven vil gi et detaljert forslag på hvilken metode som kan anvendes ved å forenkle usikkerheten ved rapportering og oppfølging av SIS-systemer ved å:

- Standardisere utstyrsgrupper for:
  - strukturering av feildata; utstyrsgruppene definerer hvilke feil som kan samles og slås sammen for å beregne feilfrekvenser for utstyr.
  - muliggjøre standardiserte (og utstyrsspesifikke) taksonomier og automatisert registrering og klassifisering av svikt i utstyr i en gruppe.
  - muliggjøre effektiv SIL-oppfølging på et SIS-system og på et passende nivå.
- Årlig eller 2 årlig oppfølging av SIF
- Vurdere feil estimat ved rapportering av feil på en type gruppe
- Vurdere påliteligheten av oppdatert feil estimat

- Rapportering av sanntidsrisiko, når feil er for mange på en bestemt gruppe utstyr, f.eks. trykkgiver vil dette være input for optimalisering av vedlikehold.

1.2 Oppgavens struktur

Oppgaven er delt inn i kapitler, der kapittel 2 tar for seg grunnleggende teori for sikkerhetsinstrumenterte systemer. Temaene i kapitel 2 dekker bakgrunn for SIS i olje og energisektoren, livssyklusen til et SIS-system, hvordan sikkerhetsintegriteten til en SIF er definert og en enkel beskrivelse på hvordan en kan sette SIL-nivå på en SIF ved bruk av en kvalitativ metode.
i kapittel 3 er det utarbeidet metoder for å kategorisere dataene på en strukturert måte, beskrevet hvordan dette foregår og definert prosessen med å sikre at kravene til sikkerhetsintegritet er imøtekommet. Videre er det beskrevet hvordan ytelseskravet og oppfølging av SIF blir ivaretatt. I kapittel 4 er resultatene av SIL-oppfølging i operativfasen, mens i kapittel 5 diskuteres påliteligheten av dataene som blir brukt for å opprettholde SIL-integriteten og andre usikkerhetsmomenter ved et SIS-system.

1.3 Avgrensninger

Oppgaven skal ikke ta for seg hele livssyklusen til et SIS-system fra valg av konsept til fjerning/nedstegning av systemet. Hovedfokuset er å se på operasjon, vedlikehold og reparasjonsdelen av livssyklusen til et SIS-system. Evaluering av SIL-nivå, konsept, risikoevaluering og krav til de forskjellige applikasjonene vil ikke bli betraktet i denne oppgaven. Utvikling av prosessystemer, kartlegging av sikkerhetsnivået til et nytt anlegg og utarbeidelse av test prosedyrer vil heller ikke bli vurdert, men en generell beskrivelse av vurderingsprosessen vil bli forklart. SIL-nivå til de forskjellige applikasjonene vil bli fastsatt som NOG 070 har beskrevet.

1.4 Bakgrunn for oppgaven

Bakgrunnen for denne oppgaven er at IEC 61508/511- samt NOG 070-normene blir mer og mer verdsatt hos instrumentingeniører i olje- og gass-industrien i Norge gjennom risikostyring. For å oppnå samsvar med Petroleumstilsynets krav som er basert på IEC-standardene må en inneha kompetansekravene som tilsynet også stiller.

Motivasjonen er å få en praktisk tilnærming til standardene og barrierestyring for å ivareta integriteten til et SIS-system gjennom hele levetiden. Terminologien og metodene kan være en vanskelig og kompleks prosess å håndtere for så å evaluere feilene som kan oppstå i et system. Analyser av SIS-systemer blir som oftest utført manuelt, som igjen forårsaker usikkerhet knyttet til de endelige resultatene. Dersom beslutningstakere ikke er enig om en standardisert metode kan dette lede til at beslutninger for å ivareta nødvendig risikoreduksjon i et system tas på feil grunnlag og kan potensielt føre til en uønsket hendelse. For å opprettholde ytelseskravene til et SIS-system er det viktig å skjønne hva som er barrierebrudd. Denne oppgaven skal undersøke og utarbeide forenklinger slik at usikkerhet i pålitelighets-analysene skal reduseres og opprettholdes gjennom hele livssyklusen.

Kapittel 2

Teori

Kapittelet inneholder det teoretiske fundament som utgjør basisen for å forstå hva et SIS-system er og hvilke krav som må etterfølges. Hensikten er å gi en systematisk oversikt over SIL-konseptet, krav til sikkerhetsfunksjoner med utgangspunkt ifra standarder, usikkerhetsbetrakninger, pålitelighet og anvendte metoder. Kapittelet gir ikke utdypende innsikt i sikkerhetsinstrumenterte systemer.

2.1 Sikkerhetsinstrumenterte systemer (SIS)

2.1.1 Bakgrunn for Sikkerhetsinstrumenterte systemer (SIS)

Gjennom årene har det vært flere store ulykker relatert til svikt i prosessystemer enten gjennom menneskelig svikt (oppfølging av rutiner og prosedyrer) eller automatiserte systemer som har feilet. IEC 61508/511 har utarbeidet et system som kan definere minimum sikkerhetsnivået i prosessystemer. Dette kan være instrumenterte systemer eller administrative systemer, som kan være prosedyrer og rutiner der en beskriver hva en skal foreta seg ved avvik i den normale driften. Her er det tatt for seg de instrumenterte sikkerhetssystemene som automatisk detekterer og håndterer avvikssituasjonen. Noen olje- og gassrelaterte systemer er typisk brann- og gassystemer (B&G), nødavstegningssystemer (ESD) og prosessavstegningssystemer (PSD).

2.1.2 Bakgrunn for sikkerhetsfunksjoner i norsk olje- og gass-industri

Petroleumstilsynet [7] (Ptil) spesifiserer i Innretningsforskriften, §8 Sikkerhetsfunksjoner, krav til sikkerhetsfunksjoner. Det er fastslått at alle sikkerhetsfunksjoner skal ha ytelseskrav. Retningslinjen til §8 spesifiserer at utforming og ytelse av aktive sikkerhetsfunksjoner skal være basert på IEC 61508 og NOG 070 (NOG 070 er en applikasjon av IEC 61508 og IEC 61511). For utforming av sikkerhetsfunksjoner i tillegg til IEC 61508 og NOG 070, henvises det til ISO 13702, ISO 13849 og NORSOK S-001. Disse kravene er også spesifisert i retningslinjen for Styringsforskriften §5 Barrierer.

I veiledning til styringsforskriftens §5 beskrives barriere som tekniske, operasjonelle og organisatoriske elementer på innretning eller landanlegg som enkeltvis eller samlet skal redusere muligheten for at konkrete feil, farer og ulykkessituasjoner inntreffer, eller som begrenser eller forhindrer skader/ulemper. [7]

2.1.3 Risikonivå norsk petroleumsvirksomhet - RNNP

I Styringsforskriften §5 Barrierer som er nevnt skal selskapene som opererer på norsk sokkel ha etablert barrierer og ha kontroll over de barrierene som er etablert. I den forbindelsen har petroleumstilsynet opprettet RNNP-rapportering for å måle utviklingen i petroleumsvirksomheten på norsk sokkel. Formålet er å foreta en vurdering av både status og trender, for å overvåke og derfor unngå storulykkerisiko innen petroliumsvirksomheten. Dette innebærer at alle selskaper som opererer på norsk sokkel må rapportere inn testdata og feilrate på blant annet sikkerhetskritiske instrumenter som brann- og gassdetektorer, ESV-ventiler osv. Innrapporteringen er ikke begrenset til utstyr, men til den helhetlige sikkerheten til innretningen. I figur 2.1 kan en se et lite utdrag fra hva som skal rapporteres. Denne rapporten vil ikke gå mer inn i hva som rapporteres til petroleumstilsynet, men det er tatt med for å beskrive at feilratene som blir rapportert ved RNNP er funnet under funksjonstesting av utstyr og vil ikke bli rett feilrate for vurdering av et SIS-system da DU-feil også kan oppdages under drift.

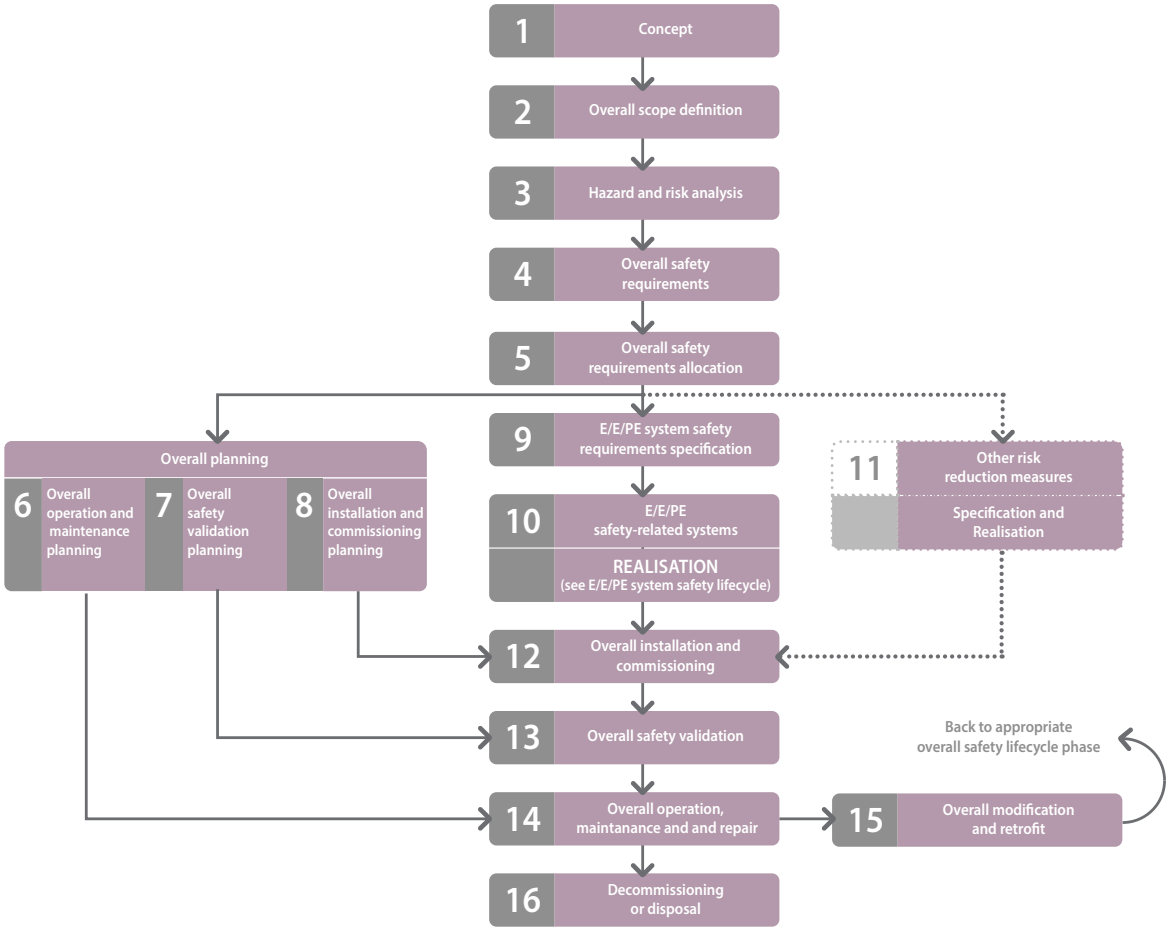
Navn på innretning:		
Data fra periode:		
Barrierer/Barriere-elementer	**Antall tester**	**Antall feil i hht definisjon**
Branndeteksjon, tilgjengelighet		
Gassdeteksjon, tilgjengelighet		
Nedstengning, tilgjengelighet • Stigerørs-ESDV		
Lukketest		
Lekkasjetest		
• Ving og master vent. (juletre)		
Lukketest		
Lekkasjetest		
• DHSV		
Trykkavlastningsventil, BDV		
Sikkerhetsventil, PSV		
Aktiv brannsikring		
Delugeventil		
Starttest		
Beredskap		
	Ant mønstr. øvelser	Gjennomsnittlig møstringstid
• Mønstringstid, øvelser		
	VSKTB krav (minutter)	Antall tester som har møtt VSKTB krav
• Forhold til VSKTB-krav		
	Antall personer	Kommentar
• Antall personer		Gjennomsnitt/ konstant

Figur 2.1: Utdrag fra RNNP skjema [8]

2.2 Livssyklusen for SIS

IEC 61508 har utviklet en ingeniørprosess for å styre designet og driften av sikkerhetskritiske systemer (SIS-systemer). Livssyklusen skisserer en sekvensiell vei fra utvikling av konseptet/designet av et nytt system til det er installert og til slutt fjernet. Denne modellen består av 16 faser som er illustrert i figur 2.2.

Figur 2.2: Livssyklus modellen til et SIS-System (IEC 61508-1) [3]



Disse 16 fasene kan deles opp i 3 forskjellige grupper:

- Pre-design (Fase 1 til 5 + 9)
- Design og installasjon (fase 6 til 8 og 10 til 13)
- Drift og modifikasjon (fase 14 til 16)

2.2.1 Pre-design

I de fem første fasene utfører man studier og analyser av prosessystemene og definerer sikkerhetskravene som er nødvendig for å ha et sikkert system. Dette blir ofte dokumentert i en kvantitativ risikovurdering (QRA) rapport for anlegget. Risikovurderingene identifiserer nødvendige sikkerhetsfunksjoner for å håndtere og kontrollere risikoen forbundet med utstyr under kontroll (EUC). Disse analysene brukes vider for å etablere «Safety Requirement Spesification» (SRS) i fase 9. Som en kan se i listen under overlapper fase 3 litt under pre-design gruppen.

- Fase 1:

  Konseptet utarbeides

- Fase 2 og 3:

  Definere omfanget av prosessen og identifisering av risiko. Her utarbeider man risiko rapport og riskreduksjonstrategi.

- Fase 3 til 5 + 9:

  Valg av SIL-nivå og utarbeidelse av «Safety Requirement Spesification» (SRS).

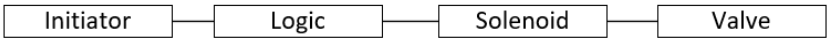
Figur 2.3: Pre-design fasen

Safety Requirement Spesification (SRS)

SRS er hoveddokumentet angående SIS-sikkerhetsrelaterte krav og spesifikasjoner og har en egen fase i livssyklusen, fase 9. Dette er et viktig dokument som realiserer sikkerhetsfunksjonene (SIF) til hver enkelt SIS. Dokumentet skal være strukturert på en måte slik at innholdet er tydelig, presist, verifiserbart og gjennomførbart. Det er ikke noen klar mal på hvordan dokumentet skal se ut, men det skal angi hva SIS er pålagt å gjøre og kravene til sikkerhetsintegritet med angivelse av hvor godt SIS krever å utføre sikkerhetsfunksjonene. IEC 61511-1 seksjon 10 gir en mer detaljert beskrivelse på hva som skal dokumenteres. I figur 2.1 illustreres et eksempel på hvordan en SIF-funksjon fra et SRS-dokument kan se ut.

Eksempelet i tabell 2.1 er lagd for å overvåke trykk/nivå i en tank. Hvis trykket/nivået i tanken blir for høyt skal ventilen stenge slik at det ikke kommer mer væske inn i tanken. SIF-funksjonen har fått et SIL 2 nivå. Initiator består av en trykktransmitter (PST) i system 10 og har løpenummer 1001. Sluttelementet er en XSV-ventil (sikkerhetsventil) som også er i system 10 med løpenummer 1001. Denne skal stenges for unngå at mer væske skal komme inn i tanken. Logikken har en PSD-funksjon (Production shutdown) som vil si at det er produksjon nedstenging. Dette kalles en «lokal» funksjonstype.

Tabell 2.1: Eksempel på hvordan en SIF funksjon kan se ut i SRS

SIL - Safety Requirement Spesification				
Topic	Requirement / Description			
Function Type	Local			
Definition of SIF	SIF 001 To prevent overpressure in tank 			
Relevant SIF ID	10-PST-1001 P&ID doc. P-XB-0100-05			
Definition of SIF Boundary	Initiator: 10-PST-1001 Logic: PSD Primary Final Element: close 10-XSV-1001			
Equipment Under Control (EUC)	Inert Gas Generator package			
Safe State	Fail Safe State for initiator is HH Inert gas valve to tank closed			
Mode of Operation	Low demand mode of operation			
Dangerous Undetected Failures	1. Transmitter fails to signal high pressure on demand 2. Logic Solver fails to initiate valve closure 3. Valve actuator fails to operate on demand 4. Valve fails to shut on demand			
Other Failures	All other failures are dangerous detected failures or safe failures			
Desired Response upon failure	Valve is closed on loss of service and generate alarm			
SIL Requirement	SIL 2			
MTTR		Initiator	logic	Final element
	MTTR (hour)	8	8	24
«Demand Rate»	low			
Trip point	1,5 barg (HH)			
De/Energise to Trip	De-energize to close the isolation valve			
Test interval		Initiator	Logic	Final element
Full Proof Test		12 months	36 months	6 months
Partial Stroke Test		-	-	3 months
Maximum Response Time	24sec			
Other Performance Requirements				
Assumptions				

Forklaring til SIF-funksjonen:

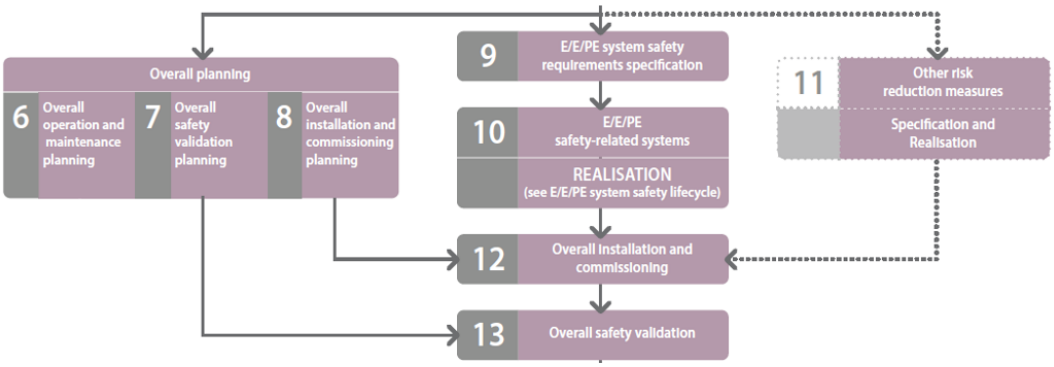
- **Function type** - Dette er en lokal SIF-funksjon som vil si at den fungerer ved nedstenging av produksjonen eller systemet den er knyttet til. Global funksjonstype gir beskyttelse for ett eller flere brannområder. Eksempler er nødstopp, isolasjon av tennkilder og ESD.
- **Definition of SIF** - Dette er SIF-nummer 001 for denne innretningen og skal unngå å få for høyt trukk/nivå i tank. Den består av en trykktransmitter (initiator), Logikk (PLS) og en ventil som blir styrt av en solonoid.
- **Definition of SIF boundary** - Dette er hvilken transmitter, logikk og ventil som inngår i denne SIF-funksjonen. Logikk er PLS som blir brukt til PSD.
- **Equipment under control (EUC)** - Dette er hvilken pakke eller system som denne SIF-funksjonen tilhører.
- **Safe State** - Dette er beskrivelsen på hva som er sikker tilstand til denne SIF-funksjonen.
- **Mode of Operation** - Dette gir en indikasjon på hvor ofte denne funksjonen skjer eller hvor ofte en kan beregne at denne hendelsen skal skje i forhold til testintervallet.
- **Dangerous Undetected Failures** - Dette er beskrivelsen på hva DU-feil vil være til denne SIF-funksjonen.
- **Other Failures** - Dette er beskrivelsen på hva andre feil vil være til denne SIF-funksjonen. Ergo her vil alle andre feil være DD-feil eller SD-feil.
- **Desired Response upon failure** - Dette sier hva som skal skje hvis en mister strøm eller actuator kontrollen.
- **SIL Requirement** - Beskriver SIL-nivået til funksjonen. Her er det SIL 2 nivå.
- **MTTR** - Mean time to repair (MTTR). Det representerer gjennomsnittlig tid som kreves for å reparere en komponent eller enhet som sviktet.
- **Demand Rate** - Hvor ofte hendelsen skjer.

- **Trip point** - Grense for at SIF-funksjonen skal utføre sin handling
- **De/Energise to Trip** - Hva som skal skje hvis en mister strømmen.
- **Test interval** - Dette er en beskrivelse på hva som skal testes og innenfor hvilket testintervall.
- **Maximum Response Time** - Max tid som kan gå fra en initierer feil deteksjonen og til ventilen skal gi tilbakemelding at den er stengt.
- **Other Performance Requirements** - Her kan en beskrive andre hensyn som gjelder ved denne SIF-funksjonen.
- **Assumptions** - Her kan en beskrive antagelser som er tatt for denne SIF-funksjonen.

2.2.2 Design og installasjon

I fase 6 til 8 og fase 10 til 13 er hvor en realiserer SIS basert på design spesifikasjonene. Parallelt med realiseringen utføres en overordnet planleggingsfase som går over i en installasjon og verifikasjonsfase. I den overordnede planleggingen utføres blant annet pålitelighetskalkulasjoner av sikkerhetsfunksjoner for å evaluere om kravene i SRS ivaretas. Som det blir nevnt i kapitel 2.3.3 anbefaler NOG 070 at generiske data blir benyttet for å fastsette SIL-nivået, men hvor dette ikke eksisterer må en utføre pålitelighetsvurderinger med tilgjengelig data for teknologien som blir benyttet.

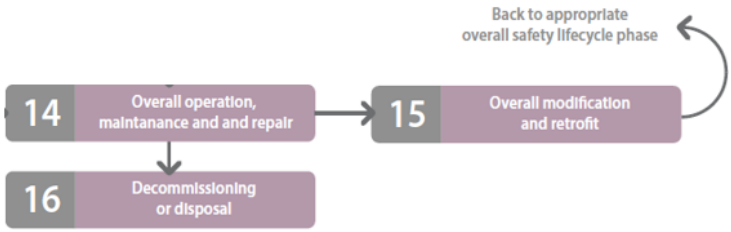
Figur 2.4: Design og installasjon fasen



2.2.3 Drift og modifikasjon

I de siste 3 fasene (fase 14 til 16) er drift, modifikasjon og decommissioning. Drift og modifikasjon er hvor en følger opp SIS-systemene slik at SIL-kravene er ivaretatt og hvis SIF-funksjonen ikke imøtekommer kravene som er satt eller at en gjør forandringer i prosessen må en utføre nye analyser. Det er fase 14 og 15 denne rapporten skal gå litt dypere inn i og anbefale en måte på hvordan en kan følge opp et SIS-system og gi input på forbedringer.

Figur 2.5: Drift og modifikasjon fasen



2.3 Sikkerhetsintegritet for en SIF

Sikkerheten som håndteres gjennom standardene IEC 61508/511 er for å minimalisere risikoen til mennesker, store økonomiske tap og/eller miljøskader. Denne funksjonen utføres ved å redusere potensiell fare i anlegg som er sikret med elektrisk, elektronisk eller programmerbart elektronisk utstyr (E/E/PE) i kombinasjon med flere andre aktive teknologier. Disse standardene har adoptert begrepet «Sikkerhetsinstrumenterte systemer (SIS)» fra prosessindustrien, hvor dette har blitt brukt i mange år. Hensikten er å utarbeide sikkerhetsinstrumenterte funksjoner (SIF). Sikkerhetsfunksjonen (SIF) som skal implementeres i et system er ment å oppnå eller opprettholde en sikker tilstand for utstyret under kontroll (EUC), med hensyn til en spesifikk farlig hendelse. Et SIS-system kan inneholde flere SIF-funksjoner. Ved gjennomføring av en risikoanalyse/vurdering identifiseres det hvilke SIL-nivå (hvis risikoen er høy nok) funksjonen skal ha. Eksempel på bruk av risk graf metoden for implementering av SIL-Nivå kan en se i kapittel 2.3.4. En SIF-funksjon deles inn i 3 delsystemer som er initiatorer, logiske

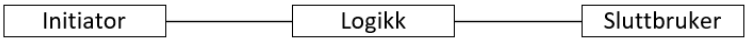
enheter og sluttelement (Se figur i tabell 2.1 under «Definition of SIF» og figur 2.6) for å utføre en sikkerhetsinstrumentert funksjon og for å forhindre at en uønsket hendelse utvikler seg. Første del er initiator som er inngangselementene, og disse brukes til å «oppdage» en farlig hendelse. Andre del av systemet er logikk som skal bestemme hva som skal utføres og siste del er den utførende delen som skal utføres i henhold til hva logikken har «bestemt». Det kan være flere initiatorer og sluttelementer i en SIF-funksjon. Sluttelement er også beskrevet som sluttbruker i denne oppgaven. Som illustrert i figur i tabell 2.1 under «Definition of SIF» er det typisk å bruke en transmitter som måler et på et prosess medium eller en detektor i et brann- og gassystem. Logikk er ofte en PLS som er implementert til å styre hele SIS-systemet, mens sluttelementene kan være ventiler, sikringer, rele'er o.l. Denne beskrivelsen er ikke begrenset til denne typen utstyr, men er bare gitt som et eksempel.

Et eksempel på en fiktiv SIF-funksjon kan en se i tabell 2.1 med tilhørende forklaring av SIF-funksjonen.

2.3.1 SIL

Sikkerhetsintegritetsnivå (SIL) er et diskret ytelseskrav/nivå (ett av fire mulige, se tabell 2.2) for å spesifisere integritetskravet til sikkerhetsfunksjonene som skal tildeles et SIS-system. Disse sorteres fra SIL 1 til SIL 4 hvor SIL 1 er minst og SIL 4 er det mest pålitelige nivået. Det må defineres et SIL-nivå for hver SIF-funksjon et anlegg har, slik at den nødvendige risikoreduksjonen oppnås. SIL-nivået er et mål på ytelsen (se tabell 2.2) som kreves av et sikkerhetsinstrumentert system for å opprettholde eller oppnå sikkerhetstilstanden. Dette sparer selskapet/ledelsen frar å måtte tolke de tekniske aspektene ved SIL, men samtidig som de skjønner hva sikkerhetsnivået til en SIF-funksjon skal være. Dette SIL-kravet gir begrensninger for valg av utstyr, programvare og tilhørende arbeidsprosesser og prosedyrer. Hvis en funksjon er definert i flere forskjellige SIF-funksjoner er det strengeste SIL-nivået som skal sette kravet for alle komponenter. For å oppfylle et SIL-krav er det nødvendig at alle deler oppnår spesifisert SIL-nivå. Eksempel er figur 2.6 der en må oppnå spesifisert SIL-nivå på alle leddene.

Figur 2.6: Illustrasjon på en enkel SIF



Som en kan se i tabell 2.2 og tabell 2.3 bruker IEC 61508-1:2010 sannsynligheten for feil på forespørsel (demand), «Probability of a dangerous Failure on Demand (PFD)» og sannsynligheten for farlig feil per time, «Probability of a dangerous Failure per Hour PFH)». Det er definert et pålitelighetsnivå (PFD og PFH) som er spesifisert for hvert SIL-nivå. Slik en ser i tabell 2.2 så må SIL 2 nivå ha sjeldnere svikt enn 1 gang per 100 operasjoner. Eller sagt på en annen måte at SIL-funksjonen må fungere i 99 av 100 operasjoner.

Tabell 2.2: Sikkerhetsnivåer for sikkerhetsfunksjoner som opererer i driftmodus «low demand mode of operation» (PFD) (IEC 61508-1:2010) [3]

SIL - Safety Integrity Level		
SIL-nivå	PFD	Svikt sjeldnere enn
1	$10^{-2} \leq$q PFD $< 10^{-1}$	1/10
2	$10^{-3} \leq$ PFD $< 10^{-2}$	1/100
3	$10^{-4} \leq$ PFD $< 10^{-3}$	1/1000
4	$10^{-5} \leq$ PFD $< 10^{-4}$	1/10 000

Tabell 2.3: Sikkerhetsnivåer for sikkerhetsfunksjoner som opererer i driftmodus med «continuous/high demand mode of operation» (PFH) (IEC 61508-1:2010) [3]

SIL - Safety Integrity Level	
SIL-nivå	PFH
1	$10^{-6} \leq$ PFH $< 10^{-5}$
2	$10^{-7} \leq$ PFH $< 10^{-6}$
3	$10^{-8} \leq$ PFH $< 10^{-7}$
4	$10^{-9} \leq$ PFH $< 10^{-8}$

Probability of failure on demand (PFD)

PFD er definert som gjennomsnittlig sannsynlighet for at et sikkerhetssystem ikke er i stand til å utføre sin sikkerhetsfunksjon etter behov [2] og kan skrives matematisk ved formel 2.1 for en enkelt komponent (1oo1). PFD brukes hvor SIS opererer med driftsmodus «on demand». PFD kvantifiserer svikt i sikkerheten på grunn av farlige udekterte feil (λ_{DU}).

$$PFD = \lambda_{DU} \times \frac{\tau}{2} \tag{2.1}$$

- $\frac{\tau}{2}$ - Gjennomsnittlig periode i tid når komponenten ikke er tilgjengelig gitt at feilen kan oppstå på et tilfeldig tidspunkt.
- λ_{DU} - konstant feilrate (feil/timer)

For nye systemer som blir tatt i bruk vil PFD-data (pålitelighetsdata) bli oppgitt av utstyrsleverandøren, men man kan eventuelt også bruke generiske datasett.. Et eksempel på dette kan en finne i tabell 5.1 i Appendiks A som også er brukt i denne rapporten. Senere kan PFD-estimatene forandre seg med hensyn til feilrate (λ_{DU}) hos selskapet eller systemet som er i bruk. λ_{DU} forteller frekvensen av farlige udetekterte feil, dvs. feil som ikke blir oppdaget ved automatisk selvtest, men blir oppdaget ved funksjonstest, operasjon av utstyret eller tilfeldig observasjon. I denne perioden er det ukjent om funksjonen til komponenten/systemet er tilgjengelig eller ikke. De farlige udetekterte feilene bidrar til PFD for komponenten/systemet.

Merk at PFD (probability of failure on demand over a period of time) faktisk er gjennomsnittlig sannsynlighet for svikt PFD_{avg} som er angitt i IEC 61508. På grunn av enkelhet betegnes PFD_{avg} som PFD i denne rapporten.

Formler for uavhengige feil og «Commen Cause Failures» (CCF)

Når en skal kvantifisere PFD for sikkerhetssystemer hvor en har redundans må en skille mellom uavhengige feil og avhengige feil (CCF). CFF er feil på to eller flere komponenter som er avhengig av hverandre eller der feil årsak representerer hendelser der flere feil oppstår på kort tid, på grunn av samme årsak.

I tabell 2.7 er det oppsummert forskjellige voteringsformler for PFD. Den første kolonnen oppgir votering. Andre kolonne inkluderer PFD-bidraget fra CCF. Tredje kolonne er PFD-bidraget fra uavhengige feil. Formlene som er oppgitt i tabell 2.7 antar at funksjonstest er utført innen testintervallet og alle feil blir funnet.

Figur 2.7: Forenklede formler for beregning av PFD (NOG 070)[2]

Voting	PFD calculation formulas		
	Common cause contribution		Contribution from independent failures
1oo1	-		$\lambda_{DU} \cdot \tau /2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^2/3$
2oo2	-		$2 \cdot \lambda_{DU} \cdot \tau /2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^3/4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^2$
3oo3	-		$3 \cdot \lambda_{DU} \cdot \tau /2$
1ooN; N = 2, 3,…	$C_{1ooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$\frac{1}{N+1} \cdot (\lambda_{DU} \cdot \tau)^N$
MooN, M<N; N = 2, 3,..	$C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$\frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU} \cdot \tau)^{N-M+1}$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU} \cdot \tau /2$

τ- tid mellom funksjonsprøving i timer (1 år = 8760 timer)
λ_{DU} - farlige udetekterte feil (feil/timer)
β - Komponentspesifikk parameter

C_{MooN} formler i figur 2.7 er fra NOG 070 [2] og er vist i tabell 2.5. En mer detaljert tabell av MooN formel er demonstrert i appendiks B. En forenklet referanse til tabell 5.2 i appendiks B er gjengitt i tabell 2.4 og tabell 2.5.

Tabell 2.4: Utvalgte numeriske verdier for modifikasjonsfaktoren ved MooN votering

Nummeriske verdier for C_{MooN} parametre							
Votering	1oo2	1oo3	1oo4	1oo5	2oo3	2oo4	2oo5
C_{MooN}	1.0	0.5	0.3	0.2	2.0	1.1	0.8

Tabell 2.5: C_{MooN} for forskjellige voteringsparametre (NOG 070)[2]

MooN parametre					
N / M	M=1	M=2	M=3	M=4	M=5
N=2	1.0	-	-	-	-
N=3	0.5	2.0	-	-	-
N=4	0.3	1.1	2.8	-	-
N=5	0.2	0.8	1.6	3.6	-
N=6	0.15	0.6	1.2	1.9	4.5

Sikkerhetsintegritet

Sikkerhetsintegritet er delt inn i tre deler: maskinvaresikkerhetsintegritet, programvare sikkerhetsintegritet og systematisk sikkerhetsintegritet. Det er to grunnleggende elementer knyttet til dette for å kunne oppfylle SIL-kravet:

- Maskinvaresikkerhetsintegritet
- Systematisk sikkerhetsintegritet

Maskinvaresikkerhetsintegritet som vanligvis er basert på tilfeldige maskinvarefeil. Dette kan normalt estimeres til et rimelig nøyaktighetsnivå via «probability of failure on demand» (PFD). Systematisk sikkerhetsintegritet har en tendens til å være vanskeligere å tallfeste. Dette skyldes mangfoldet

av årsaker til feil. Systematiske feil kan forekomme i design, implementering, operasjon og modifisering, og kan påvirke maskinvare så vel som programvare. IEC 61508 klassifiserer disse feilene med bakgrunn til årsak, effekt og påvisbarhet (detektering) som er forklart under.

- Tilfeldige «hardware» feil.

  Dette er fysiske feil som oppstår på et tilfeldig tidspunkt ved komponenter som kan være aldring, stress, ytre påkjenning og lignende.

- Systematiske feil.

  Dette er ikke fysiske feil som er relatert til bestemte årsaker som designfeil eller menneskelige feil. Disse feilene kan bare elimineres ved en modifisering av design eller produksjonsprosessen, operasjonelle prosedyrer, dokumentasjon eller andre relevante faktorer.

2.3.2 Feilklassifisering

Vi har 4 obligatoriske feilklassifiseringer som blir dekket av de beskrivelsene over. Etter å ha vurdert feil må disse kodene settes manuelt slik at en ikke bruker alle farlige feil med i kalkulasjonene for SIF data. Da vil en få feil på oppdaterte pålitelighetsdata fra anlegget. Disse er utstyrsuavhengige feilklassifiseringer, men viktig å forstå ved å definere feil modus. Se figur 3.1

- **DU-feil** (λ_{DU}) - Dangerous Undetected (farlig udetektert feil)

  DU-feil er den feilen som ikke oppdages ved automatisk selvtest. Et eksempel på dette kan være at man ikke får noen melding om at en trykkgiver har fryst og ikke gir noen forandring av signal ved forandring i prossesen.

- **DD-feil** (λ_{DD}) - Dangerous Detected (farlig detektert feil)

  DD-feil den feilen som oppdages ved automatisk selvtest. Eksempel er når en detektor gir melding til kontrollsystemet om at den er gått i feil.

- **SD-feil** (λ_{SD}) - Safe Detected (sikker detektert feil)

  SD-feil er sikre feil som oppdages ved automatisk selvtest. Eksempel er når en giver gir melding til kontrollsystemet om at den er gått i feil og opererer prosessen i en sikker tilstand.

- **SU-feil** (λ_{SU}) - Safe Undetected (sikker udetektert feil)

  SU-feil sikre feil som ikke oppdages ved automatisk selvtest. Eksempel feil som ikke påvirker sikkerheten til prosessen hvis instrumentet går i feil.

Disse feilene brukes til kvantitative analyser for feilfrekvenser. Feilene deles inn i følgende elementer ref tabell 2.6:

Tabell 2.6: Beskrivelse av feilfrekvensene

feilrate	type feil
λ_S	Safe failure (λ_{SU} + λ_{SD})
λ_{SD}	Safe Detected failure
λ_{SU}	Safe Undetected failure
λ_D	Dangerous failure (λ_{DU} + λ_{DD})
λ_{DD}	Dangerous Detected failure
λ_{DU}	Dangerous Undetected failure

2.3.3 Valg av SIL-klassifisering og dokumentering

For å velge SIL-nivå på applikasjoner er NOG 070 [2] ofte brukt. Denne retningslinjen er utarbeidet for industrier slik at en har en forenklet og standardisert metode for å sette minimum SIL-nivå. Standarden er utarbeidet gjennom et samarbeid mellom operatører, ingeniør- , konsulent- og leverandørselskaper for norsk sokkel. Kravene i NOG 070 [2] er utarbeidet gjennom risikobasert tilnærming. Funksjoner som varierer fra hva som er beskrevet i NOG 070 må behandles etter IEC 61511 metodikken for sikkerhetsintegritetsnivå og bør baseres på en kvalitativ eller kvantitativ risikobasert metode ifølge IEC 61511.

2.3.4 Eksempel på Risk graf metoden (kvalitativ metode)

IEC 61511-3 beskriver forskjellige metoder for å bestemme SIL-nivået til en prosess. Risk graf metoden og LOPA (Layer Of Protection Analysis) er de mest brukte metodene for å bestemme SIL-nivå for et prosessystem. IEC 61511-3 Vedlegg D er en risikobasert tilnærming ved bruk av risk graf som er tilpasset behovene i prosessindustrien. Dette er en mye brukt metode for å bestemme sikkerhetsintegritetsnivået (SIL) for sikkerhetsinstrumenterte funksjoner (SIF). Rapporten vil bare gi en enkel forklaring av risk graf metoden slik at leser får litt bedre forståelse for hvordan en kommer fram til et bestemt SIL-nivå.

Det er 4 parametere som en må ta hensyn til ved bruk av denne metoden som en kan se i figur 2.8. En kort definisjon på disse 4 parametrene er listet under, men i tabell 2.7 til tabell 2.10 er disse parametrene forklart bedre. Parameterne F, P og W bør evalueres uavhengig av hverandre og en må være konservativ ved antagelsene slik at en sikrer rett SIL-nivå blir angitt for SIF.

- C - Konsekvensen av den farlige hendelsen
- F - Tilstedeværelse av personell (sannsynligheten for at det eksponerte området er okkupert)
- P - Sannsynligheten for å unngå den farlige situasjonen
- W - Etterspørsel («Demand») Antall ganger per år som den farlige situasjonen ville oppstå i fravær av at SIF ble vurdert

C-Parameter

Konsekvensparameteren (C) ser på risikoen for personell og da potensiell alvorlig skade og/eller omkomne ved en farlig hendelse i området. Dette er en estimert konsekvens ved en farlig hendelse.

Tabell 2.7: Beskrivelse på konsekvens parameter (C)

Beskrivelse på C-Parameter	
C-Parameter	beskrivelse
C_0	Ingen risk for personell
C_A	Mindre skade
C_B	Liten fare for brannfarlig / giftig utslipp Moderat skade Område av C (= NxV): 0,01 til 0,1
C_C	Moderat til stor fare for brannfarlig / giftig utslipp Alvorlig eller permanent skade. Potensial for enkelt dødsfall Område av C (= NxV): 0,1 til 1,0
C_D	Katastrofal fare for brannfarlig / giftig frigjøring Flere dødsfall Område av C $>$ 1,0

F-Parameter

Tilstedeværelse parameter (F) ser på sannsynligheten for at det eksponerte området er bemannet ved tidspunktet for den potensielle farlige hendelsen.

Tabell 2.8: Beskrivelse av tilstedeværelse parameter (F)

Beskrivelse på F-Parameter	
F-Parameter	beskrivelse
F_A	Sjelden til hyppigere tilstedeværelse av personell. Tilstedeværelse mindre enn 0,1. ($<$ 10% av tiden.)
F_B	Hyppig til permanent tilstedværelse av personell

P-Parameter

Unngåelsesparameter (P) ser på sannsynligheten for at personell kan unngå den farlige hendelsen som måtte oppstå selv om sikkerhetsfunksjonen skulle svikte.

Tabell 2.9: Beskrivelse av sannsynlighetsparameter (P)

	P_A bør bare velges hvis følgende stemmer
Advarsel	Innretningen kan varsle operatøren om at SIS har sviktet
Barrierer	Uavhengige barrierer er gitt for å stenge ned slik at faren kan unngås eller gjør det mulig for alle personer å evakuere til et trygt område
Tid	Tiden til operatøren blir varslet og en farlig hendelse har oppstått overstiger 1 time før en setter igang aksjon

W-Parameter

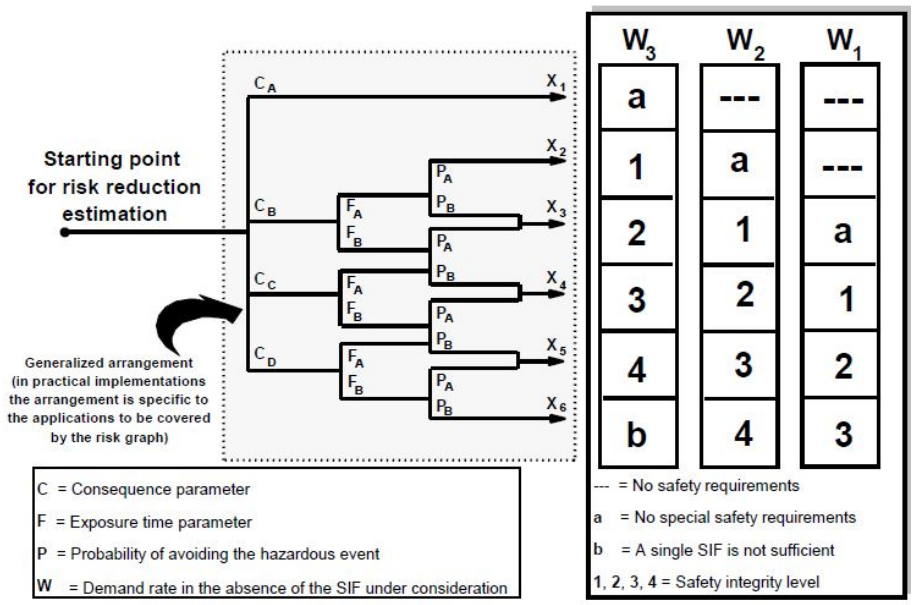
«Demand» parameteren (W) ser på hvor ofte (antall ganger per år) den farlige hendelsen kan oppstå ved svikt av SIF-funksjonen. SIL-nivå fra andre krediterte beskyttelsestiltak skal også vurderes her.

Tabell 2.10: «Demand» parameter (W)

Beskrivelse på W-Parameter	
W-Parameter	beskrivelse
W_0	«Demand» rate mindre enn 0,01 (D) per år
W_1	«Demand» rate mellom 0,01 og 0,1 (D) per år
W_2	«Demand» rate mellom 0,1 og 1 (D) per år
W_3	«Demand» rate mellom 1 og 10 (D) per år

Risk graf

Ved å vurdere de forskjellige parameterne over (tabell 2.7 til tabell 2.10) kan en følge stien som er vist i figur 2.8 for å anslå et eventuelt SIL-nivå. Under risk graf figuren er det utarbeidet et forenklet eksempel på bruk av denne metoden.



Figur 2.8: Risk graf (IEC 61511-3:2016) [1]

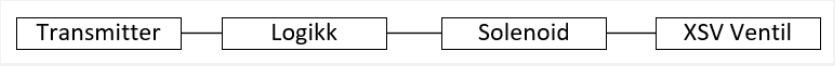
Eksempel på Risk graf metoden

I eksempelet som følger er det brukt en trykktransmitter for å overvåke piggesluse for tilbakeslag av trykk fra stigerør under «pigging» operasjon. Trykktransmitteren (16-PST-1001) skal videre stenge ventil (16-XSV-1001) ved for høyt trykk (PSHH). Trykkgrensen vil bli oppgitt i SRS som vil være det styrende dokumentet for aktiveringer/tripp som ikke blir behandlet her. Dette eksempelet er veldig forenklet og er bare vist for å gi en lett forståelse på hvordan en kan bestemme SIL-nivået til en funksjon ved bruk av risk graf metoden. Det er ikke tatt hensyn til alle funksjoner, farer og konsekvenser i prosessen da dette eksempelet er isolert til bare å gi en forståelse på hvordan en kan sette SIL-nivå ved bruk av risk graf metoden. Når SIL-nivået er satt kan en velge ut utstyr som skal styre prosessen. Det er her en vurderer og kalkulerer PFD-parameterne.

Generell info:

- Tag: 16-PST-1001
- Initiator (funksjon): 16-PSHH-1001

  (Pressure safety transmitter aktiverer ventil ved «high high» alarm.)
- Votering: 1oo1
- Logikk: PSD
- Sluttelement:16-XSV-1001
- Votering: 1oo1



Figur 2.9: Illustrasjon på SIF funksjonen

Tabell 2.11: Integritets nivå identifikasjon

Risk graf metoden																
Beskyttelses funksjon	Hendelse som kan føre til fare	Funksjonskrav som er nødvendig for å forhindre fare	Konsekvens	Andre beskyttende tiltak	IL nivå kreditert fra andre beskyttende tiltak	Risk graf kommentarer	1. Sikkerhet					2. Miljø				IL nivå basert på risk graf
							C	F	P	W	SIL	E	P	W	EIL	
Isolere høytrykkskilde i tilfelle tilbakeslag fra stigerør	Pigging pumpe tripper mens pigging er i drift og stigerøret er under høyt trykk.	Isoler pigginglinjen ved høyt trykk ved "Heater"	1.Sikkerhet: Brudd på linjen, etterfulgt av hydrokarbonutslipp. Brann/ eksplosjon.				C_B	F_B	P_B	W_2	IL2					2
			2. Miljø: lekkasje på plattformen som overskrider dreneringskapasiteten.									C_B	P_B	W_2	IL2	

Tabell 2.12: Funksjonsliste

Funksjonsliste										
Beskrivelse	Initiator	Logikk	Sluttelement	IL basert på risk graf	NOG 070 krav	Total IL	P&ID	EUC	Andre like funksjoner	Kommentar
pig sluse	16-PSHH-1001	PSD	16-XSV-1001	IL2	IL2	IL2	P-XB-0100-05	pig sluse		
	1oo1									

Resultat ved anvendelse av «Risk graf metoden»

Dette er basisen for bruk av risk graf metoden hvor en dokumenter beskyttelsesfunksjon, potensiell hendelse, funksjonskrav, konsekvens og tar anvendelse av eventuelle andre krediterte IL-nivå som beskyttende tiltak. Videre så er selve risk grafen vurdert hvor en i dette tilfellet ender med en SIL 2 funksjon. Se tabell 2.11. Videre er det utarbeidet en funksjonsliste/tabell (tabell 2.12) som beskriver funksjonen til SIF og hvor en har sammenlignet SIF-funksjonen med NOG 070 sine lignende krav. Resultatet av denne analysen vil videre bli dokumentert i SRS-dokumentet som er det styrende dokumentet for SIF-funksjonen.

Dette eksempelet er for å gi et forenklet eksempel ved anvendelse av Risk graf metoden, og eksempelet er ikke beregnet for bruk i et virkelig SIS-system da en kan ha andre kriterier for vurderingen.

Kapittel 3

Metode

For å opprettholde den påkrevde ytelsen til et sikkerhetssystem må det regelmessig utføres en SIL-verifikasjon av SRS. Hvor ofte denne verifikasjonen utføres er ikke fastsatt, men bør utføres regelmessig. Ofte skjer dette hvert år eller annet hvert år. For å lette arbeidet med å utføre denne SIL-verifikasjonen bør det utarbeides et system slik at alle involverte parter har samme forståelse for kritikaliteten til feil som blir rapportert inn i selskapenes systemer. Dette kapittelet inneholder en metode som er utarbeidet for å kunne forbedre kvaliteten på rapporteringen og lette arbeidet med å gjennomføre SIL-verifikasjon. Metoden beskriver fremgangsmåten for innsamling, kategorisering og analyse av data for å kunne besvare oppgavens problemstilling. Valget av denne tilnærmingen er basert på like feil som kan oppstå i forskjellige typer instrumenter. En mer detaljert beskrivelse følger i delkapitlene.

3.1 Datainnsamling

Det finnes en rekke metoder for å samle inn og registrere data for et instrumentert system. Mange selskaper bruker SAP, ofte kan disse datasamlingene overføres til programmer som brukes for behandling av data, som f.eks. Excel. Gjennom en dialog med Vår Energi fikk vi låne registrerte data på feil som kunne bearbeides i vår metode for å kategorisere utstyrsklasser, feilmodus og analysere disse dataene. Ved å bruke realistiske datainnsamlinger kan en sammenligne metoden denne rapporten er basert på mot selskapets metode. En kan også lage en systemanalyse for deler av anlegget for å bestemme videre testintervall og eventuelt se på forbedringer hvor en har mange like feil. En kan enkelt lage en kort praktisk illustrasjon med påfølgende diskusjon for å foreslå en eventuell modifikasjon. Basert på oppgavens problemstilling har det vært nødvendig å kunne identifisere og validere ulike utstyrsgrupper og feilmoduser for å håndtere usikkerhet ved kvantifisering av systemets pålitelighet. I oppgaven er det blitt valgt å operasjonalisere og relatere usikkerhet i metoden til feilmodusene. Kategoriene som er utarbeidet kan ikke betraktes som gjensidig utelukkende, der forskjellige forhold vil kunne være representert av flere faktorer.

Innsamling av data vil generelt bli utført manuelt i selskapenes systemer, men kan også samles inn automatisk gjennom SAS-systemet til innretningen. Hvordan innsamlingen av data foregår er blitt beskrevet i delkapittel 3.3. Normalt sett vil automatisk rapportering av feil bli kategorisert som DD-feil ettersom dette er detektert feil. Feilklassifiseringene er bedre beskrevet i kapittel 2.3.2.

3.2 Utstyrsklasser og feilmodus

For å kunne analysere alle typer feil som potensielt kan forekomme i instrumenterte systemer er det viktig å kunne kategorisere utstyr som er blitt installert og hvilke type feil som kan oppstå. I dette delkapittelet er det utarbeidet utstyrsklasser og feilmoduser for hver utstyrsklasse. Det er også utarbeidet en arbeidsprosess på hvordan en skal gå fram for å rapportere feil som har oppstått i et SIS-instrument. En må merke seg også at det er bare tatt hensyn til utstyrsklasser og feilmoduser som vil ha med instrumentering å gjøre. Det vil være nødvendig å utarbeide lignende basis for andre utstyrsgrupper som motorer, batteripakker (UPS) osv. Grunnen for at det ikke er behandlet her er for at denne rapporten tar for seg instrumenteringen som går på styring av annet prosessutstyr, HVAC, mekanisk og ikke selve utstyret. eksempler på dette er brannvanspumper, vanntette dører osv. Ventiler er tatt med pga at en har en del instrumentering til dette utstyret som ventilene er avhengig av.

3.2.1 Grunnleggende forståelse for feilkoder

Ved å definere feilmoduser er det viktig å forstå kritikaliteten til disse. En beskrivelse av kritikalitet for de forskjellige feilmodusene er forklart her slik at en skjønner hva en feilmodus representerer. Videre så følger det en tabell (tabell 3.3) som beskriver de forskjellige feilmodusene. Ikke alle kritikalitetene er tatt med i tabell 3.3, men de vil gjelde hele denne rapporten. Det er tatt med en del mer koder for ventiler da en enkelt kan se hva som er galt, men det trenger ikke være farlige feil for funksjonaliteten. Dette er også begrunnet med at det er enkelte feil som skal rapporteres til forskjellige avdelinger og Petroleumstilsynet skal også ha innrapportert forkjellige dataer med tanke på RNNP-rapporteringen som er beskrevet i kapittel 4.

Tabell 3.1: Beskrivelse av feilmodus

Beskrivelse av feilmodus		
Type feil	Kode	Beskrivelse
Farlig/kritisk feil	FF	Feil eller svikt med potensial for å sette det sikkerhetsinstrumenterte systemet i en farlig tilstand eller ut av operativ tilstand.[4] Sikkerhetsfunksjon er svekket.
Degradert feil	DG	Utstyrets evne til å utføre nødvendig sikkerhetsfunksjon (eller opprettholde produksjonen) fortsatt er intakt, men er redusert. Feil kan over tiden utvikle seg til sikker feil eller farlig/kritisk feil hvis ikke blir utbedret.
Ikke kritisk feil	IKF	Feil eller svikt i en utstyrsenhet som ikke forårsaker en umiddelbar opphør av evnen til å utføre den nødvendige funksjonen [4] eller svekker funksjonssikkerheten. Denne inkluderer degraderte feil.
Sikker feil	SF	Dekker feilmodusene som enten forårsaker en falsk drift av utstyret og / eller opprettholder sikkerhetsfunksjonen til utstyret . Disse feilene er ikke farlig med hensyn til utstyrets sikkerhetsfunksjon, men kan ofte være kritisk for produksjon. Ikke-kritiske feil

3.2.2 Feilkoder

Ved valg av feilkoder er det tatt utgangspunkt i ISO 14224[4] standarden. Dette er en europeisk standard som Norge er bundet til å innføre gjennom CEN-CENELECs interne krav. Dette er en standard og ikke et absolutt krav, derfor vil enkelte koder være innført, mens andre ikke er med. Koder som er innført har nødvendigvis ikke noe med SIF, men er tatt med for å få en helhetlig kodeportefølje for det relevante utstyret som skal vurderes. Standarden er utarbeidet for Petroleumindustri, petrokjemisk industri og naturgassindustri. Den tar også for seg innsamling og utveksling av pålitelighets- og vedlikeholdsdata for utstyr generelt.

DFP (defekt passiv brann beskyttelse) er ikke en ISO 14224[4] feilmodus, men er introdusert her for å kunne rapportere skade på brannisolering, hovedsaklig på ventiler og rør, men også på struktur. Denne modusen er ikke kritisk, men må utbedres snarlig for å ha den overordnede sikkerheten i prosessen.

DEX (Defekt EX-beskyttelse) er ikke en ISO 14224 [4] feilmodus, men er introdusert her da Petroleumtilsynet setter krav til tennkildekontroll gjennom Innretningsforskriften [7] §10a Tennkildekontroll. Videre så er det IEC 60079-17 [5] som brukes for å utføre inspeksjon og vedlikehold på EX-utstyr. en må merke seg her at DEX-feilmodus er blitt definert som en farlig feil og for at en ikke skal rapportere feilaktige DEX-feil er det utarbeidet en egen forklaring på dette. I IEC 60079-17 er det utarbeidet en sjekkliste til de forskjellige Ex-kategoriene og der er det oppført punkter som ikke går på funksjonaltietet av selve utstyret. Tanken er at når en skal rapportere en DEX-feil skal feilen påvirke EX-integriteten til utstyret. Hvis den ikke påvirker Ex-intigriteten skal den ikke rapporteres som DEX, men »other» (OTH). DEX-feil er ikke en del av SIS-kategorien og vil ikke bli betraktet som en feil på en SIF. Det stilles krav til EX-kompetanse for å jobbe med slikt utsyr og denne tabellen (tabell 3.2) er ikke absolutt, men heller utarbeidet som et eksempel for å få en bedre forståelse for hva som kan vurderes til en DEX feil. Begrunnelsen for at DEX er definert som en farlig feil er at dette utstyret kan være en tennkilde ved utslipp av brennbare gasser.

Tabell 3.2: Vurdering av DEX feil

Evaluering av EX svekkelser (DEX)		
Feil beskrivelse	Feildefinisjon	Beskrivelse
Teflon mangler på nippel	degradert feil	Feil skal ikke rapporteres som DEX, men må utbedres snarest for å unngå vannintrengelse.
Mangler bolt i lokket til EX e kapsling	degradert feil	Feil skal ikke rapporteres som DEX, men må utbedres snarest for å unngå vannintrengelse.
Mangler bolt i lokket til kapsling og har vanninntregning	Farlig feil	Feil skal rapporteres som DEX og må utbedres omgående eller isoleres.
Ex d kapsling med ødelagt flammespalte.	Farlig feil	En evaluering av kompetente personer må utføres, men ved større skade enn godtatt av leverandør av kapsling skal rapporteres.
Ex datablad mangler i databasen	Ikke kritisk feil	Ex datablad må hentes av leverandør og legges i databasen til bruker. Påvirker ikke funksjonaliteten.
EX skilt uleselig eller ikke på utstyr	Ikke kritisk feil	Hvis databasen har datablad og en kan verifisere at dette er samme utstyr samt godkjent utstyr er det ikke behov for ex skilt. Ref. 60079-17[5] seksjon 4.3.1.2

Feilkodebeskrivelse

Det er blitt utarbeidet en liste med relevante feilkoder. Det er tatt utgangspunkt i ISO 14224 standarden, men det er foreslått å holde disse kodene til et minimum for å forenkle rapporteringen/registreringen av feilene i et system. I tillegg til disse kodene må rapporteringen inneholde et felt med fritekst hvor en kan beskrive mer detaljert hva som er feil, hva som er utført osv. I tabell 3.3 kan en se foreslåtte feilkoder og hvilke koder som er brukt i denne rapporten. Ved hver feilkode følger en forklaring på hva denne koden representere og en beskrivelse på feilmodusen.

Tabell 3.3: Definisjon på feilkoder

Feilkodebeskrivelser		
Feilkode	Feilmodus	Beskrivelse
AIR	Abnormal instrument reading	Gjelder ventiler: Falsk alarm, feil instrument indikasjon
DEX	Defect EX-protection	Se egen definisjon på dette.
DOP	Delayed operation	Gjelder ventiler: Ventil åpner ikke innen spesifisert tid
ELP	External Leakage-process medium	Gjelder ventiler: Ekstern lekkasje av prosess medium (olje, gass, kondensat, vann)
ELU	External Leakage-Utility medium	Gjelder ventiler: Ekstern lekkasje av hjelpe medium. (Smøring, kjølevann etc)

Fortsetter neste side

Tabell 3.3 – Fortsettelse fra forrige side

Feilkodebeskrivelser		
Feilkode	Feilmodus	Beskrivelse
ERO	Erractic output	Intrumentet gir ustabilt/varierende signal som ikke er innenfor spesifisert krav.
FTC	Failure to close on demand	Gjelder ventiler: Ventil går ikke til lukket posisjon ved aktivering
FTF	Failure to function	Instrumentet gir ikke signal. Eksempler: Forurenset eller tildekket instrument gjør at ingen eller begrenset testmedie får tilgang til instrumentet. Eventuelt instrument dekker feil område(ikke ihht spesifikasjonene for installasjonen.
FTO	Failure to open on demand	Gjelder ventiler: Ventil går ikke til åpen posisjon ved aktivering
INL	Internal leakage	Gjelder ventiler: Intern lekkasje av prosess- eller hjelpe medium høyere enn spesifisert verdi
LCP	Leakage in closed position	Gjelder ventiler: Intern lekkasje gjennom ventilen i lukket posisjon
LOO	Low output	Instrumentet gir for lavt signal. Eksempel kontrollrom får bekreftet signal fra instrument eller lavere signal enn faktisk signal skal være.
NOO	No output	Instrumentet gir ikke signal. Eksempler: Aktivering av instrument i felt forandrer ikke alarmutgang/signal på instrument tilstand.
OTH	Other	Feil som ikke er definert som farlige og andre feil som ikke er dekket av de andre kodene.
PLU	Plugged/ Choked	Gjelder ventiler: Gjennomstrømsbegrenset/blokkert på grunn av tilsmussing, forurensning, gjenstander, ising, osv
SER	Minor in-service problems	Løse deler, tilsmusset, misfarging
STD	Structural deficiency	Materielle skader (sprekker, slitasje, bruddkorrosjon eller redusert integritet)
DPF	Defect passive fire protection	Skade på brannisolasjon

Utstyrsgrupper

Listen med feil modus taksonomier som er foreslått er det også tatt utgangspunkt fra ISO 14224 standarden. Her har en holdt seg til instrumenterte utstyrsgrupper mens det vil være naturlig å ha utstyrsgrupper utover instrumenteringen da en utfører tester og vedlikehold på rent mekanisk utstyr som for eksempel sikkerhetsventiler (PSV), vanntette dører osv. Dette er ikke SIS-utstyr, men det er utstyr som er rapporteringspliktig til Petroleumstilsynet. I tabell 3.4 kan en se foreslåtte feil modus taksonomier, hvilke utstyrsgrupper disse tilhører og grad av kritikalitet. Det er også beskrevet hva som er selve sikkerhetsfunksjonen slik at en kan gi en bedre vurdering ved å sette feil modus under registrering av observert feil.

Tabell 3.4: Definisjon på utstyrsgrupper, type utstyr, feil definisjon, feil modus og forklaring på sikkerhetsfunksjonen til utstyret

Utstyrsgrupper				
Utstyrsgruppe	Utstyr	Feil definisjon	Feil modus	Sikkerhetsfunksjon
Branndetektorer (Gruppe 1)	Røyk	Farlig feil	ERO	Instrumentet skal gi alarm/tripp signal ved tilstedeværelsen av røyk, varme eller flamme avhengig av type instrument
	Tidlig røyk		FTF	
	Varme		LOO	
	Røyk/varme Flamme		NOO	
		Sikker / Degradert feil	OTH	
		Farlig feil	DEX	

Fortsetter neste side

Tabell 3.4 – Fortsettelse fra forrige side				
Utstyrsgrupper				
Utstyrsgruppe	Utstyr	Feil definisjon	Feil modus	Sikkerhetsfunksjon
Gassdetektorer (Gruppe 2)[1]	Punktgass, linjegass, H2, H2S, O2, oljetåke	Farlig feil	ERO	Instrumentet skal gi alarm/tripp signal ved tilstedeværelsen av gass avhengig av instrument
			FTF	
			LOO	
			NOO	
		Sikker / Degradert feil	OTH	
		Farlig feil	DEX	
Manuelle trykknapper (Gruppe 3)	ESD knapper, Nødstopp knapper	Farlig feil	FTF	Utstyret skal gi alarm/tripp signal ved aktivering
			NOO	
		Sikker / Degradert feil	OTH	
		Farlig feil	DEX	
Prosess transmittere (Gruppe 4)	Temperatur, Flow, trykk, nivå	Farlig feil	ERO	Utstyret skal gi alarm/tripp signal ved aktivering av spesifiert setpunkt.
			FTF	
			LOO	
			NOO	
		Sikker / Degradert feil	OTH	
		Farlig feil	DEX	
Fortsetter neste side				

[1]Se tabell 5.4 i appendiks C for respons tid for gassdetektorer

Tabell 3.4 – Fortsettelse fra forrige side

Utstyrsgrupper				
Utstyrsgruppe	Utstyr	Feil definisjon	Feil modus	Sikkerhetsfunksjon
Blowdown ventiler (Gruppe 5)[2]	BDV ventiler	Degradert feil	AIR	Ventil skal åpne ved aktivering innenfor spesifisert tid uten feil. Her inngår også hjelpetag/utstyr som limit switcher, Solenoider, osv for å sikre funksjonaliteten til hovedventilen
		Farlig feil	DEX	
			DOP	
		Degradert feil	ELP	
			ELU	
			FTC	
		Farlig feil	FTO	
		Degradert feil	INL	
			LCP	
		Sikker / Degradert feil	OTH	
			PLU	
			SER	
			STD	
			DPF	
Shutdown ventiler (XSV ventiler) (ESV ventiler) (Gruppe 6)[3]	Shutdown ventiler	Degradert feil	AIR	Ventil skal åpne ved aktivering innenfor spesifisert tid uten feil. Her inngår også hjelpetag/utstyr som limit switcher, Solenoider, osv for å sikre funksjonaliteten til hovedventilen
		Farlig feil	DEX	
			DOP	
			ELP	
			ELU	
			FTC	
		Degradert feil	FTO	
		Farlig feil	INL	
			LCP	
		Sikker / Degradert feil	OTH	
		Degradert feil	PLU	
			SER	
			STD	
			DPF	

Fortsetter neste side

[2]Se tabell 5.4 i appendiks C for respons tid for BDV ventiler
[3]Se tabell 5.4 i appendiks C for respons tid for XSV/ESV ventiler

Tabell 3.4 – Fortsettelse fra forrige side

Utstyrsgrupper				
Utstyrsgruppe	Utstyr	Feil definisjon	Feil modus	Sikkerhetsfunksjon
Limit switch (Gruppe 7)	Endebrytere (mekanske, induktive, kapasative og magnetiske)	Degradert feil	AIR	Utstyret skal gi tilbakemelding på aktivert og/eller ikke-aktivert posisjon
		Farlig feil	DEX	
			FTF	
		Sikker / Degradert feil	OTH	
PLS/Logikk (Gruppe 8)	PLS, I/O kort	Farlig feil	FTF	Utstyret skal gi utgangssignal basert på inngangssignal
			ERO	
		Sikker / Degradert feil	OTH	
Solenoid (Gruppe 9)	Pilotventiler, solenoider	Farlig feil	DEX	Utstyret skal skifte posisjon ved akrivering / deaktivering
			FTF	
		Sikker / Degradert feil	OTH	
Sikringer/rele (Gruppe 10)	Sikringer, Rele, kontaktorer	Farlig feil	DEX	Utstyret skal isolere elektrisk utstyr ved aktivering / deaktivering
			FTF	
		Sikker / Degradert feil	OTH	

3.3 Observasjonsmetode

Det er hensiktsmessig å ha en kategori som sier hvordan en feil eller flere feil har blitt oppdaget i et SIS-system. Grunnen til dette er at en kan se på underforliggende årsaker til hva som må forbedres for å finne de feilene som kan oppstå ved andre systemer i anlegget. Eksempler er hvis en finner like feil ved tilfeldig observasjon må kanskje en evaluering av vedlikeholdsprosedyren gjennomføres for å sjekke dette periodisk. Kanskje en må ha kontinuerlig tilstandsovervåkning. En annen grunn er at en kan skille mellom kritikaliteten på feilene som igjen kan brukes til analyse av SIL-systemet. Kritikaliteten til feilen blir oppgitt ved valg av feil modus, men når en velger observasjonmetode forteller det om feilen er en DU, DD, SD eller SU. Og det er ekstremt viktig å ha kontroll på dette da det er DU-feil som er de mest kritiske feilen som en kan få. Det er viktig å skjønne at observasjonsmetoden alene ikke sier noe om feil som er oppdaget.

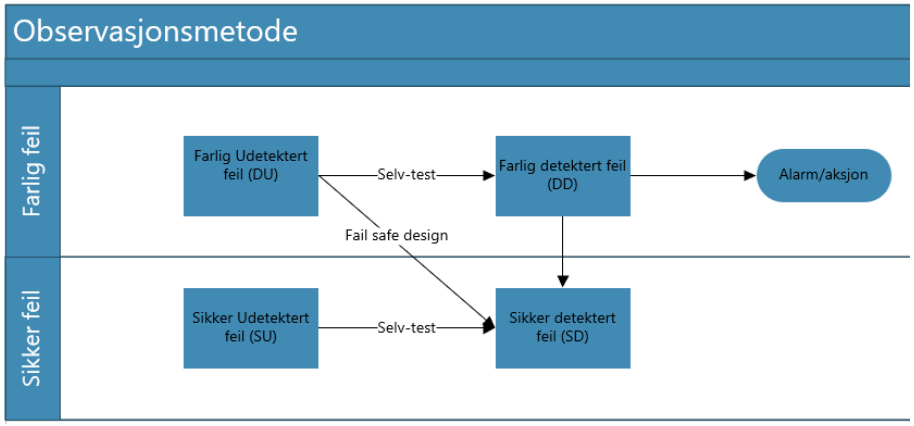
ISO 14224 tabell B.4 [4] beskriver 11 forskjellige observasjonsmetoder for å detektere feil som har oppstått i et system. Ikke alle disse metodene vil være relevante for å registrere feil som er oppstått i et SIS-system så her har en valgt 6 forskjellige metoder:

1. Periodisk vedlikehold
    - Periodisk service, planlagt vedlikehold (vedlikeholdsprogrammet), preventiv vedlikehold, Ex-integritetssjekk, o.l.
2. Funksjonstesting
    - Dette er typisk kjøring av ventiler, trip-funksjoner (ESD, PSD) kjøring av pumper, testing av B&G detektorer osv.
3. Inspeksjon
    - Ex-integritetssjekk o.l.
4. Periodisk tilstandsovervåking
    - Tilfeldig observasjon ved bruk av utstyr som ikke er i bruk hele tiden, men bare periodisk. Eksempel ved kjøring av brannpumper og man får feilmelding/alarm (detektert feil under testing)
5. Kontinuerlig tilstandsovervåking
    - Selv test av instrumenter/detektorer, overvåkning på ESD-knapper, diagnostikk av kontroll systemer o.l.

6. Tilfeldig observasjon
    - HMS-runder, tilfeldig oppdagelse av personell, rapporteringskort o.l.

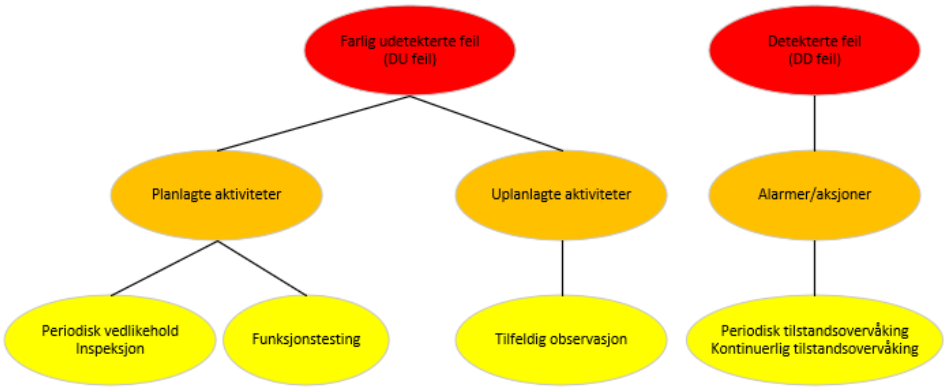
Feil som blir oppdaget ved disse metodene vil det være »kontinuerlig tilstandsovervåking» som kommer under DD-kategorien. Funksjonstesting kommer litt under periodisk vedlikehold, men er holdt som egen kategori da denne typen vedlikehold bare går på å teste funksjonaliteten til utstyret og ikke ser på for eksempel Ex-integriteten ol. I tillegg så er det viktig at en utarbeider en konkret beskrivelse av hva som er feil og eventuelt risikovurderer, samt beskriver hva som er blitt utbedret hvis det er gjort noe forsøk på å rette opp feilen. Dette kan ved senere anledning gi grunnlag for re-evaluering av feil modus, rapportering til kontrollorganer (Ptil), erfaringsoverføring osv. Arbeidsflyten for å opprettholde et SIS-system i operasjon kan ses i figur 3.5

I figur 3.1 er det illustrert sammenhengen mellom de forskjellige feiltypene og hvordan de samhandler med hverandre når en har selvtest av utstyr og feil safe design slik at en kan unngå farlige detekterte feil (DD) og farlige udekterte (DU) feil i anlegget.



Figur 3.1: Observasjonsmetode for å detektere feil og sammenhengen mellom feiltyper

I figur 3.2 vises en hierarkisk illustrasjon på hvordan de forskjellige metodene brukes for å avsløre feil i anlegget. Nederst i gule bobler kan en se de 6 forskjellige metodene for å observere feil. I de oransje boblene kan en se under hvilke aktiviteter disse metodene kommer under. De røde boblene illustrere hvilken type kategori disse feilen kommer under.

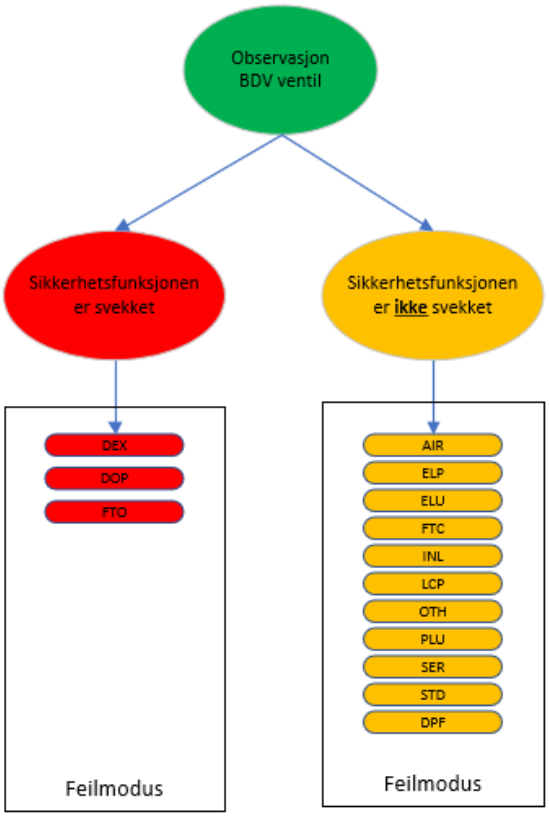


Figur 3.2: Hierarki for kartlegging av feil

3.4 Feilregistrering og klassifiserng

Arbeidsflyt for feilregistrering og klassifisering

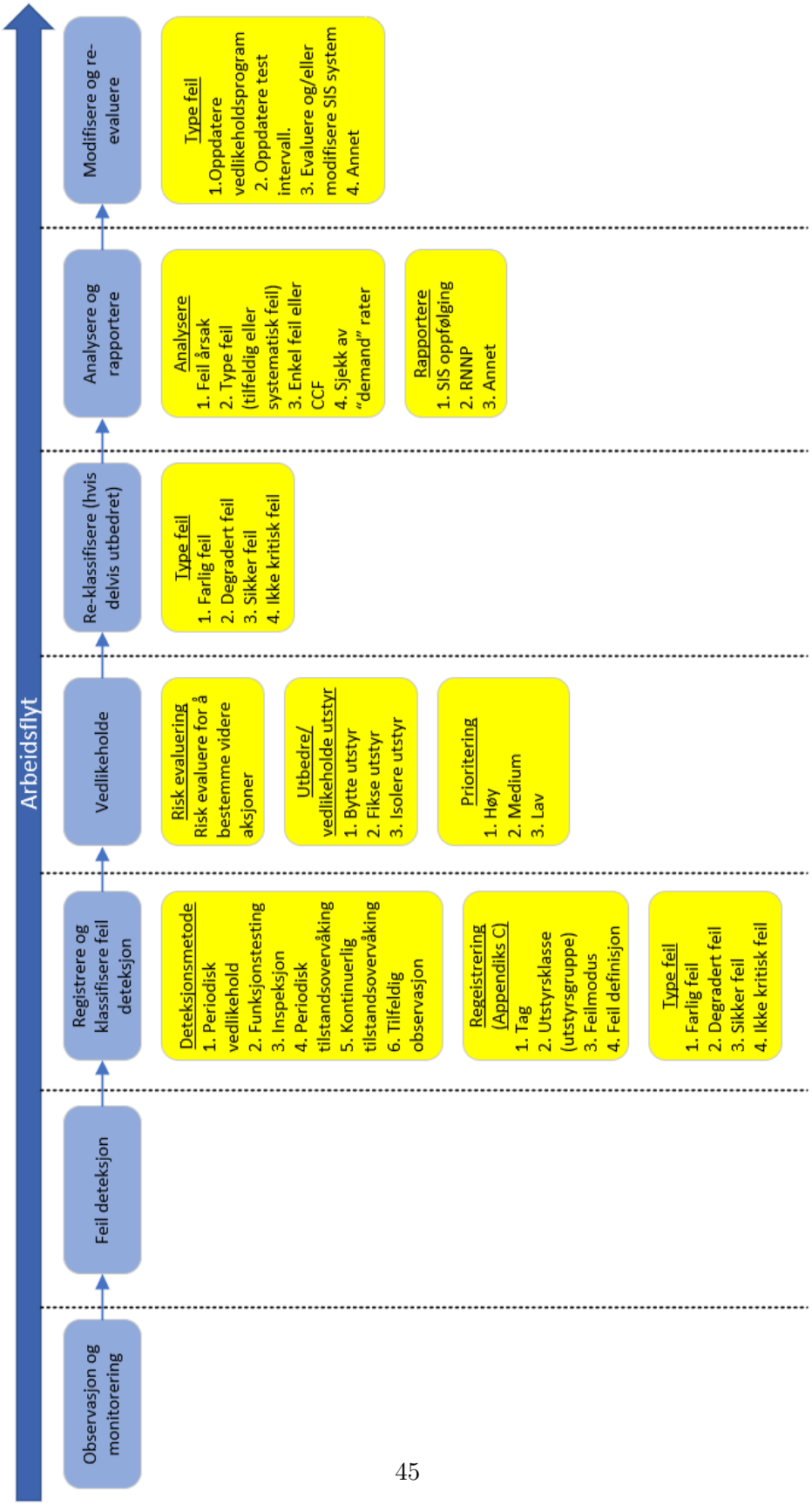
Når en feil blir oppdaget i prosessanlegget skal dette registreres i selskapets registreringssystem. Det er i dette systemet selskapet må ha implementert utstyrsklasser, feilmoduser/feilkoder som skal gi en kort beskrivelse på hvilken feil som er oppdaget. Videre så må registreringssystemet ha et fritekstområde hvor en kan legge inn en detaljert beskrivelse på feilen som er oppdaget.



Figur 3.3: Eksempel for BDV-ventil

3.5 Oppfølging av SIS-system

I figur 3.4 er det illustrert et forslag på arbeidsflyt for oppfølging av SIS-system. De 4 første kolonnene er det oftest driftspersonell som utfører. I første kolonne fra venstre er hvor en observerer en feil, « Observasjon og monitorering». Dette kan være en tilfeldig observasjon av offshore personell eller driftspersonell samt at en kan få en alarm i kontrollsystemet. Det er samme fremgangsmåte for detekterte feil som for udetekterte feil. I andre kolonne har vi selve feil deteksjonen, « Feil deteksjon». I kolonne 3 er registrering av den observerte feilen. Her er det viktrig at feilen blir registrert rett. En må registrere feilen med rett tag, i rett utstyrsgruppe med rett feil modus og med en beskrivelse av feilen som er blitt observert. Dette må utføres selv om feilen er blitt fikset på stedet slik at en kan følge opp om dette er en alvorlig feil som påvirker SIF eller om det er en systematisk feil som må gjennomgåes. I kapittel 3 Metode er det en grundig beskrivelse av forslag til rapportering og registrering. Dette er også illustrert i vedlegget « Arbeidsfiler» under fanen « Rapportering av feil». I kolonne 4 « Vedlikeholde» risk-evalueres feilen (denne kan også utføres når en registrerer feilen) setter prioritet og vurderer hva som må utføres hvis ikke feilen blir utbedret med det samme. I kolonne 5 « Re-Klassifisere» vurderer man feilen på ny. Dette kan for eksempel gjøres i sammarbeid med offshore-orginisasjonen og land-organisasjonen slik at feilen får en verifisering av eventuelt teknisk avdeling. I de 2 siste kolonnene er det land organisasjonen som tar seg av. Kolonne 6« Analysere og rapportere» er det oftest teknisk avdeling og teknisk sikkerhet som vurderer SIS-oppfølging og eventuelt rapportering til RNNP (Ptil). Her vurderes feil årsaken, og utfører nye PFD-kalkulasjoner. I den 6. og siste kolonnen oppdaterer man vedlikeholdsprogrammet, SRS og testintervall hvis en finner det nødvendig.



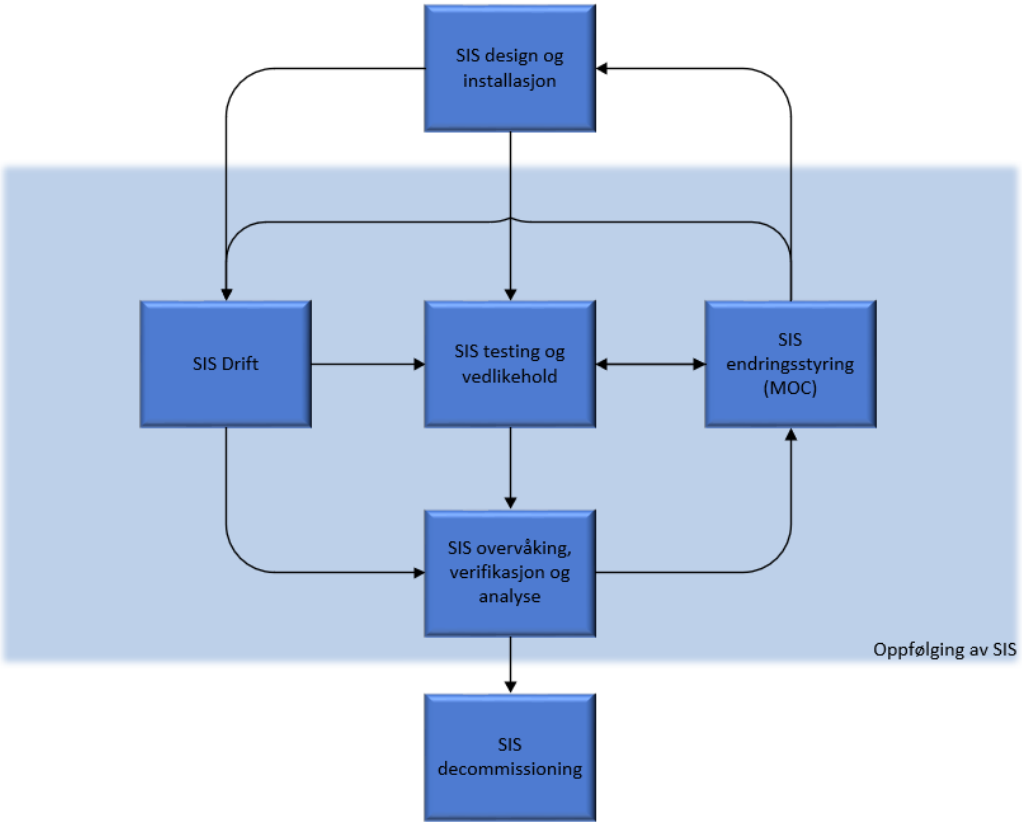
Figur 3.4: Arbeidsflyt for oppfølging av SIS-system

3.5.1 Hovedaktiviteter

Ved oppfølging av SIS er det knyttet til flere hovedaktiviteter i den operative fasen. Dette er illustrert i figur 3.5.1 [2]. Disse aktivitetene inkluderer:

- SIS-drift
- SIS-testing og vedlikehold
- SIS-endringsstyring (MOC)
- SIS-overvåking, verifikasjon og analyse

Figur 3.5: Hovedaktiviteter til oppfølging av SIS (NOG 070 [2])



Det vil ikke bli gjennomgått noen grundigere beskrivelse av hovedaktivitetene ved oppfølging av et SIS-system da en del allerede er beskrevet i andre kapitler i denne rapporten. Det som ikke er blitt beskrevet noe om er » SIS endringsstyring (MOC)». SIS endringsstyring er en viktig del av oppfølging av SIS-systemer. Endringstyring skal sikre at endringer i ethvert SIS blir korrekt gjennomgått, godkjent og planlagt før endringen gjøres og sikre at den nødvendige sikkerhetsintegriteten til SIS-systemet opprettholdes i tilfelle endringer blir utført i SIS-systemet.

3.5.2 Ytelseskravet og oppfølging av en SIF

Individuelle komponeneter i en SIF

I en SIF er det behov for å ha en kvalitativ oppfølging av individuelle komponenter i tillegg til kvantitativ oppfølging på utstyrsgruppe. Dette må utføres for å identifisere gjentagende feil som oppstår i anlegget. Feilrater (failure rate) i et SIS-system kalles MTBF (mean time between failure) som tilsvarer en gjennomsnittlig tid mellom feil, typisk over 50-100 år. Da vil det være lav sannsynlighet for at en komponent feiler flere ganger i løpet av en begrenset periode på for eksempel 3-4 år. Dersom det dukker opp mer enn én feil i en komponent i løpet av denne perioden, blir disse feilene ofte klassifisert som systematiske feil. Oftere testing vil ikke forbedre PFD i slike tilfeller og en bør heller identifisere individuelle komponenter og undersøke den underliggende årsaken. Den underliggende årsaken kan da ofte vise seg at det er feil design, menneskelig feil/svikt, feil på enkelt komponent eller lignende. Da er det også viktig å ikke bare se på antall feil i et system, men også se på hvor ofte samme komponent feiler.

Fullstendig SIF

IEC 61508/511 setter ytelseskravet for en fullstendig SIF i et SIS-system og ikke bare for enkeltkomponenter, ergo en må slå sammen PFD-kalkulasjonene fra alle komponentene i en SIF-sløyfe for å se om SIL-kravet er godkjent. En kan se et forenklet kalkulert eksempel på en fullstendig SIF i tabell 3.6 hvor en har lagt sammen fullstendig SIF og verifiserer at den er SIL 2 godkjent. Her er PFD-budsjettet til SIF vist og en kan se hvor mye hver enkelt komponent bidrar med. Da er det enkel å se hvor en skal oppgradere i SIF-sløyfen hvis en ikke klarer SIL-nivået. Dette kan en også se på når en oppdaterer testintervallet etter en periode hvor en har hatt noen feil på en type gruppe utstyr eller enkeltkomponenter.

Det forventet antall DU-feil i et SIS-system kan kalkuleres ut ifra formel 3.1. beskrivelse av parameterne kan finnes i tabell 3.5.

$$E_{(x)} = n \times \tau \times \lambda_{DU} \tag{3.1}$$

Formel 3.1 kalkulerer forventede feil for en type utstyr [2].

Eksempel hvis en har 350 transmittere, test perode på 3 år med en λ_{DU} på 5.00×10^{-7}

$$E_{(x)} = 350 \times 3 \times 8760 \times 5.00 \times 10^{-7} \approx 4 \tag{3.2}$$

Av kalkulasjonen kan en forvente 4 feil på transmitterne over en 3 års periode.

Tabell 3.5: Beskrivelse av parameterne

Parameter	Enhet	Beskrivelse
n	-	Antall tag innenfor en utstyrsgruppe som har vært drift
x	-	Antall DU-feil innenfor en utstyrsgruppe
τ	Timer	Operativ tid innenfor observasjonsperiode

testintervall for en SIF

Testintervall som en kommer fram til bør avrundes mot ett tillatt testintervall. En må være konservativ når en tar avrundingen slik at testintervallet heller mot det strengeste intervallet når en havner mellom 2 forskjellige testintervall. Valgte testintervall er tatt fra bransjen og inkluderer 1M, 2M, 3M, 4M, 6M, 9M, 12M, 18M, 24M, 36M, 48M[1], osv. Videre så er det ikke anbefalt å mer enn doble testintervallet fra en observasjonsperiode til en annen selv om kalkulasjonene gir en dobling av testintervallet.

[1]Med stor M menes måneder, for eksempel 48M er 48 måneder

3.5.3 Verifisering av PFD budsjettet til en SIF

Ved design av et SIS-system er det viktig at en fordeler bidraget i en SIF mer eller mindre likt for hvert ledd i sløyfen. Dette vil gjøre at en ikke får for mye bidrag på en del av sløyfen. Av naturlige årsaker så vil enkelte elementer ha mer påvirkning på budsjettet enn andre elementer. Hvis en skulle komme nærme grensen for SIL-nivået kan en enkelt se hvor en kan finne annet utstyr for å forbedre integriteten sil SIF-sløyfen. Man kan også lett identifisere hvilke ledd som er svake eller er mer utsatt for feil. I tabell 3.6 kan man se fordelingen av PFD-budsjettet på 2 måter. Det er anbefalt å bruke den måten hvor en ser PFD-budsjettet av SIL-nivå siden en kan se hvor mye en har å gå på i forhold til selve SIL-nivået. I eksempelet ser man at de største bidragene kommer fra ventil, transmitter og logikk. Hvis en får for mye bidrag på et element kan redundans være med å løse utfordringen. Dette kommer en mer innpå i kapittel 4, resultat. PFD data er hentet fra appendiks A

Tabell 3.6: PFD beregning av en SIF-funksjon hvor en verifiserer om den opprettholder SIL-nivået. Eksempelet er fra SRS tabell 2.1, Feilrate fra tabell 5.1 og PFD data er fra NOG 070 [2]

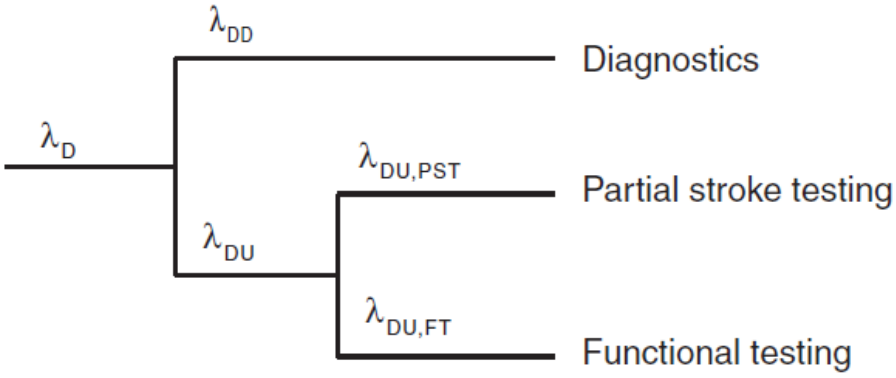
PFD beregning					
Komponent	Feilrate λ_{DU}	Test intervall (τ)	PFD	PFD budsjett av SIF	PFD budsjett av SIL-nivå
Trykk Transmitter [1]	5.00×10^{-7}	8760 timer	2.19×10^{-3}	27.4%	21.9%
Logikk	-	8760 timer	1.62×10^{-3}	20.3%	16.2%
Solonoid	-	8760 timer	6.77×10^{-5}	0.8%	0.7%
Aktuator	-	8760 timer	9.32×10^{-4}	11.7%	9.3%
Pilot ventil	-	8760 timer	5.70×10^{-4}	7.1%	5.7%
Ventil inkl. aktuator	-	8760 timer	2.61×10^{-3}	32.7%	26.1%
Total for funksjon			7.99×10^{-3}	100%	79.9%
SIL 2 oppfylt					Ja

[1] For trykk transmitter er formel 5.1 brukt for å få rett PFD data med tanke på feilrate.

3.5.4 Virkningen ved bruk av partiell testing av ventiler (PST)

Ved større prosessanlegg kan det være resurskrevende å teste ventiler for ofte og det kan være flere ventiler som ikke en har mulighet for å teste under produksjon. For å få et lenger testintervall på ventiler kan en vurdere mulighetene for å installere utstyr som kan utføre partiell test av ventil. Ved en partiell test av ventil beveger ventilen seg typisk mellom 10% - 20%. Dette vi da ikke påvirke prosessen vesentlig og en utsetter ikke prosessanlegget for fare for å stenge ned. Videre så må en vurdere PST-dekningen. PST-dekning kan variere avhengig av ventilutforming, drifts- og miljøforhold og antas ofte å være mellom 60 - 70% [10]

Figur 3.6: Oversikt over de aktuelle feilratene til en sikkerhetsventil [12]



De tre feilfrekvensene i figur 3.6 (λ_{DD}, $\lambda_{DU,PST}$ og $\lambda_{DU,FST}$) kan utrykkes i termer av λ_D som en kan se av formel 3.3, 3.4 og 3.5 [12].

$$\lambda_{DD} = \theta_{DC} \times \lambda_D \tag{3.3}$$

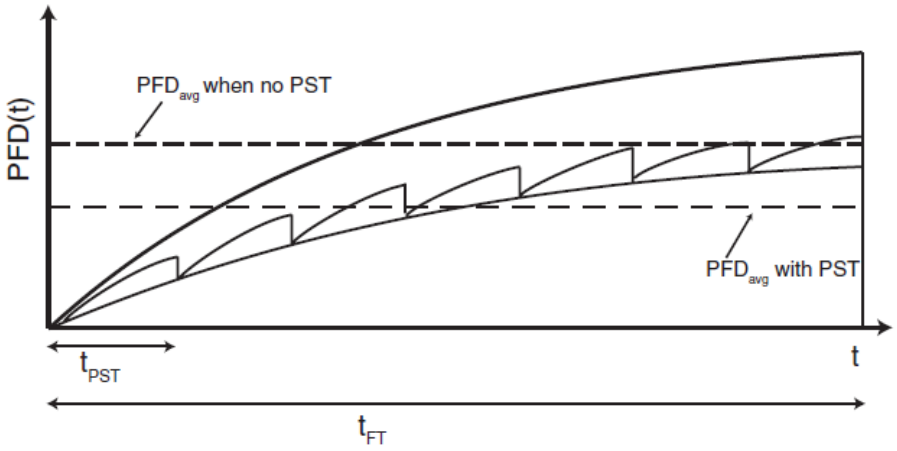
$$\lambda_{DU,PST} = (1 - \theta_{DC}) \times \theta_{PST} \times \lambda_D \tag{3.4}$$

$$\lambda_{DU,FST} = (1 - \theta_{DC}) \times (1 - \theta_{PST}) \times \lambda_D \tag{3.5}$$

θ_{DC} er i dette tilfellet $PST_{covarage}$.

Effekten av PST bidraget er illustrert i figur 3.7 hvor t_{FT} i denne figuren er FST. Kalkulasjonene i formel

Figur 3.7: PST-bidrag til PFD [12]



Forenklede formeler hvor en inkluderer PST-bidraget i testintervallet av en sikkerhetsventil er vist i formel 3.6 og 3.7. En sammenligning hvor en tar kredit for PST er beskrevet i kapittel 4.1.5

$$PFD = PST_{covarage} \times \left(\lambda_{DU} \times \frac{\tau_{PST}}{2}\right) + (1 - PST_{covarage}) \times \left(\lambda_{DU} \times \frac{\tau}{2}\right) \tag{3.6}$$

Formel 3.6 for å kalkulere ny PFD ved bruk av partiel test av ventiler (PST) [6]

$$\tau_{new} \leq \frac{\tau - \tau_{PST} \times PST_{covarage}}{1 - PST_{covarage}} \tag{3.7}$$

Formel 3.7 for å kalkulere nytt testintervall ved bruk av partiel test av ventiler (PST) [6]

Tabell 3.7: Beskrivelse av parametre i formel 3.1, 3.6 og 3.7

Parameter	Beskrivelse
$E_{(x)}$	Forventet antall DU-feil
x	antall observerte /registrerte DU-feil
τ_{new}	Nytt testintervall
τ_{PST}	PST testintervall (antall mnd)
$PST_{covarage}$	Den vurderte dekningen av PST
τ	Eksisterende testintervall mellom funksjonsprøving
λ_{DU}	Farlige udetekterte feil

Kapittel 4

Resultat

Det finnes flere tilnærmingsmetoder for å oppdatere testintervallet til utstyr som er dokumentert i SRS. Analysen som er blitt presentert i denne oppgaven viser en metode som baserer seg på design feilfrekvens og design testintervall for de forskjellige utstyrsgruppene som er utarbeidet i metodekapitelet. Kalkulasjonene har blitt dokumentert i et separat vedlegg 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 vedlegget «arbeidsfiler » før dette kapittelet leses. Dette kapittelet viser analyser fra en gjennomgang av et SIS-system ved å oppdatere testintervallet til de SIF'ene som har behov for dette ved for høy feilfrekvens og har feil antagelser ved design. Dette blir presentert i forskjellige scenarioer (delkapitlene) ved at en utfører en nøyere analyse av de forskjellige situasjonene som er simulert i vedlegget «arbeidsfiler».

Det er videre viktig å minne på at det er utført kalkulasjoner på en fiktiv SRS hvor en har tatt utgangspunkt i pålitelighetsdata og utarbeidet forskjellige SIF'er som er fra NOG 070. Excel-arket hvor en behandler alle SIF'er er mulig å bruke i sanne systemer, men hvor en mulig må legge til flere sub-nivåer/systemer for sluttelementer hvis en har data for andre utstyrgrupper som for eksempel separat aktuator, solenoid/kontroller osv.

Ved flere forhold har det også vært nødvendig å vurdere faktorer slik at en kan utføre denne analysen. Der det har vært nødvendig har en beskrevet dette i kapitelet «Metode» og gitt en forklaring hva som er lagt til grunn for disse antagelsene.

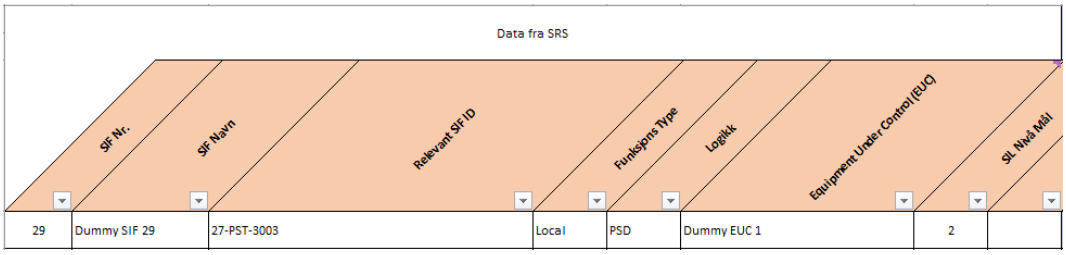
4.1 Beskrivelse av oppgaven som er utført i Excel-arket

SIF-data fanen

I vedlegget «Arbeidsfiler» er det 7 faner hvor fanen «SIF-data» er selve hoved-kalkulasjonene for SIF'ene. Fanen «Oppdatert feilrate» estimerer ny λ_{DU} for bruk i «SIF-data». Fanen «Feilrate estimat tilnærming» er beskrevet i kapittel 4.1.3. «Rapportering av feil» fanen er hvor en rapporterer feil og som er tatt med i kalk-ulasjonene i «SIF-data». Dette er beskrevet i kapittel 4.1.2. I appendiks A har vi tatt med PFD-data som er med i fanen «Utstyr Lambda og PFD», men i Excel er den mer dynamisk med tanke på kalkulasjonene som blir utført i Excel-arket. «Responstid ventil» er ikke brukt noen steder, men er tatt med for dette går på rapportering av utstyrsgruppe 5 og 6 (BDV ventiler og XSV ventiler) for feil-kode DOP. Denne listen er også representert i appendiks C. I den siste fanen kalt «PFD formler og kalkulasjoner» er brukt til å kalkulere votering av initiator og sluttelement i fanen «SIF-data».

Data fra SRS

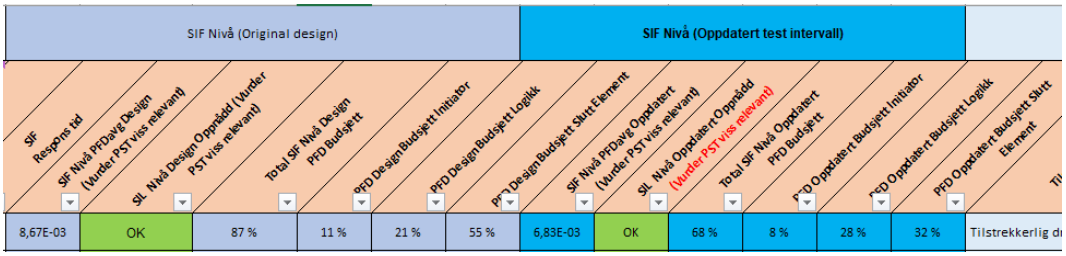
Fanen for SIF-data er bygget opp slik at en tar utgangspunkt i data fra SRS, eksempel tabell 2.1. Da har en tatt med SIF-nummer, SIF-navn (her har vi bare dummy navn), SIF-ID, funksjonstype, logikktype, EUC og SIL-nivå. Se figur 4.1



Figur 4.1: Utklipp fra «SIF-data» i vedlegg «Arbeidsfiler», data fra SRS

SIF-nivå

Videre så har SIF-nivå for design som en sammenligner med oppdatert SIF-nivå, figur 4.2. Her kan en se at en bruker prinsippet beskrevet i delkapittel 3.5.3 hvor en sjekker PFD-bidraget totalt og for de forskjellige delelementene i SIF'en. Dette gjør det lettere å se eventuelt hvilke element som gjør at en ikke opprettholder SIL-nivået. En beskrivelse av dette vil bli forklart senere i dette kapittelet. En har også tatt med om sløyfen opprettholder SIL-nivået og PFD_{avg}.

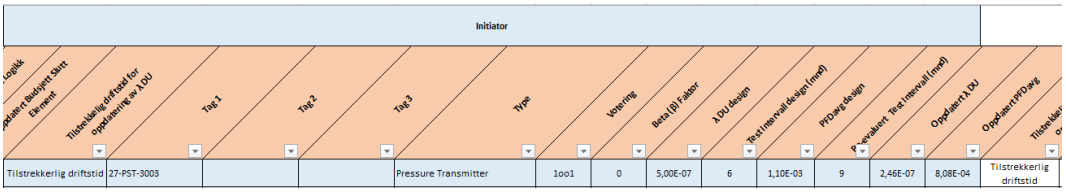


Figur 4.2: Utklipp fra «SIF data» i vedlegg « Arbeidsfiler», SIF nivå

Initiator

I initiator kolonnen (figur 4.3) har en tatt med alle relevante data som angår initiator elementet. Type instrument, votering, β-faktor, λ_{DU} for design og λ_{DU} oppdatert etter feil registrering, vurderer om driftstid er tilstrekkelig og kanskje det viktigste av alt testintervallet for funksjonsjekk.

« Tilstrekkelig driftstid» blir kalkulert i fanen « oppdatert feilrate». Hvis det viser seg at en ikke har tilstrekkelig driftstid for en type transmitter vil en ikke bruke ny λ_{DU} for å oppdatere feilraten i kalkulasjonene, ref. delkapittel 4.1.3. En vil da bruke generiske data fra NOG 070 til en får nok driftstid.
Voteringen av transmitterne har innvirkning på PFD_{avg} kalkulasjonene. Hvis en har en votering på 2oo3 vil kalkulasjonen bli som formel 5.2, hvor τ er re-evaluert testintervall og en bruker oppdatert λ_{DU}. For design data bruker en ikke oppdaterte verdier for testintervall og λ_{DU}.
Re-evaluert testintervall er kalkulert i « Oppdatert feilrate» fanen. testintervallet er kalkulert etter beskrivelsene i delkapittel 4.1.1 og er vist i figur 4.4



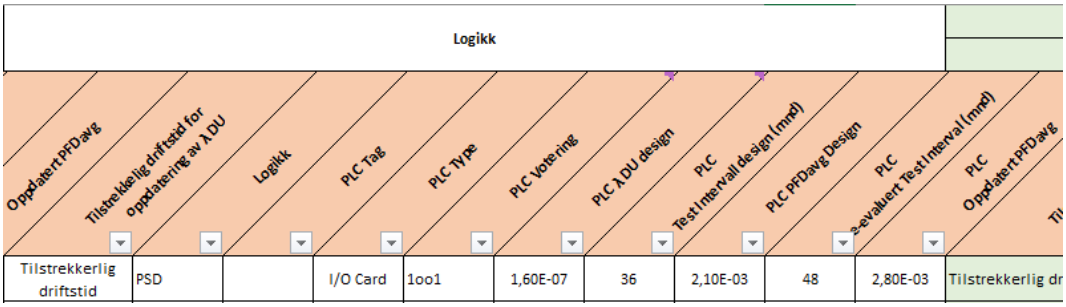
Figur 4.3: Utklipp fra « SIF data» i vedlegg « Arbeidsfiler», initiator

M1 metode	Tau,0	6	Måneder
Timer mellom test intervall	Ti	7,40E+03	Timer
Måneder mellom test intervall	T1	10,13	måneder
	"T1"	9	måneder
Periode 2	Driftstid (år)	3	År
	Antall feil (x)	0	stk
	Ti	1,55E+03	Timer
	T2	2,12	Måneder
	"T2"	2	Måneder

Figur 4.4: Utklipp fra beregning av testintervall for trykktransmitter i vedlegget « Arbeidsfiler»

Logikk

I « logikk» kolonnen (figur 4.5) er det bare tatt med sikkerhets programmerbar logisk styring (PLS) inkludert I/O. Da PLS ikke har noen votering er formel 2.1 blitt benyttet for kalkulasjon av PFD_{avg}. testintervallet er kalkulert etter beskrivelsene i delkapittel 4.1.1 og er vist i figur 4.6



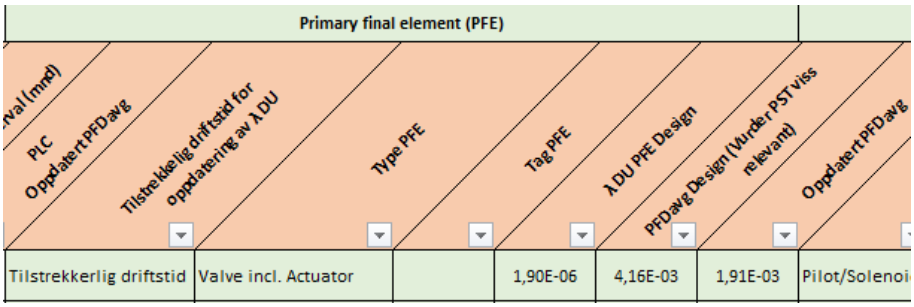
Figur 4.5: Utklipp fra « SIF data» i vedlegg « Arbeidsfiler», logikk

M1 metode	Tau,0	36	Måneder
Timer mellom test intervall	Ti	4,58E+04	Timer
Måneder mellom test intervall	T1	62,76	måneder
	"T1"	48	måneder
Periode 2	Driftstid (år)	3	År
	Antall feil (x)	0	stk
	Ti	9,81E+03	Timer
	T2	13,44	Måneder
	"T2"	12	Måneder

Figur 4.6: Utklipp fra beregning av testintervall for I/O i vedlegget « Arbeidsfiler»

Primary final element (PFE)

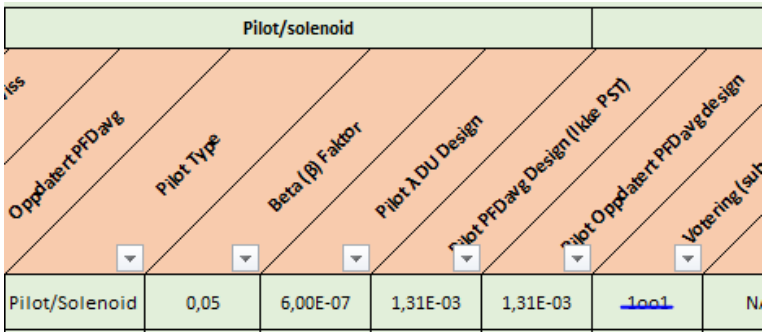
Kalkulasjonene for feilrate (λ_{DU}) og nytt testintervall for « primary final element» (PFE) er utført med samme metode som initiator, men når en skal finne Oppdatert PFD_{avg} sjekkes det om en har brukt PST fra designfasen som er vist i formel 3.6. Dataene for « primary final element» er vist i figur 4.7.



Figur 4.7: Utklipp fra « SIF data» i vedlegg « Arbeidsfiler», Primary final element

Pilot/solenoid

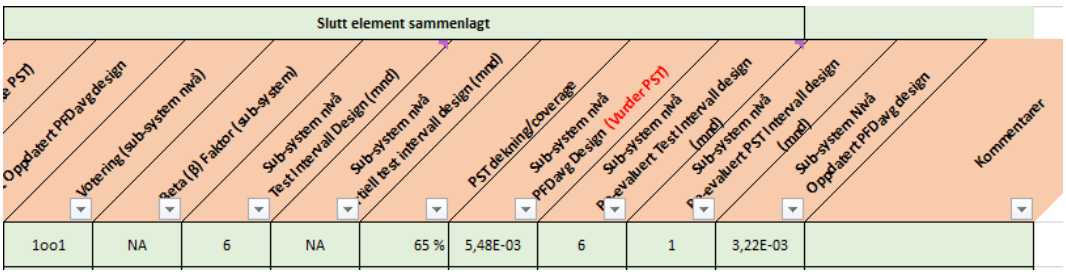
«Pilot/Solenoid» elementet har ikke noen votering, og er dessuten integrert med PFE-utstyret. Eksempel på dette kan være en ventil med aktuator som ikke blir benyttet alene som et sluttelement. Dette medfører at en bare bruker den forenklede formelen vist ved formel 2.1 for kalkulasjon av PFD_{avg}. testintervallet vil følge hovedelementet (PFE). Dataene for «Pilot/Solenoid» er vist i figur 4.8.



Figur 4.8: Utklipp fra « SIF data» i vedlegg « Arbeidsfiler», Pilot/solenoid

Sluttelement sammenlagt

I « sluttelement sammenlagt» (figur 4.9) har en tatt med alle relevante data som angår primary final elementet og pilot/solenoid elementet da disse er avhengig av hverandre for funksjonaliteten. PFD_{avg} for PFE og pilot/solenoid legges sammen da disse er direkte relatert med hverandre for å fungere. Voteringen av « sluttelement sammenlagt» har innvirkning på PFD_{avg} kalkulasjonene. Ofte er sluttelementet det største bidraget til budsjettet for en SIF-sløyfe. En votering hvor flere sluttelementer må fungere ved feil bør unngås for et SIL-nivå på 2 eller høyere. Hvis en har en votering vil kalkulasjonen bli som formel 5.2, hvor τ er re-evaluert testintervall og en bruker oppdatert λ_{DU}. Re-evaluert testintervall er kalkulert i « Oppdatert feilrate» fanen. testintervallet er kalkulert etter beskrivelsene i delkapittel 4.1.1 og er vist i figur 4.9. Vurdering av å forlenge testintervallet (FST) kan en benytte seg av PST som er gjennomgått i kapittel 4.1.5.



Figur 4.9: Utklipp fra « SIF data» i vedlegg « Arbeidsfiler», Sluttelement sammenlagt

4.1.1 Oppdatering av testintervallet

For oppdatering av testintervallet er det brukt en metode som tar utgangspunkt i data fra designfasen. En bruker $\lambda_{DU,0}$, τ (testintervallet ved design), β_1, α_1 og antall DU-feil (x) oppdaget i testperioden.

Metoden er konservativ som betyr at algoritmen bruker 70% feil (feilprosenten) og sammenligner dette med design feilraten ($\lambda_{DU,0}$) og design testintervallet τ_0. Ved å gjøre dette finner en det høyeste tillatte testintervallet som tilsvarer med design feilraten og testintervallet. For å klare dette må en anvende den inverse kjikvadrat fordelingen i formelen. Den inverse kjikvadrat fordelingen brukes til å sammenligne faktiske og forventede resultater. Se formel 4.1.

$$\tau_i \leq \frac{\lambda_{DU,0} \times \tau_0}{\lambda_{DU,i}^{70U}} = \frac{2 \times \lambda_{DU,0} \times \tau_0 \times (\beta_i + T_i)}{Z_{0.30,2\times(\alpha_i+x_i)}} \quad \text{timer} \tag{4.1}$$

Formel 4.1 er for å kalkulere nytt testintervall etter en periode med oppdagede DU-feil [6]

Formel 4.2 er kalkulert testintervall fra eksempelet som blir brukt i kapittel 4.1.3

$$\tau_i = \frac{2 \times 1,03 \times 6 \times (2.00 \times 10^6 + 2.07 \times 10^6)}{Z_{0.30,2\times(1+1)}} = \quad 3.65 \times 10^3 \text{timer} \tag{4.2}$$

Formel 4.2 er for å kalkulere nytt testintervall for eksempelet som blir brukt i kapittel 4.1.3

Dette tilsvarer 5 mnd, men siden vi har valgt å avrunde til intervallene 1M, 2M, 3M, 4M, 6M, osv[1] velges det konservative intervallet her og ender opp med 4 mnd testintervall.

[1] Se kapittel 3.5.2 «testintervall for en SIF»

4.1.2 Rapportering av feil

De utstyrsgruppene, feilkodene og feilmodusene som er blitt definert i kapittel 3.2 er gjenspeilet i feil rapporteringsskjema «Rapportering av feil» i vedlegg «Arbeidsfiler». I figur 4.10 viser bare et lite utklipp av de viktigste kolonnene som er beskrevet i kapittel 3.2. Det som er viktig å få med seg er at en bare kan velge de feilmodusene som er definert for de utstyrsgruppene. Feil klassifiseringen må foretas manuelt etter vurdering av feilen. Det kan bli vurdert etter hva som er blitt beskrevet i en «langtekst». Det som er viktig å forstå er at en må ikke rapportere en farlig feil konsekvent som DU-feil. Da kan det fort bli mye feil ved oppdatering av SIF-data hvor en bare bruker DU-feil for å oppdatere λ_{DU}. Feilklassifiseringen har mye å si hvordan feilen er blitt observert. Derfor er også observasjonsmetode tatt med. Videre så er det viktig at en har sporing av feilrapporteringen gjennom en arbeidsordre og tag. For analysen sin del så kan det være fordelaktig å vite om feilen er funnet gjennom funksjonstesting. En enkel og kortfattlig beskrivelse av feilrapporteringen burde også være med for enkelhet skyld da en kan sile ut de feilene som har lite relevans med funksjonaliteten til utstyret.
Dette som en ser i Excel arket vil typisk være en modul i SAP eller andre rapporteringsdatabaser.

Gruppen har tatt med DU-feil som er brukt videre for kalkulering av feilrate og oppdatering av SIF-data. Disse feilene som er lagt inn er fiktive feil, men er feil som kan oppstå i et realistisk anlegg.

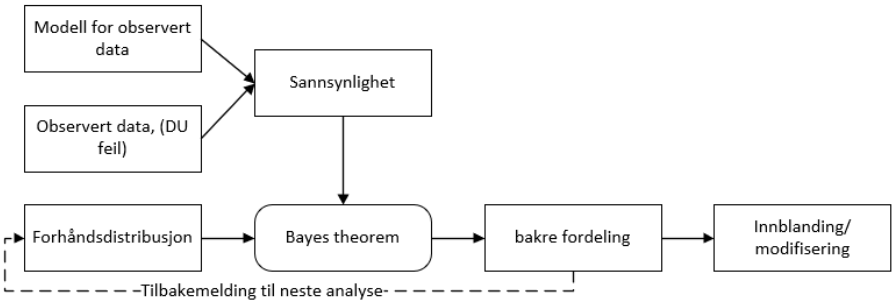
Utstyrsgruppe	gruppe	Feil modus	Observasjonsmetode	Feil klassifisering
Gass detektorer	2	NOO	Kontiniuerlig tilstandsovervåking	SD Feil
Blowdown ventiler	5	DPF	Inspeksjon	NA
Brann detektorer	1	OTH	Funksjonstesting	NA
Prosess transmittere	4	ERO	Tilfeldig observasjon	DU Feil
Prosess transmittere	4	ERO	Funksjonstesting	SD Feil
Gass detektorer	2	NOO	Kontiniuerlig tilstandsovervåking	DD Feil
Gass detektorer	2	OTH	Inspeksjon	NA
Brann detektorer	1	ERO	Periodisk vedlikehold	DU Feil
Blowdown ventiler	5	OTH	Funksjonstesting	NA
Gass detektorer	2	LOO	Funksjonstesting	DU Feil
Blowdown ventiler	5	OTH	Tilfeldig observasjon	NA
Gass detektorer	2	FTF	Kontiniuerlig tilstandsovervåking	DD Feil
Logikk	8	FTF	Kontiniuerlig tilstandsovervåking	DD Feil
Gass detektorer	2	LOO	Kontiniuerlig tilstandsovervåking	DD Feil
Gass detektorer	2	LOO	Kontiniuerlig tilstandsovervåking	DD Feil
Limit switch	7	FTF	Funksjonstesting	NA
Prosess transmittere	4	OTH	Tilfeldig observasjon	NA
Prosess transmittere	4	FTF	Tilfeldig observasjon	DU Feil
Manuelle trykknapper	3	FTF	Funksjonstesting	DU Feil
Shutdown ventiler	6	DOP	Funksjonstesting	DD Feil

Figur 4.10: Utklipp fra feil rapporteringsskjema i vedlegg « Arbeidsfiler»

4.1.3 Estimering av DU-feilrate ved bruk av Bayesian tilnærming

Ved estimering av oppdaterte feilrater λ_{DU} er det anbefalt [6] å bruke Bayesian tilnærmingen da denne er mindre avhengig av operativ erfaring for komponentene. [10] Den gir også mindre svingninger fra observasjonsperiode til observasjonsperiode. I figur 4.11 kan en se framgangsmåten til Bayesian tilnærming.

Figur 4.11: Bayesian dataanalyseprosessen [10]



I kapittel 4.1.3 og kapittel 4.1.4 har vi sammenlignet Bayesian tilnærming og estimering av feilrater ved bruk av operativ erfaring på samme SIF. λ_{DU} er tatt fra appendiks A, antall komponenter og feil er antagelser som er valgt for eksempelet. Driftstid er valgt i henhold til kalkulasjonene som er vist under og vil bli forklart senere. Dette eksempelet kan en finne i vedlegget Excel-arket «Arbeidsfiler»[1] hvor en kan prøve seg på andre kombinasjoner for å finne feil rater.

[1]Se vedlegget i excel ark «Arbeidsfiler» fanen «feilrate estimat tilnærming» for utregninger som vi bli gjennomgått i dette delkapittelet.

SIF-data:[2]

Initiator:	Logikk:	Sluttelement:
Trykktransmitter	PLS	Ventil
Driftstid: 4 år	8 år	3 år
$\lambda_{DU,0}$: 5.00×10^{-7}	1.60×10^{-7}	1.90×10^{-6}
Antall komponenter: 59	98	37
Antall feil: 1	1	0

I SIF-datatabellen ovenfor er det antatt at det er 59 trykktransmittere, 98 PLS'er (logikk) og 37 ventiler (XSV). I driftstiden er det avsløret 1 DU-feil hos logikk og 1 hos initiator i det sikkerhetsinstrumenterte anlegget. Initiator, logikk og sluttelement er blitt vurdert hver for seg. Dette kan en se i de etterfølgende kalkulasjonene.

[2]For beregninger av logikk og sluttelement henvises det til vedlegget «Arbeidsfiler» fanen «feilrate estimat tilnærming».

Initiator

Et konservativt estimat av oppdatert feilrate vil i dette tilfellet bli gitt av formel 4.3 hvor en får $\beta_1 = 2.00 \times 10^6$ og hvis en sjekker om operativ erfaring fra periode 1 er tilstrekkelig ved 3 år kan en se at dette ikke er godt nok. Se kapittel 4.1.4.

$$\beta_i = \frac{1}{\lambda_{DU,0}} \quad \text{, hvor } \alpha_i = 1 \tag{4.3}$$

Forenklet formel for å kalkulere usikkerhetsparameter [6] β_i og α_i for periode i=1

Driftstid / Testperiode 1:

$$T_i = t \times n \tag{4.4}$$

$$T_1 = 3 \times 8760 \times 59 = 1.55 \times 10^6 \quad \text{timer} \tag{4.5}$$

Beregner den samlede driftstiden for perioden i=1

Ved å sjekke om denne driftstiden er lang nok for å kunne anvende tallene må dette sjekkes opp mot[6]:

$$\lambda_{DU,0} \times T1 > 1 \tag{4.6}$$

I dette tilfellet får vi:

$$5.00 \times 10^{-7} \times 1.55 \times 10^6 > 1 \tag{4.7}$$

$$0.78 > 1 \quad \text{, Ikke godkjent} \tag{4.8}$$

Dette vil si at denne test perioden ikke er god nok for å vurderes som en seperat test periode og vi må forholde oss til design λ_{DU}.

Derimot har vi en driftstid på 4 år vil vi få $1.03 > 1$, Godkjent driftstid. Dette samsvare med hva som er beskrevet i SIF-data boksen. Dette betyr at vi må ha 4 års driftstid før vi kan bruke erfaringsdata fra eget anlegg (gjelder transmittere) for bruk av feilraten.

Et konservativt feil estimat av design «Failure rate» estimat [6]:

$$\lambda_{DU-CE,0} = 2 \times \lambda_{DU} \tag{4.9}$$

$$\lambda_{DU-CE,0} = 2 \times 5.00 \times 10^{-7} = 1.00 \times 10^{-6} \quad \text{, per time} \tag{4.10}$$

Oppdatert «Failure rate» estimat for periode 1 [6].

$$\lambda_{DU,1} = \frac{\alpha + x_1}{\beta_1 + T_1} \tag{4.11}$$

$$\lambda_{DU,1} = \frac{1+1}{2.00 \times 10^6 + 2.07 \times 10^6} = 4.90 \times 10^{-7} \tag{4.12}$$

For driftsperiode 1 vil en da ha forandret $\lambda_{DU} = 4.90 \times 10^{-7}$ per timer mot 5.00×10^{-7} per timer som var design λ_{DU}. Dette indikerer at anlegget har en dårligere feilfrekvens enn det som var ved design.

Ved en periode 2 vil en ha en ny observasjons periode eller driftstid (T2) som her i eksempelet er satt til 2 år og vi antar 2 DU-feil har oppstått i denne perioden.

Driftstid / Testperiode 2:

$$T_2 = 2 \times 8760 \times 59 = 1.03 \times 10^6 \quad \text{timer} \tag{4.13}$$

Det konservative estimatet av «failure rate» $\lambda_{DU,1}$ for denne nye perioden (T2) er basert på forkunnskaper fra periode 1 er [6]:

$$\lambda_{DU-CE,1} = \frac{Z_{0.10,2}(\alpha_1 + x_1)}{2(\beta_1 + T_1)} \tag{4.14}$$

Vi anvender formelen for X^2-fordeling også kalt kji-kvadratfordeling med 10% prosentilen i denne kalkulasjonen for nytt estimat av $\lambda_{DU,1}$ [6]

$$\lambda_{DU-CE,1} = \frac{Z_{0.10,2}(1+1}{2(2.00 \times 10^6 + 2.07 \times 10^6)} = 9.56 \times 10^{-7} \tag{4.15}$$

Ny β og α vil da bli [6]:

$$\beta_2 = \frac{\lambda_{DU,1}}{(\lambda_{DU-CE,1} - \lambda_{DU,1})^2} \tag{4.16}$$

$$\beta_2 = \frac{4.90 \times 10^{-7}}{(9.56 \times 10^{-7} - 4.90 \times 10^{-7})^2} = 2.30 \times 10^6 \tag{4.17}$$

$$\alpha_2 = \beta_2 \times \lambda_{DU,1} = 2.30 \times 10^6 \times 4.90 \times 10^{-7} = 1.10 \tag{4.18}$$

Ved andvendelse av formel 4.12 igjen vil en få oppdatert den nye estimerte «Failure rate».

$$\lambda_{DU,2} = \frac{1.1 + 2}{2.30 \times 10^6 + 1.03 \times 10^6} = 9.42 \times 10^{-7} \tag{4.19}$$

Med tanke på at vi har ytterligere 2 feil i testperiode 2 (T2) øker dette feilfrekvensen igjen og vi vil ha en feilfrekvens på 9.42×10^{-7} per timer.

I fanen «Feilrate estimat tilnærming» i excel filen «Arbeidsfiler» vedlegget (se figur 4.12) kan en finne samme kalkulasjoner som er vist ovenfor.

Figur 4.12: Feilrate kalkulasjon for SIF-data

Trykktransmitter				
Forklaring	Beskrivelse		Enhet	Kommentar
	λ DU (NOG 070)	5,00E-07	per time	
	Driftstid	4	År	
	Antall komponenter	59	stk	
	Antall feil (x)	1	stk	
Driftstid / Testperiode 1	T1	2,07E+06	Timer	
Estimated failure rate	λDU-CE,0	1,00E-06	per time	
	β_1	2,00E+06	Faktor	
	α_1	1	Faktor	
Failure estimat periode 1	λDU,1	4,9E-07	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig		1,03		DU,0*T1>1, Hvis Ok, denne test perioden er god nok for å vurdere som en seperat test periode
Driftstid / Testperiode 2	T2	1,03E+06		
	Antall feil (x)	2	stk	
	λDU-CE1	9,56E-07	Per time	
	β_2	2,3E+06		
	α_2	1,1E+00		
Failure estimat periode 2	λDU,2	9,42E-07		

4.1.4 Estimering av DU-feilrate ved bruk av operativ erfaring

Her skal vi se på estimering av DU-feilrate ved bruk av operativ erfaring. Denne tilnærmingen er ikke anbefalt å bruke hvis en ikke har nok operativ erfaring innen spesifikk utstyrsgruppe. Dette skal en få se ved at vi bruker samme eksempelet som er brukt i kapittel 4.1.3.

Operativ erfaring er normalt oppfylt hvis [6]:

$$n \times \tau > 3 \times 10^6 \quad \text{timer} \tag{4.20}$$

Kalkulerer om driftstiden er oppfylt:

$$59 \times 4 \times 8760 > 3 \times 10^6 \quad \text{timer} \tag{4.21}$$

$$2.07 \times 10^6 > 3 \times 10^6 \quad , \text{Ikke godkjent} \tag{4.22}$$

Som en ser blir ikke driftstiden oppfylt og en må ha lenger driftstid på anlegget for å få godkjent driftstid. Da denne estimeringen av feilrate ikke kan brukes vil en ofte bruke design λ_{DU} eller prøve Bayesian tilnærmingen, se kapittel 4.1.3.

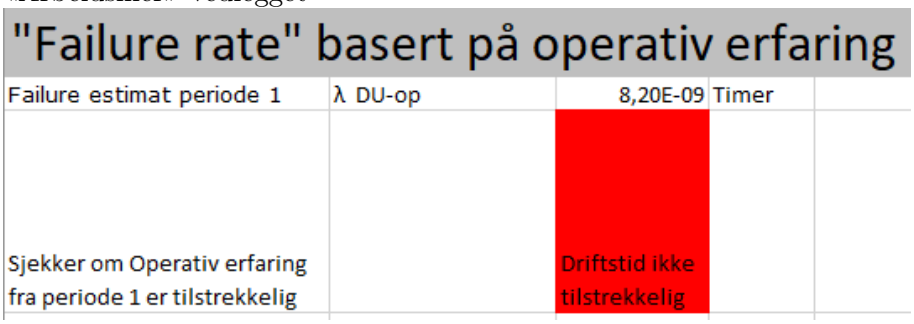
Ved å ha en driftstid på 6 år kan en bruke DU-feilrate fra operativ erfaring. Kalkulasjonen for λ_{DU-op} bli som formel 4.23.

$$\lambda_{DU-op} = \frac{x}{n \times t} \tag{4.23}$$

$$\lambda_{DU-op} = \frac{1}{59 \times 6 \times 8760} = 3,22 \times 10^{-7} \tag{4.24}$$

Ved bruk av samme kriterier som i kapittel 4.1.3 får vi ikke nok driftstid og dermed vil λ_{DU} få helt andre verdier. Disse verdiene vil føre til at en muligens ikke holder SIL-nivåer.

Figur 4.13: Feilrate kalkulasjon for SIF-data ved bruk av operativ erfaring i «Arbeidsfiler» vedlegget



I oppgaven har en brukt Bayesian tilnærmingen da den gir et mer rett estimat på feilraten og hvis den ikke har nok driftstid er design λ_{DU} brukt videre i kalkulasjonene.

4.1.5 Opprettholde SIL-nivået ved bruk av PST

Tradisjonelt sett har en utført en «full stroke test» (FST) av sikkerhetsventiler, men i senere tid har en innført «partial stroke test» (PST) som kan utsette (ikke erstatte) FST-test av sikkerhetsventiler. Det å utføre en PST-test innebærer at ventiler operer innenfor 10%-20% av området for ventilen. Dette kan redusere at ventiler «henger» hvis den ikke blir operert på lang tid og en kan også detektere farlige feil ved at ventilen har blitt operert ved en PST. En av fordelene er også at en ikke har behov for å stanse produksjonen hvis en sikkerhetsventil er stansavhengig for å kunne stenge. Ved å ta en PST vil ikke produksjonen bli noe særlig påvirket og kan gå som vanlig. Dermed kan en forlenge testintervallet for en FST. PST vil ha et eget testintervall i tillegg til FST, men bare oftere. I denne rapporten har en introdusert PST for å kunne forlenge FST. Hvor ofte dette testintervallet er avhengig av ventilen, FST testintervallet, SIL-nivået og PST-dekningsfaktoren. Som nevnt tidligere antas PST-dekningen ofte å ligge mellom 60% og 70%. I denne rapporten har en antatt 65% siden det er tatt utgangspunkt i generiske data for ventiler.

I figur 4.14 og figur 4.15 er det demonstrert på samme SIF (SIF 29) fordelen med å implementere PST. Ved 1 feil på ventiler i test perioden så vil oppdatert testintervall gå ned til 9 mnd, men total budsjettet for SIF vil bli for høyt for SIL-nivået. Ved å implementere 3 mnd PST intervall i tillegg vil SIL-nivået opprettholdes for SIF 29.

Figur 4.14: Viser PFD budsjettet for SIF 29

Data fra Safety Requirement Spesification (SRS)		SIF Nivå (Original design)						SIF Nivå (Oppdatert test intervall)						
SIF Nr.	SIF Navn	SIF Nivå PFDavg Design (Vurder PST viss relevant)	SIL Nivå Design Oppnådd (Vurder PST viss relevant)	Total SIF Nivå Design PFD Budsjett	PFD Design Budsjett Initiator	PFD Design Budsjett Logikk	PFD Design Budsjett Slutt Element	SIF Nivå PFDavg Oppdatert (Vurder PST viss relevant)	SIL Nivå Oppdatert Oppnådd (Vurder PST viss relevant)	Total SIF Nivå Oppdatert PFD Budsjett	PFD Oppdatert Budsjett Initiator	PFD Oppdatert Budsjett Logikk	PFD Oppdatert Budsjett Slutt Element	Vot
29	Dummy SIF 29	9,64E-03	OK	96 %	11 %	21 %	64 %	9,12E-03	OK	91 %	8 %	28 %	55 %	1oo1
29	Dummy SIF 29	9,64E-03	OK	96 %	11 %	21 %	64 %	1,18E-02	SIL Ikke Oppnådd	118 %	8 %	28 %	82 %	1oo1

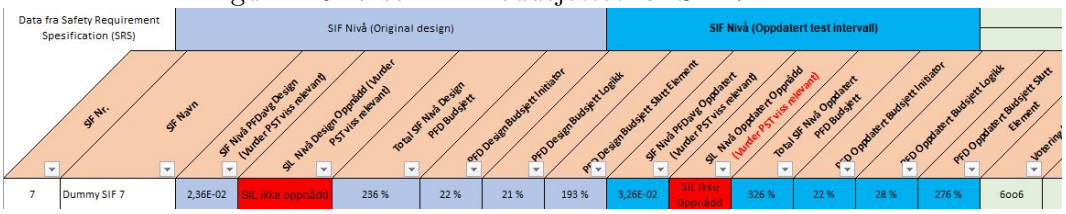
Figur 4.15: Viser PFD budsjettet med oppdatert testintervall med og uten PST

SIF Nivå (Oppdatert test intervall)						Final Element								
						Slutt element sammenlagt								
...esign Budsjett Slutt Element	SIF Nivå PFDavg Oppdatert (Vurder PST viss relevant)	SIL Nivå Oppdatert Oppnådd (Vurder PST viss relevant)	Total SIF Nivå Oppdatert PFD Budsjett	PFD Oppdatert Budsjett Initiator	PFD Oppdatert Budsjett Logikk	PFD Oppdatert Budsjett Slutt Element	Votering (sub-system nivå)	Beta (β) Faktor (sub-system)	Sub-system nivå Test Interval Design (mnd)	Sub-system nivå Oppnåelig test intervall design (mnd)	PST dekning/Coverage	Sub-system nivå PFDavg Design (Vurder PST)	Sub-system nivå Re-evaluert Test intervall design (mnd)	Sub-system nivå Re-evaluert PST Intervall design (mnd)	Sub-system Nivå Oppdatert PFDavg design	
9,12E-03	OK	91 %	8 %	28 %	55 %	1oo1	NA	12	2	65 %	6,44E-03	9	3	5,51E-03	
1,18E-02	SIL Ikke Oppnådd	118 %	8 %	28 %	82 %	1oo1	NA	12	2	65 %	6,44E-03	9	NA	8,21E-03	

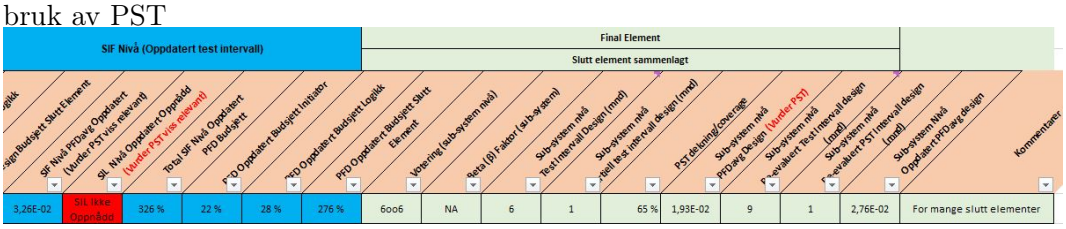
4.1.6 SIL ikke oppnådd ved for mange sluttelementer

I figur 4.16 og 4.17 er det demonstrert at en ikke klarer SIL 2 nivå som er definert for denne SIF (SIF 7) pga for mange sluttelementer. Ergo en har for mange sluttelementer som må fungere (6oo6) for å sikre sikker tilstand ved feil. En får for høy PFD i forhold til hva som er tillatt for spesifisert SIL-nivå 2. Se tabell 2.2
Siden SIF ikke er godkjent fra designfasen burde denne deles opp i flere SIF'er hvis mulig eller gjøre en endring i designet gjennom SIS endringsstyring (MOC). Se kapittel 3.5.1. Mulige design løsninger kan være redundans på ventilene.

Figur 4.16: Viser PFD budsjettet for SIF 7



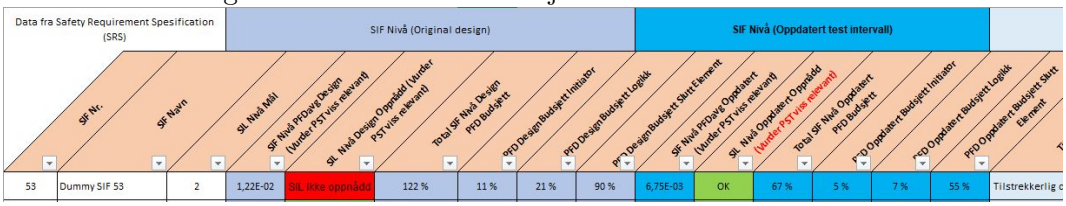
Figur 4.17: Viser at en ikke klarer å oppnå SIL 2 nivået for SIF 7 selv ved bruk av PST



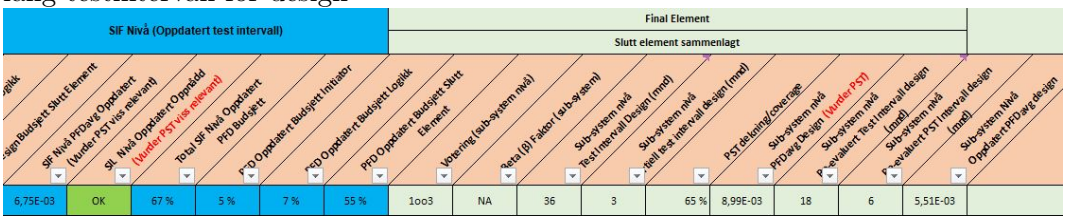
4.1.7 SIL ikke oppnådd ved for lang testintervall på design

I dette eksempelet (figur 4.18 og 4.19) kan en se at det har blitt vurdert et for langt testintervall og en klarer ikke å opprettholde SIL 2 nivået som er definert for denne SIF. Ved å sjekke PFD-design budsjettet kan man se at sluttelementet har hele 90% av PFD-budsjettet for SIL-nivået. Sjekker man videre så er testintervallet for sluttelementet på 3 år (FST) og PST på 3 mnd. Ved å utføre ny kalkulasjon på sluttelementet ender man opp på 18 mnd FST og 6 mnd PST. Dette gjør at vi klarer å holde SIL-nivået ved å øke testintervallet.

Figur 4.18: Viser PFD-budsjettet for SIF 53



Figur 4.19: Viser at en ikke klarer å oppnå SIL 2 nivået for SIF 53 ved for lang testintervall for design

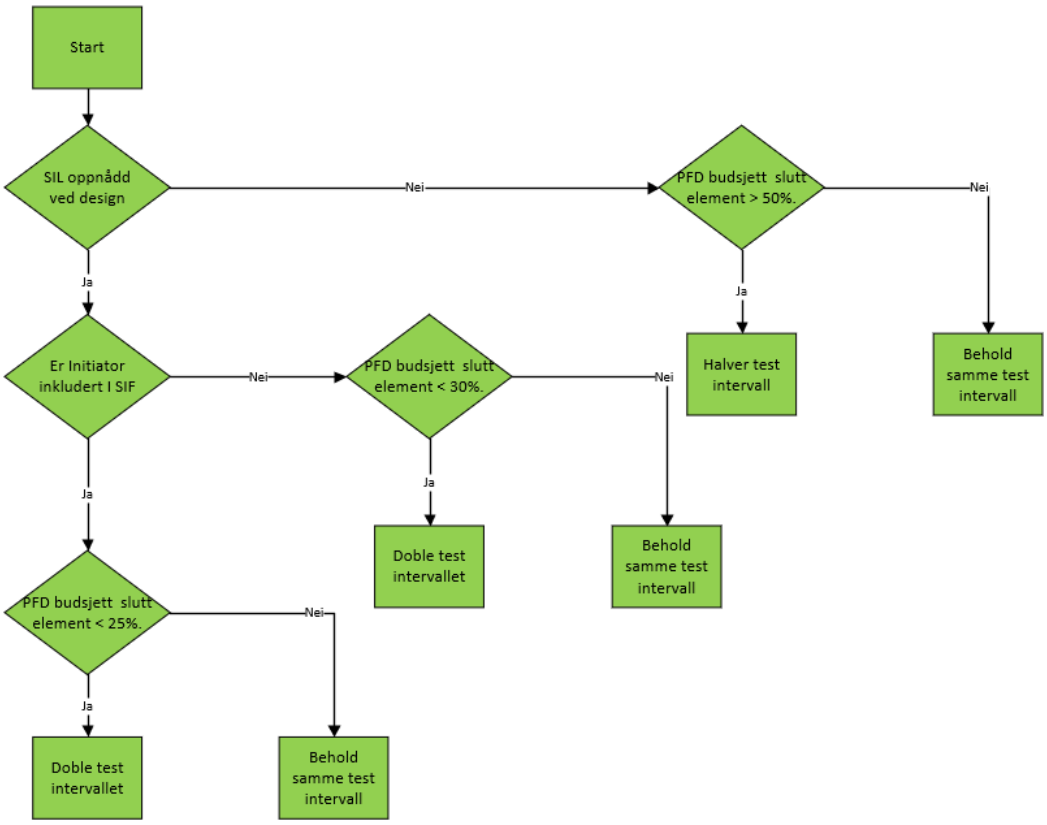


4.1.8 Sammenligne 2 forskjellige metoder

Her er det brukt 2 forskjellige metoder for å vurdere testintervallet for sluttelementene. Se figur 4.21 og figur 4.22. i rad 2, 4 og 6 er metoden som er beskrevet i denne rapporten, mens i rad 1, 3, og 5 er det blitt brukt en metode som var beskrevet i tidligere IEC standard.

Denne metoden utfører noen logiske tester (se figur 4.20) om SIL er oppnådd ved design. Etter å ha utført disse logiske sjekkene beregner den PFD_{avg} ved bruk av formel 5.2

Figur 4.20: Viser de logiske testene i et flytskjema



Slik en kan se av figur 4.21 har en beholdt samme testintervall, men sluttelementet har en større del av PFD budsjettet enn ved metoden som er brukt i denne oppgaven. Det er ikke anbefalt å ha over 50% av budsjettet på ett element, men dette er en vurdering som eierne av anlegget må ta.

Figur 4.21: Viser PFD budsjettet for 3 forskjellige SIF hvor det er brukt 2 forskjellige metoder for oppdatering av testintervallet

Data fra Safety Requirement Spesification (SRS)			SIF Nivå (Original design)						SIF Nivå (Oppdatert test intervall)							
SIF Nr.	SIF Navn	SIL Nivå Mål	SIF Nivå PFDavg Design (Under PST viss relevant)	SIL Nivå Design Oppnådd (Under PST viss relevant)	Total SIF Nivå Design PFD Budsjett	PFD Design Budsjett Initiator	PFD Design Budsjett Logikk	PFD Design Budsjett Slutt Element	SIF Nivå PFDavg Oppdatert (Under PST viss relevant)	SIL Nivå Oppdatert Oppnådd (Under PST viss relevant)	Total SIF Nivå Oppdatert PFD Budsjett	PFD Oppdatert Budsjett Initiator	PFD Oppdatert Budsjett Logikk	PFD Oppdatert Budsjett Slutt Element	Voteri
83	Dummy SIF 91	2	7,58E-03	OK	76 %	0 %	21 %	55 %	6,26E-03	OK	63 %	1 %	7 %	55 %	1oo1	
83	Dummy SIF 92	2	7,58E-03	OK	76 %	0 %	21 %	55 %	4,43E-03	OK	44 %	1 %	7 %	37 %	1oo1	
84	Dummy SIF 93	2	7,58E-03	OK	76 %	0 %	21 %	55 %	6,26E-03	OK	63 %	1 %	7 %	55 %	1oo1	
84	Dummy SIF 94	2	7,58E-03	OK	76 %	0 %	21 %	55 %	4,43E-03	OK	44 %	1 %	7 %	37 %	1oo1	
85	Dummy SIF 95	2	7,58E-03	OK	76 %	0 %	21 %	55 %	6,26E-03	OK	63 %	1 %	7 %	55 %	1oo1	
85	Dummy SIF 96	2	7,58E-03	OK	76 %	0 %	21 %	55 %	4,43E-03	OK	44 %	1 %	7 %	37 %	1oo1	

Figur 4.22: Viser sluttelementene med tilhørende data for 3 forskjellige SIF hvor det er utført 2 metoder for oppdatering av testintervallet

Final Element									
Slutt element sammenlagt									
Logikk / Oppdatert Budsjett Slutt Element	Votering (sub-system nivå)	Beta (β) Faktor (sub-system)	Sub-system nivå Test Intervall Design (mnd)	Sub-system nivå tiell test intervall design (mnd)	PST dekning/coverage	Sub-system nivå PFDavg Design (Under PST)	Sub-system nivå evaluert Test Intervall design (mnd)	Sub-system nivå evaluert PST Intervall design (mnd)	Sub-system Nivå Oppdatert PFDavg design	Kommentarer
1oo1	NA	6	NA	65 %	5,48E-03	6	NA	5,48E-03		Utregning ved bruk av en tidligere IEC standard
1oo1	NA	6	NA	65 %	5,48E-03	4	NA	3,65E-03		
1oo1	NA	6	NA	65 %	5,48E-03	6	NA	5,48E-03		Utregning ved bruk av en tidligere IEC standard
1oo1	NA	6	NA	65 %	5,48E-03	4	NA	3,65E-03		
1oo1	NA	6	NA	65 %	5,48E-03	6	NA	5,48E-03		Utregning ved bruk av en tidligere IEC standard
1oo1	NA	6	NA	65 %	5,48E-03	4	NA	3,65E-03		

Kapittel 5

Diskusjon

Sikkerhets- og pålitelighetsvurderinger bygger på en rekke antagelser om et SIS-system og hvilke forhold dette skal driftes under. Hvis beslutningstakere ikke er klar over usikkerhetsnivået knyttet til deres system kan resultatene bli feiltolket. Personell som jobber med slike system, typisk driftspersonell må også ha en forståelse om viktigheten ved å rapportere riktig slik at ingeniører kan utføre nødvendig og riktige beslutninger for å kunne ha den risk reduksjonen som SIS-systemet er designet for. I tillegg til alle beregninger setter NOG 070 kompetanse krav for definerte roller innen oppfølging av SIS-systemer. Disse rollene er basert på hoved-aktivitetene som er nevnt i kapittel 3.5.1.

Det å bruke generiske data fra NOG 070 eller PDS håndbok for å utføre kalkulasjoner i et SIS-system er mer pålitelig enn å gå for data som er fra leverandørene til utstyret. NOG 070 og PDS håndboken har faktiske tall som er rapportert inn over flere års bruk av utstyret og vil være mer korrekt enn hva som blir oppgitt fra leverandør. I oppgaven er det blitt brukt data fra leverandør til level transmitter radar type da det ikke var oppgitt noen data for denne typen i NOG 070. En kan se at feilrate tallene er svært gode i forhold til andre type transmittere. Se vedlegg og Excel-ark «Arbeidsfiler». Leverandører bruker ofte en «Failure mode and effects analysis» (FMEA) som er en system analyse for pålitelighet. Denne FMEA analysen blir brukt for å identifisere feil rater som er en systematisk og proaktiv metode for evaluering for å identifisere risiko. Det er derfor viktig å forstå at selv om utstyr er SIL sertifisert og har SIL-sertifikater ikke gir noen garanti for at sikkerheten i tiltenkt prosess er bedre. En kan få en god og kanskje bedre sikkerhet ved å utforme et godt design på en prosess ved å bruke utprøvd utstyr i forhold til å bruke SIL-sertifisert utstyr ved en dårlig design av SIS system. Eksempelvis så betyr det ikke at en SIF blir SIL 2 godkjent ved å bruke komponenter som er SIL 2 eller bedre for så å definere SIF sløyfen som SIL 2. Dette er vist gjennom kalkulasjonene som er blitt utført i denne oppgaven.

Systematiske feil har også fått lite oppmerksomhet som blir introdusert under spesifikasjon, design, drift eller vedlikehold / testing, noe som kan føre til svikt

i sikkerhetsfunksjonen under visse forhold i et SIS-system. Disse feilene blir ikke kvantifisert i IEC 61508 og IEC 61511 i motsetning til tilfeldige maskinvarefeil. Det viser seg ifølge Sintef at disse feilene har større frekvens en forutsatt under design og det finnes flere potensielle forbedringsområder. Eksempelvis så kan en unngå kopiering av system til system, men heller utforme design etter forholdene, utføre rot årsak analyser, oppdatere prosedyrer, rutiner og instrukser for installasjonen og heve kompetanse generelt for personell som er involvert i SIS-systemene.

Beslutningstakere for et SIS-system vi bestå av flere ingeniører innen forskjellige disipliner og vil ikke være en enkeltperson i en bedrift eller organisasjon. Det at gruppen som har jobbet med oppgaven bare har elektro- og automasjonsbakgrunn har begrenset en del beslutninger som er foretatt, men er utført etter antagelser i bransjen for olje og energi sektoren. Dette har medført at en stor del av rapporten har blitt å beskrive antagelser som er gjort, hvorfor og gitt en stor oppmerksomhet på teori kapitelet som ellers ikke ville ha vært nødvendig ved en bachelor oppgave.

Foreslått videre arbeid

Som nevnt baserer denne oppgaven seg på designfeil frekvens og design testintervall for å oppdatere dette etter en periode hvor en har hatt feil i de forskjellige utstyrsgruppene som er utarbeidet i metode kapitelet. En tar bare hensyn til udetektert feil når en skal oppdatere testintervallet og vurdere SIL-nivået. Mulig videre arbeid kan være å analysere feilfrekvensene av de farlige detekterte feilene mot de farlige udetekterte feil for å se om det er noen sammenheng i antall farlige feil som oppstår i et SIS-system. En kan evaluere om en skulle ha likestilt farlige detekterte feil med farlige udetekterte feil.

Referanser

[1] Teknisk standard, International Electrotechnical commission, IEC 61511-3:2016 Functional safety - Safety instrumented systems for the process industry - Part 3: Guidance for the determination of the required safety integrity levels, IEC, 2016, 2

[2] Teknisk standard, Sammarbeid prosjekt med operatør selskaper, leverandører, ingeniørselskaper, kontraktører og konsulenter, 070 - Norwegian oil and gas, Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry (Recommended SIL requirements, Norsk olje og gass, 2018, 3,

[3] Teknisk standard, International Electrotechnical commission, IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, IEC, 2010, 2,

[4] Teknisk standard, International Orfanization for Standardization (ISO), ISO 14224:2016 - Petroleumindustri, petrokjemisk industri og naturgassindustri. Innsamling og utveksling av pålitelighets- og vedlikeholdsdata for utstyr, International Orfanization for Standardization (ISO), 2016

[5] Teknisk standard, International Electrotechnical commission, IEC 60079-17:2013 Electrical installations inspection and maintenance, IEC, 2013, 2013

[6] Teknisk rapport, Solfrid Håbrekke (SINTEF), Stein Hauge (SINTEF), Mary Ann Lundteigen (NTNU), Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase, Sintef, 2021, 2

[7] Regelverk for Petroleumsvirksomhet, Innretningsforskriften, https://www.ptil.no/,

[8] Risikonivå i norsk petroleumsvirksomhet, Risikonivå i norsk petroleumsvirksomhet, https://www.ptil.no/, https://www.rnnp.no/,

[9] PFD data, Sintef PDS data handbook, Sintef, 2010, 2010

[10] Bok, Rausand, Barros, Høyland System reliability theory, Wiley, 2021, 3

[11] Bok, Rausland Reliability of safety-Critical Systems, Theory and Applications, Wiley, 2014,

[12] Rapport, Rausand, Lundteigen, The effect of partial stroke testing on the reliability of safety valves, https://www.researchgate.net/, 2007, https://www.researchgate.net/publication/251190143_The_effect_of_partial_stroke_testing_on_the_reliability_of_safety_valves

Vedlegg

- Datablad SIL sertifikat Rosemount 5408 Level Transmitter (Radar)
- Excel ark «Arbeidsfiler»

Appendiks A

Tabell 5.1 inneholder feil rater (λ_{DU}) og PFD_{avg} som er fra NOG 070 [2] og er brukt som design i denne rapporten.

Tabell 5.1: PFD data

SIL - Safety Integrity Level				
Utstyr	Utstyrsgruppe	β	NOG 070 λ_{DU} data	PFD_{avg}
Pressure Transmitter	Process transmitter	6	5.00×10^{-7}	2.20×10^{-3}
Temperature Transmitter	Process transmitter	6	3.00×10^{-7}	1.30×10^{-3}
Level Transmitter[1]	Process transmitter	6	1.00×10^{-6}	4.40×10^{-3}
Level Transmitter[2]	Process transmitter	-	7.90×10^{-8}	3.46×10^{-4}
Smoke Detector	Fire detector	7	5.00×10^{-7}	2.20×10^{-3}
Gas Detector, LOS	Gas detector	7	6.00×10^{-7}	2.60×10^{-3}
Gas Detector, IR Point	Gas detector	7	6.00×10^{-7}	2.60×10^{-3}
Flame Detector	Fire detector	7	5.00×10^{-7}	2.20×10^{-3}
Push Button	Manual Push Button	4	3.00×10^{-7}	1.30×10^{-3}
Flow Transmitter	Process transmitter	6	7.00×10^{-7}	3.10×10^{-3}
I/O Card	Logic	5	1.60×10^{-7}	7.00×10^{-4}
Valve incl. Actuator	Valve[3]	5	1.90×10^{-6}	8.30×10^{-3}
Pilot/solenoid	Solenoid	5	8.00×10^{-7}	2.60×10^{-3}
Generic Circuit Breaker	Circuit Breaker/Relay	5	3.00×10^{-7}	1.30×10^{-3}
Generic relay	Circuit Breaker/Relay	5	2.00×10^{-7}	8.80×10^{-4}

$$PFD = \lambda_{DU} \times \frac{\tau}{2} \tag{5.1}$$

[1] Level Transmitter (Displacement type)
[2] Rosemount 5408 Level Transmitter (Radar) Se vedlegg
[3] Tilhører utstyrsgruppe for blow down ventiler og shutdown ventiler

Appendiks B

Kalkulasjon av PFD ved votering

Formel 5.2 er brukt ved kalkulasjon av PFD hvor en har votering av elementer med mer en 1oo1. Deler av formel 5.2 er blitt brukt for å regne ut tabell 5.2 hvor en også har brukt parametre fra tabell 5.3.

$$C_{MooN} \times \beta \times \lambda_{DU} \times \frac{\tau}{2} + \frac{N!}{(N-M+2)! \times (M-1)!} \times (\lambda_{DU} \times \tau)^{N-M+1} \quad (5.2)$$

Tabell 5.2: PFD kalkulasjon formel

MooN	N	M	C_{MooN} factor	$\frac{N!}{(N-M+2)!\times(M-1)!}$	N-M+1
1oo2	2	1	1.0	0.3333	2
1oo3	3	1	0.5	0.25	3
1oo4	4	1	0.2	0.2	4
1oo5	5	1	0.2	0.1667	5
1oo6	6	1	0.15	0.1428	6
2oo3	3	2	2.0	1	2
2oo4	4	2	0.8	1	3
2oo5	5	2	0.8	1	4
2oo6	6	2	0.6	1	5
3oo4	4	3	2.8	2	2
3oo5	5	3	1.6	2.5	3
3oo6	6	3	1.2	3	4
4oo5	5	4	3.6	3.3333	2
4oo6	6	4	1.9	5	3
5oo6	6	5	4.5	5	2
1oo1	1	1	0	0.5	1
2oo2	2	2	0	1	1
3oo3	3	3	0	1.5	1
4oo4	4	4	0	2	1
5oo5	5	5	0	2.5	1
6oo6	6	6	0	3	1
7oo7	7	7	0	3.5	1

Tabell 5.3: C_{MooN} for forskjellige voteringsparametre (NOG 070)[2]

MooN parametre					
N / M	M=1	M=2	M=3	M=4	M=5
N=2	1.0	-	-	-	-
N=3	0.5	2.0	-	-	-
N=4	0.3	1.1	2.8	-	-
N=5	0.2	0.8	1.6	3.6	-
N=6	0.15	0.6	1.2	1.9	4.5

Appendiks C

Tabell 5.4 viser til maks responstid for forskjellige typer sikkerhetsutstyr. For detektorer er S-001:2020 kapittel 13.4.7 brukt, Logikk S-001:2020 kapittel 11.4.5 og for sikkerhets ventiler S-001:2020 kapittel 10.4.5, hvis ikke annet er evaluert under design av systemene vil 1s/tommer være gjeldende.

Tabell 5.4: Respons tid

Element	Gruppe	Størrelse	Response tid (s)
Gass detektor	-	-	2
Logikk	-	-	2
Sikkerhetsventiler	<22 tommer	0,5	1
Sikkerhetsventiler	<22 tommer	1	2
Sikkerhetsventiler	<22 tommer	2	4
Sikkerhetsventiler	<22 tommer	3	6
Sikkerhetsventiler	<22 tommer	4	8
Sikkerhetsventiler	<22 tommer	5	10
Sikkerhetsventiler	<22 tommer	6	12
Sikkerhetsventiler	<22 tommer	7	14
Sikkerhetsventiler	<22 tommer	8	16
Sikkerhetsventiler	<22 tommer	9	18
Sikkerhetsventiler	<22 tommer	10	20
Sikkerhetsventiler	<22 tommer	11	22
Sikkerhetsventiler	<22 tommer	12	24
Sikkerhetsventiler	<22 tommer	13	26
Sikkerhetsventiler	<22 tommer	14	28
Sikkerhetsventiler	<22 tommer	15	30
Sikkerhetsventiler	<22 tommer	16	32
Sikkerhetsventiler	<22 tommer	17	34
Sikkerhetsventiler	<22 tommer	18	36
Sikkerhetsventiler	<22 tommer	19	38
Sikkerhetsventiler	<22 tommer	20	40
Sikkerhetsventiler	<22 tommer	21	42
Sikkerhetsventiler	≥22 tommer	22	43

Appendiks D

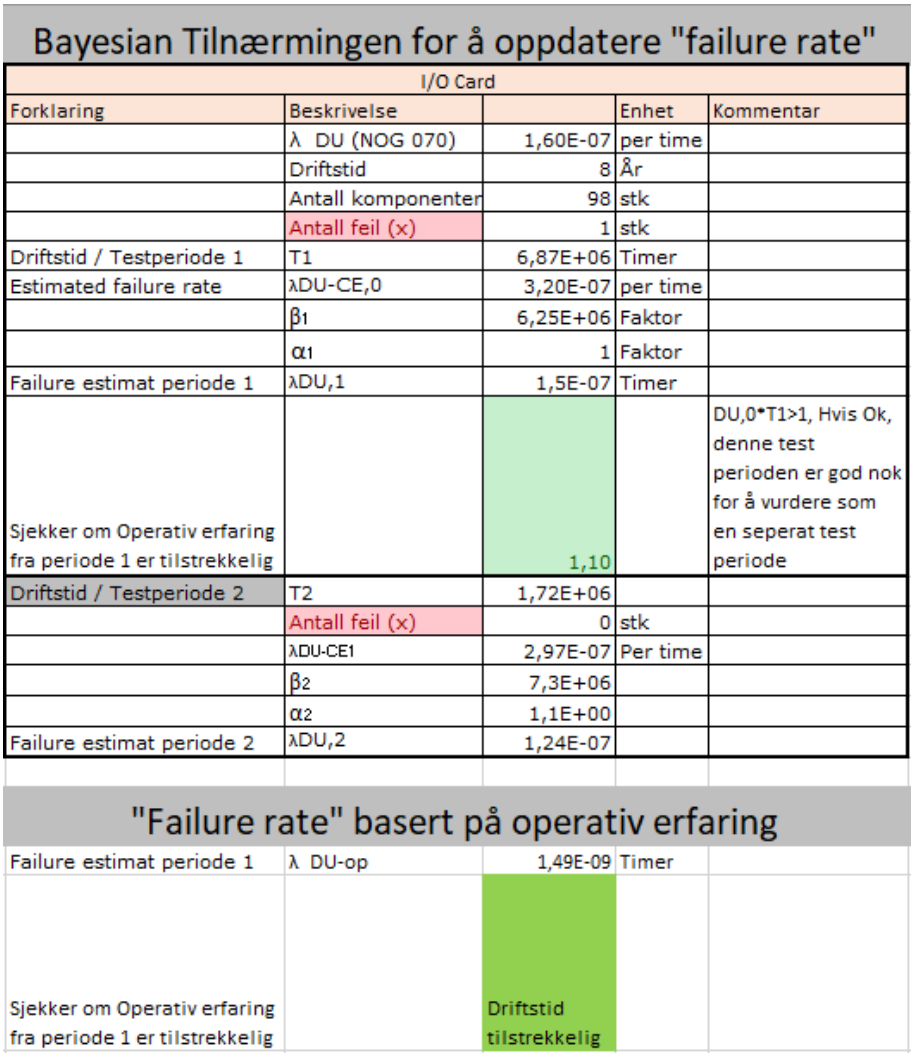
Trykktransmitter				
			Enhet	Kommentar
	λ DU (NOG 070)	5,00E-07	per time	
	Driftstid	4	År	
	Antall komponenter	59	stk	
	Antall feil (x)	5	stk	
Driftstid / Testperiode	T1	2,07E+06	Timer	
Estimated failure rate	DU-CEi	1,00E-06	per time	
	DU-CEi			
	Betai	2,00E+06	Faktor	
	Betai			
	alpha1	1	Faktor	
	DU,1	1,5E-06	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig	DU,0	1,03		DU,0*T1>1, Hvis Ok, denne test perioden er god nok for å vurdere som en seperat test periode
	T2	1,03E+06		
	DU-CE1	9,56E-07	Per time	
	Beta2	5,5E+06		
	alpha2	8,1E+00		
Failure estimat	DU,2	1,55E-06		
M1 metode	Tau,0	6	Måneder	
Timer mellom test intervall	Ti	1,27E+03	Timer	
Måneder mellom test intervall	T1	1,74	måneder	
	"T1"	1	måneder	
Periode 2	Driftstid (år)	3	År	
	Antall feil (x)	0	stk	
	Ti	4,57E+03	Timer	
	T2	6,26	Måneder	
	"T2"	6	Måneder	
M2 metode	Tau,0	6	Måneder	
	Budget	1	% Antatt	
	Ti	1,16E+04	timer	
	T1	15,9	Måneder	
	"T1"	12	Måneder	

Figur 5.1: MS-Excel feil rate kalkulasjon for trykktransmitter

Appendiks E

Bayesian Tilnærmingen for å oppdatere "failure rate"				
Trykktransmitter				
Forklaring	Beskrivelse		Enhet	Kommentar
	λ DU (NOG 070)	5,00E-07	per time	
	Driftstid	4	År	
	Antall komponenter	59	stk	
	Antall feil (x)	1	stk	
Driftstid / Testperiode 1	T1	2,07E+06	Timer	
Estimated failure rate	λDU-CE,0	1,00E-06	per time	
	β_1	2,00E+06	Faktor	
	α_1	1	Faktor	
Failure estimat periode 1	λDU,1	4,9E-07	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig		1,03		DU,0*T1>1, Hvis Ok, denne test perioden er god nok for å vurdere som en seperat test periode
Driftstid / Testperiode 2	T2	1,03E+06		
	Antall feil (x)	2	stk	
	λDU-CE1	9,56E-07	Per time	
	β_2	2,3E+06		
	α_2	1,1E+00		
Failure estimat periode 2	λDU,2	9,42E-07		
"Failure rate" basert på operativ erfaring				
Failure estimat periode 1	λ DU-op	8,20E-09	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig		Driftstid ikke tilstrekkelig		

Figur 5.2: MS-Excel feil rate Bayesian og operativ erfaringsmetoden, initiator



Bayesian Tilnærmingen for å oppdatere "failure rate"				
I/O Card				
Forklaring	Beskrivelse		Enhet	Kommentar
	λ DU (NOG 070)	1,60E-07	per time	
	Driftstid	8	År	
	Antall komponenter	98	stk	
	Antall feil (x)	1	stk	
Driftstid / Testperiode 1	T1	6,87E+06	Timer	
Estimated failure rate	λDU-CE,0	3,20E-07	per time	
	β_1	6,25E+06	Faktor	
	α_1	1	Faktor	
Failure estimat periode 1	λDU,1	1,5E-07	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig		1,10		DU,0*T1>1, Hvis Ok, denne test perioden er god nok for å vurdere som en seperat test periode
Driftstid / Testperiode 2	T2	1,72E+06		
	Antall feil (x)	0	stk	
	λDU-CE1	2,97E-07	Per time	
	β_2	7,3E+06		
	α_2	1,1E+00		
Failure estimat periode 2	λDU,2	1,24E-07		
"Failure rate" basert på operativ erfaring				
Failure estimat periode 1	λ DU-op	1,49E-09	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig		Driftstid tilstrekkelig		

Figur 5.3: MS-Excel feil rate Bayesian og operativ erfaringsmetoden, logikk

Bayesian Tilnærmingen for å oppdatere "failure rate"				
Valve incl. Actuator				
Forklaring	Beskrivelse		Enhet	Kommentar
	λ DU (NOG 070)	1,90E-06	per time	
	Driftstid	3	År	
	Antall komponenter	35	stk	
	Antall feil (x)	0	stk	
Driftstid / Testperiode 1	T1	9,20E+05	Timer	
Estimated failure rate	λDU-CE,0	3,80E-06	per time	
	β_1	5,26E+05	Faktor	
	α_1	1	Faktor	
Failure estimat periode 1	λDU,1	6,9E-07	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig		1,75		λDU,0*T1>1, Hvis Ok, denne test perioden er god nok for å vurderes som en seperat test periode
Driftstid / Testperiode 2	T2	6,13E+05		
	Antall feil (x)	0		
	λDU-CE1	2,69E-06	Per time	
	β_2	1,7E+05		
	α_2	1,2E-01		
Failure estimat periode 2	λDU,2	1,52E-07		
"Failure rate" basert på operativ erfaring				
Failure estimat periode 1	λ DU-op	0,00E+00	Timer	
Sjekker om Operativ erfaring fra periode 1 er tilstrekkelig		Driftstid ikke tilstrekkelig		n*t ≥ 3,00E+06, Hvis Ok, denne test perioden er god nok for å vurderes som en seperat test periode

Figur 5.4: MS-Excel feil rate Bayesian og operativ erfaringsmetoden, slutt-element