Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: **Risikostyring, offshore sikkerhet.** **Master i teknologi.**	Vårsemesteret, 2013 Konfidensiell
Forfatter: **Åge Kristiansen**	…… (signatur forfatter)
Fagansvarlig: **Roger Flage (UiS)** Veileder(e): **Roger Flage (UiS)** **Erik Korssjøen (Kongsberg Maritime)**	
Tittel på masteroppgaven: **Dokumentasjon av krav i IEC 61511-1 og usikkerhet knyttet til SIL**	
Studiepoeng: 30	
Emneord: IEC 61511-1 Instrumenterte sikkerhetssystem Sikkerhetsintegritetsnivå Usikkerhet og antakelser GAP-analyse	Sidetall: 77 Stavanger, 17. Juni 2013

FORORD

Oppgaven ble skrevet ved instituttet for industriell økonomi, risikostyring og planlegging ved Universitetet i Stavanger (UiS) og markerer avslutningen på en 2-årig masterstudie innen risikostyring. Den ble skrevet våren 2013 i samarbeid med Kongsberg Maritime, som gav meg en problemstilling, tilgang til prosjektdokumentasjon og utstyr som gjorde det mulig å fullføre oppgaven. Arbeidet med masteroppgaven har gitt meg stor innsikt i IEC 61511-standarden [1], noe som er særdeles nyttig ved arbeid med instrumenterte sikkerhetsfunksjoner i olje- og gassindustrien.

Jeg vil takke faglig ansvarlig og veileder ved UiS, førsteamanuensis Roger Flage, for god faglig veiledning, gode råd og innspill underveis. Jeg vil også takke Erik Korssjøen i Kongsberg Maritime for forslag til oppgave, godt samarbeid og råd underveis. En stor takk rettes også til min samboer Therese, som har vært til stor støtte, både med ekstra tak på hjemmefronten og som korrekturleser.

Kongsberg 16. juni 2013

Åge Kristiansen

SAMMENDRAG

I olje- og gassektoren stilles det strenge krav til sikkerhetssystemer hvor det er særdeles viktig å ha et system man kan stole på når en farefull hendelse kan oppstå. Instrumenterte sikkerhetssystem (SIS) er uavhengige systemer, som skal fungere som barrierer for å forhindre farlige hendelser. IEC 61511-1 [1] setter både kvalitative og kvantitative pålitelighetskrav til SIS, og er derfor en viktig standard for leverandører og brukere av slike sikkerhetssystemer.

Denne oppgaven består først av en litteraturstudie, hvor man ser på regelverket gitt av Petroleumstilsynet (PTIL), feil som kan oppstå i et SIS og de forskjellige livstidsfasene. Videre blir det sett nærmere på usikkerheter og antakelser som kan ligge bak kvantifiserte pålitelighetstall, som blir presentert i prosjekter hvor IEC 61511-1 [1] er gjeldene. Kravene i IEC 61511-1 [1] må dokumenters at de er oppfylt og antakelser som har blitt gjort under design må komme tydelig fram. Det kan bli både kostbart og tidkrevende for en leverandør hvis kravene ikke er godt dokumentert med en god struktur som har sporbarhet tilbake til alle gitte krav. Med en god dokumentasjon blir det også enklere å verifisere at kravene er oppfylt.

For å redusere usikkerheter rundt antakelser som kan bli gjort under design av sikkerhetsutstyret, blir det foreslått et merkesystem, hvor alt utstyr som skal benyttes i et SIS blir merket. Når sikkerhetsutstyret er merket med begrensinger til blant annet miljøforhold, som tilsvarer de forhold som ble antatt under design, kan man få et mer pålitelig utstyr ved at designantakelser og reelle forhold er samstemte.

Å kunne dokumentere på en oversiktlig og strukturert måte er viktig for å kunne ha sporbarhet tilbake til kravene i IEC 61511-1 [1] og kundens SRS. Det er også viktig å inkludere oppfyllelse av kravene til programvaren i SAR, hvor programvaren til hver SIF blir vist på en strukturert og oversiktlig måte. Sikkerheten til utstyret som brukes i en SIS må opprettholdes igjennom alle livsfasene til systemet, og derfor må det være et dokument som beskriver begrensningene for eksempel til verktøy og brukerprogramvare.

INNHOLD

1 INNLEDNING

Instrumenterte sikkerhetssystemer blir mye brukt i dagens prosessindustri som en av flere barrierer for å forhindre, kontrollere eller begrense farlige hendelser. Petroleumstilsynet sine forskrifter krever at et prosessanlegg skal ha fungerende barrierer som kan kontrollere farlige hendelser, og bringe prosessen tilbake til en sikker tilstand [2]. Men det skal også stilles krav til ytelsen til en barriere, og her setter IEC 61511-1 [1] integritetskrav til et instrumentert sikkerhetssystem, både kvantitative og kvalitative, for på den måten få verifisert om systemet har tilfredsstillende pålitelighet.

1.1 Bakgrunn og motivasjon

For en underleverandør som leverer utstyr til et instrumentert sikkerhetssystem kan kravene til design og dokumentasjon variere etter kundens ønske. IEC 61511-1 [1] er en internasjonal standard, utgitt av International Electrotechnical Commission i 2003, for å standardisere kravene til et instrumentert sikkerhetssystem i et prosessanlegg. Den bygger på den generiske standarden IEC 61508 [3] og er utviklet spesielt for prosessindustrien for velprøvd utstyr/ maskin- og programvare som har et begrenset eller fast programspråk. Det er derfor flere og flere brukere av SIS som ønsker at nye sikkerhetssystemer oppfyller kravene til IEC 61511-1 [1], og at de kan dokumenteres i alle livstidsfaser. Dette stiller igjen krav til at leverandørindustrien har kjennskap til kravene og kan dokumentere disse. Det er derfor viktig å få kartlagt hva kravene til de forskjellige instrumenterte sikkerhetsfunksjonene er i IEC 61511-1 [1], slik at kravene er tydelig dokumentert og man lett kan verifisere om sikkerhetssystemene er i henhold til de kravene som er gitt.

En vanlig praksis for en leverandør, og som kunden ofte stiller krav til, er at utstyret blir sertifisert. Det vil si at et eksternt firma, som for eksempel TÜV Rheinland eller Exida, validerer og tester utstyret i henhold til en standard, som IEC 61508 [3]. Resultatet av testen blir vanligvis utgitt med en rapport og et sertifikat som viser forskjellige pålitelighetstall. På den måten kan en leverandør dokumentere at utstyret kan bli inkludert i en SIS hvor det er krav til at IEC 61508 [3] skal følges. Men det er viktig å vite hva som ligger bak pålitelighetstallen. Hvilke antakelser om ble gjort og om det er usikkerhet i tallene. Hvis det for eksempel ble antatt at utstyret kan stå i et utstyrsrom på en båt, kan det da stå i et kjøretøy på land? Det er derfor viktig at alle antakelser som ble gjort, og usikkerheten som ligger i pålitelighetstallene er grundig dokumenter for å forhindre at utstyret blir brukt på en feil måte.

Kongsberg Maritime leverer i dag kontrollsystemer til en rekke instrumenterte sikkerhetssystemer i prosessindustrien innenfor det maritime miljøet. Det kan være brann- og gassanlegg, nødavstengningssystemer eller styresystemer for sidepropeller.

Kongsberg Maritime sitt sikkerhetssystem har blitt validert og sertifisert av en internasjonal bedrift opp mot den generiske standarden IEC 61508 [3]. De ønsker derfor å se nærmere på

sporbarheten til sikkerhetsfunksjonene i dokumentasjonen, og å kartlegge hvordan kravene skal dokumenteres på en god måte i henhold til IEC 61511-1 [1]. Dette gjelder spesielt med tanke på brukerprogramvaren, da denne varier ut fra kundens ønske. Videre, som nevnt tidligere, er der også viktig å se om antakelser som har blitt gjort under designen av utstyret står tydelig beskrevet i dokumentasjonen.

Med dette håper Kongsberg Maritime å øke kvaliteten på gjennomføringen av prosjekter og å kunne dokumentere alle krav på en oversiktlig og standardisert måte med sporbarhet tilbake til krav fra kunden og IEC 61511-1 [1]. I tillegg er det viktig å øke bevisstheten rundt usikkerhet og antakelser som kan ligge bak pålitelighetstall som blir presentert fra for eksempel sertifiseringsbedrifter.

1.2 Problemstilling

Det denne oppgaven omhandler er instrumenterte sikkerhetssystem og kravene i IEC 61511-1 [1] fra en leverandør av sikkerhetsutstyr til olje- og gassindustrien sitt ståsted. Hovedpunktene som skal gjennomgås er da følgende:

- Hva et instrumentert sikkerhetssystem er og hvilke feil som kan oppstå.
- Er det antakelser og usikkerhet rundt pålitelighetstall og hvordan skal disse eventuelt komme tydelig fram?
- Hvordan dokumentere, på en god og oversiktlig måte, at kravene i IEC 61511-1 [1] er oppfylt og har sporbarhet tilbake til gitte krav?

Oppgaven vil beskrive hva et instrumentert sikkerhetssystem er og forskjellige typer feil som kan oppstå igjennom livstidløpet. Videre vil antakelser og usikkerhet som kan ligge bak pålitelighetstall bli diskutert, og det blir gitt en mulig løsning på hvordan antakelser fra design kan komme tydeligere fram.

For å se på dokumentasjon og hvordan oppfyllelse av kravene i IEC 61511-1 [1] kan bli vist, tas det utgangspunkt i et leveringsprosjekt fra Kongsberg Maritime (KM). Gjennom en GAP-analyse skal prosjektdokumentasjonen til KM bli vurdert opp mot kravene for å se om alle relevante krav i henhold til leveringen er god dokumentert. Prosjektet som jeg skal se nærmere på er en drillrigg hvor Kongsberg Maritime har levert kontrollsystemet, og en bestemt instrumentert sikkerhetsfunksjon i et sikkerhetssystem blir utgangspunktet for analysen, for å kartlegge dokumentasjon og sporbarhet.

1.3 Avgrensninger

Denne oppgaven er begrenset til bruken av IEC 61511-1 [1] i leveringsprosjekt for underleverandør av sikkerhetsutstyr, og omfatter kun sikkerhetsfunksjoner som inneholder elektriske-/ elektroniske-/ programmerbare elektroniske komponenter. Det betyr at fokuset vil være på de punktene og kapitlene i IEC 61511-1 [1] som en typisk underleverandør skal oppfylle. Med det menes at

- fare og risikovurdering,
- tildeling av sikkerhetsfunksjoner til beskyttelseslag,
- uavhengig validering og
- styresystem for planlegging og gjennomføring av funksjonell sikkerhet,

kun blir nevnt.

For å begrense arbeidsomfanget i GAP-analysen har det blitt valgt én instrumentert sikkerhetsfunksjon i et prosjekt, gjennomført av Kongsberg Maritime, til å utføre analysen på. Den er også begrenset til prosjektdokumentasjonen og det som står beskrevet der. Hovedansvaret for hele livssyklusen til SIS ligger hos eieren, og derfor er GAP-analysen også begrenset til kun å omfatte de deler av livssyklusen som Kongsberg Maritime var involvert i, det vil si at kapittel 6 - 9 og 13 - 18 i IEC 61511-1 [1] ikke er inkludert i analysen. Kapittel 13 er også kun en veiledning til fabrikk aksepttesten (FAT).

Da oppgaven baserer seg på «IEC 61511-1 [1] vil definisjoner og uttrykk ha samme betydning som i den standarden.

1.4 Definisjoner/ forklaringer

AIM 2000: Dette er systemplattformen for kontroll og overvåking som Kongsberg Maritime bruker for sikkerhetssystemer og selvstendige systemer [4].

Feilrate: IEC 61508 [3] definerer feilrate som en pålitelighetsparameter $\lambda(t)$ til en enhet (enslig komponent eller et system) slik at $\lambda(t).dt$ er sannsynligheten for feil av enheten innen $[t, t + dt]$ forutsatt at den ikke har feilet i løpet av $[0, t]$. I «nyttig liv»-fasen er feilraten til en enslig komponent mer eller mindre konstant, $\lambda(t)= \lambda$.

Fellesfeil: IEC 61511-1 [1] beskriver to typer fellesfeil: Fellesårsaksfeil og fellesmodusfeil.

Fellesmodusfeil: Lik feil i to eller flere kanaler som forårsaker det samme feilaktige resultat [1].

Fellesårsaksfeil: Feil, som er et resultat av en eller flere hendelser, forårsaker feil i to eller flere adskilte kanaler i et flerkanalssystem, som fører til systemfeil [1].

Instrumentert sikkerhetsfunksjon: Sikkerhetsfunksjon med et spesifisert sikkerhetsintegritetsnivå som er nødvendig for å oppnå funksjonell sikkerhet. Det kan enten være en instrumentert sikkerhetsbeskyttelsesfunksjon eller en instrumentert sikkerhetskontrollfunksjon [1].

Instrumentert sikkerhetssystem: Instrumentert system brukt til å implementere en eller flere sikkerhetsfunksjoner [1].

K-Safe: Kongsberg Maritime sitt sikkerhetssystem [5] og er en del av AIM 2000.

Programvaremodul: En programvaremodul er en uavhengig programvarerutine som utfører en algoritme og kommuniserer med andre moduler og/ eller inngangs-/ utgangssystemet via inngangs- / utgangsterminaler. Hver modul består av et grafisk symbol, en programvarealgoritme og en tilhørende datastruktur som er unik for hver konkrete modul [6].

Pålitelighet: Et uttrykk for evnen en komponent eller et system har til å utføre en tiltenkt funksjon. (Aven [7]).

Risiko: Kombinasjon av frekvensen av hendelse til skade, og alvorlighetsgraden til den skaden [1].

Sikkerhetsbarriere: Enten et fysisk eller ikke fysisk hjelpemiddel som er påtenkt å forhindre, kontrollere eller begrense uønskede hendelser eller ulykker. (Sklet [8]).

Skanningsoppgaver: En del av programvaresystemet som administrer utførelsen til funksjonsmoduler, og som også skanner de tilkoblede I/O-kortene. Skanningsoppgaven kontrollerer også tid- og utførelsessekvens [6].

Tvangskjøring: Tvangskjøringsfunksjonen skal sette utgangssignal til en forhåndsbestemt tilstand, uavhengig av forandringer i logikktilstander [6].

Undertrykking: Utkobling av en sikkerhetsaksjon, men tillater visning av tilhørende alarmer i tillegg til manuell/ automatisk kontroll [6].

Usikkerhet: Graden av tvil i vår evne til å fange inn de relevante faktorer i modeller, dataen og/ eller kalkulasjonene. (Lundteigen [9])

Visningsvindu (VDU): Det visuelle grensesnittet mellom kontrollsystemet (AIM 2000) og operatøren [6].

1.5 Forkortelser

AIM – Advanced Integrated Multifunction System
C&E – Årsak og virkning
CAP – Kritisk aksjonspanel
CAT – Kundens aksepttest
DC – Diagnostisk dekning
DCR – Kontrollrommet til boring
DMS – Document Management System
ECR – Kontrollrommet til motoren
EMC - Elektromagnetisk kompatibilitet
EUC – Utstyr under kontroll
FAT – Fabrikkens aksepttest
FMEA – «Feilmodus og effekt»-analyse
FOST – Final Output Stage Test
HFT – Toleransen til maskvarefeil
HMI – «Menneske og maskin»-grensesnitt
IAT – Intern aksepttest
ICMS – Integrated Control and Monitoring System
IEC- International Electrotechnical Commission
I/O – Inngang/ utgang
KFDD – Kongsberg Functional Design Document
KM – Kongsberg Maritime
LAN – Lokalt nettverk
MTTR - Gjennomsnittlig gjenopprettelsestid
NP – Ikke-programmerbar (Non-programmable)
PE – Programmerbar elektronikk
PES – Programmerbart elektronisk system
PFD – Sannsynligheten for å feile ved behov
PFH – Sannsynligheten for å feile per time
PTIL - Petroleumstilsynet
RAIC – Remote Analogue Input Card
RCU – Remote Controller Unit
RDIO – Remote Digital Input/ Output Card
RIO – Remote Input Output Card
SFF – Fraksjon av sikre feil
SPBus – Simrad Process Bus
SPHub – Simrad Process Hub
SPTerm – Simrad Process Terminal
SIF – Instrumentert sikkerhetsfunksjon
SIS – Instrumentert sikkerhetssystem
SIL – Sikkerhetsintegritetsnivå
VDU – Visningsvindu
VMS – Fartøyets styringssystem

1.6 Oppgavens struktur

Oppgaven vil begynne med en forklaring på hva et instrumentert sikkerhetssystem er, hva det inneholder og hvilket regelverk som gjelder for et slikt system. Videre kommer en beskrivelse av forskjellige typer feil som kan oppstå, både i programvaren og maskinvaren og gjennomgang av livssyklusen til et typisk SIS.

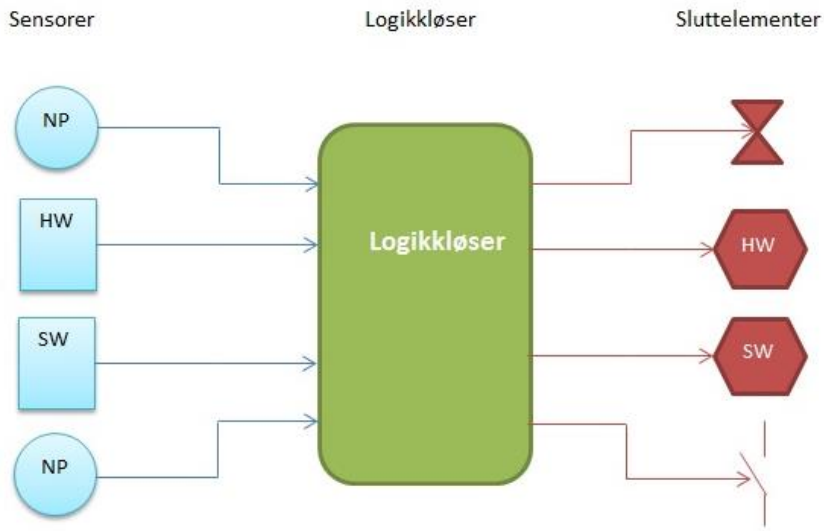
Oppgaven ser videre på antakelser og usikkerhet som kan ligge bak pålitelighetstall og hvilke begrensninger de kan gi SIS. Det blir så lagt fram et forslag til hvordan eventuelle antakelser som har blitt gjort under designen av utstyr til SIS kan komme tydelig fram.

Videre vil det være fokus på et leveringsprosjekt fra Kongsberg Maritime, med en beskrivelse av prosjektet og det sikkerhetssystemet som blir levert. Prosjektdokumentasjonen fra Kongsberg Maritime vil så bli gjennomgått i en GAP-analyse etterfulgt av en oppsummering og forslag til forbedring. Til slutt vil hele oppgaven bli oppsummert i en konklusjon.

2 INSTRUMENTERTE SIKKERHETSSYSTEM

I prosessindustrien er det mange hendelser som kan gjøre prosessen ustabil og føre til skade på mennesker, miljø og fysiske verdier. For å opprettholde en høy sikkerhet i et prosessanlegg er det derfor nødvendig med et system som bringer anlegget tilbake i sikker tilstand hvis noe kritisk skulle skje, som for eksempel høyt trykk i et rør. Denne oppgaven har et instrumentert sikkerhetssystem (SIS) som fungerer som en av barrierefunksjonene i et prosessanlegg.

Oppbygningen til et instrumentert sikkerhetssystem er vist i figur 2.1 og består hovedsakelig av en hvilken som helst kombinasjon av sensorer, logikkløsere og sluttelementer.



Figur 2.1, eksempel på et instrumentert sikkerhetssystem (basert på figur 7 i [1]**)**

Når en uregelmessighet blir detektert av en sensor, vil logikken behandle signalet den mottar og sende ut et signal til et sluttelement, som vil utføre en aksjon. Hvilke aksjoner som blir aktivert ligger i programvaren og/ eller i maskinvaren til logikkløseren. Inngangssignaler kan være votert slik at det krever M utav N sensorer for å aktivere gitte utganger. Et M-utav-N-system, for eksempel 2-utav-3, blir ofte brukt i branndeteksjon for å redusere falske alarmer ved at det kreves to detektorer for å bekrefte at det virkelig er en brann, mens en detektor kan for eksempel kun gir alarm i kontrollsystemet [10]. En bestemt sikkerhetsfunksjon som blir utført av SIS, enten en kontrollfunksjon eller beskyttelsesfunksjon, kalles for en instrumentert sikkerhetsfunksjon (SIF). Et eksempel på en SIF kan være at ved deteksjon av flamme skal brannpumpene starte. En flammedetektor vil da ved aktivering sende et signal til logikkløseren som vil aktivere et utgangssignal, som igjen vil starte brannpumpen.

En vanlig måte i olje og gassindustrien er å dele SIS inn etter hvilken funksjon de har [9]. For eksempel kan alle SIF som skal aktivere utstyr til bruk i nødavstengning, være i

nødavstengningssystemet (ESD). Andre SIS kan typisk være brann- og gassystem (F&G) og prosessnedstengningssystemer (PSD).

Det er også forskjell på behovet til forskjellige SIF, det vil si hvor ofte man forventer at det er behov for en aktivering. Noen SIF er det kontinuerlig behov for, som for eksempel sidepropeller på en båt for å holde fartøyet på rett plass. For andre SIF, som for eksempel en ventil som skal lukke hvis det er overtrykk i en tank, kan man forvente at behovet er mindre.

En nærmere forklaring rundt begrepene kommer senere i oppgaven, men først skal vi se litt på regelverket fra Petroleumstilsynet (PTIL).

2.1 Regelverk

Når man leverer utstyr til bruk i et SIS som kan benyttes i petroleumsvirksomhet på norsk sokkel er det viktig å vite hvilket regelverk som gjelder, og vi skal derfor se litt nærmere på Petroleumstilsynet (PTIL) sitt regelverk og forskrifter. Rammeforskriften § 11 [11] forteller oss noe om prinsippene for risikohåndtering, blant annet at risiko skal reduseres så langt det er praktisk mulig, og styringsforskriften § 4 [2] sier at de ansvarlige skal velge løsninger som reduserer sannsynligheten for at det oppstår skade, feil eller fare-/ ulykkessituasjoner. Videre i styringsforskriften § 5 [2] står det at barrierer skal opprettes for å redusere sannsynligheten for at feil og fare-/ ulykkessituasjoner utvikler seg og for å begrense mulige skader og ulemper. Det skal også være tilstrekkelig uavhengighet mellom barrierene, der hvor det er nødvendig med flere enn en barriere.

Forskriftene omfatter også innsamling av data, og styringsforskriften § 19 [2] sier at data som har betydning for helse, miljø og sikkerhet skal samles inn og bli brukt til overvåking og kontroll av tekniske, operasjonelle og organisatoriske forhold. Dette er viktig med tanke på kvantitativ pålitelighet og feilrater, da data som blir samlet inn kan brukes til å opprette generiske databaser for feilrater basert på erfaringsdata. Man kan også da få vurdert om de feilratene som er antatt under design stemmer overens med de reelle feilratene. Dataene skal også brukes for å se på effektiviteten av vedlikeholdet, som skal evalueres systematisk til forbedring av vedlikeholdsprogrammet (aktivitetsforskriften § 49 [12]).

Ser man i innretningsforskriften § 8 [13] står det blant annet at en innretning skal være utstyrt med nødvendige sikkerhetsfunksjoner som til enhver tid kan
a) oppdage unormale tilstander,
b) hindre at unormale tilstander utvikler seg til fare- og ulykkessituasjoner,
c) begrense skadene ved ulykker.
Det skal fastsettes krav til ytelsen for sikkerhetsfunksjoner. Status for sikkerhetsfunksjoner skal være tilgjengelig i det sentrale kontrollrommet.

Som vi ser skal det fastsettes krav til ytelsen til sikkerhetsfunksjonen og man må da kunne dokumentert at sikkerhetsfunksjonen har den ytelsen som kravet tilsier. Ser man under veiledningen til forskriften, refererer PTIL til IEC 61508 [3] og OLF-070 [14] som stiller kvantitative og kvalitative krav til ytelse og veiledning på hvordan de skal oppfylles.

En annen viktig ting er å ha oversikt over sikkerhetssystemet og hvilke deler av det som eventuelt er ute av drift. Aktivitetsforskriften § 26 [12] stiller krav til tiltak og begrensninger som gjelder når det er nødvendig med overbroing eller utkobling av hele eller deler av sikkerhetssystemet. Det skal foreligge en statusoversikt over alle overbroinger, utkoblinger og andre svekkelser slikt at en til enhver tid har kontroll på hvilke sikkerhetsfunksjoner som er gjeldende. Nødvendige forhåndsregler, som for eksempel brannvakter eller vakt med gassmåler, må da gjennomføres for å opprettholde sikkerheten som den funksjonen skulle ha hatt.

IEC 61511-1 [1] **og OLF-070** [14]
Vi så at PTIL, under veiledningen til innretningsforskriften § 8 [13], refererer til IEC 61508 [3]. IEC-61508 [3] er en generisk standard som setter krav til alle livssyklusaktivitetene for systemer som inneholder elektriske og/ eller elektroniske og/ eller programmerbare elektroniske (E/E/PE) elementer som blir benyttet til å utføre en sikkerhetsfunksjon. IEC 61511-1 [1] er en standard som er utviklet for prosessindustrien, innenfor rammeverket av IEC 61508 [3], og som dekker hele livsløpet til SIS. Brukerveilederen OLF-070 [14] ble utviklet i samarbeid med oljeindustrien og Oljeindustriens Landsforening (OLF), og skal virke som en retningslinje for bruk av IEC 61508 [3] og IEC 61511-1 [1] i den norske oljeindustri, med det formålet å forenkle bruken av standardene.

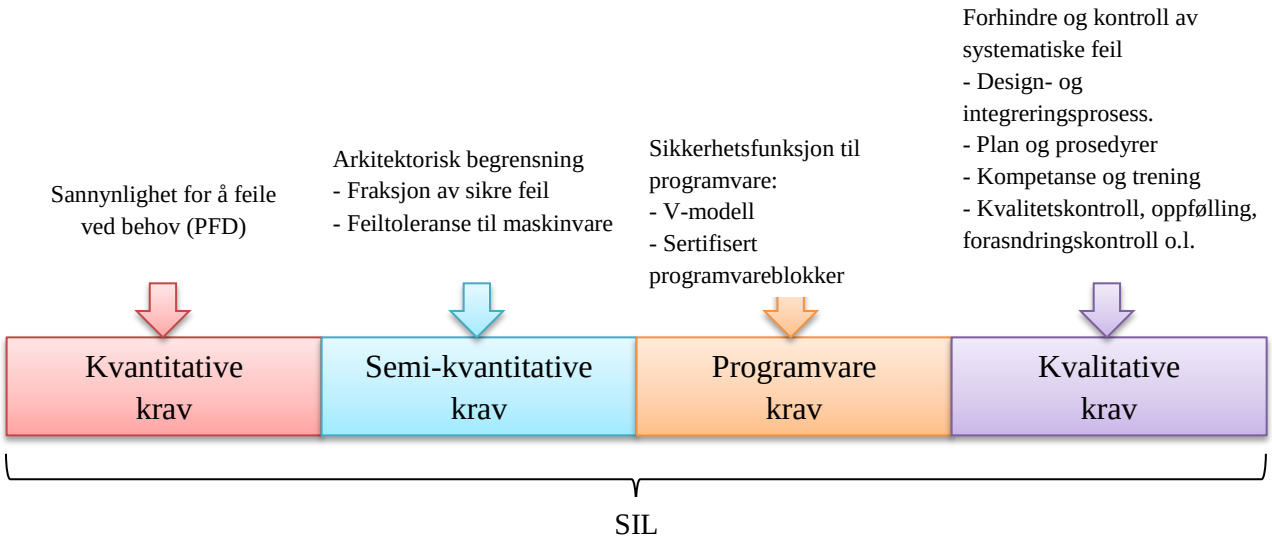
2.2 Feil i et instrumentert sikkerhetssystem

I et SIS stilles det krav til pålitelighet da sikkerhetssystemet er en del av barrierestrategien for å redusere risikoen, og med en feil i SIS øker risikoen for at en farlig hendelse kan eskalere. Det er mange typer feil som kan oppstå i et SIS, alt fra svikt i maskinvare, menneskelige feil, dårlig design som gjør systemet ustabilt eller fellesfeil, som kan få hele systemet til å svikte. En vanlig måte å kategorisere feil på er å skille mellom tilfeldig maskinvarefeil, systematiske feil og fellesfeil [15]. Maskinvarefeil er feil som oppstår i utstyret på grunn av redusert levetid og slitasje mens systematiske feil er feil som er årsaksbestemte hvor man ikke kan, i motsetning til maskinvarefeil, bytte ut en komponent med en identisk for å fjerne feilen [1]. En fellesfeil oppstår når en enslig feil resulterer i en korresponderende feil i flere komponenter [15].

IEC-61511-1 [1] setter krav til påliteligheten til SIS, både når det gjelder rene kvantitative krav, som sannsynligheten for at funksjoner skal feile, og kvalitative krav som prosedyrer og validering av utstyr og programvare. Påliteligheten til SIS er kategorisert i IEC 61511-1 [1] ved hjelp av fire sikkerhetsintegritetsnivå (SIL1-4), hvor det ikke bare er krav til hver enkel

komponent i systemet, men også til hele sikkerhetssystemets design og operasjon igjennom hele livsløpet [16]. SIL 4 er det strengeste kravet, altså det sikkerhetsnivået hvor krav til pålitelighet og gjennomføring er strengest og til SIL 1 stilles det lavest krav. For utvikling og modifikasjon av brukerprogramvare til SIF, gjelder de samme kravene for SIL 1 til SIL 3. Hvor kravet til SIL-nivået er 4 kan ikke IEC 61511-1 [1] benyttes, da må man bruke IEC 61508 [3].

En oversikt over de forskjellige kravkategoriene som settes til en SIF er vist i figur 2.2.1.



Figur 2.2.1, en oversikt over forskjellige krav til SIL (basert på figur i [17]**).**

Man ser ut fra figur 2.2.1 at det er både kvalitative og kvantitative krav for å oppfylle et SIL-nivå. I tillegg er det viktig at det gitte SIL-nivået opprettholdes igjennom hele livssyklusen til SIS.

2.2.1 Kvantitative og semi-kvantitative krav

IEC 61511-1 [1] skiller mellom to ulike operasjonsmoduser, behovsmodus og kontinuerlig modus. Med behovsmodus menes det at SIF kun blir aktivert når prosessen gir et behov. For eksempel en avstengingsventil som kun skal stenge hvis trykket i en tank er over et gitt nivå. Med en farlig feil i ventilen vil prosessen være trygg så lenge trykket i tanken ikke stiger over den fastsatte grensen. For SIF i behovsmodus er det derfor svært viktig å teste funksjonen med faste mellomrom for å få verifisert at den virker. Denne testen kalles for funksjonstesten og skal teste hele SIF med et fast tidsintervall τ. Siden denne testen skal avdekke udetekterte farlige feil, er det viktig at testen blir gjennomført ved at funksjonen aktiveres under så realistiske forhold som mulig. For SIF som opererer i kontinuerlig modus, det vil si at behovet for funksjonen er større enn en gang i året [3], vil SIF kontinuerlig forhindre farlige hendelser, og ved en farlig feil i SIF vil en potensiell farefull situasjon oppstå hvis ikke det har blitt tatt spesielle aksjoner for å forhindre det.

Tilfeldig maskinvarefeil

En tilfeldig maskinvarefeil er en feil som kan oppstå til en tilfeldig tid i alle deler av et system og omfatter feil i selve komponentene til sikkerhetsfunksjonene, fra sensorene til sluttelementene [1]. Den er et resultat av den begrensede levetiden til maskinvaren, der aldring og stress er viktige faktorer. Kravene i IEC 61511-1 [1] omfatter to pålitelighetsaspekter til maskinvaren. Det er kvantitative mål for å fastsette et pålitelighetsnivå til sikkerhetsfunksjonen og nødvendige begrensninger i arkitekturen for å sikre en nødvendig feiltoleranse til maskinvaren [16]. For å beregne den kvantitative påliteligheten til en komponent benyttes de egenskapene at en tilfeldig maskinvarefeil oppfører seg likt, og er ikke avhengig av arkitekturen eller designen til systemet. Komponenten har altså den samme feilraten uavhengig av systemet, og ved å benytte feilrater til komponenten kan man beregne sannsynligheten for at komponenten ikke fungerer.

Denne verdien kalles sannsynligheten for å feile ved behov, PFD [14]. For SIF som opererer i behovsmodus beregner man PFD_{avg}, også kalt MFDT (Mean Fractional Dead Time) [7]. Man kan beregne PFD_{avg} ved bruk av følgende formel, der testintervallet for en funksjonstest er gitt ved τ [14]:

$$PFD_{avg} \approx \frac{1}{2} \cdot \tau \cdot \lambda_{DU}$$

Feilraten, λ_{DU}, er den totale raten til udetekterte farlige feil. Med udetekterte menes at feilen ikke har blitt oppdaget av diagnostiske tester, men at den kun kan bli oppdaget av en funksjonstest eller ved et behov fra prosessen. IEC 61511-1 [1] definerer farlige feil som: «Feil som har potensiale til å føre det instrumenterte sikkerhetssystemet i en farlig eller feiler-å-fungere tilstand.» Feil som blir oppdaget av diagnostiske tester, og som blir utbedret med en gang, blir klassifisert som raten av farlige detekterte feil, λ_{DD}. Dette gjelder under den antakelsen at detekterte farlige feil blir reparert umiddelbart og at SIL-nivået bli opprettholdt med alternative metoder mens reparasjonen pågår. Raten av sikre feil, $\lambda_{s,}$ er den raten av feil som ikke har potensiale til å føre SIF i en farlig eller feiler-å-fungere tilstand [1]. Det kan være for eksempel at en sensor aktiveres uten å nå alarmgrensen, slik at sikkerhetsfunksjonen aktiveres uten at faren er tilstede, under den forutsetning at sikkerhetsfunksjonen går til en sikker tilstand.

En måte å gjøre feil sikre er å designe sikkerhetsfunksjonen slik at hvis en feil oppstår så vil systemet gå til en sikker tilstand. For eksempel er elektromagneter som holder branndører åpne normalt spenningssatte og vil miste spenningen under en aksjon. Hvis en elektromagnet slutter å fungere vil branndørene likevel lukkes og anlegget vil gå til en sikker tilstand.

For SIF i behovsmodus blir PFD_{avg} sjekket opp mot tabell 3 i IEC 61511-1 [1] som setter krav til PFD-verdiene for å oppnå forskjellige SIL-nivå. For SIF i kontinuerlig modus blir PFD per time sammenlignet med tabell 4.

Toleransen til maskinvarefeil

IEC 61511-1 [1] stiller også krav til arkitekturen til maskinvaren, basert på de ulike feilratene til komponentene, for å kunne tilfredsstille et bestemt SIL-nivå. Dette kravet kalles toleransen til maskinvarefeil (HFT) og begrenser friheten til designen av sikkerhetsfunksjonene. En HFT på 1 betyr at i et «1-utav-2»- eller «2-utav-3»-system vil systemet fortsatt fungere selv om en av komponentene er ute av drift. Man vil altså ha en fungerende SIF selv om en av komponentene i funksjonen feiler.

IEC 61511-1 [1] sier at hensikten med minimum HFT er å demme opp for potensielle mangler i designen av SIF, som følge av antakelser gjort i designen sammen med usikkerhet i feilratene til komponentene eller delsystemer. Hvis en hendelse skjer, og det instrumenterte sikkerhetssystemet inneholder en uoppdaget feil i en komponent, er det viktig å ha et redundant system for å opprettholde barrierens funksjon. Det stilles derfor krav at alle komponentene i et SIF, fra sensoren til sluttelementet, skal ha minimum toleranse for maskinvarefeil. Begrepet fraksjon av sikre feil, SFF, blir brukt for å bestemme kravet til maskinvarefeiltoleransen til de forskjellige SIL-nivåene. SFF brukes til å måle andelen av sikre feil mot den totale feilraten. En måte å regne ut SFF på er ved hjelp av denne formelen [14]:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}}$$

Raten av sikre feil, λ_S, og farlige detekterte feil, $\lambda_{DD,}$ blir summert og dividert på den totale feilraten til komponenten ($\lambda_{TOT} = \lambda_S + \lambda_{DD} + \lambda_{DU}$) og hvis prosentandelen av sikre feil er under verdiene gitt i tabell 5 og tabell 6 i IEC 61511-1 [1] for et gitt SIL-nivå, stilles det større krav til HFT. IEC 61511-1 [1] skiller mellom kompleksiteten til komponentene, det vil si at programmerbare elektroniske logikkløsere har strengere krav til HFT (tabell 5) enn sensorer, sluttelementer og ikke-programmerbare elektroniske logikkløsere (tabell 6).

2.2.2 Systematisk integritetssikkerhet

En systematisk feil er en feil som har blitt til på en deterministisk måte og som kun kan fjernes ved å gjøre endringer i designen eller i produksjonsprosessen, operasjonsprosedyrer og lignende [1]. PDS-metoden [18], som er en metode utviklet av SINTEF [19] for å kvantifisere pålitelighetsmål knyttet til SIS, argumenterer for at kun ved å kvantifisere tilfeldige maskinvare feil vil man bare få en begrenset andel av de reelle feil. Det blir derfor foreslått en metode på hvordan bidraget til systematiske feil også kan inkluderes i kvantifisert pålitelighetsmål [16]. Men denne metoden skal vi ikke gå innpå i denne oppgaven.

Istedenfor benyttes kvalitative krav, som prosedyrer og styringsverktøy, for å minimalisere sannsynligheten for systematiske feil. Det er mange mulige årsaker for at en systematisk feil kan oppstå, og den kan skje i alle faser i sikkerhetssystemets levetid. Noen mulige feilkilder kan være

feil i programvaren, dårlig design, installasjonsfeil eller operasjonsfeil [20]. En måte å detektere systematiske feil på er å simulere årsakene til at feilen oppstår og derfor er testing av systemet en svært viktig metode for å kvalitetssikre, og øke den systematiske integritetssikkerheten.

Programvarefeil kan være et resultat av feil i selve programmeringen, kompilatorfeil eller feil under oppgradering. Designen til programmet kan også være dårlig strukturert slik at mange unødvendige feil og feilmeldinger oppstår som kunne vært fjernet med en smartere løsning. Det er derfor viktig at programvaren er enkel, oversiktlig og testbar for å redusere muligheter for systematiske feil. IEC 61511-1 [1] anbefaler bruk av velprøvde programvaremoduler, hvor brukerprogramvaren blir utviklet ved en kombinasjon av disse, noe som gir et oversiktlig brukerprogram.

2.2.3 Fellesfeil

IEC 61511-1 [1] ser på to typer av fellesfeil:

Felles-årsak feil: Feil som kommer av en eller flere hendelser, og forårsaker feil i to eller flere separate kanaler i et multikanalssystem, som fører til systemfeil. For eksempel kan denne type feil være kabelbrudd i en felleskabel til to redundante sensorer, som forårsaker at begge feiler.

Felles-tilstandsfeil: Felles-tilstandsfeil er samme feil i to eller flere kanaler som forårsaker det samme feilaktige resultat. Et eksempel på denne type feil er to identiske redundante komponenter fra samme leverandør i en SIF, som på grunn av samme hendelse feiler. En hendelse kan være tåke, som feilaktig aktiverer to identiske gassdetektorer i en «2-utav-3»-funksjon. En måte å unngå denne type feil på er å benytte ulike teknologier [21], for eksempel en trykkmåler og en vektsensor for å måle nivået i en tank. Hvis en hendelse skjer som forårsaker feil på trykkmålere vil man fortsatt kunne måle nivået med vektmåleren.

Det er spesielt viktig i designfasen å ha fokus på fellesfeil, og SIS bør være designet slik at sannsynligheten for fellesfeil blir redusert. Man ser her at uavhengighet er en nøkkelfaktor i forhindring av fellesfeil, og IEC 61511-1 [1] setter krav til, og anbefaler vurdering av uavhengighet igjennom hele livssyklusen for komponenter, forskjellige systemer og beskyttelseslag. Med beskyttelseslag menes hvilken som helst uavhengig mekanisme som reduserer risiko ved kontroll, avverging eller begrensning [1].

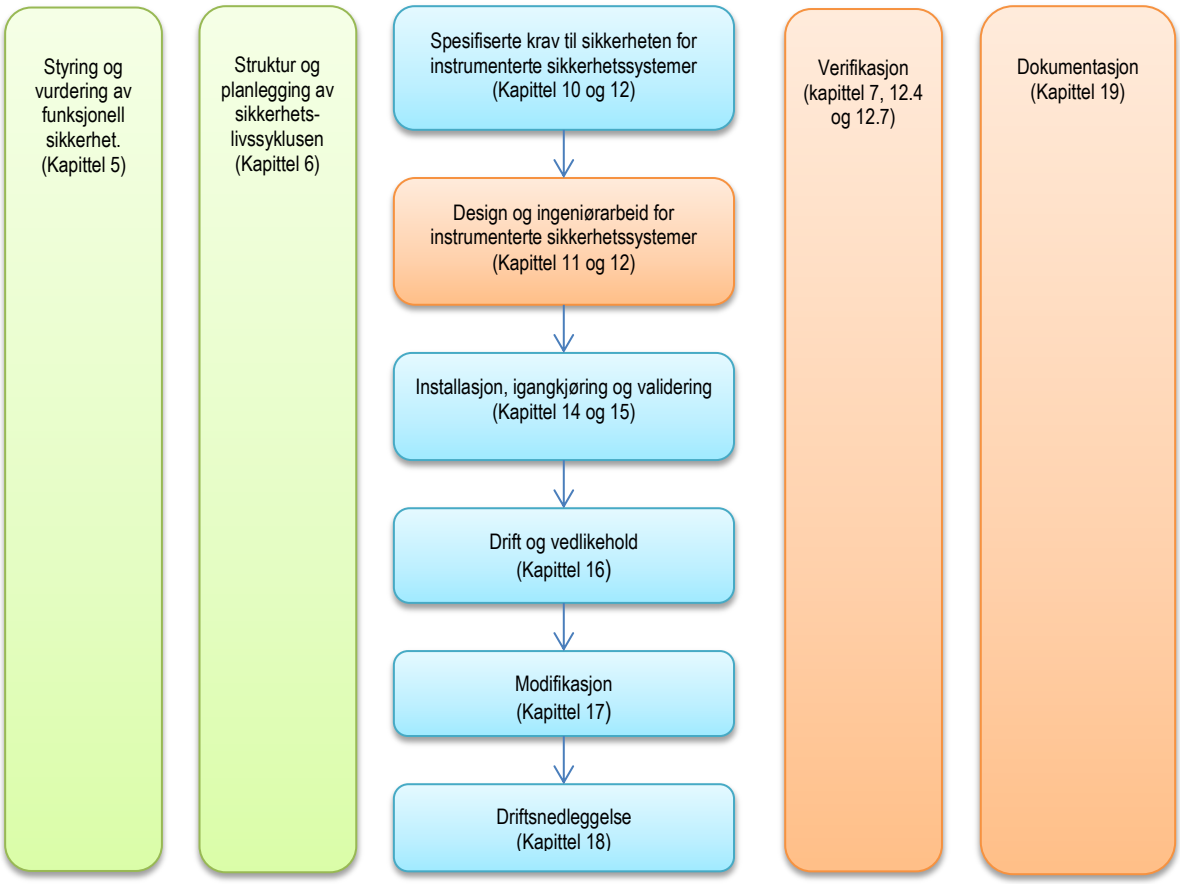
Fellesfeil er klassifisert som avhengighetsfeil [22] og kan ikke klassifiseres som tilfeldig maskinvarefeil og kan derfor heller ikke kvantifiseres med konstant feilrate til komponentene. For å kompensere for fellesfeil, bruker man en β-faktor i utregning av påliteligheten til tilfeldige maskinvarefeil, og benytter β-faktoren-modellen som vist i OLF-070 [14]. Der ser man at en forenklet måte å beregne PFD_{avg} i et 1-utav-2 system, er å multiplisere PFD_{avg} med β-faktoren. PFD-metoden [18] er en utvidet versjon av β-faktoren-modellen og er mye brukt i den norske

oljeindustrien [23]. Den skiller mellom ulike voteringer, som 1-utav-3 og 2-utav-3, ved å tilføre en C_{MooN}-faktor. β_{MooN} er da C_{MooN} mulitiplisert med β. Dette står også beskrevet i OLF-070 [14].

I IEC 61508 [3] del 6 kan man finne verdien til β-faktoren, hvor man blant annet besvarer spørsmål i tabell D1, og ut fra svarene får man forskjellige verdier. Den enkleste måten er å bruke de mest konservative verdiene, som for logikkløsere er 5 % og for sensorer og sluttelementer 10 %.

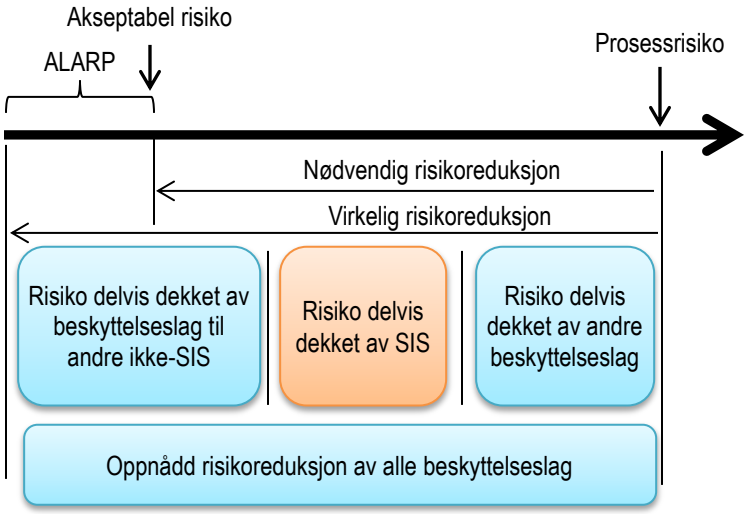
2.3 Livssyklus til SIS

Kravene i IEC 61511-1 [1] dekker hele sikkerhetslivssyklusen til SIS fra designfasen til driftsnedleggelse. Kravene som ikke er beskrevet i detalj er risikoanalyser og tildeling av sikkerhetsfunksjoner til beskyttelseslag, altså krav til beskyttelse, mengde og type. En oversikt over en typisk livssyklus til et SIS for en leverandør er vist i figur 2.3.1, der hovedkravene vil ligge i design- /ingeniørarbeidsfasen, verifikasjon, som interne tester, og dokumentasjon, kapittel 11, 12 og 19 i IEC 61511-1 [1]. Men det er viktig for en underleverandør å gi nødvendig informasjon til alle de forskjellige fasene og aktivitetene.



Figur 2.3.1, livssyklus til SIS (basert på figur 8 i IEC 61511-1 [1]**).**

Fare- /risikovurdering og tildeling av sikkerhetsfunksjoner til beskyttelseslag
I IEC 61511-1 kapittel 5.2.3 står det at farer skal bli identifisert, risiko skal bli evaluert og den nødvendige risikoreduseringen skal bli bestemt. Figur 2.3.2 viser en oversikt over en generell metode å redusere risiko på der man ser at SIS er en del av et barrieresystem sammen med andre barrierer, for å kunne redusere risikoen til et akseptabelt nivå.



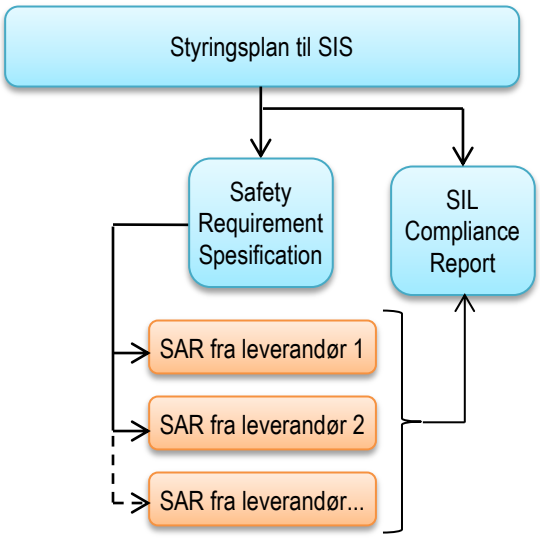
Figur 2.3.2, oversikt over en generell risikoreduksjon (basert på figur 1.1 i OLF-070 [14]**).**

Man må derfor verifisere at SIS, og dermed hver SIF, reduserer risikoen tilstrekkelig slik at den totale risikoreduksjonen er innenfor grensen til den akseptable risikoen. I OLF-070 [14] står minimumskravet til SIL beskrevet for en del sikkerhetsfunksjoner og delfunksjoner som er vanlige i norsk olje – og gassindustri. Det er derfor vanlig å benytte denne metoden for å bestemme SIL-kravet til de forskjellige SIF. For andre funksjoner som ikke er beskrevet der må metoder som Layer Of Protection Analysis (LOPA) benyttes [24].

IEC 61511-1 [1] gir ikke detaljerte krav til risikovurdering og tildeling av sikkerhetsfunksjoner til beskyttelseslag, men setter krav til at disse aktivitetene skal gjennomføres.

Dokumentasjon

Figur 2.3.3 gir en oversikt over en typisk dokumentflyt i et prosjekt med de dokumentene som er viktige for å kunne dokumentere at krav i henhold til IEC 61511-1 [1] er oppfylt.



Figur 2.3.3, dokumentasjon av SIS (basert på figur i [17]**).**

Styringsplanen til SIS: Den består av et eller flere dokumenter som skal inneholde planleggingen av de forskjellige livstidsfasene til SIS, hvor hver fase blir definert med betingelser til informasjon, resultat og valideringsaktiviteter. Det /de skal også beskrive styringsaktivitetene som er nødvendige for å forsikre at de funksjonelle sikkerhetsmålene blir nådd.

Safety Requirement Spesification (SRS): Dette dokumentet inneholder spesifiserte krav til designen av SIF for å oppnå et bestemt sikkerhetsintegritetsnivå [14].

Safety Analysis Report (SAR): For å dokumentere at kravene i SRS har blitt oppfylt må leverandørene av utstyr til SIS levere en SAR hvor kravene er dokumentert. En SAR er påkrevd i OLF-070 [14] som også gir et eksempel på innhold i et slikt dokument.

SIL Compliance Report: Denne rapporten dokumenterer om SIS er i henhold til IEC 61511-1 [1] og de kravene som er gitt i SRS, med utgangspunkt i SAR fra leverandørene.

Styring og vurdering av funksjonell sikkerhet

Styringen og kontroll av prosesser som dekker hele livsløpet til SIS er helt nødvendig for at et SIS skal kunne operere sikkert igjennom hele livstidsløpet. IEC 61511-1 [1] stiller for eksempel krav til kompetanse, prosedyrer som skal være på plass, hvilke aktiviteter som skal gjennomføres og evaluering av endelig løsning. Resultatet blir vanligvis dokumentert i ett eller flere

styringsdokumenter. Det er viktig at en styringsplan, for å sikre at krav til integritetsnivå og funksjonell sikkerhet blir møtt, er etablert så tidlig som mulig i et prosjekt, og at det blir fulgt opp gjennom alle prosjektfaser.

Validering

En av nøkkelaktivitetene i styring av funksjonell sikkerhet er verifikasjons- og valideringsaktiviteter for å forsikre at det ønskede sikkerhetsnivået har blitt nådd. Viktige verifikasjonsaktiviteter er vurderinger og tester i alle faser, fra interne tester under design til ferdigstillelsestester under installasjon. Funksjonstesten er også en viktig del av valideringen og skal være klart beskrevet i et vedlikeholdsprogram. Typiske valideringstester for en leverandør av sikkerhetsutstyr, som logikkløsere, vil være interne aksepttester (IAT), fabrikkakseptester (FAT) hvor utstyret blir testet for eksempel hos ingeniørselskapet eller verft og kundeaksepttest (CAT) hvor eieren av utstyret verifiserer at utstyret er godkjent til den oppgaven det er tiltenkt.

Spesifiserte krav til sikkerheten (SRS)

Alle spesifikke krav til sikkerhetssystemet og komponentene blir beskrevet i ett eller flere dokumenter som vanligvis kalles for Safety Requirements Specification (SRS) [14] og som legger grunnlag for designen og ingeniørarbeidet til SIS. Dokumentene skal følge hele livsfasen til SIS og bli oppdatert hvis ny informasjon eller endringer skjer i løpet av forskjellige livsfasene. Innholdet i SRS skal dekke kravene i IEC 61511-1 kapittel 10 [1] som blant annet stiller krav til:

- Design og arkitektur.
- Pålitelighet og tilgjengelighet.
- Støttesystemer.
- Testintervaller og vedlikehold.
- Maskinvarespesifikasjoner.
- Menneskelig maskingrensesnitt.
- Programvare.

IEC 61511-1 [1] stilles også krav til utvikling av brukerprogramvaren og sier at det skal være en SRS for dette. SRS inneholder også krav til pålitelighet og data knyttet opp til den kvantitative beregningen av integritetsnivået, som blant annet frekvensen på testintervall, feilrater på utstyret som skal brukes og beregnede gjennomsnittsreparasjonstid. Det er derfor viktig ved endringer av SIS at SRS også blir endret slik at man finner rett informasjon og de antakelser som har blitt gjort.

Design og utvikling av SIS
Kravene i SRS gir grunnlaget for designen og utvikling av instrumenterte sikkerhetsfunksjoner. Et instrumentert sikkerhetssystem kan bestå av komponenter fra mange forskjellige leverandører, som logikkløser fra en leverandør, en flammedetektor fra en annen osv. Det er derfor viktig at alle leverandørene kjenner til kravene i IEC 61511-1 [1] og SRS så tidelig som mulig i designfasen slik at man kan få verifisert at utstyret kan benyttes i den tiltenkte SIF.

Som en del av dokumentasjonen på utstyret som levers, skal hver leverandør utvikle en Safety Analysis Report (SAR) som skal bevise at alle relevante krav i SRS og i IEC 61511-1 [1] er oppfylt [14].

Installasjon, utprøving og validering
Målet med denne fasen er å få installert hele sikkerhetssystemet etter kravene og spesifikasjonene gitt tidligere. Det er også viktig å installere utstyret med tanke på tilgjengelighet når det gjelder funksjonstester og vedlikehold. Alle funksjoner testes og valideres etter installasjon i samsvar med prosedyrer og gjeldene krav.

Operasjon og vedlikehold
Under operasjon og vedlikehold er det viktig at sikkerhetsintegritetsnivået for SIS opprettholdes igjennom hele livsløpet, og at det kan dokumenters. En av nøkkelaktivitetene er funksjonstesten som skal avdekke udetekterte farlige feil. Denne skal teste hele SIS, med et fast tidsintervall gitt i SRS, og feil som blir avdekket skal bli reparert på en sikker måte. Testen skal også dokumenteres sammen med eventuelle feil og mangler som blir oppdaget. Det er viktig at alle feil blir dokumentert slik at man får en god erfaringsdatabase for utstyret, og kan evaluere om de antakelsene under design er gjeldende.

Modifikasjon
Skal en modifikasjon utføres på et installert SIS, skal en analyse utføres for å bestemme inngrepet til endringen på det eksisterende SIS. Dette for å forsikre at sikkerhetsnivået er tilstede etter endringen. Det er også viktig at nødvendig dokumentasjon, som SRS, blir oppdatert hvis endringer blir foretatt på SIS.

Avvikling
Før avvikling av et sikkerhetssystem er det nødvendig med en skikkelig gjennomgang av hva som skal gjøres, og at nødvendige godkjenninger er på plass. Et sikkerhetssystem skal også være aktiv og operativ under hele avviklingsfasen, det vil si at alternativer som opprettholder samme funksjon blir opprettet. For eksempel ved oppgradering av et brann- og gassanlegg kan man installere og starte opp det nye anlegget først før man avvikler det gamle systemet.

3 ANTAKELSER OG USIKKERHET VED SIL

For å gjøre kvantitative beregninger i henhold til IEC 61511-1 [1] og retningslinjene fra oljedirektoratet OLF-070 [14] legges det en del antakelser for å forenkle og generalisere utregningene. De estimerte pålitelighetsverdiene og kvantifisert risiko blir brukt med det formålet at den skal ha verdi for beslutningstakerne, men da er det også viktig at antakelsene og usikkerhetene har blitt vurdert. Denne delen av oppgaven vil derfor prøve å synliggjøre de usikkerhetene som finnes ved bruk av kvantifiserte pålitelighetstall og se på en mulig løsning.

Frekventistisk sannsynlighet

I denne oppgaven blir kun den frekventistiske metoden til å beregne sannsynlighet og pålitelighetstall (PFD) vurdert. Den frekventistisk metode er definert som fraksjonen av antall ganger en hendelse skjer hvis situasjonen som analyseres blir gjentatt uendelig antall ganger [25]. Sannsynligheten blir da tolket som den relative frekvensen til hendelsen. Denne metoden blir også kalt for klassisk sannsynlighet [7].

Usikkerhet

Usikkerhet er et viktig begrep, og blir blant annet tolket innen prosjektlederfaget som: «Mangel på informasjon, kunnskap og kontroll på et aktuelt saksforhold» [26]. Lundteigen [9] definerer usikkerhet i forbindelse med SIS på denne måten: «Graden av tvil i vår evne til å fange inn de relevante faktorer i modeller, dataen og/ eller kalkulasjonene.» Innen pålitelighetsanalyser, der man kvantifiserer sannsynligheter for at utstyret eller komponenter feiler, er det derfor viktig å ha mest mulig kunnskap og informasjon om de aktuelle forhold for å minske usikkerheten som er i de estimerte verdiene og modellene. En mer detaljert beskrivelse av usikkerhet som kan ligge i estimerte feilrater og sannsynlighetstall blir nærmere beskrevet senere, men først skal vi se nærmere på selve begrepet usikkerhet.

Man vurderer vanligvis usikkerheten ved å skille mellom to hovedtyper [27]:

Aleatorisk usikkerhet: Den aleatoriske usikkerheten er den statistiske variasjon i en populasjon. Som eksempel kan vi se på levetiden til en komponent. Man vet ikke hvor lang levetiden er men man kan tilpasse en statistisk fordeling, for eksempel en eksponentialfordeling med en gitt feilrate, for å si noe om sannsynligheten for at levetiden blir større en 8750 timer. Men om levetiden blir større enn 8750 timer er det ingen som vet. Kiureghian og Ditlevsen [27] sier derfor at aleatorisk usikkerhet er karakterisert som usikkerhet som modellbyggeren ikke forutser muligheten til å fjerne. Denne usikkerheten kalles også for «Stokastisk usikkerhet» [28].

Epistemisk usikkerhet: En epistemisk usikkerhet omhandler manglende kunnskap / viten om verden, det vil i hovedsak si mangel på kunnskap om grunnleggende fenomener. Som eksempel kan vi ta levetiden til en komponent. Man kjenner ikke til den ekte feilraten til komponenten men man kan redusere usikkerheten med å anskaffe mer bakgrunnsinformasjon, som levetid til

tilsvarende komponenter i samme miljøforhold og lignende. Denne usikkerheten er det derfor, i motsetning til den aleatoriske, mulig å redusere.

Av den grunn mener noen at det kun finnes én type usikkerhet, den epistemiske usikkerhet, siden all usikkerhet kan reduseres ved tilføring av mer kunnskap [28]. Man kan for eksempel skaffe bedre modeller med flere parametere slik at man mer nøyaktig kan forutse en hendelse. Men det er også viktig å skille mellom disse to usikkerhetene, som Lundteigen [9] sier at en aleatorisk usikkerhet er nyttig til å si noe om våre begrensninger til å forklare alle aspekter i verden. Daniel P. Thunnissen [29] deler usikkerhet inn i fire hovedkategorier, i tillegg til aleatorisk- og epistemisk usikkerhet, beskriver han også ambiguitetsusikkerhet og interaksjonsusikkerhet.

Ambiguitet/ tvetydig usikkerhet: Denne usikkerheten omhandler bruk av upresise definisjoner og terminologier som skaper usikkerhet da involverte parter kan være i tvil om hva som egentlig menes. Denne type usikkerhet ser man også går igjen innen pålitelighetsfaget, og da særlig når det gjelder definisjoner av integritetsnivå (SIL) og ulike standarder som benyttes [30].

Interaksjon-/ samhandlingsusikkerhet: Daniel P. Thunnissen forklarer denne usikkerheten som usikkerhet som oppstår ved uforventet samhandling av flere hendelser eller disipliner. Den kan også oppstå ved uenighet mellom eksperter rundt en gitt usikkerhet når kun subjektive estimater eller ny data er framskaffet som kan gi bedre estimater til tidligere resultat.

For å bedre forstå hvilke usikkerheter som kan være tilstede ved bruk av IEC 61511-1 [1] skal vi gå nærmere innpå feilratene til komponenter i instrumentert sikkerhetssystem, og først skal vi se på vanlige kilder til generiske feilrater.

3.1 Fastsettelse av feilraten til komponenter

Det finnes ulike måter å framskaffe feilrater til komponentene i et SIS. Som vi så i forskriftene fra PTIL så var det krav til at data som har betydning for sikkerhet skal samles inn. Og en av grunnene er at man skal bygge opp generiske databaser hvor man kan finne informasjon som feildata til ulike typer av utstyr. Nedenfor er de mest vanlige databasene til feilrater for elektroniske komponenter [31]:

MIL-HDBK-217F Standard: Military Handbook: Reliability Prediction of Electronic Equipment, MIL-HDBK-217F [32] er en standard som ble utviklet av det amerikanske forsvarsdepartementet i 1961 og som senere har blitt revidert og oppdatert. Den inneholder feilratemodeller til en rekke ulike komponenter til bruk i elektroniske systemer, som transistorer, dioder, releer og så videre. Feilratene er basert på statistiske analyser av reelle feil, og for å tilpasse de reelle arbeidsforholdene benyttes ulike konstanter.

EPRD: Databasen EPRD – Electronic Parts Reliability Data [33] inneholder feilrater til elektroniske komponenter, som er anskaffet igjennom overvåking av komponentene i felten over en lang tid. For ikke-elektroniske komponenter benyttes NPRD – databasen [34].

Siemens SN 29500: SN 29500 standarden fra Siemens inneholder feilratedata ved referanseforhold, og metoder for å beregne feilrater basert på belastning og påvirkning. Den ble sist oppdatert i 1999 [35].

OREDA databasen: OREDA står for «Offshore Reliability Data» og er en prosjektorganisasjon hvor hovedfokuset er å samle og utlevere pålitelighetsdata blant de deltagende selskapene. Fra 2009 har prosjektet blitt styrt av Det Norske Veritas (DNV) [36]. En bok som inneholder statistiske analyser av forskjellig prosessutstyr kan bestilles.

Andre kilder til feilrater er:

- PRISM© - Reliability Prediction and Database for Electronic and Non-electronic Parts
- Telcordia SR-332 – Reliability Prediction Procedures for Electronic Equipment

De estimerte feilratene bruks så til å beregne påliteligheten til enkeltmodulene i SIF, som blir beregnet ved hjelp av verktøy som pålitelighetsblokkdiagram, feiltreanalyser og lignende.

Siden feilratene er estimert ut fra generiske feilrater og erfaringsdata så inneholder de usikkerhet som kan reduseres ved hjelp av bedre bakgrunnsinformasjon, bedre modeller og estimeringsverktøy. Man har derfor epistemisk usikkerhet knyttet til feilraten.

3.2 Sikkerhetsintegritet til maskinvare

For å regne ut påliteligheten til enkeltmoduler eller delmoduler i SIF brukes det i IEC 61511-1 [1] kvantitative metoder, hvor man beregner sannsynligheten for at komponenten eller modulen feiler ved behov (PFD). Standarden skiller også mellom behovsmodus og kontinuerlig modus som vi har sett på tidligere. I behovsmodus blir gjennomsnittsverdien, basert på testintervallet, brukt som pålitelighetsmål, mens i kontinuerlig modus brukes PFD per time. For å se nærmere på usikkerheten rundt PFD-tallene er det viktig å vite hvordan man kommer fram til verdien og hva som er vanlige antakelser.

For å beregne PFD_{avg}, som er den verdien som blir brukt når funksjonen er i behovsmodes, er det to viktige parametere som blir brukt:

- Funksjonstestintervallet, τ
- Feilraten for udetekterte farlige feil, λ_{DU}

Følgende antakelser er gjort ved utledning av PFD_{avg} i en 1-utav-1-funksjon:

- Komponentene har en eksponential sannsynlighetsfordeling med konstant feilrate.
- En komponent er å anse som «så god som ny» etter en reparasjon eller en funksjonstest.
- Systemet er i en sikker tilstand under reparasjon.
- $\lambda_{DU} \cdot \tau \leq 0{,}2$

Sannsynligheten for at systemet ikke virker er gitt ved levetidsfordelingen F(t), som ved en eksponentiellfunksjon blir følgende [37]:

$$F(t) = \int_0^t f(t)dt = 1 - e^{-\lambda_{DU}t}$$

hvor λ_{DU} er feilraten for farlige udetekterte feil. Komponenten sin overlevelsesfunksjon er gitt ved:

$$R(t) = 1 - F(t)$$

Tar man gjennomsnittet av levetidsfunksjonen over tiden mellom funksjonstestene får man PFD_{avg}:

$$PFD_{avg} = \frac{\int_0^\tau F(t)dt}{\tau} = 1 - \frac{1}{\tau} \cdot \int_0^\tau R(t)dt$$

Med en konstant feilrate λ_{DU} får vi at:

$$R(t) = e^{-\lambda_{DU}\tau}$$

Man får da ved å regne ut integralet til PFD_{avg} at:

$$PFD_{avg} = 1 - \frac{1}{\lambda_{DU}\tau} \cdot \left(1 - e^{-\lambda_{DU}\tau}\right)$$

Ved bruk av Taylor rekke, Maclaurin serie, får vi:

$$PFD_{avg} = 1 - \left(1 - \frac{\lambda\tau}{2} + \frac{(\lambda\tau)^2}{3!} - \frac{(\lambda\tau)^3}{4!} \ldots\ldots\right)$$

Siden vi har antatt at $\lambda_{DU} \cdot \tau \leq 0{,}2$ [38] får vi følgende tilnærming til et 1-utav-1-system:

$$PFD_{avg} \approx \frac{\lambda\tau}{2}$$

Ved å bruke denne tilnærmingen til PFD_{avg} vil vi alltid få et konservativt resultat, og dette resultatet er svært mye brukt i pålitelighetsregning på komponenter i sikkerhetsfunksjoner og er også foreslått i OLF-070 [14].

Funksjonstest og feilrate

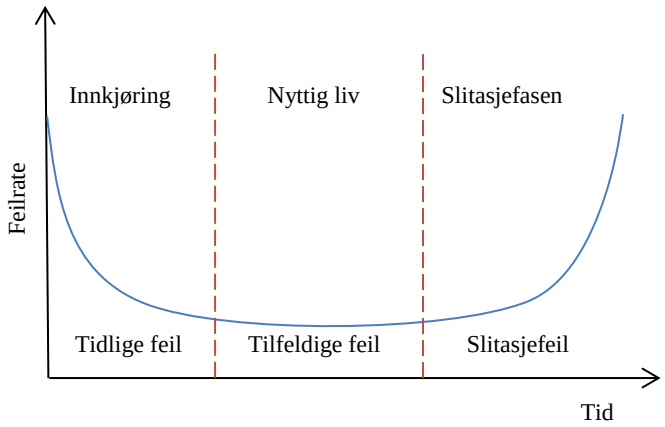
Som vi har sett så er det to hovedparametere i en 1-utav-1-funksjon. Funksjonstestintervallet τ og feilraten til udetekterte farlige feil, $\lambda_{DU,}$ og disse to avgjør om en SIF oppfyller kravene til et gitt SIL-nivå. Begge disse parameterne inneholder epistemisk usikkerhet som man kan redusere med mer bakgrunnskunnskap. Feilratene man har til de ulike komponentene blir vanligvis estimert ut ifra generiske feilrater som er gitt av tilgjengelig erfaringsdata, eller at man tester komponentene under tilsvarende forhold som komponenten eller enheten skal operere i. I tillegg kan estimatmodeller, programfeil og feil data føre til at estimatene ikke blir gode. Funksjonstestintervallet inneholder også usikkerhet da det blir gitt med den antakelsen at det er nok resurser til å utføre testen i gitte intervaller.

Hvis man ser på en 1-utav-2-funksjon, ser man i OLF-070 [14] at formelen for utregning av PFD_{avg} blir følgende:

$$PFD_{avg} = \beta \cdot \lambda_{DU} \cdot \frac{\tau}{2} + [(1-\beta) \cdot \lambda_{DU} \cdot \tau]^{2/3} + 2 \cdot (1-\beta) \cdot \lambda_{det} \cdot MTTR \cdot \lambda_{DU} \cdot \frac{\tau}{2}$$

Man har nå tre parametere til som det er epistemisk usikkerhet knyttet til, nemlig β som er faktoren for fellesfeil, λ_{det} som er feilraten for detekterte feil og MTTR som er gjennomsnittlig gjenopprettelsestid.

Ser man på en typisk utvikling av feilrater over tid vil en typisk form på feilraten danne en såkalt «badekar-kurve», figur 3.2.1. [7]. I innkjøringsfasen utsettes ofte komponentene for systematiske feil, som fabrikasjonsfeil eller installasjonsfeil, mens under slitasjefasen øker sannsynligheten for tilfeldig maskinvarefeil.



Figur 3.2.1, badekarskurve (basert på figur B.2. i [7]**).**

Det er i den perioden hvor feilraten er konstant, den såkalte «nyttig liv»-perioden til komponenten, at den feilraten som blir estimert under designfasen er gjeldende. Man antar derfor at feilraten er konstant og at komponenten er «så god som ny» etter en funksjonstest. Mot slutten av komponentens levetid vil imidlertid feilraten øke kraftig, og den estimerte feilraten har derfor ingen verdi lengre. Man ser her viktigheten med at antakelsene som ble gjort under estimering av PFD-verdien, nemlig at komponenten virkelig er så god som ny. Hvis ikke så vil feilraten aldri ha den antatte verdien og man vil kanskje ha et PFD-tall som er høyere enn kravene til SIL-nivået.

For elektriske og elektroniske komponenter kan man anta en konstant feilrate, og dermed at en eksponentiellfunksjon er en god modell [39]. Men noe utstyr, som for eksempel en blokkventil, kan ha en feilrate som er mer avhengig av tid, med en lav feilrate tidlig i operasjonsfasen og som øker etter hvert. En Weibull-fordeling hadde vært en bedre modell her enn en eksponentiell-fordeling med konstant feilrate.

For å sikre en konstant feilrate igjennom hele livsløpet er det derfor viktig med gode vedlikeholdsrutiner og inspeksjoner. Ytre påvirkning som ekstremkulde, fuktighet eller høy konsentrasjon av partikler kan også øke feilraten og levetiden til komponenten. Og slike forhold må også tas hensyn til når det gjelder vedlikehold og tester. Feil og mangler må dokumenteres slik at man får en mest mulig reel feilrate og kan utføre funksjonstester ut fra erfaringsdata. OLF-070 [14] beskriver to metoder for å revidere testintervallet, en forenklet metode for estimering av ny PFD og feilrate, og en mer omfattende metode, inkludert et numerisk eksempel der nytt tidsintervall blir estimert. Det er viktig at prosedyrer på hvordan håndtere og registrere feil og hvilken tilleggsinformasjon som skal noters har blitt utviklet og brukes under operasjonsfasen.

For å lindre på usikkerhet og antakelser gjort i design setter IEC 61511-1 [1] krav til minimum maskinvarefeil toleranse (HFT). Er dette bra nok? Å gi et krav til arkitekturen slik at hvis en

komponent feiler, så hindrer det ikke SIF å få prosessen til en sikker tilstand hvis en hendelse skjer, øker pålideligheten til SIS. Men siden en sikker feil blir definert ut fra hvordan man detekterer den, eller om den er ufarlig, så fjerner ikke arkitektoniske krav den epistemiske usikkerheten som ligger i pålitelighetstallene.

Det er også knyttet til usikkerhet rundt hvordan de forskjellige leverandørene tolker sikre feil og hvilke antakelser som blir gjort, noe som Goble diskuterer [40]. Vi kan altså ha ambiguitetsusikkerhet rundt definisjoner og arbeidsprosesser som gjør at vi kanskje ikke kan sammenligne SFF-tallene til komponenter fra forskjellige leverandører [16].

Vi vet nå at det finnes usikkerhet bak pålitelighetstallene som IEC 61511-1 [1] setter krav til. Vi skal derfor kort se på ulike metoder og hjelpemidler for å visualisere eller redusere usikkerhetene.

3.3 Kort om usikkerhetsmål

Det har nå blitt vist at et sikkerhetssystem inneholder både epistemisk og aleatorisk usikkerhet. Det er derfor viktig å vite at pålitelighetstall inneholder usikkerhet, og å ha kjennskap til de antakelser og arbeidsmetoder som er gjort under design. Pålitelighetstallene er basert på bakgrunnskunnskap som inneholder usikkerhet, men det å skaffe mer bakgrunnskunnskap, bedre og mer komplekse modeller og gode estimeringsverktøy til nye komponenter med lite erfaringsdata kan både være tidkrevende og kostbart. Det vises nå noen metoder som kan vise hvilken effekt ulike antakelser og usikkerhet kan ha på utgangen til systemets pålitelighet. I tillegg hvordan man kan finne de komponentene i et system som er mest kritiske.

Sensitivitetsanalyse

En sensitivitetsanalyse er viktig siden den viser hvor følsomt utdata er i forhold til endringer i inndata. Man kan på den måten se hvordan resultater er avhengig av de antakelsene som er gjort ved å gjøre endringer vekk fra antakelsene på inndata til systemet for å se hvor mye systemets utdata endrer seg. En sensitivitetsanalyse er ikke en usikkerhetsanalyse da den ikke sier noe om usikkerhetene i de ulike modellene og parameterne, men kan gi et underlag for å vurdere usikkerheten [41].

Usikkerhetsanalyse

En usikkerhetsanalyse, i motsetning til sensitivitetsanalyse, ser på usikkerheten i de ulike parameterne p_i i påliteligheten til systemet h. En slik analyse peker derfor på fastsettelse av usikkerhet i analyseresultatet som stammer fra usikkerhet i analysens informasjon [42]. For eksempel kan en parameter p_i i et system h ha ulike verdier med tilhørende estimerte sannsynligheter. Man kan da kalkulere en sannsynlighetsfordeling over systemets pålitelighet h basert på sannsynligheten til de ulike verdiene til p_i. Med mål som standardavvik og varians, som er mål på spredningen og den underliggende variasjonen til fordelingen, kan vi si noe om usikkerheten til systemets pålitelighet, h [25].

Kritikalitetsmål

Å identifisere de komponentene som er mest kritiske er viktig med tanke på sikkerhet og pålitelighet. Med kritisk menes de komponentene som har det høyeste potensialet til å påvirke systemets pålitelighet. Det er også viktig med tanke på usikkerhet at disse komponentene blir identifisert slik at man kan gjøre disse kritiske komponentene mer pålitelige, som å øke kvaliteten på komponenten, bruke komponenter med mindre usikkerhet og lignende.

Forbedringspotensial: Det er spesielt i designfasen dette er viktig, da man har muligheten til å gjøre endringer til mer reduserte kostnader enn under operasjon som kan føre til nedetid og produksjonsstans. Metoden som benyttes da er at forbedringspotensialet til komponent *i*, I_i^A beregnes på følgende måte [7]:

$$I_i^A = h_i - h$$

hvor h_i er påliteligheten til systemet når komponent *i* er i den beste tilstand og *h* er påliteligheten til systemet.

Birnbaums mål: En annen metode som kan benyttes er Birnbaums mål som sier at den mest kritiske komponenten er den komponenten som ved en liten forbedring av dens pålitelighet har den største effekt på systemets pålitelighet. Birnbaums mål finner vi ved å partiellderivere systempåliteligheten med hensyn på komponentpåliteligheten pi, og er definert ved [7]:

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

Man får dermed differansen mellom systempåliteligheten når komponent *i* antas å virke perfekt og den samme komponenten har feilet. Denne metoden er aktuell å benytte i systemets driftsfase.

3.4 Diskusjon

Ved estimering av pålitelighetstall og sannsynligheter for at systemet eller komponenten feiler vil det alltid være usikkerhetsmomenter. Usikkerhet er knyttet opp mot manglende bakgrunnsinformasjon som inkluderer blant annet erfaringsdata, operasjonsforhold, feilaktig informasjon og statistisk variasjon.

En kvantifisering av integritetsnivået, SIL, gir en god indikasjon til beslutningstakerne som raskt kan avgjøre om de estimerte pålitelighetstallene som blir presentert oppfyller de kravene som er satt til funksjonen. For eksempel hvis en sikkerhetsfunksjon har som krav at den skal oppfylle et visst SIL-nivå, så kan man sjekke PFD-tallene til de forskjellige komponentene opp imot kravene for å få verifisert om komponentene kan benyttes som en del av funksjonen. Men da må man være sikker på at de estimerte PFD-tallene ikke inneholder usikkerhet som gjør at man får uventede utfall. Ser man direkte på kvantifiserte pålitelighetstall, som PFD, kan man lett overse usikkerheter som kan skjule seg i bakgrunnsinformasjonen [43].

Vi skal nå se på sikkerhetssystemet til Kongsberg Maritime, som vi kommer nærmere innpå i GAP-analysen. Feilratene til enkeltkomponenter ble hentet fra MIL-HDBK-217F [32], som gir generiske feilrater som man multipliserer med ulike faktorer, som for eksempel temperatur og miljøforhold, for å få mest mulig reelle feilrater som er tilpasset de omgivelser som utstyret skal operere i. Man får da et estimat på feilraten, basert på bakgrunnsinformasjon, som avviker mer eller mindre fra den reelle feilraten til komponenten og systemet. MIL-HDBK-217F [32] har to forskjellige metoder for å estimere feilraten på, «parts count»-analyse og «parts stress»-analyse. «Parts count»-analysen er den enkleste metoden, og egner seg best i begynnelsen av designen, da denne ikke krever så mye informasjon for å gjennomføres. Det matematiske uttrykket for utregning av feilraten ved bruk av denne metoden er [32]:

$$\lambda_{EQUIP} = \sum_{i=1}^{i=n} N_i \cdot \left(\lambda_g \cdot \pi_Q\right)_i$$

hvor λ_{EQUIP} er den totale feilraten til utstyret (feil per 10^6 time), N_i er antallet til den i-te generiske del, λ_g er feilraten til den i-te generiske del (feil per 10^6 time), π_Q er kvalitetsfaktoren til den i-te generiske del og n er antall forskjellige kategorier av generiske deler i utstyret. Man ser her at den eneste informasjonen man trenger er den generiske feilraten til komponenten λ_g, og en kvalitetsfaktor π_Q. Det er antatt at utstyret står i samme miljø og at de generiske feildataen hentes fra det miljøet som utstyret skal operere i [32, pp. A-1].

«Part stress»-analysen krever derimot mer detaljer og er derfor mer egnet til bruk i senere faser av designutviklingen. Framgangsmåten her er å multiplisere den generiske feilraten med flere

miljø- og operasjonsfaktorer. Som eksempelet kan vi se på framgangsmåten for å utregne en feilrate til en lavfrekvent diode:

$$\lambda_p = \lambda_b \cdot \pi_T \cdot \pi_S \cdot \pi_C \cdot \pi_Q \cdot \pi_E$$

Feilraten til komponenten λ_p er nå avhengig av en rekke faktorer. Den generiske feilraten λ_b, temperaturfaktoren π_T, elektrisk stressfaktor π_S, konstruksjonsfaktor til kontaktflaten π_C, kvalitetsfaktor π_Q og miljøfaktor π_E.

Ut fra dette kan vi se at det er mange antakelser som blir gjort under design som må være gjeldende for hele livsløpet til utstyret. For eksempel så blir et spesielt utstyr utviklet til bruk i et bestemt miljø og under gitte forhold, men hvis leverandøren ønsker å utvide markedet til andre bransjesektorer, da kan det være er at de pålitelighetstallene som man kom fram til under utvikling ikke er gjeldende lengre. Hvis vi ser på temperaturfaktoren π_T til den lavfrekvente dioden, så øker den fra 1,0 til 1,4 når man går fra en omgivelsestemperatur på 25 °C til 35 °C, og hvis man ser på miljøfaktoren π_E så er den på 1,0 i kontrollerte omgivelser på fast underlag på land (kode G_B), men for marine forhold, i beskyttet utstyrsrom (kode N_S) er miljøfaktoren på 9,0.

Dette er et veldig enkelt eksempel, men det viser viktigheten med å ta hensyn til antakelsene gjort til pålitelighetsutregningene under design. Man kan kanskje tro at det ikke er noen forskjell på å installere utstyr i et utstyrsrom på en båt i motsetning til å installere det samme utstyret i et utstyrsrom på land, men som man ser av MIL-HDBK-217F [32] så kan pålitelighetstallene bli veldig forskjellig.

En annen ting er hvor gode de generiske feilratene er og hvordan de har kommet fram til de. Er det tatt hensyn til behovsraten til utstyret som står i en bestemt funksjon? For eksempel hvis man har et PFD-tall til en komponent i en funksjon som sier at den feiler mindre enn 1 av 100 ganger det er behov for den, som er SIL2-kravet for en funksjon i behovsmodes [1]. Man kan altså forvente en feil under operasjon hvis komponenten operere under samme forhold i mer enn 100 år, siden i behovsmodus er kravet at det kun skal være behov for funksjonen mindre enn en gang i året [3]. Man ser her at å skaffe seg tilstrekkelig erfaringsdata er utfordrende. Man kan for eksempel ikke aktivere funksjonen 100 ganger etter hverandre i løpet av en begrenset tidsperiode. For eksempel blir en funksjon i operasjon påvirket av aldring og miljø som utsetter funksjon og komponentene for ytre påvirkning. Man har derfor usikkerhet i PFD-tallene som ikke er synlige før man går i detalj og ser hva som ligger bak estimatene.

Man trenger derfor et system som klart viser hvilke antakelser som har blitt gjort under design, og en forsikring om at de generiske feilratene er mest mulig korrekte.

3.5 Forslag til forbedring

Som man ser så er det epistemisk usikkerhet i de kvantifiserte feilratene som blir brukt til å utregne PFD-tall, og da i hovedsak rundt hvilke antakelser som har blitt gjort under estimering av feilraten. Disse må komme tydelig fram da disse gir begrensninger til installasjon og operasjonsforhold.

Hvis man ser på to eksempler på sertifikater fra ulike sertifiseringsselskaper til forskjellig utstyr, som for eksempel TÜV Rheinland [44] eller Exida [45], så er feilratene ikke merket med begrensninger for miljø og operasjonsforhold. TÜV Rheinland henviser for eksempel kun til rapporten som beskriver hva som ligger til grunn for sertifikatet. Jeg argumenterer derfor at en nødvendig informasjon rundt hvilke antakelser som har blitt gjort i forbindelse med estimering av feilraten til komponentene, ikke alltid er enkelt å finne. Utstyr kan derfor bli installert i andre miljø og under andre forutsetninger enn de som var lagt til grunn under design, og som vi så i diskusjonen kan dette gå utover påliteligheten til systemet. Et forbedringsforslag er derfor å merke utstyret med en kodemerking som skal fortelle hvilke forhold som utstyret er designet for.

For elektrisk utstyr til bruk i eksplosjonsfarlige omgivelser, det vil si i områder hvor en eksplosjonsfarlig atmosfære kan antennes av gnister forårsaket av elektrisk strøm, er det krav til at utstyret skal merkes. Utstyret blir derfor merket med en kode som forteller hvor utstyret kan monteres eller spesielle betingelser [46]. En slik merking hjelper til å forsikre at utstyret blir brukt i de omgivelser de er tiltenkt. Det er også andre fordeler som jeg skal komme tilbake til senere.

Det som er viktig med et slikt merkesystem er at det setter krav til hvor utstyret kan installeres, som i hvilke omgivelser og ytre påvirkning. Dette argumenteres med at det er disse parameterne, hvis vi tar utgangspunkt i MIL-HDBK-217F [32], som påvirkes av hvor utstyret blir installert og som har betydning etter design. En endring av kvalitet på enkeltkomponenter eller design kan ikke gjøres i etterkant uten å beregne nye pålitelighetstall og nye feilrater. Hvilken behovsrate utstyret har er også viktig, noe som kom fram under diskusjonen, da dette også påvirker den reelle feilraten. Et forslag på hvordan man kan merke utstyr til bruk i instrumenterte sikkerhetsfunksjoner kan være:

SE-X-Exx-Tx-AExxx
1 - 2 - 3 -4 - 5

En forklaring til koden finnes under, i tabell 3.5.1:

Tabell 3.5.1: Oversikt over bokstavkode til merking av sikkerhetsutstyr.

Siffer	Bokstavkoder	Forklaring
1.	SE: Safety Equipment	Dette for å vise at det er instrumentert sikkerhetsutstyr som har krav til sikkerhetsintegritet.
2.	C: Kontinuerlig D: Behov	Behovsraten til komponenten.
3.	Exx: Miljøforhold E_{GB}: Land, mild E_{GF}: Land, utendørs E_{GM}: Land, flyttbar E_{NS}: Marine, beskyttet E_{NU}: Marine, ubeskyttet E_{SS}: Under vann	Denne forteller hvilket miljø utstyret kan stå i. Her har jeg klassifisert det på samme måte som i MIL-HDBK-217F [32], som et eksempel på løsning. I tillegg bør undervannsutstyr være med.
4.	Tx: Temperaturklasse. T1: -20 °C til < 0 °C T2: 0 °C til < 20 °C T3: 20 °C til < 40 °C T4: 40 °C til < 60 °C T5: 60 °C til < 80 °C T6: 80 °C til < 100 °C	Viser temperaturklassen til utstyret, altså i hvilken omgivelsestemperatur utstyret skal stå i under normale forhold, varmen som utstyret avgir må også tas med i beregningene.
5.	AExx: Virkelig miljø.	For å få gode erfaringsdata fra utstyr som står i samme miljø er det viktig med en kode som enkelt kan spores tilbake til erfaringsdatabaser. Forskjellen fra denne koden og siffer 3 er at miljøkode Exx sier hvilket miljø utstyret kan stå i, mens dette sifferet skal fortelle i hvilket miljø utstyret faktisk står i.

Forslaget er ment som et eksempel på hvordan man kan merke sikkerhetsutstyr på, så eventuelle temperaturklasser og miljø må tilpasses behovet. Kanskje er det også behov for flere siffer for å dekke andre viktige hensyn og antakelser som blir gjort under designfasen.

Behovsraten til komponenten: Grunnen til at behovsraten til komponenten er med kan argumenteres med at slitasje på utstyr som står i ro over en lang periode kan være annerledes enn for utstyr som er oftere i bruk. For eksempel kan en ventil ruste fast og/ eller få opplagring av leire som kan øke feilraten.

Miljøklasse: Som vist i diskusjonen over så brukes det forskjellige verdier til miljøfaktoren π_E etter hvilket miljø som er tiltenkt utstyret. Det betyr at hvis man benytter utstyr i et annet miljø enn det som er antatt under design kan verdiene til de estimerte feilratene til enkeltkomponentene være mer unøyaktige og akseptkriterier kan oppnås på feil grunnlag. Det er derfor viktig å få tydelig fram hvilket miljø utstyret ble designet for, og at det stemmer med det reelle miljøet.

Temperaturklassen: De samme argumentene kan vi bruke ovenfor arbeidstemperaturen til utstyret. Elektronisk utstyr i drift blir påvirket av omgivelsestemperaturen og de avgir også varme. For å redusere usikkerheten rundt antakelsene om rett områdetemperatur til

komponentene, er det viktig å merke utstyret med temperaturklasse. Man blir derfor sikker på at utstyret benyttes i miljøer med rett omgivelsestemperatur og at temperaturen som ble antatt under design stemmer med virkeligheten.

Virkelig miljø: Leverandører av sikkerhetsutstyr ønsker vanligvis å designe utstyr uten for mange begrensninger på hvor utstyret skal stå. Hvis vi ser igjen på estimering av feilrater fra MIL-HDBK-217F [32] så gir en miljøfaktor for utstyr installert i utstyrsrom på båt, π_E=9, en høyere feilrate enn utstyr installert på land π_E=1. Det bør derfor være rimelig å anta at utstyr som er designet for å stå i utstyrsrom på båt også kan stå på land. Her kan sensitivitetsanalyser verifisere hvilke miljø og temperaturforhold utstyret kan stå i. Så i de tilfeller hvor utstyret blir installert i et mildere miljø en antatt under design, altså at påliteligheten til utstyret dekker flere miljø og temperaturforhold, benyttes denne koden for å skille mellom antatt og reelle antakelser.

Et annet viktig argument for å merke sikkerhetsutstyr er å få gode databaser med mest mulig reelle feilrater. For eksempel hvis sikkerhetsutstyr feiler så har man sporbarhet tilbake til rett feilrate i databaser som kan oppdateres raskt, og man kan være sikker på at utstyret har stått i samme miljø hele levetiden. Det er viktig at merkeskiltet følger utstyret og at det er fastmontert, slik at man kan i størst mulig grad kan stole på de erfarte feilratene.

Et slikt merkesystem bør altså være i samsvar med databaser, være fastmontert på utstyret, stå i et eventuelt sertifikat og i databladet til utstyret. På den måten kan beslutningstakere få verifisert at utstyret de ønsker passer til det miljøet det er tiltenkt, man kan oppdatere databaser på en god måte og man kan redusere usikkerhet rundt antakelser gjort under design.

Man får også en bedre verifikasjon for at antakelsene om temperatur og ytre påvirkning gjort under design stemmer med de faktiske omgivelsene utstyret ble installert i. Man kan dermed redusere epistemisk usikkerhet ved at et slikt system kan hjelpe til med å få sikrere erfaringsdata til utstyret.

Som vi ser er det viktig å ha god dokumentasjon for å kunne dokumentere antakelser gjort i designfasen. Det er også viktig å redusere ambiguitetsusikkerhet, som kan reduseres ved god og strukturert dokumentasjon. For å se nærmere på hvordan man kan dokumentere at alle relevante krav gitt i IEC 61511-1 [1] er oppfylt, vil det bli utført en GAP-analyse på et prosjekt, som ble utført med Kongsberg Maritime som leverandør av logikkløser til sikkerhetssystemet.

4 GAP-ANALYSE PÅ WEST ELARA

Som leverandør av logikkløsere til prosessindustrien er det viktig for Kongsberg Maritime (KM) å levere utstyr og programvare i henhold til gjeldende krav og med tilfredsstillende dokumentasjon. Som en verifikasjonssjekk ønsker de å se på et gjennomført prosjekt for å kartlegge eventuelle avvik i dagens prosedyrer og dokumentasjon opp imot kravene i IEC 61511-1 [1]. Målene for en slik analyse er å få en oversikt over hva IEC 61511-1 [1] stiller krav til, og hva som eventuelt trengs å endres på i eksisterende dokumentasjon for å kunne, på en oversiktlig måte, dokumentere at kravene er oppfylt. Verktøyet som brukes i denne rapporten er en GAP-analyse som er en metode som brukes for å kartlegge dagens situasjon opp mot en ideell situasjon, og gir derfor et godt utgangspunkt for videre arbeid. Beslutningstakere kan dermed bruke resultatene fra analysen og få konkrete forslag for å nå ønskede mål [47].

For å begrense omfanget av GAP-analysen har jeg valgt et konkret prosjekt og en konkret sikkerhetsfunksjon i et sikkerhetssystem, hvor KM var leverandør av logikkløseren. Dette kan forsvares med at mye av kontrollsystemet, prosedyrer, dokumentasjon og programvare blir utviklet og brukt av mange funksjoner, slik at kun å se på en SIF gir et godt bilde på avvik i dokumentasjonen i et kontrollsystem levert av Kongsberg Maritime.

For å oppfylle kravene i IEC 61511-1 [1] sier standarden i kapittel 4 at det må vises at hvert av kravene i kapittel 5 til 19 er tilfredsstillende oppfylt til de definerte kriteriene, og dermed at målene for hvert kapittel har blitt møtt. I punkt 19.2.5 står det også at dokumentasjonen skal være sporbar tilbake til kravene i standarden. Dette blir derfor utgangspunktet for analysen, hvor IEC 61511-1 [1] blir gjennomgått punkt for punkt innenfor de livtidsfaser som er aktuelle for KM, for å se om kravene er dokumentert oppfylt.

4.1 Prosjektet som er utgangspunktet for analysen

For at GAP-analysen skal være mest mulig relevant er det viktig at det prosjektet analysen skal utføres på oppfyller noen kriterier. Prosjektet må være ferdig levert til kunden og blitt avsluttet for mindre enn 3 år siden. Det må være et prosjekt som er typisk for Kongsberg Maritime, være i olje- og gassbransjen og inneholde instrumenterte sikkerhetsfunksjoner.

Jack-up riggen West Elara, som er eid av Seadrill Limited, ble bygget for å utføre produksjons- og boreoperasjoner for aktører innen oljebransjen, og stod klar for drift i 2011. Riggen er av Gusto MSC design og ble konstruert av Jurong Shipyard Pte LTd. i Singapore. Den er designet for å operere i tøffe omgivelser med en vanndybde på opptil 150 meter, og har en boredybde ned til 10670m [48].

Kongsberg Maritime var en underleverandør til Jurong Shipyard under konstruksjonen av riggen, og var ansvarlig for å levere et integrert kontroll- og overvåkingssystem (ICMS) med følgende undersystemer:

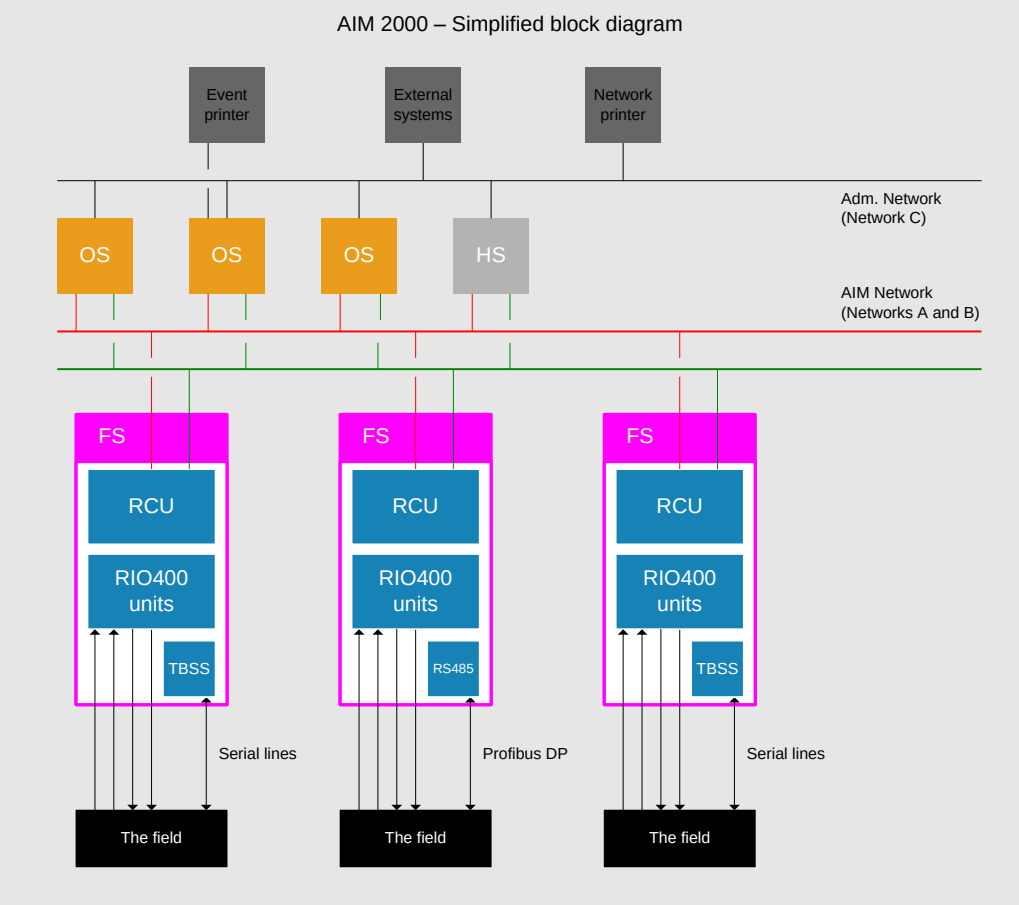
- Nødavstengingssystem (ESD)
- Brann- og gassystem (F&G)
- Spenningssysteringssystem (PMS)
- Fartøy styringssystem (VMS)

Kontrollsystemet fra Kongsberg Maritime, AIM 2000, inneholder sikkerhetssystemet K-Safe, som er det systemet som er designet for å møte kravene fra IEC 61511-1 [1]. Dette prosjektet oppfylte dermed alle kriteriene og ble utgangspunktet for GAP-analysen.

Den valgte sikkerhetsfunksjonen er en flammedeteksjon, flammedetektor 811-BFFZ04-101 som befinner seg i brannsone FZU04 - Mud Treatment Room. OLF-070 [14] definerer en flammedeteksjon som en global delfunksjon, det vil si at i dette tilfellet vil delfunksjonen være fra en detektert flamme av detektoren til en aktivert utgang fra logikkløseren. SIL-kravet til brann- og gassfunksjoner er gitt av filosofidokumentet til brann- og gassystemet fra Jurong Shipyard, som krevde et minimumskrav på SIL2 [49, p. 9]. I dette prosjektet var det ikke utgitt en SRS fra kunden, det vil si at sporbarhet tilbake til kravene ikke alltid er gjeldende. Men for å gjøre analysen på et mer generelt grunnlag kommer jeg til å se på prosjektdokumentasjonen som om en SRS eksisterer.

4.2 Leveransen fra Kongsberg Maritime

Prosjektdokumentasjonen [4] gir følgende informasjon om kontrollsystemet: AIM 2000 er et fordelt kontrollsystem som er basert på «Kongsberg Maritime»-teknologi og som ble levert til West Elara, figur 4.2.1.



Figur 4.2.1, eksempel på AIM 2000-topologi (figur hentet fra ICMS-KFDD [4]**).**

Arkitekturen er basert på et lokalt redundant datanettverk som kobler sammen alle nødvendige stasjoner. Nettverket består av et Ethernet-basert lokalt nettverk (LAN), nettverk A og B, som er det redundante hovednettverket, mens nettverk C er et administrativt nettverk. Nettverk A og B kommuniserer med alle de forskjellige tilkoblede stasjonstypene som utfyller forskjellige oppgaver:

Operatørstasjon (OS): Operatørstasjonene er grensesnittet mellom brukeren og prosessen. Den sørger for et grafisk grensesnitt mot AIM 2000 sine bildetyper, utstyr til å navigere i bildene og en lagringsplass for kontrollernes (RCU) programfiler og konfigurasjonsdata.

Historiestasjon (HS): Historiestasjonen lagrer «time series» som kan bli brukt i historiske trenddiagrammer og rapporter. En historiestasjon kan også operere som en operatørstasjon, som en enslig kombinert enhet, men dette skal kun skje under testing.
Feltstasjon: En feltstasjon er et kombinert prosess- og feltgrensesnitt. Den inneholder kontrollerenheter (RCU) og grensesnitt mot feltutstyr og AIM 2000-systemet. Kontrollenhetene inneholder prosesslogikken for et bestemt prosessområde, programmet, konfigurasjonen og dataen som er tilknyttet det prosessområdet som blir kontrollert, og er operativ selv om både nettverk A og B feiler. Både programmet og konfigurasjonen blir permanent lagret på en operasjonsstasjon.

Både maskinvare og programvaren i AIM 2000 innehar typegodkjenningssertifikater fra Det Norske Veritas og American Bureau of Shipping [50]. Sikkerhetssystemet, K-Safe, som er en del av AIM 2000, inneholder i tillegg SIL-sertifisering fra TÜV Rheinland [44] [51].

4.3 GAP-analysen

Analysen er bygget opp slik at alle de relevante kravene i IEC 61511-1 [1] blir gjennomgått, og er delt inn på følgende måte:

- Styring av funksjonell sikkerhet.
- Spesifiserte sikkerhetskrav til SIS.
- Design av SIS og teknisk arbeid.
- Integrasjon av brukerprogrammet med SIS.
- Dokumentasjon.
- Oppsummering og anbefalinger.
- Forslag til forbedringer.

Prosjektdokumentene som Kongsberg Maritime leverer i prosjekter, for å dokumentere funksjonene, er i hovedsak:

- Safety Analysis Report (SAR) [52].
- Kongsberg Functional Design Document [6] [4].
- Failure Mode and Effect Analysis (FMEA) [53].
- Testprosedyrer (FAT/ CAT) [54] [5].
- Vedlikeholdsmanual [55].
- Operasjonsmanual [56].
- Kvalitetsplan [57]

Safety Analysis Report (SAR) [52]*:* Dette dokumentet skal dokumentere at alle kravene gitt i kundens kravdokument, vanligvis et «Safety Requirement Spesification»-dokument (SRS), er oppfylt. Kongsberg Maritime sin prosjektbaserte SAR blir utviklet fra en generisk SAR, som

inneholder informasjon om arkitektoniske løsninger, pålitelighetstall og spesielle operasjonsmoduser til sikkerhetssystemet.

Kongsberg Functional Design Document (KFDD): KFDD beskriver design og funksjonalitet til forskjellige deler av kontrollsystemet, vanligvis F&G, ESD/PSD og ICMS. Formålet med dokumentet er å beskrive funksjonene og grensesnittene i Kongsberg Maritime sitt kontrollsystem i henhold til kravene for riggen. Det blir også brukt som en del av operasjonsdokumentasjonen. I dette prosjektet ble KFDD delt inn i flere dokumenter til hvert system, F&G-KFDD [6] og ICMS-KFDD [4].

Failure Mode & Effect Analysis (FMEA) [53]: Formålet med dokumentet er å gi en beskrivelse av de forskjellige feilmodusene til utstyret, referert til deres funksjonelle mål, og å detektere mulige kritiske svakheter på blokk-nivå.

Testprosedyrer: FAT- og CAT-prosedyrene [54] [5] beskriver gjennomføring av testene som skal verifisere at programvarefunksjonaliteten i F&G-KFDD [6] og C&E-dokumentene [58] er implementert korrekt. Intern aksepttest (IAT) og fabrikkens aksepttest (FAT) benytter den samme testprosedyren for gjennomføring av testene. Prosedyren til kundens aksepttest (CAT) inneholder, i motsetning til FAT-prosedyren [54], også test av maskinvaren sammen med programvaren og blir dermed en mer komplett testprosedyre.

Vedlikeholdsmanual [55]*:* Dette dokumentet fungerer som et referansedokument med henvisning til dokumenter som beskriver funksjonene og vedlikehold til det forskjellige utstyret i systemet. Vedlikeholdsfasen er utenfor arbeidsomfanget til denne analysen.

Operasjonsmanual [56]*:* Operasjonsmanualen gir en beskrivelse av hvordan man opererer systemet i drift. Den beskriver blant annet systemet, hvordan man navigerer i menneske-maskingrensesnittet (HMI), alarmer som vises og normal drift. Operasjonsfasen er utenfor arbeidsomfanget til denne analysen.

Konfigurasjonsmanualen [59]*:* Dette er et generisk dokument til internt bruk, som brukes som en veiledning til å konfigurere K-Safe. Dokumentet er ikke ment for utlevering til kunder, men kan bli vist på oppfordring da det inneholder parameterinnstillinger, programvarebeskrivelse og konfigurasjonsløsninger.

Kvalitetsplan [57]:Dokumentet beskriver organisasjonen og styrings- og kvalitetsmål.

4.3.1 Styring, vurdering og revisjon av funksjonell sikkerhet

Kapittel 5 i IEC 61511-1 [1] inneholder hovedkravene til styringen av funksjonell sikkerhet. Hovedmålet for kapittelet er å identifisere styringsaktivitetene som er nødvendig for å forsikre at målene til funksjonell sikkerhet har blitt møtt.

Hovedansvaret for styringen av funksjonell sikkerhet i prosjektet ligger hos eieren (Seadrill) som er/ var delaktig i, og styrer alle livssyklusfasene til SIS. Dette prosjektet hadde ikke et eget styringsdokument for sikkerhet, så i dette tilfellet hadde ikke underleverandørene til sikkerhetssystemet et felles styresett og strategi for å oppnå et sikkert system. Men som delaktig i livsyklusaktiviteter stilles det noen krav til Kongsberg Maritime. Blant annet hvilken kompetanse de forskjellige ansvarlige har og hvilket kvalitetssystem som brukes.

Organisasjon og ressurser

Det stilles krav til kompetansen til personell som er involvert i aktiviteter som inngår i livssyklusen til SIS. I kvalitetsplanen for prosjektet [57] finnes organisasjonskartet med de personene som hadde ansvaret for de forskjellige systemene, og en beskrivelse av ansvar og myndighet. Krav til utdannelse og erfaring til personer som innehar de forskjellige ansvarsområdene står også beskrevet. Videre har Kongsberg Maritime et sertifiseringssystem hvor ingeniørene som jobber med forskjellige systemer, som sikkerhetssystemet K-Safe, må igjennom for å bli sertifisert til å jobbe med utstyret [60]. I nevnte sertifikat står det at SIL-kurs er et valgfritt alternativ, men det er en fordel at personer som jobber med et instrumentert sikkerhetssystem har kjennskap til gjeldende regelverk.

Implementering og overvåking

I all hovedsak er det eieren av systemet som er ansvarlig for grunnleggende prosedyrer, men det er også viktig at underleverandørene har systemer og prosedyrer for å styre deres leveranse til prosjektet og for å oppfylle kravet om kvalitetsstyringssystem. Kongsberg Maritime sitt kvalitetsstyringssystem oppfyller kravene til ISO-9001:2000 [57] og i leveransen til «West Elara»- prosjektet ble følgende hovedprosedyrer benyttet:

- PRO-0001 - Preventive Action [61].
- PRO-0002 – Control of Documents [62].
- PRO-0003 – Handling of Non-conforming products and corrective action [63].
- PRO-0004 – Audit, Procedure for Quality Audits, Internal and Supplier for KM [64].
- PRO-0021 - Delivery Process Start-up [65].
- PRO-0022 - Delivery Process Planning [66].
- PRO-0023 - Delivery Process Engineering [67].
- PRO-0024 - Delivery Process Production Assembly Test [68].
- PRO-0025 - Delivery Process Commissioning [69].
- PRO-0026 - Delivery Process Close Out [70].

Gjennomgang av kravene i IEC 61511-1 [1]**:**
Tabell 4.3.1.1 viser en gjennomgang av kravene i IEC-standarden. Hoveddokumentet i denne fasen har vært kvalitetsplanen [57] som henviser til alle gjeldende prosedyrer for gjennomføring av prosjektet, og hvilken kompetanse de ulike ansvarshaverne skal ha.

Tabell 4.3.1.1: Resultat av kapittel 5.

Punkt:	**Krav (fullstendig i IEC 61511-1 [1]):**	**Avvik? (Ja/Nei)**	**Forklaring:**
5.0 Styring av funksjonell sikkerhet			
5.2.2 Organisasjon og ressurser			
5.2.2.1	Ansvarlige personer skal være identifisert og fortalt hvilket ansvar de har.	Nei	Organisasjonskart er utfylt med navn til personer med nøkkelstillinger i prosjektet, og ansvarsområder står beskrevet i kvalitetsplanen [57]. På den måten vet stillingshaverne hvilket ansvar de har.
5.2.2.2	Personell skal være kompetente til oppgaven.	Nei	Hvilke krav som stilles til personer med ansvar står beskrevet i kvalitetsplanen [57]. Det er også utviklet sertifikater og spesifisert opplæring til de forskjellige oppgavene [60].
5.2.5 Implementering og overvåking			
5.2.5.2	Krav til underleverandør om å levere i henhold til spesifikasjon, og ha et kvalitetssystem.	Nei	KM har et styringssystem som er sertifisert i henhold til ISO 9001:2000 som gjør seg gjeldene i prosedyrene nevnt i kapittelet. Dette er dokumentert i kvalitetsplanen [57]. Dokumentasjon og tester som FAT/CAT [54] [5] verifiserer at utstyret er levert i henhold til spesifikasjoner.

Konklusjon
I kvalitetsplanen til prosjektet [57] står det beskrevet hvordan prosjektet kan oppfylle kvalitetskrav i henhold til ISO 9001:2000. Når det gjelder opplæring og ansvar står navnene på de ulike personene som har ansvarsstillinger i organisasjonskartet. Det er ikke utgitt noen form for oversikt over kvalifikasjonene til de ulike ansvarspersonene, som Curriculum Vitae, så det er opp til Kongsberg Maritime å se til at kravene til kvalifikasjon er oppfylt og være sikker på at personellet i de ulike rollene har den nødvendige kompetansen.

4.3.2 Spesifiserte sikkerhetskrav til SIS

De spesifiserte sikkerhetskravene til SIS blir vanligvis utviklet av eieren for å definere hvilke krav som settes til SIF, som igjen setter begrensninger til design av utstyr. Om punktene i kravdokumentet er oppfylt er en del av valideringsprosessen hvor leveransen fra alle underleverandører blir sjekket opp mot dette dokumentet for å se om utstyret følger gitte krav. Underleverandører, som KM var i dette prosjektet, svarer på kravene i en SAR [52], hvor alle oppfylte krav skal være dokumentert.

Generelle krav

I «West Elara»-prosjektet hadde ikke Seadrill eller Jurong utgitt en SRS, så kravene til brann- og gassystemet står i all hovedsak i filosofidokumentene fra Jurong [49] og i C&E-diagram [71]. I OLF-070 [14], vedlegg E, står alle kravene fra kapittel 10 i IEC 61511-1 [1] listet opp i tabell E.2. For å løse mangelen på SRS i dette prosjektet vil derfor alle de kravene i tabell E.2. som er relevante for KM sin leveranse, og den aktuelle SIF, bli sjekket opp mot dokumentasjonen til KM for å se om de har blitt dokumentert. Se tabell 4.3.2.1.

Tabell 4.3.2.1: Spesifiserte sikkerhetskrav til SIS, vedlegg E i OLF-070 [14]**.**

Punkt	Referanse til IEC-61511,10.3 [1]	Avvik? (Ja/ Nei)	Forklaring:
6	Krav for funksjonstestintervall.	Nei	Funksjonstesttiden er satt til 8760 timer. Dokumentert i SAR [52, p. 60].
8	SIL og operasjonsmodus for hver SIF.	Nei	KM har et SIL 2 nivå på flammedeteksjon og lav behovsrate. Dette er dokumentert i SAR [52, p. 8].
10	Beskrivelse av SIS-prosessen sine utgangsaksjoner og kriteriene for en suksessfull operasjon.	Nei	Beskrivelse av flammedeteksjon finnes i F&G-KFDD [6, p. 24]. Dette stemmer overens med Jurong sitt filosofidokument [49]
13	Krav relatert til NE eller NDE for utløsing.	Nei	NE-utganger er definert med «sikker feil» og aksjon som «spenningsløs». NDE-utganger er definert med «sikker feil» som spenningsløs og nedstengning som «spenning på». NDE trenger spenning for å aktivere en nedstenging. Dokumentert i SAR [52, p. 33].
14	Krav til omstart av SIS etter nedstenging.	Nei	SAR-rapporten skriver at K-Safe-systemet skal være fullstendig operativ etter en nedstenging. [52, p. 27]
16	Feilmodus og ønsket respons fra SIS.	Nei	Oppførsel og respons til maskinvarefeil/ svikt og programvarefeil/ svikt står beskrevet i SAR-rapporten. [52, p. 49] og i FMEA [53]
17	Alle spesifikke krav relatert til prosedyrer for oppstart og omstart av SIS.	Nei	SAR-rapporten [52, p. 26] skriver hvordan systemet vil oppføre seg ved oppstart/ omstart. Men en grundigere beskrivelse finnes i operasjonsmanualen [56] for systemet, hvor det står prosedyrer for start og nedstenging av systemet.

20	Håndhevelse av sikkerhetskravene til programvaren.	Ja	KM sin SAR [52, p. 53] inneholder informasjon om programvare med henvisning til blant annet konfigurasjonsmanualen [59], men den blir ikke utgitt i prosjekter. En mer prosjektspesifisert beskrivelse av programvaren ville gitt en bedre oversikt over hvilke krav som er oppfylt.
25	Alle ekstreme miljøforhold som er sannsynlig at SIS blir utsatt for skal bli identifisert.	Nei	Sikkerhetssystemet skal motstå yttergrensene for alle miljøforhold som det er sannsynlig at oppstår i løpet av livssyklusen. Dette er dokumentert i SAR [52, p. 54]. Det står også i SAR [52, p. 38] at feilratene er basert på «Navy Sheltered»-miljø.

SAR [52] dekker de fleste punktene som står i kapittel 10 i IEC 61511-1 [1] som er gjeldende for KM sin leveranse, men det som mangler er en skikkelig dokumentasjon av programvaren, som for eksempel hvilke programvaremoduler som blir brukt i de forskjellige SIF. Konfigurasjonsmanualen [59] er et generisk dokument som ikke er prosjektspesifisert og som ikke blir utgitt til kunden.

Det som også er viktig i SAR er å få tydelig fram alle antakelsene som er gjort for å tilfredsstille kravene til SIS, slik at man kan se om kravene er oppfylt for det gjeldende sikkerhetssystemet. Det gjelder spesielt antakelser som har blitt gjort under estimering av pålitelighetstall (PFD), og kan blant annet være miljøforhold, operasjonelle forhold eller vedlikehold. Dette er beskrevet i SAR [52] hvor det står at feilratene er basert på et «Navy Sheltered»-miljø, som stemmer overens med TÜV-rapporten [51]. En beskrivelse rundt hva som ligger i «Navy Sheltered» er ikke nevnt, så det burde vært beskrevet. Det samme gjelder temperaturforhold, som står beskrevet i TÜV-rapporten [51].

Spesifiserte sikkerhetskrav til brukerprogramvaren

Det er spesifiserte krav til brukerprogramvaren for hvert delsystem som er nødvendig for å sikre at funksjonene, arkitekturen og planleggingen er i samsvar med de sikkerhetskravene som er gitt til SIS som helhet. Kravene til brukerprogramvaren er gitt i IEC 61511-1 [1], kapittel 12.2, hvor det også står at et dokument som beskriver de spesifiserte kravene til brukerprogramvaren skal være utviklet. Et slikt dokument, som eieren av sikkerhetssystemet vanligvis utvikler, var ikke utgitt i dette prosjektet, så Kongsberg Maritime brukte C&E [71] og filosofidokumenter [49] fra Jurong Shipyard til å utvikle programvaren. Et av kravene i IEC 61511-1 [1] er at programvareutvikleren skal se igjennom informasjonen og kravene i spesifikasjonen for å avklare eventuelle mangler, uklarheter og lignende som kan skape utfordringer i en senere fase.

4.3.3 Design av SIS og teknisk arbeid

Målet med å analysere designfasen for West Elara er å vurdere og analysere om Kongsberg Maritime sitt bidrag til designet av det instrumenterte sikkerhetssystemet er i henhold til IEC-61511-1 [1], kapittel 11 og 12.4, og at kravene er dokumentert.

Generelle krav

Sikkerhetssystemet som KM leverer, K-Safe, kan ha forskjellige løsninger avhengig av hvilket SIL-nivå det stilles krav til. Den løsningen som var benyttet i dette prosjektet, K-Safe-2, var designet for bruk i SIL2 funksjoner og inneholdt alle sikkerhetsfunksjonene for brann- og gassdeteksjon. En K-Safe-2 løsning benytter redundante kontrollere (RCU) og prosessbuss (SPBus) med delt inngangs/ utgangskort (RIO) [52]. Konfigurasjonsmanualen [72, p. 24] beskriver at sikkerhetssystemet er et uavhengig system som opererer i tillegg til andre kontrollsystemer, det vil si at det ikke er andre instrumenterte funksjoner i dette systemet. Brann- og gassystemet er også uavhengig av andre sikkerhetssystemer, som ESD, dette er ikke dokumentert i KM sin dokumentasjon men kan vises i C&E-diagrammene [58], som KM har bygget logikken etter.

Når det gjelder kravet i punkt 11.2.3 i IEC 61511-1 [1], som omhandler funksjoner med forskjellig integritetsnivå, må man være påpasselig med at det ikke er noen andre sikkerhetsfunksjoner som krever et høyere integritetsnivå. OLF-070 [14], tabell 7,1, gir samtlige delfunksjoner i et brann- og gassystem som er omtalt i tabellen, et minimumskrav på SIL2. Man kan derfor lett anta at alle sikkerhetsfunksjoner til et brann- og gassystem har SIL2-krav hvis retningslinjen i OLF-070 [14] følges. Men denne retningslinjen dekker ikke alle sikkerhetsfunksjoner som kan inngå i et SIS, som for eksempel ventilasjonsstyring. Det er derfor viktig at man ikke blindt lager en design som dekker et SIL2 krav uten å sjekke hvilke funksjoner som er med. Det gjelder spesielt for KM, da logikkløseren deler både programvare og maskinvare til mange forskjellige sikkerhetsfunksjoner.

IEC 61511-1 [1] setter også krav til designen med tanke på menneskelige begrensninger, både at det skal settes konkrete krav og at designen skal rette seg etter dem. Dokumentasjonen fra KM sier lite om oppfyllelse av kravene, og dokumentasjonen fra Seadrill stiller ingen konkrete krav, utenom at Norsok S-002 [73] skal følges. Men en beskrivelse av hvordan systemet skal opereres står i ICMS-KFDD [4], som fungerer som et operatørdokument, og beskriver menneskelig brukergrensesnitt. Det er antatt at leseren av dokumentet har deltatt på AIM 2000 sitt treningsprogram. Dokumentet «AIM Safe Safety System» [50] fra KM nevner at: «AIM-systemet har et ensformig HMI-grensesnitt, som reduserer opplæringen for operatører, forenkler avgjørelsesprosesser og gir enklere vedlikehold.» Dette burde kanskje vært inkludert i et KFDD eller SAR [52], eller referert til.

Kravet om at SIS skal forbli i sikker tilstand er dokumentert i F&G-KFDD [6]. Det sier at brann- og gassystemet i en alarmsituasjon låser alle utgangene, og systemet forblir derfor i sikker tilstand fram til omstart av utgangene. Ved en feil i flammedetektoren, for eksempel ved tap av spenning, vil systemet gå i sikker tilstand fordi logikken tolker en feil som en reel brannalarm. Dette er dokumentert i C&E-diagrammene [58]. Det er også krav om manuell aktivering av systemet, noe som kan bli gjort fra de kritiske aksjonspanelene (CAP). De ble plassert i sentralt

kontrollrom (CCR), kontrollrommet til motoren (ECR) og kontrollrommet til boring (DCR), og inneholder blant annet statuslamper og trykknapper for manuell aktivering av brannpumper. Ved en oppdagelse av brann kan ESD-trykknappene bli brukt for å forhindre eskalering og bekjempelse av faren [6].

Krav til systemoppførsel ved deteksjon av en feil
SAR [52, p. 49] beskriver systemets oppførsel ved feil og sier at alle typer feil skal gi en melding eller alarm til operatørkonsollen. Ved feil i følgende utstyr skal dette skje:

- Feil i kontrollerne (RCU):
    - Hvis den ene kontrolleren i en 1-utav-2 løsning feiler, skal feilen isoleres og den andre kontrolleren skal ha styringen.
    - Hvis begge kontrollerne feiler vil utgangene gå til en sikker tilstand.
- Feil på inngangskortet:
    - Logikken vil avgjøre hva som er den beste løsningen. F&G-KFDD [6] lister opp feilgrensene (strømverdier) til detektoren og C&E-diagrammet [58] forteller aksjoner ved feil (strømbrudd).
- Feil på utgangskortet:
    - Utgangene går til en forhåndsdefinert sikkerfeil-tilstand.

Det er ikke fastsatt en prosedyre for hvordan opprettholde sikkerheten hvis reparasjonstiden overskrider gjennomsnittlig gjenopprettelsestid (MTTR). MTTR er i SAR [52] satt til å være 1 time, noe som eieren av SIS må vurdere, og etablere prosedyrer for hvordan opprettholde sikker tilstand hvis reparasjonstiden overgår denne grensen.

Krav til maskinvarens feiltoleranse.
Kravene til maskinvarens feiltoleranse til en K-Safe-2 løsning står beskrevet og listet opp i SAR [52, p. 32]. Tallene der er hentet fra IEC 61508 [3] del 2, tabell 2 og 3, og man får da litt andre definisjoner på komponenttypene enn det IEC 61511-1 [1] opererer med. IEC 61508 [3] skiller mellom «type A»- og «type B»-delsystemer, som noe grovt kan skilles ved at delsystemer som inneholder programmerbar elektronikk er type B og ikke-programmerbar elektroniske delsystemer er type A [14]. Denne løsningen kan også benyttes ifølge IEC 61511-1, kapittel 11.4.5 [1].

En viktig ting er at logikkløseren blir brukt under de samme forholdene som ble antatt under utregning av SFF. I TÜV-rapporten [51] kan vi se at feilratene fra enkeltkomponenter ble utregnet basert på MIL-HDBK-217F [32] for et marint utstyrsrom (Naval Sheltered) med en områdetemperatur på +35 °C. MIL-HDBK-217F definerer Naval Sheltered som beskyttede omgivelser eller under dekk på overflateskip eller ubåter. Den antakelsen er dekkende for utstyr om bord i utstyrsrom på en rigg.

Detektoren, levert av Autronica, oppfyller også kravene til maskinvarens feiltoleranse og er verifisert og sertifisert av Exida som en uavhengig tredjepart [45]. Kravet til flammedetektoren, for å benytte tabell 6 i IEC 61511-1 [1], er at den dominerende feilmodusen er til sikker tilstand eller at farlige feil blir detektert, altså at kravene i IEC 61511-1 [1] punkt 11.3 er oppfylt.

Krav for valg av komponenter og delsystemer.
K-Safe-systemet er utviklet i henhold til IEC61508 [3] del 2 og 3, og systemet er sertifisert av TÜVReinland [44] [52, p. 48]. Systemet er dermed dokumentert at det følger IEC 61508 [3], men som vist i delkapittelet over er det viktig å oppfylle betingelsene og at antakelsene gjort under sertifiseringen stemmer overens med de reelle omgivelsene. Det er også viktig å sjekke at den aktuelle utgivelsen av programvare eller oppgraderinger er inkludert i godkjenningen, så man får verifisert at godkjenningen gjelder for de modulene og logikkløseren man skal bruke.

Man skal også kunne dokumentere at det valgte utstyret er egnet til bruk i det aktuelle SIS, og dokumentasjonen som skal bevise at gitte krav er oppfylt er KM sin SAR [52]. Den inneholder spesifikke egenskaper og kvantifiserte feilverdier til bruk i utregning av pålitelighetstall til de aktuelle funksjonene, under de antakelser som står beskrevet der. Den prosjektspesifiserte SAR [52] inneholder for det meste kun informasjon om maskinvaren til KM. For en mer detaljert programvareinformasjon må konfigurasjonsmanualen [59] til programvaren benyttes.

Om det valgte utstyret er i samsvar med kravene til SIS og de spesifiserte kravene i et SRS-dokument, må sjekkes igjennom validering ved en gjennomgang av alle SAR-dokumentene fra underleverandørene. Det er derfor viktig at forhold som kan gå utover designen blir avklart i en så tidlig fase som mulig. Det er også viktig at SRS inneholder krav om de forhold som er listet opp i kapittel 10 i IEC 61511-1 [1], som går direkte på utforming av SIS, og spesifiserte sikkerhetskrav til brukerprogramvaren, kapittel 12.2. Uansett gjelder alle kravene i IEC 61511-1 [1], selv om alle nødvendigvis ikke er beskrevet i kravdokumentasjonen.

Feltutstyr
Feltutstyret i den analyserte SIF er en multi-spektrum IR flammedetektor, AutroFlame X33AF [74], som ble levert av Autronica Fire and Security. Detektoren, som normalt opererer innenfor 4-20mA, ble fysisk koblet til et av Kongsberg Maritime sine analoge inngangskort, RAIC-400, med en egen analog inngangskanal. Brukerprogramvaren til detektoren er konfigurert med alarmgrenser på strømverdier. Ved normal operasjon vil strømmen i sløyfen være på 4mA, men hvis strømmen synker til under 1,5mA vil en generell feilalarm aktiveres [6]. Detektoren kan også utstyres med passordbeskyttelse for å forhindre feil konfigurasjon av parameterne til detektorene [75].

For diskrete utgangssignaler som blir aktivert av brann- og gassystemet, er utgangskortet RDIO-401S utstyrt med følgende innebygde tester [52, p. 52]:

- Selvdiagnostikk og feilidentifikasjon.
- Innebygd FOST (Final Output Stage Test).
- Deteksjon av linjefeil.
- Innstillinger for sikre feil.

Grensesnitt

Operatørstasjonene (OS) er grensesnittet mellom brukeren/ operatøren og prosessystemet, og gir et grafisk brukergrensesnitt mot bildene i AIM 2000. Den lagrer også programfiler og konfigurasjonsdata til kontrollerne (RCU). En operatørstasjon består av minst én fargeskjerm til presentasjon av AIM-bilder, minst ett operatørpanel for implementering av data og kommandostyring, og et pekeverktøy som mus eller «trackball» [4].

I prinsippet kan derfor hele AIM 2000 systemet bli styrt og kontrollert fra en operatørstasjon, men det er lagt inn adgangsmekanismer for å begrense og styre adgangen til forskjellige funksjoner. Man kan begrense hvilke kontrollere (RCU) som er synlig i operatørstasjonen, operatørstasjonsgrupper kontroller hvilke prosessområder som kan bli styrt og adgangskontroll gir begrensninger til brukeres tilgjengelige funksjoner [4]. K-Safe er ikke avhengig av operatørstasjonene og en feil i disse vil ikke påvirke sikkerhetsfunksjonen i å få systemet til en sikker tilstand [52].

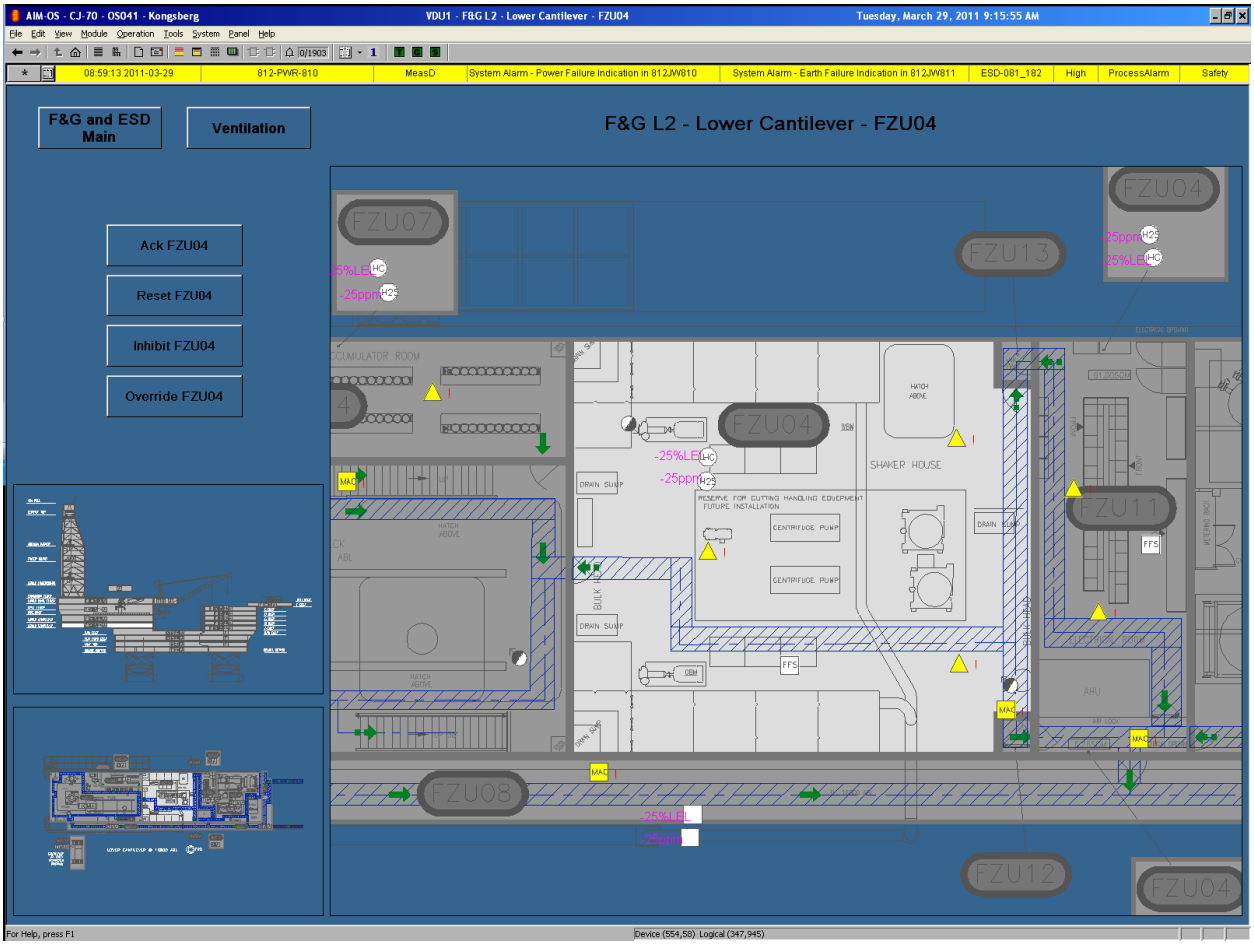
<u>Operatørgrensesnitt:</u>

Et godt system skal minimalisere en operatørs behov for valgmuligheter og å gjøre omkoblinger mens systemet kjører. Det er også viktig å forhindre, på en best mulig måte, at feil kan bli gjort ved for eksempel feil tastetrykk og lignende. AIM 2000 har opprettet forskjellige brukergrupper som begrenser tilgangen til forskjellige operasjoner. Disse er beskyttet med brukernavn og passord. Kommandogrupper over forskjellige deler av systemet, som F&G, ESD o.l. er opprettet og en operatør må aktivere den kommandogruppen han vil jobbe med. Dette for å forhindre at forskjellige personer på forskjellige operatørstasjoner jobber med den samme prosessen og skaper konflikter. For å forhindre endring av konfigurasjoner er brukeren nødt til å aktivere konfigurasjonsmodus. Systemet vil så gå tilbake til standard brukeroppsett etter en fastsatt tid hvis operatørstasjonen ikke blir brukt [6].

Under testing, eller andre nødvendige operasjoner, kan operatører forhindre utganger å bli aktivert, men inngangene vil fortsatt være aktive og gir alarm til operatørstasjonen hvis en farlig situasjon blir detektert i felt [6].

IEC 61511-1 [1] foreslår bruk av bekreftelsessteg for å bekrefte at operasjonen du ønsker å utføre er korrekt. AIM 2000 har to steg for å undertrykke signaler, ett for å velge «inhibit» og ett for å slå den av eller på, i tillegg må man være i rett brukergruppe og rett innloggingsnavn [4].

AIM 2000 opererer i all hovedsak med tre nivåbilder hvor man kan få oversikt og mer detaljert statusinformasjon. Som eksempel viser figur 4.3.3.1 et nivå-3-bilde av brannområdet FZU04, hvor flammedetektoren er plassert. En detaljert beskrivelse av hele systemet finnes i ICMS-KFDD [4] hvor blant annet visning av alarmer og fargekoder står beskrevet. Siste gjeldende alarm ligger øverst i bildet, rett under verktøylinjen, som hele tiden holder brukeren oppdatert på situasjonen. Man ser blant annet status over brannområdet, om noen signaler har undertrykking eller er tvangskjørt og man kan kvittere ut alarmer og omstarte området. Man har også oversikt over hele resten av prosessen på oversiktsbildene nede til venstre i bildet.



Figur 4.3.3.1, brannområde FZU04, «level 3»-bilde (Hentet fra Mimic 5.13.3) [76].

Statusen til flammedetektoren vises i «nivå 3»-bilde, mens statusen til brannområdet/ modulen blir vist i «nivå-1»- og «nivå-2»-bildene.

AIM 2000 har også andre verktøy for systemoversikt, som trendbilder, hendelseslister og lignende, og er beskrevet nærmere i KFDD-dokumenter levert i prosjektet. Kravene i IEC 61511-1 [1] til operatørgrensesnitt er dermed godt dokumentert [4].

Vedlikehold- / ingeniørgrensesnitt: Vedlikeholdsgrensesnittet til AIM 2000 er det samme som for operatørgrensesnittet. Forskjellen er at man nå har flere tilgjengelige funksjoner som er nødvendig for testing/ utkoblinger. Man har derfor de samme sikkerhetsfunksjonene i dette grensesnittet som ved vanlig operasjon [4, p. 70]. I ICMS-KFDD [4] står det beskrevet tilgangen til de forskjellige brukergruppene.

Kommunikasjonsgrensesnitt: Kommunikasjonsgrensesnittene skal ikke ved en feil sette sikkerhetsfunksjonene til systemet ute av stand til å bringe prosessen i en sikker tilstand [1]. Kongsberg Maritime sitt prosessnettverk, som alle sikkerhetsdatamaskinene er koblet til, kontrollerer trafikken på nettverket, nettverk A og B, ved hjelp av lokale brytere (switches). Disse to sikrer en adekvat uavhengighet mellom forskjellige sikkerhetssystemer og prosesskontrollsystemet. Andre tester, som «CRC-checksum»-test (Cyclic Redundancy Check) og overvåking av signaler mellom de forskjellige datamaskinene, sikrer også en sikker kommunikasjon. Dette er dokumentert i SAR [52, p. 16] som også sier at nettverket er godkjent av TÜV [44] som en del av sertifiseringsprosessen.

Designkrav til vedlikehold eller testing

En flammedetektor testes vanligvis ved at man aktiverer detektoren i felt og ser at man får et aktivt signal inn til kontrolleren og at alle utgangene som skal ha aksjoner blir aktivert. Så for flammedetektoren er tilkomst og siktlinje hovedpunktene under design med tanke på vedlikehold. Når det gjelder KM sitt utstyr, så beskriver SAR [52] hovedprinsippene for hvordan de forskjellige komponentene som inngår i SIF skal testes.

Deteksjon av flamme er i OLF-070 [14] definert som en global delfunksjon, som starter fra en flamme er synlig i detektoren, til en aktiv utgang fra logikkløseren. Det betyr at testen må inkludere de nødvendige utgangskortene i tillegg. Her kan man med fordel dele opp testen slik at man tester detektorene sammen med logikkløseren i én omgang, og så tester man sluttelementene sammen med logikkløseren i andre omgang. På den måten slipper man å aktivisere/ teste de samme detektorene mer enn en gang når detektorene inngår i flere sikkerhetsfunksjoner.

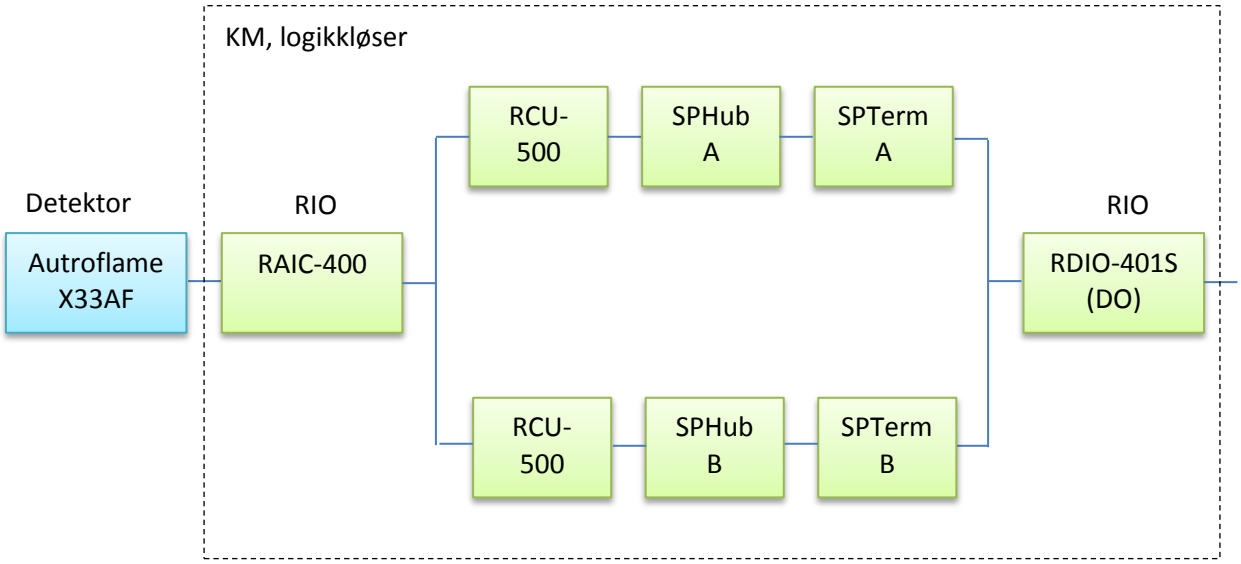
Kontrollerne, RIO-kortene og spenningssystemet ble installert i fire kabinetter som ble plassert i forskjellige lokale utstyrsrom, hvor feltkabelen fra flammedetektoren ble koblet direkte til

inngangskortet [6]. Det fysiske utstyret fra KM som inngår i test- og vedlikeholdsaktiviteter er således testbart og lett tilgjengelig for vedlikehold.

Styring av testen og nødvendig undertrykking/ overbroing eller utkobling av signaler, utføres på operatørstasjonene hvor man også kan se hvilke innganger og utganger som blir aktivert og hvilke verdier de har [6]. Hvilke funksjoner man har lov til å utføre på operatørstasjonene er avhengig av brukertilgang og adgangskontroll. Tvinging av signaler og utganger, undertrykking eller å utføre overbroing kan sette SIF ut av funksjon og man kan miste sikkerhetsfunksjonen. Gode prosedyrer må derfor være på plass for å kunne gjennomføre slike operasjoner på en sikker måte. Det er i dette tilfelle eieren/ operatørselskapet sitt ansvar. Alle utkoblede signaler kommer opp som hendelser i hendelseslisten [6, p. 50], på nivåbildene (figur 4.3.3.1) og de har fargekoden cyan [72, p. 94].

Sannsynlighet for at SIF feiler

Kalkulasjonene for K-Safe-2, finnes i SAR [52, p. 60]. Denne funksjonen er i behovsmodus så den kvantifiserte pålitelighetsverdien er PFD_{avg}. Her er det antatt at logikkløseren, fra inngang til utgang, må være innenfor 15 % av det totale kravet til PFD_{avg} til en SIL2-løsning, for at hele SIF skal oppfylle kravet. For denne funksjonen, med analog inngang (RAIC-400), digital utgang (RDIO-401S), redundant RCU og seriell kommunikasjon (SPHub og SPTerm), er den totale PFD-verdien beregnet til $6{,}43E^{-04}$. Autronica-detektoren er sertifisert av Exida [45] som har vurdert detektoren til å kunne være i en SIL2-løsning, med den antakelsen at PFD_{avg} for sensoren er innenfor 35 % av den totale PFD_{avg} for SIL2-kravet gitt i IEC 61511-1 [1].



Figur 4.3.3.2, modulene i den instrumenterte delfunksjonen (basert på SAR [52]**)**

Ifølge OLF-070 [14] er SIL-kravet til en deteksjon fra en brann-/ gassdetektor SIL2, og filosofidokumentet fra Jurong [49] sier at designen til F&G-systemet skal møte SIL2-kravene i IEC 61508 [3]. For å oppnå dette må PFD_{avg} ligge mellom $\geq 10^{-3}$ til $< 10^{-2}$ ifølge tabell 3 i IEC-61511-1 [1].

Feilratene til Autroflame X33AF, i tabell 4.3.3.1, er hentet fra Exida-sertifikatet [45] og funksjonstestintervallet er antatt å være på 8760 timer, det samme som er oppgitt i SAR [52] til KM. Tallene i tabell 4.3.3.2 er hentet fra KM sin SAR [52].

Tabell 4.3.3.1: Autroflame X33AF mA m/ HART [45]**.**

Utstyr	**λ_{SD}**	**λ_{SU}**	**λ_{DD}**	**λ_{DU}**	**τ [timer]**	**SFF**
X33AF mA	0	$3{,}63E^{-7}$	$2{,}615E^{-6}$	$1{,}33E^{-7}$	8760	95,7 %

Tabell 4.3.3.2: KM logikkløser [52, p. 39]**.**

Utstyr	**λ_{tot}**	**λ_{DU}**	**β**	**τ [timer]**
RAIC-400	$1{,}35E^{-05}$	$1{,}35E^{-7}$	0,05	8760
RCU500, med SPBus	$1{,}75E^{-05}$	$2{,}15E^{-7}$	0,05	8760
SPHub	$3{,}96E^{-06}$	$1{,}98E^{-7}$	0,05	24*
SPTerm	$6{,}63E^{-06}$	$3{,}32E^{-7}$	0,05	24*
RDIO 401S (DO)	$1{,}74E^{-05}$	$1{,}39E^{-7}$	0,05	24*

**FOST-test: Testen aktiverer alle utgangskanalene med et intervall på 24 timer som fører til at SPHub, SPTerm og RDIO 410S som får et funksjonstestintervall på τ = 24 timer* [52, p. 29]

Ved kalkulasjon av PFD vil de tilnærmede formlene i OLF-070 i tabell D.4 [14] bli brukt og et funksjonstestintervall på τ = 8760 timer som er antatt i SAR [52]. Den totale PFD_{avg} til logikkløseren skal ligge innenfor 15 % av den totale PFD_{avg} til sikkerhetsfunksjonen [52].

Total $PFD_{avg,\ log}$ skal altså være mindre enn $1{,}5*10^{-3}$.

PFD, KM logikkløser:

$$PFD_{avg,RAIC} \approx \frac{\lambda_{DU,RAIC} \cdot \tau_{RAIC}}{2} = \frac{1{,}35 \cdot 10^{-7} \cdot 8760}{2} = 5{,}913 \cdot 10^{-4}$$

$$PFD_{avg,RCU} \approx \frac{\lambda_{DU,RCU} \cdot \tau_{RCU}}{2} = \frac{2{,}15 \cdot 10^{-7} \cdot 8760}{2} = 9{,}417 \cdot 10^{-4}$$

$$PFD_{avg,SPHub} \approx \frac{\lambda_{DU,SPHub} \cdot \tau_{SPHub}}{2} = \frac{1{,}98 \cdot 10^{-7} \cdot 24}{2} = 2{,}376 \cdot 10^{-6}$$

$$PFD_{avg,SPTerm} \approx \frac{\lambda_{DU,SPTerm} \cdot \tau_{SPTerm}}{2} = \frac{3{,}32 \cdot 10^{-7} \cdot 24}{2} = 3{,}984 \cdot 10^{-6}$$

$$PFD_{avg,RDIO} \approx \frac{\lambda_{DU,RDIO} \cdot \tau_{RDIO}}{2} = \frac{1{,}39 \cdot 10^{-7} \cdot 24}{2} = 1{,}668 \cdot 10^{-6}$$

RCU og SPBus, 1-utav-1:

$$PFD_{avg,RCU+SPBus,1oo1} \approx PFD_{avg,RCU} + PFD_{avg,SPHub} + PFD_{avg,SPTerm} = 9{,}4706 \cdot 10^{-4}$$

RCU og SPBus, 1-utav-2:

$$PFD_{avg,RCU+SPBus,1oo2} \approx \beta \cdot PFD_{avg,RCU+SPBus,1oo1} = 4{,}7353 \cdot 10^{-5}$$

Total PFD_{avg} for K-Safe-2:

$$PFD_{avg,log} \approx PFD_{avg,RAIC} + PFD_{avg,RCU+SPBus,1oo2} + PFD_{avg,RDIO} = 6{,}403 \cdot 10^{-4}$$

Logikkløseren oppfyller dermed kravene til sannsynligheten for å feile ved behov, PFD_{avg}, for en SIL 2 funksjon med de antakelsene gjort i SAR [52]. Vi har også tidligere sett at de miljøforhold og temperaturforhold som er antatt i TÜV-rapporten [51] stemmer med de reelle omgivelsene.

Arkitektoniske begrensninger

For å sjekke HFT i henhold til IEC 61511-1 [1], kalkulerer man fraksjon av sikre feil, SFF, og sjekker komponentene opp mot tabell 5 eller tabell 6 i [1].

$$SFF = \frac{(\lambda_{tot} - \lambda_{DU}) \cdot 100}{\lambda_{tot}}$$

$$SFF_{RAIC} = \frac{(\lambda_{tot,RAIC} - \lambda_{DU,RAIC}) \cdot 100}{\lambda_{tot,RAIC}} = \frac{(1{,}35 \cdot 10^{-5} - 1{,}35 \cdot 10^{-7}) \cdot 100}{1{,}35 \cdot 10^{-5}} = 99\%$$

$$SFF_{RCU} = \frac{(\lambda_{tot,RCU} - \lambda_{DU,RCU}) \cdot 100}{\lambda_{tot,RCU}} = \frac{(1{,}75 \cdot 10^{-5} - 2{,}15 \cdot 10^{-7}) \cdot 100}{1{,}75 \cdot 10^{-5}} = 98{,}7\%$$

$$SFF_{SPHub} = \frac{(\lambda_{tot,SPHub} - \lambda_{DU,SPHub}) \cdot 100}{\lambda_{tot,SPHub}} = \frac{(3{,}96 \cdot 10^{-6} - 1{,}98 \cdot 10^{-7}) \cdot 100}{3{,}96 \cdot 10^{-6}} = 95\%$$

$$SFF_{SPTerm} = \frac{(\lambda_{tot,SPTerm} - \lambda_{DU,SPTerm}) \cdot 100}{\lambda_{tot,SPTerm}} = \frac{(6{,}63 \cdot 10^{-6} - 3{,}32 \cdot 10^{-7}) \cdot 100}{6{,}63 \cdot 10^{-6}} = 94{,}9\%$$

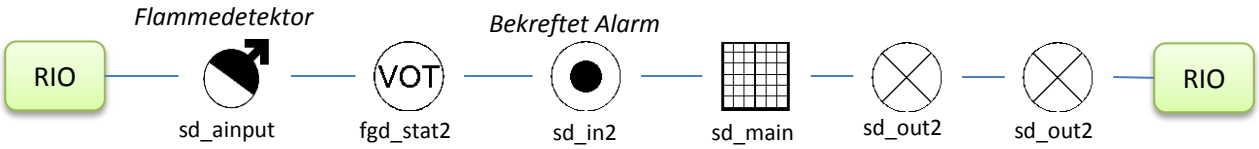
$$SFF_{RDIO} = \frac{\left(\lambda_{tot,RDIO} - \lambda_{DU,RDIO}\right) \cdot 100}{\lambda_{tot,RDIO}} = \frac{(1{,}74 \cdot 10^{-5} - 1{,}39 \cdot 10^{-7}) \cdot 100}{1{,}74 \cdot 10^{-5}} = 99{,}2\%$$

For programmerbare elektroniske logikkløsere benyttes tabell 5 i IEC 61511-1 [1] og man ser der at minimum HFT er 0 for alle komponentene ved et SIL2-nivå med en SFF > 90 %. Det er derfor ingen arkitektoniske begrensninger til logikkløseren.

Diagnostikk dekning (DC): K-Safe-systemet inneholder diagnostiske funksjoner for både programvaren og maskinvaren. Disse funksjonene, sammen med den definerte sikre tilstanden, representerer alle sikre feil og farlige detekterte feil. En oversikt over alle diagnostiske tester som «K-Safe»-systemet utfører, og som har blitt godkjente av TÜV [51], finnes i SAR-dokumentet [52, p. 51].

Tester for å sjekke følsomhet til elektromagnetisk støy og til klimatiske og mekaniske forhold er beskrevet i TÜV-rapporten [51] men har ikke blitt beskrevet i prosjektdokumentasjonen.

Design og utvikling av brukerprogramvare
KM bruker modulbasert programmering for å utvikle brukerprogramvaren til SIS, hvor modulene skal være utviklet, oppgradert og vedlikeholdt i henhold til IEC 61508 [52]. Hvordan de er utviklet, eller en referanse til prosedyrer, er ikke beskrevet. Modulene som skal brukes i sikkerhetssystemer er listet opp i tabell 6.1. i konfigurasjonsmanualen [59].



Figur 4.3.3.3, brukerprogramvaremodulene som er brukt i SIF [59]**.**

Figur 4.3.3.3 viser de modulene som flammedeteksjonsfunksjonen inneholder [59]:
sd-ainput: Modulen leser det analoge signalet fra RIO-kortet.
fgd_stat2: Modulen representerer voteringslogikken og selv om flammedetektoren ikke ble votert, ble voteringsmodulen allikevel inkludert. Dette er et standard oppsett fra Kongsberg Maritime for å være proaktiv mot endringer.
sd_in2: Denne modulen representerer årsakslinjen i C&E-diagrammet. Årsakmodulen vil kun bli tilbakestilt etter at en detektoralarm er inaktiv og kvittert.
sd_main: Modulen framstiller matrisen i C&E-diagrammet og kobler årsakene og effektene sammen. Det er utviklet ett C&E-diagram for hvert brannområde.
sd_out2: Effekten til C&E-diagrammet blir framstilt av denne modulen. En brann- og gassfunksjon har to sd_out2 moduler. En til brannområdet og en direkte til RIO.

Ved bruk av modulbasert programmering kan IEC 61511-1 [1] benyttes for systemet så lenge disse modulene er utviklet i henhold til IEC 61508 [3]. Det er viktig å bemerke at selv om man bruker moduler som basis for brukerprogramvaren, så må det ikke ligge mye annen logikk bak som styrer modulene. For eksempel spesiell voteringslogikk eller tellesekvenser. Da må IEC 61508 [3] benyttes.

K-Safe har innebygde tester for å overvåke og sjekke integriteten til dataen. For analoge inngangssignaler blir blant annet signalstyrken fra detektoren overvåket med forskjellige alarmgrenser på strømstyrken. En oversikt over de diagnostiske testene i hver modul står beskrevet i brukermanualen for modulene (MUM), som beskriver i detalj hvilke egenskaper hver modul har og hvilke parametere som normalt brukes [77].

Hoveddokumentet til brukerprogramvaren i dette prosjektet er konfigurasjonsmanualen [59] til sikkerhetssystemer. Dokumentet inneholder følgende informasjon i henhold til IEC 61511-1 [1]:

- Juridisk enhet: Kongsberg Maritime står som eier av programvaren til logikkløseren, dokumentert i systembeskrivelsen.
- Dokumentet beskriver grunnleggende prinsipper, det beskriver alle modulene som inngår i sikkerhetssystemet, typiske konfigurasjonsmetoder, sekvenser, alarmer, symboler osv.
- Manualen har ikke sporbarhet til de funksjonelle kravene gitt av Jurong Shipyard i «F&G Design Philosophy»-dokumentet [49]. Disse er kun generelt referert til i F&G-KFDD [6].
- Retningslinjer og standardfunksjonene er beskrevet.
- Innganger og utganger: Dette er listet opp i I/O-listen [78] som det er referert til i konfigurasjonsmanualen.
- Alle endringer ble gjort i ICR-databasen i IAS Change Register og i henhold til prosedyre PRO-2105 [79]. Men det er ikke en eneste referanse til prosedyren i konfigurasjonsmanualen [59].

Konfigurasjonsmanualen [59] er en generisk konfigurasjonsmanual til både ESD, PSD og F&G. Det er viktig å ha et prosjektspesifisert dokument som spesifikt beskriver brukerprogramvaren til de ulike funksjonene, hvilke moduler som er brukt, verktøy osv. Dette må være sporbart tilbake til kravdokumentene fra kunden og kravene i IEC 61511-1 [1].

Arkitekturkrav til brukerprogramvaren

Designen av arkitekturen til brukerprogrammet skal være basert på kravene i kundens SRS. I dette prosjektet ble arkitekturen basert på Jurong Shipyard sitt «brann- og gassfilosofi»-dokument [49] og C&E-diagrammene [71] og den skal oppfylle de kravene som står beskrevet der. Et kravdokument som står beskrevet i punkt 12.4.3.1 og punkt 12.2.2.1 i IEC 61511-1 [1] var ikke utviklet.

Konfigurasjonsmanualen [59, p. 144] beskriver arkitekturen til brukerprogramvaren, hvor hver programvaremodul vises sammen med koblingene mellom dem, mens F&G-KFDD [6] beskriver brann- og gassystemet. Beskrivelsen av selve koblingen mellom de ulike maskinvaremodulene til logikkløseren finnes i SAR-dokumentet [52]. De nevnte dokumentene inneholder også spesifikasjonene til de ulike modulene.

Testene som er innebygd i logikkløseren og brukerprogramvaren for å verifisere sikkerhetsintegriteten til all data står beskrevet i SAR [52, p. 51], der alle testene innebygd i de forskjellige modulene i logikkløseren er nevnt.

Krav til støtteverktøy, brukermanualer og programvarespråk
I dette prosjektet ble følgende hovedverktøy brukt for å utvikle brukerprogramvaren til den aktuelle SIF:
CETool: Verktøy til å opprette/ endre C&E matriser og tag-koblinger
CEOnline: Brukes for å vise C&E-bildet i AIM
CEProvider: Oppdatere CEOnline-filer basert på ps-filen, som er programvaren sin konfigurasjonsfil.
Offline Configuration Tool, OCT: Blir brukt sammen med CETool til å opprette ps- og io-filer (io-filene omfatter IO-kortet og IO-signaler som er koblet sammen til programvaremodulene i ps-filene).
Generic Variant Utility: Dette er et hjelpeverktøy som brukes til å generere bilder i AIM til sikkerhetsapplikasjoner.

Det er også en del verktøy som følger prosjektet ut levetiden. Disse er listet opp i ICMS-KFDD [4, p. 171] sammen med lisensinformasjonen. Prosedyrer for bruk av verktøyene er det ikke referert til eller nevnt i prosjektdokumentasjonen. Men konfigurasjonsmanualen [59] refererer til hjelpefiler for verktøyene. Det står en beskrivelse av disse verktøyene i konfigurasjonsmanualen [59, p. 276], men det står ikke, som IEC 61511-1 [1] anbefaler, en redegjørelse på hvorfor disse verktøyene er valgt og kjente svakheter som kan føre til feil i programvaren. Simulering av signaler og operasjoner kan gjøres direkte i AIM 2000 på operatørstasjoner, hvor testverdier kan gis og resultatet leses i for eksempel trend-diagrammer.

Sikkerhetsmanualen er i IEC 61511-1 [1] definert som en manual som beskriver hvordan utstyret, delsystemet eller systemet kan blir sikkert anvendt. IEC 61511-1 [1] setter ikke krav til at det må være et eget dokument, men åpner for at informasjonen kan være implementert i andre brukermanualer. Så informasjon rundt oppfyllelse av kravene i punkt 12.4.4.7 i IEC 61511-1 [1] står i forskjellige dokumenter:

- F&G-KFDD [6, p. 71] og SAR [52, p. 51] beskriver hvilke tester som overvåker og sjekker systemet for eventuelle feil. Hvordan man skal konfigurere testene står beskrevet i konfigurasjonsmanualen [59].
- En liste over programvaremoduler til bruk i sikkerhetsprogramvare finnes i tabell 6,1 i konfigurasjonsmanualen [59].
- Konfigurasjonsmanualen [59] beskriver også test og nedstengingslogikk.
- SAR [52, p. 51] sier at RCU 500 bruker vakthund (watchdog).
- Verktøyene som er installert, og som brukes til konfigurasjon av sikkerhetssystemer, står beskrevet i konfigurasjonsmanualen [59]. Det vises til hjelp-filer i dokumentet men ikke hvor hjelp-filene finnes eller begrensninger til verktøyet. Det står hvilke begrensninger programmeringsspråket har, hvilke sikkerhetsmoduler som skal benyttes samt hvordan man skal konfigurere dem.
- Kravet til det integrerte sikkerhetsnivået som utstyret eller systemet kan brukes i, står beskrevet i F&G-KFDD [6] og i SAR [52]. Der står det beskrevet at F&G-systemet er designet til bruk i SIL2-systemer og at løsningen har blitt sertifisert av TÜV [44].

Konfigurasjon av brukerprogramvare og bruk av verktøyer er noe som krever kompetent personell med erfaring innen sikkerhetssystemet fra Kongsberg Maritime. Konfigurasjonsmanualen [59] blir derfor ikke utgitt men kan bli vist til kunden på oppfordring. Men det bør komme tydeligere fram i prosjektdokumentasjonen hvilke begrensninger kunden eller andre brukere har for å opprettholde sikkerheten til systemet.

Krav for utvikling av brukerprogramvaren

Kongsberg Maritime utvikler programvaremoduler i programmeringsspråket C, som er et fult variabelt programmeringsspråk, noe som krever oppfyllelse av IEC 61508 [3].

Man skal kunne dokumentere robuste brukerprogrammoduler der man beskriver testene som blir gjort, en full definisjon av inngangs- og utgangsgrensesnitt og konfigurasjonssjekker. Brukerprogrammodulene blir utviklet i henhold til IEC 61508 [3], men det er ikke beskrevet hvilke prosedyrer som blir brukt under utvikling av modulene. Det som står i SAR [52] er at det blir benyttet v-modellen i IEC 61508 [3] del 3 figur 5, men det burde også stå hvilke interne prosedyrer som blir benyttet for å oppfylle v-modellen. I prosjekter som ikke krever nye programvaremoduler benyttes de ferdige sikkerhetsmodulene som er listet opp i SAR [52] tabell 6.1.

En full oversikt over alle modulene som Kongsberg Maritime har utviklet, blant annet med beskrivelse, historie og hva som er den siste versjon, finnes i «Module User Manual» [77], som er et oppslagsverk utviklet i «HTML Help files». Her kan man sjekke hvilken modul som er den siste versjonen, slik at man får verifisert om den er godkjent til bruk i sikkerhetsfunksjoner som har krav til sikkerhetsintegritet.

Når man benytter ferdige moduler får man en god oversikt over arkitekturen til programvaren, og man kan enkelt se hvordan programmet er bygget opp, se figur 4.3.3.3. Men som nevnt tidligere så er det viktig at det ikke ligger mye logikk skjult bak programvaremodulene som gjør at man får et usikkert og uoversiktlig program.

Krav til testing av modulene til brukerprogramvaren
For å teste selve brukerprogramvaren og konfigureringen ble det gjennomført interne tester, Internal Acceptance Test (IAT) og test sammen med kunden, Factory Acceptance Test (FAT) [54]. Disse testene følger faste prosedyrer (den samme prosedyren benyttes for både IAT og FAT) hvor alt som skal testes er beskrevet, sammen med det utstyret som skal brukes, og krever at hvert punkt blir signert. For å se hvilke utganger som skal bli aktive ved en spesifisert aktivert inngang brukes C&E-diagrammer [71]. En mer omfattende test sammen med maskinvaren er integrasjonstesten, Customer Acceptance Test (CAT) [5], som er siste godkjenningstest før, i dette tilfelle, kunden utførte ferdigstillelsestester. Da blir alt utstyret fra alle forskjellige leverandører testet for å forsikre at hele systemet virker i henhold til de kravene som er satt.

Krav til integrasjonstest av brukerprogramvare
Under CAT [5] gjøres det en mer komplett integrasjonstest hvor man tester fra inngangskortet og til utgangskortet. Man setter en manuell verdi på inngangskortet og verifiserer at man får et signal på rett utgangskort. Testprosedyren beskriver ikke krav til å tilkoble feltutstyr for å verifisere, i dette tilfelle, at detektoren virket, så den fasen kom ikke før under ferdigstillelsesfasen, noe som Kongsberg Maritime ikke var ansvarlig for i dette tilfellet. Hvem som har ansvar for de forskjellige aktivitetene skal stå klart i planleggingsdokumentet for styring av SIS.

Gjennomgang av kravene i IEC 61511-1 [1]**:**
I tabell 4.3.3.3 står oversikten over om Kongsberg Maritime oppfyller kravene i IEC 61511-1 [1] med tanke på dokumentasjon av designen til SIS og teknisk arbeid, det vil si kravene i kapittel 11 og 12.4 i IEC 61511-1 [1]. Kun de kravene innenfor KM sitt arbeidsomfang i det aktuelle prosjektet og den aktuelle SIF har blitt vurdert.

Tabell 4.3.3.3: Resultat av kapittel 11 og 12,4 i IEC 61511-1 [1]**.**

Punkt:	**Krav (fullstendig i IEC 61511-1 [1])**	**Avvik? (Ja/ Nei)**	**Oppfyllelse**
11.2 Generelle krav			
11.2.1	Designet skal være i henhold til SRS.	Ja	Se kapittel 4.4.3. og konklusjonen i dette kapittelet.
11.2.6	Krav til menneskelige begrensninger.	Nei	ICMS-KFDD [4] fungerer som et operatørdokument og beskriver menneskelig brukergrensesnitt. Det er antatt at leseren av dokumentet har deltatt på AIM 2000 sitt treningsprogram.
11.2.7	Krav om å forbli i sikker tilstand etter at systemet har satt prosessen i en sikker tilstand.	Nei	Dette er dokumentert i F&G-KFDD [6] som sier at F&G-alarmer må bli kvittert ut av en operatør. Hvis ikke blir det innen 2 minutter vil plattformalarmen bli aktivert.
11.2.8	Krav til manuell aktivering.	Nei	Dette er dokumentert i F&G-KFDD [6] som beskriver funksjonen til CAP. Denne aktiverer funksjonen manuelt uavhengig av logikken.
11.2.9	Krav til uavhengighet.	Nei	Dette er dokumentert i F&G-KFDD [6], som sier at sikkerhetssystemet er uavhengig og et tillegg til andre kontrollsystem. En hendelse i kontrollsystemet vil ikke hindre sikkerhetssystemet fra å gå til sikker tilstand.
11.2.10	Krav til sikkerhetskomponenter og prosesskontrollfunksjoner.	Nei	Denne SIF blir ikke brukt til annet enn flammedeteksjon. Dokumentert i C&E [58].
11.2.11	Delsystemer som ikke går til sikker tilstand ved spenningstap.	Nei	Hvis ikke begge kontrollerne fungerer vil alle utgangene gå til sikker tilstand. Dette er dokumentert i F&G-KFDD [6]. En detektorfeil vil aktivere en brannalarm, dette er dokumentert i C&E [58].
11.3 Krav for systemoppførsel ved deteksjon av en feil			
11.3.1	Krav til delsystemer som kan tolerere en enslig maskinvarefeil.	Nei	Hvis begge kontrollerne ikke fungerer vil alle utgangene gå til sikker tilstand. Dette er dokumentert i F&G-KFDD [6]
11.3.2	Krav til delsystemer som ikke er redundant.	Nei	En detektorfeil vil aktivere en brannalarm, dette er dokumentert i C&E [58].
11.4. Krav til maskinvarens feiltoleranse			
11.4.1	Krav om feiltoleranse til maskinvare.	Nei	SAR [52] beskriver HFT.
11.4.5	Minimum HFT.	Nei	Dokumentert i SAR [52]. Dette punktet i IEC 61511-1 ble brukt som en erstatter for 11.4.2 til 11.4.4.

11.5 Krav for valg av komponenter og delsystemer			
11.5.2.1	Er komponentene/ delsystemene i henhold til IEC 61508 [3] eller IEC 651511-1 [1]?	Nei	Utstyret er i samsvar med IEC 61508 [3] og dokumentert i SAR [52] og TÜV-rapporten [51].
11.5.2.3	Valgt utstyr skal være velegnet.	Nei	Dokumentert i prosjektdokumentasjonen. Se kapittel 4.4.1.
11.5.2.4	Utstyret skal være i overenstemmelse med SRS.	Nei	Dette prosjektet hadde ikke et SRS-dokument fra eieren, kun filosofidokument [49] og C&E-diagram [71]. Utstyret fra KM er i henhold til disse dokumentene, dokumentert i prosjektdokumentasjonen. Se kapittel 4.4.1.
11.6 Feltutstyr			
11.6.2	Diskrete innganger/ utganger.	Nei	Flammedetektoren har analog inngang, og digitale utganger på RDIO 401S-kortet har innebygde tester. Dokumentert i SAR-rapporten [52].
11.6.3	Egne dedikerte ledere til inngangskortet.	Nei	Flammedetektoren deler verken signalledere eller inngangskanalen. Dokumentert i I/O listen. [78]
11.6.4	Skrivebeskyttet flammedetektor.	Ja	Flammedetektoren kan være skrivebeskyttet. Dokumentert i datablad til detektoren [75]. Men det er ikke spesifisert i dokumentasjonen fra KM om den skal være av eller på.
11.7 Grensesnitt			
11.7.1.1	Feil som kan oppstå i prosesskontroll-grensesnittet.	Nei	En feil i en operatørstasjon vil ikke kunne påvirke funksjonene til SIS. Dokumentert i SAR [52, p. 32]
11.7.1.2	Minimalisere operatørens valgmuligheter og behov for omkobling.	Nei	Flere brukergrupper og kommandogrupper er laget for å sette begrensninger til de forskjellige brukerne. Dette er dokumentert i F&G-KFDD [6, p. 50].
11.7.1.3	Omkoblingsbrytere skal ha brukerbeskyttelse.	Nei	Systemet har forskjellige brukergrupper med forskjellige muligheter. Dette er dokumentert i F&G-KFDD [6, p. 50].
11.7.1.4	Statusinformasjon til SIS.	Nei	Alarmer og statusinformasjon som er tilgjengelig er godt dekket i F&G-KFDD [6] og «Alarm System Philosophy»-dokumentet. [80]
11.7.1.5	Operatørgrensesnittet skal forhindre endringer i brukerprogramvaren.	Nei	Flammedetektoren er ikke avhengig av informasjon fra andre kontrollsystem og man trenger konfigurasjonstilgang for å kunne gjøre endringer i brukerprogramvaren. Dette er dokumentert i F&G-KFDD [6].

11.7.2.1	Feil i vedlikeholdsgrensesnittet skal ikke påvirke evnen SIS har til å bringe prosessen til sikker tilstand.	Nei	Feilhåndtering og pålitelighet er den samme i AIM 2000 uavhengig av hvilken bruker man er innlogget med, men tilgjengelige funksjoner er endret. Dokumentert i ICMS-KFDD [4]. En feil i en operatørstasjon vil ikke kunne påvirke funksjonene til SIS. Dokumentert i SAR [52, p. 32]
11.7.2.2	Grensesnittet skal ha de funksjonene som er nevnt i kravet, med adgangsbeskyttelse.	Nei	En oversikt over brukertilgangen finnes i ICMS-KFDD [4, p. 133]. Navn på brukergruppen og tilganger kan endres alt etter hva kravet er fra leverandøren.
11.7.2.3	Vedlikeholdsgrensesnittet skal ikke bli brukt som operatørgrensesnitt.	Nei	Grensesnittet er passordbeskyttet og brukeren vil bli logget ut etter en viss tid hvis ikke operatørstasjonen er i bruk. Dokumentert i ICMS-KFDD [4, p. 69].
11.7.2.4	Krav til etablering og utkobling av lese- / skrivetilgang.	Nei	Bare «system»- og «Admin»-brukere har tilgang til dette. Dette er dokumentert i ICMS-KFDD [4, p. 133]. Prosedyrer for endring av brukergruppene og sikkerhetstiltak må komme fra eierne av SIS.
11.7.3.1	Ingen feil i kommunikasjonsgrensesnittet skal forhindre SIS i å bringe prosessen til sikker tilstand.	Nei	Nettverket er beskyttet av brytere, «switcher», som forhindrer unødvendig trafikk, og ingen feil i nettverket vil forringe sikkerhetsnivået. Dokumentert i SAR [52, p. 16] og TÜV-rapporten [51].
11.7.3.2	SIS skal kunne kommunisere med BPCS og ytre enheter uten å forstyrre SIF.	Nei	Brytere i nettverk A og B skaper uavhengighet mellom prosesskontrollsystemet og sikkerhetssystemet. Dokumentert i SAR [52, p. 16].
11.7.3.3	Kommunikasjonsgrensesnittet skal være robust til å motstå elektromagnetisk interferens uten å skape farlige feil i SIF.	Ja	Elektromagnetisk forstyrrelse og overspenning er ikke nevnt i SAR eller prosjektdokumentasjonen. Men det som er nevnt i F&G-KFDD [6] er at kontrollerne (RCU) lagrer alle prosessdataene og konfigurasjon, og kan operere selv om nettverket bryter sammen. TÜV-rapporten [51] dokumenterer testing for EMC, men dette bør også stå i prosjektdokumentasjonen.
11.7.3.4	Kommunikasjonsgrensesnittet skal være egnet til å kommunisere mellom utstyr med forskjellig jordingspotensial.	Ja	Dette er ikke nevnt i prosjektdokumentasjonen.

11.8 Designkrav til vedlikehold eller testing			
11.8.1	Designen skal tillate tesing.	Nei	KM sin design tillater testing og undertrykking av aktuelle utganger. Man kan også teste programvaren på operatørstasjonen. Dokumentert i SAR [52, p. 27].
11.8.3	Krav til overbroing.	Nei	En oversikt i alle områdebildene i VDU viser om utstyr i modulen/ brannsonen har overbroing eller blir tvangskjørt. Dette er dokumentert i F&G-KFDD [6] Det er også begrensninger til de forskjellige brukerne når det gjelder tilgang til overbroing. Dokumentert i ICMS-KFDD [4].
11.8.4	Tvinging av innganger/ utganger i PE SIS.	Nei	Kongsberg har ikke laget driftsprosedyrer men gitt forskjellige brukere adgang til funksjoner i AIM 2000. Tvinging av innganger/ utganger vil bli visualisert i VDU og i hendelseslister. Dette er dokumentert i ICMS-KFDD [4]. Prosedyrer for operasjon må komme fra eieren av systemet.
11.9 Sannsynlighet for at SIF feiler			
11.9.1	PFD til hver SIF skal være kalkulert og innenfor gitte krav.	Nei	Dette er dokumentert i SAR [52] og er innenfor gitte krav for KM sitt utstyr.
11.9.2	Den kalkulerte PFD til hver SIF skal ta hensyn til gitte punkt. Se IEC 61511-1 [1]	Ja	De nevnte faktorene i punktet er tatt hensyn til i TÜV-rapporten [51] men SAR [52] mangler beskrivelse av følsomhet til EMC forstyrrelser.
12.4 Design og utvikling av brukerprogramvare			
12.4.2.2	Designmetoden skal være i samsvar med utviklingsverktøyet og restriksjoner i det anvendte delsystemet til SIS.	Ja	En tydelig beskrivelse av restriksjoner for å opprettholde sikkerheten må være i prosjektdokumentasjonen. Noen restriksjoner er gitt i konfigurasjonsmanualen [59], som hvilke sikkerhetsmoduler som er tillatt, men alle restriksjoner bør være tydelig skrevet i et eget kapittel.
12.4.2.3	Den valgte designmetoden og brukerprogramvaren bør besette egenskaper som forenkler de punkt nevnt i forskriften.	Nei	Designmetoden er beskrevet i konfigurasjonsmanualen [72] og bruk av godkjente sikkerhetsmoduler gir en god oversikt over brukerprogramvaren. Modulbasert brukerprogram forenkler kompleksiteten i programvaren.

12.4.2.4	Krav til den oppnådde designen i henhold til punktene gitt i underkapittelet. Krav til blant annet sporbarhet.	Ja	K-Safe har en rekke tester som sjekker integriteten til all data som blir kommunisert. Dette er godt dokumentert i SAR [52]. Systemet kan testes, og grunnleggende testing er beskrevet i F&G-KFDD [6]. Den ferdige designen har reservert kapasitet til modifisering. Beskrevet i konfigurasjonsmanualen [72]. I den står det også beskrevet hvordan forskjellige SIF skal designes for å holde størrelse og kompleksitet til et minimum. Men de dokumenterte kravene er ikke sporbare tilbake til de gitte kravene. Mange av opplysningene står i forskjellige dokumenter som gjør det hele uoversiktlig.
12.4.2.7	Minimum innhold i dokumentasjonen til brukerprogramvaren.	Ja	Mange av kravene er oppfylt, men det som mangler er sporbarhet til funksjonskravene, hvor man beviser at hvert krav til de forskjellige SIF er oppfylt. Det er heller ikke referanser til endringsdatabasen. Det er viktig at all informasjon om brukerprogramvaren kommer i ett dokument, så kan man ha referanser til mer utfyllende dokumenter.
12.4.3 Krav til brukerprogramvarens arkitektur			
12.4.3.1	Arkitekturens design skal være i henhold til de spesifiserte kravene.	Nei	Det ble ikke utviklet et spesielt kravdokument til arkitekturen i dette prosjektet.
12.4.3.2	Beskrivelse av arkitekturen til brukerprogramvaren	Ja	Beskrivelsen til arkitekturen finnes i SAR [52], F&G-KFDD [6] og konfigurasjonsmanualen [59]. Men det hadde vært en fordel å få all informasjonen i ett dokument eller et dokument som referer til andre dokument hvor informasjonen står. Hvilke programvaremoduler som blir benyttet til hver SIF finnes kun som generisk informasjon i konfigurasjonsmanualen [59].
12.4.3.3	De metodene og teknikkene som er brukt for å utvikle brukerprogramvaren bør være identifisert og begrunnelse for valg.	Nei	Metoden for utvikling av brukerprogramvaren står beskrevet i konfigurasjonsmanualen [59] som brukes som en veiledning for utviklingen. IEC 61511-1 [1] anbefaler velprøvde brukerprogramvaremoduler.
12.4.3.4	Restriksjoner identifisert i sikkerhetsmanualen.	Ja	Det var ikke utviklet en sikkerhetsmanual for dette prosjektet. Men det bør være et dokument som setter begrensninger til konfigurasjon og programmeringsmetoder.

12.4.3.5	Funksjonene som er brukt for å opprettholde sikkerhetsintegrasjon til all data.	Nei	Diagnostiske tester er listet opp i SAR [52, p. 51]
12.4.4 Krav til støtteverktøy, brukermanual og applikasjonsspråk			
12.4.4.1	Verktøy skal være valgt.	Nei	Verktøyene som skal brukes til konfigurasjon av brukerprogramvare står beskrevet i konfigurasjonsmanualen [59].
12.4.4.2	Tilgjengeligheten til egnede verktøy.	Nei	En liste over verktøyene som er installert og har lisens finnes i ICMS-KFDD [4]. Der finnes de viktigste verktøyene som CETools, CEProvider og CEOnline.
12.4.4.3	Dekkende prosedyrer for bruk av verktøyene bør være tilgjengelig.	Ja	Prosedyrer for verktøyene er ikke beskrevet, og heller ikke en beskrivelse av rett bruk med tanke på å opprettholde sikkerheten. I konfigurasjonsmanualen [59] henvises det kun til hjelpefiler uten å spesifisere det. IEC-61511-1 [1] setter ikke krav til punktet men sier at det bør være oppfylt.
12.4.4.4	Krav til programvarespråket.	Nei	Brukerprogramvaren er modulbasert med egne sikkerhetsmoduler. Dette er beskrevet i konfigurasjonsmanualen [59].
12.4.4.6	Krav til prosedyrene til programmeringsspråket.	Nei	Konfigurasjonsmanualen [59] dekker dette punktet. Den viser typiske programfunksjoner basert på modulene og hvordan konfigurere de.
12.4.4.7	Sikkerhetsmanualen	Ja	Det var ikke utviklet en egen sikkerhetsmanual i dette prosjektet. Konfigurasjonsmanualen [59] dekker mange av punktene men ikke sikker bruk av verktøy og begrensninger til bruken.
12.4.4.8	Verktøyenes egnethet skal verifiseres.	Ja	En kort beskrivelse er gitt i konfigurasjonsmanualen [59] men verktøyets egnethet er ikke verifisert.
Krav til utvikling av brukerprogramvare:			
12.4.5.1	Informasjon som skal være tilgjengelig før starten av detaljert brukerprogramdesign.	Nei	Konfigurasjonsmanualen [59] er en retningslinje på hvordan designe sikkerhetsbrukerprogram.
12.4.5.2	Brukerprogramvaren bør være produsert på en strukturert måte.	Nei	Konfigurasjonsmanualen [59] gir retningslinjer som gir en strukturert måte å utvikle brukerprogramvaren på.
12.4.5.3	Designen av hver modul skal være robust.	Nei	Definisjon av innganger og utganger finnes i IO lister [78], looptegninger og i konfigurasjonsmanualen [72]. Brukerprogramvaren har innebygd diagnostiske tester og konfigurasjonen blir testet av IAT, FAT [54] og CAT [5].

12.4.5.4	Designen av hver modul i brukerprogramvaren og de strukturelle testene som skal gjennomføres på hver modul skal være spesifisert.	Ja	Konfigurasjonsmanualen sier at sikkerhetsmodulene til bruk i sikkerhetssystem er utviklet, oppgradert og vedlikeholdt i henhold til IEC 61508 [3]. Men det er ikke spesifisert hvilke tester som har blitt gjort eller referanser til prosedyrer.
12.4.5.5	Hva brukerprogrammet bør være. Se spesifikke punkt i IEC 61511	Nei	Ved modulbasert godkjent design, bruk av konfigurasjonsmanualen [59] og TÜV sertifisering [44] er punktet oppfylt.
12.4.5.6	Brukerprogramvaren skal bli gjennomgått.	Nei	IAT oppfyller dette punkt. Den er en intern FAT [54].
Krav til test av modulene til brukerprogramvaren			
12.4.6.1	Konfigurasjonen, skal sjekkes fra inngang til utgangen,.	Nei	Dokumentert i IAT/ FAT prosedyrer [54], der står det beskrevet hvordan alle innganger og utganger blir sjekket i henhold til C&E [71] og gjeldende krav.
12.4.6.2	Hver modul som brukes i brukerprogrammet skal testes.	Nei	Modulene blir testet i IAT/ FAT [54], i tillegg er de utviklet, oppgradert og vedlikeholdt i henhold til IEC 61508 [3]. Dokumentert i konfigurasjonsmanualen [59]
12.4.6.3	Testresultatene skal være tilgjengelige.	Nei	Testresultatene fra IAT/ FAT [54] er tilgjengelige i dokumentdatabasen til prosjektet.
12.4.7 Krav til integrasjonstest av brukerprogramvaren			
12.4.7.1	Testen skal vise at alle modulene til brukerprogramvaren og komponentene/ delsystemene samarbeider korrekt.	Nei	CAT [5] dekker testomfanget, og omfatter integrering av programvare, system og enkeltkomponenter.
12.4.7.2	Testresultatet skal være tilgjengelig.	Ja	Resultatet av testen er tilgjengelig sammen med feil som er oppdaget og som har blitt registrert i avviksregisteret. Det som ikke står skrevet er grunnen til feil, det er kun nevnt hva som feilet [5].
12.4.7.3	Alle endringer skal vurderes ved en sikkerhetsinnvirkningsanalyse.	Ja	Det står ikke beskrevet i CAT-prosedyren [5] hvordan endringer eller modifikasjoner skal håndteres.

Konklusjon

Mange av punktene er oppfylte i F&G-KFDD [6], ICMS-KFDD [4], konfigurasjonsmanualen [59] og SAR [52], men det mangler en god struktur slik at man får sporbarhet tilbake til gitte krav. Spesielt mangler det et prosjektdokument som beskriver brukerprogramvaren til de forskjellige SIF. Begrensninger og rett bruk av programvare og verktøy må også være grundig beskrevet slik at man oppnår sikker bruk uten at sikkerhetsintegriteten forringes.

4.3.4 Integrasjon av brukerprogramvaren med SIS

En integrasjonstest i dette prosjektet var CAT [5] hvor Kongsberg Maritime har en generisk prosedyre på hvordan en slik test skal gjennomføres. Feil som kom fram under CAT ble registrert i en mangelliste, hvor feil ble beskrevet og utbedret senere.

Testresultatet fra CAT [5] er tilgjengelig i dokumentmappen for prosjektet (DMS), hvor også mangellisten er tilgjengelig. For å oppfylle kravene i IEC 61511-1 [1] må feil som blir oppdaget under testing dokumenteres nøye ved blant annet å dokumentere:

- Grunnen til feilen.
- En analyse av feilen.
- Korrektive tiltak, sammen med omprøving og verifiseringer.

Gjennomgang av kravene i IEC 61511-1 [1]**:**
Kravene i IEC 61511-1 [1] blir gjennomgått i tabell 4.3.4.1.

Tabell 4.3.4.1: Resultat av kapittel 12.5.

Punkt:	**Krav (fullstendig i IEC 61511-1 [1]):**	**Avvik? (Ja/Nei)**	**Forklaring:**
12.5 Integrering av brukerprogramvare i SIS-delsystemer			
12.5.2.1	Integrasjonstester skal være spesifisert så tidlig som mulig.	Nei	CAT-prosedyren [5] er et generisk dokument som er tilgjengelig i prosjektets startfase.
12.5.2.2	Endringer eller modifikasjoner skal være gjenstand for en sikkerhetsinnvirkningsanalyse.	Ja	Mangler referanse til endrings-/ modifikasjonsprosedyrer i CAT-dokumentet [5] slik at det klart kommer fram hva som kreves.
12.5.2.3	Informasjon som skal være tilgjengelig	Ja	En beskrivelse av hvilken informasjon som skal være tilgjengelig, bør stå i CAT-prosedyren [5].

Konklusjon
CAT-prosedyren [5] sier ikke noe om hvordan man skal håndtere forandringer av design, eller hvilken prosedyre som skal bli brukt. KM har endringsprosedyrer, som prosedyrer for revisjon [64] og avvikshåndtering [63], så en mer utdypende forklaring/ prosedyre på hvordan mangler skal bli klarert og godkjent burde stått i CAT-prosedyren [5]. En beskrivelse av informasjon som skal være tilgjengelig når man registrerer en mangel bør også stå i CAT-prosedyren [5], slik at man kan forsikre seg om at all informasjon er tilgjengelig.

4.3.5 Dokumentasjon

Å ha god dokumentasjon er viktig i et sikkerhetssystem. Nødvendig informasjon skal være tilgjengelig igjennom hele livsløpet, og skal være forståelig for alle involverte i andre livsløpsfaser. En forståelig dokumentasjon gjør også valideringsprosesser enklere, og man kan unngå mange diskusjoner og revisjoner hvis kravene er tydelig og presist dokumentert.

Hovedprosedyren til dokumenthåndtering er prosedyren PRO-0002 [62]. Det stiller krav til identifisering av dokumentene, revisjonshåndtering og gjennomsyn. I tillegg beskriver prosedyren PRO-0005 [81] hvordan og hvor lenge dokumentene skal lagres. Kunden får tilgang til Kongsberg Maritime sitt dokumentsystem via fjerntilgang, hvor de kan hente ut dokumentasjon til hjelp i operasjon og vedlikehold. Kongsberg Maritime vedlikeholder systemdokumentene og tegningene slik at informasjonen stemmer så langt det lar seg gjøre. Dette kommer fram av anbudet [82]. Vi skal nå se om kravene i IEC 61511-1 [1], kapittel 19 er oppfylt.

Gjennomgang av kravene i IEC 61511-1 [1]**:**
Kravene i IEC 61511-1 [1] er gjennomgått og resultatet er presentert i tabell 4.3.5.1

Tabell 4.3.5.1: Resultat av kapittel 19.

Punkt:	**Krav (fullstendig i IEC 61511-1 [1]):**	**Avvik? (Ja/Nei)**	**Forklaring:**
19.2.1	Dokumentene som standarden krever skal være tilgjengelige.	Ja	Alle dokumentene er tilgjengelig i Kongsberg Maritime sitt dokumentsystem, men konfigurasjonsmanualen [59] ble ikke utgitt til kunden. Deler av denne bør være utgitt da SAR [52] ikke inneholder detaljert programvareinformasjon.
19.2.2	Dokumentasjonen bør: - Beskrive installasjonen, systemet og utstyret, og bruken av den. - Være nøyaktig. - Være lett å forstå. - Være passende til den bruken den er ment for. - Være tilgjengelig.	Ja	Dokumentasjonen er ikke nøyaktig nok. Den er ikke spesifisert mot hver SIF men har mer generisk informasjon. Dette gjelder spesielt for konfigurasjonsmanualen [59] som er et generisk dokument. Dette punktet er ikke et krav men IEC-61511-1 [1] sier at det bør være oppfylt.
19.2.3	Dokumentasjonen skal ha en unik identitet.	Nei	Alle dokumentene har et eget unikt dokumentnummer som beskrevet i prosedyren KM-PRO-0002 [62]. Dokumentnummeret blir automatisk generert av dokumentstyringssystemet.
19.2.4	Dokumentene skal ha en benevning som forteller informasjonstype.	Nei	Dokumentene har egen tittel, som SAR, KFDD, FMEA som forteller klart hvilken type dokument det er.

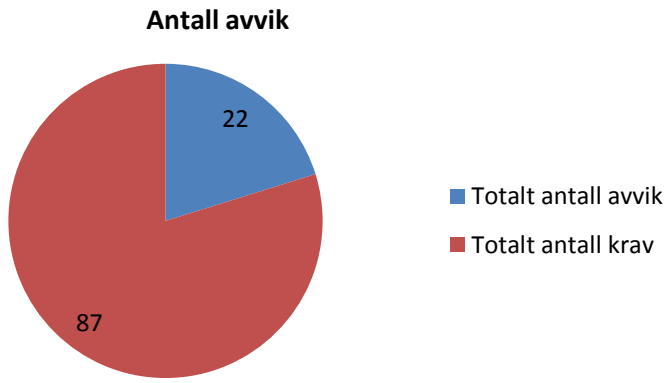
19.2.5	Dokumentene skal være sporbare til kravene i standarden.	Ja.	Dokumentene er ikke sporbare tilbake til kravene. Det er kun henvist generelt til IEC 61508 [3].
19.2.6	Dokumentene skal ha revisjonsindeks som gjør det mulig å identifisere forskjellige versjoner av informasjonen.	Nei	Revisjonssystemet består av et alfabetisk system hvor første utgivelse får revisjon A, neste B osv. sammen med dato fra når revisjonen ble gjeldende.
19.2.7	Dokumentene skal være strukturert slik at det kan søkes etter informasjon. Og det skal være mulig å identifisere siste revisjon.	Nei	Dokumentsystemet DMS er inndelt med systemnummer som gjør det enkelt å finne dokumentene. Siste revisjon finnes også i dokumentsystemet hvor kun siste revisjon til dokumentet er tilgjengelig.
19.2.8	All relevant dokumentasjon skal være godkjent og være i et kontrollsystem.	Nei	Dokumentene blir både sjekket og godkjent av andre enn personen som laget dokumentet. Alle dokumenter blir systematisk plassert i dokumentkontrollsystemet DMS. Dette er beskrevet i PRO-0002 [62].
19.2.9	Dokumenter som skal vedlikeholdes (se standarden [1])	Nei	KM leverer dokumentasjon til kunden som en del av leveransen i en delt database. KM vedlikeholder systemdokumenter og tegninger. Dette kommer fram av anbudet [82].

Konklusjon:
Hovedmanglene er et offentlig programvaredokument som kan beskrive løsninger og oppfyllelse av kravene som IEC 61511-1 [1] setter til programvaren. I tillegg skal oppfyllelsen av kravene være sporbare tilbake til kravene i IEC 61511-1 [1] og bør også være sporbar til kundens kravdokumentasjon.

4.4 Oppsummering og anbefalinger:

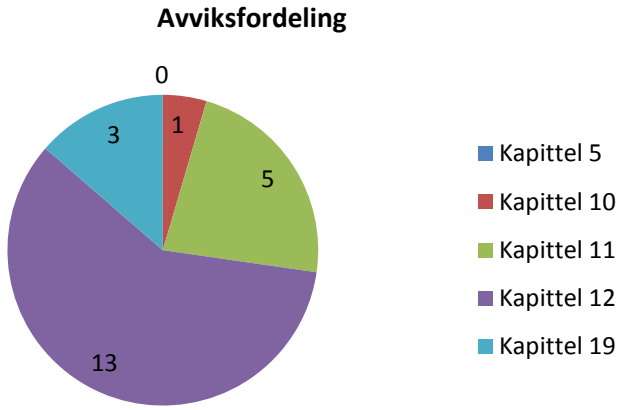
For å oppsummere antall avvik som ble registrert vises nå en oversikt over antallet og fordelingen av avvik i de forskjellige kapitlene i IEC 61511-1 [1]. Det er viktig å påpeke at denne analysens mål var å få en oversikt over hva standarden stiller krav til, og hva som eventuelt må endres på i eksisterende dokumentasjon for å kunne, på en oversiktlig måte, dokumentere at kravene er oppfylt. Når det gjelder terminologien «en oversiktlig måte» vil det være analytikerens subjektive mening hva som ligger i det uttrykket. Det var også mangel på en SRS fra kunden i prosjektet, slik at de forskjellige SIF ikke var skikkelig identifisert, noe som gjorde sporbarhet tilbake til kravene vanskelig.

Som nevnt i innledningen til analysen står det i IEC 61511-1 [1] i kapittel 4 at for å oppfylle kravene i standarden skal det vises at kravene i kapittel 5 til 19 har blitt oppfylt i henhold til de definerte kriteriene. Man må derfor kunne dokumentere at kravene er oppfylt. I tillegg står det at dokumentasjonen skal være sporbar tilbake til kravene i IEC 61511-1 [1]. Antall avvik ble da som vist i figur 4.4.1:



Figur 4.4.1, antall avvik i GAP-analysen.

Avviksfordelingen mellom de forskjellige kapitlene i IEC 61511-1 [1] er vist i figur 4.4.2:



Figur 4.4.2, avviksfordeling mellom kapitlene i IEC 61511-1 [1]**.**

Hvis man ser på avviksfordelingen mellom de forskjellige kapitlene ser vi at kapittel 12 i IEC 61511-1 [1] har flest avvik. Det var ingen avvik i kapittel 5, styring av funksjonell sikkerhet, som er ett kapittel hvor Kongsberg Maritime hadde begrenset ansvar da dittee kapittelet i hovedsak retter seg mot eieren av SIS, det vil si de som er ansvarlig for hele livssyklussen til sikkerhetssystemet.

Det er mye informasjon i konfigurasjonsmanualen [59], SAR [52] og «KFDD»-dokumentene [6] [4] som dekker mange av punktene gitt i IEC 61511-1 [1] og sammen med et sertifisert system er mye av verifikasjonen i orden. Men det er noen hovedpunkter som bør nevnes.

Sporbarhet:
Kongsberg Maritime bruker generiske dokumenter som legger grunnlaget for de prosjektspesifiserte dokumentene. Dette er en bra måte å gjøre det på, men man må spesifisere prosjektdokumentasjonen på en bedre måte slik at man får sporbarhet tilbake til kravene fra kundens kravdokumentasjon. Dette gjelder spesielt for brukerprogramvaren som ikke har et eget prosjektdokument og som bare generelt er beskrevet i SAR [52]. Det er også krav i IEC 61511-1 [1] at dokumentasjonen er sporbar tilbake til kravene i standarden.

Verktøy
Det mangler en komplett beskrivelse av verktøyene som blir brukt, hvordan de brukes og hvilke begrensninger de har. Noe står i konfigurasjonsmanualen [59] men kun med begrenset informasjon.

Testprosedyrer
Det mangler en god beskrivelse og oversikt over de prosedyrer som skal brukes ved en oppdagelse av feil og mangler. Hvilken informasjon som kreves ved en feil, som grunnen til at feilen oppsto og analyse av feilen, bør også stå i CAT-prosedyren [5].

4.5 Forslag til forbedring

Som underleverandør er det viktig å levere en dokumentasjon som er mest mulig i samsvar med kundens forventninger og i henhold til kravene. Det er derfor viktig å standardisere dokumenttypene slik at kunden, og de som jobber i prosjektene, vet hvor de skal finne informasjon og hvordan dokumentene skal opprettes. Ulike dokumentnavn kan skape forvirring da man ikke vet hvor og i hvilket dokument man kan forvente å finne ønsket informasjon. Dette er også viktig med tanke på sporbarhet tilbake til kravene i IEC 61511-1 [1]. Så for å standardisere dokumentasjonen mest mulig etter IEC 61511-1 [1] har jeg følgende forbedringsforslag:

Sikkerhetsmanual
Sikkerhetsmanualen er definert i IEC 61511-1 [1] som en manual som definerer hvordan utstyret, delsystemet eller systemet kan bli anvendt på en sikker måte. Den skal derfor beskrive aspekter av installasjon, vedlikehold, konfigurasjon, programmering og operasjon som negativt kan påvirke sikkerheten til utstyret. Det skal også beskrive hvordan man opprettholder kravene i SRS igjennom livssyklusen [83]. Dette dokumentet er et viktig dokument da feil bruk av utstyr kan påvirke sikkerheten. Man kan for eksempel i utvikling eller modifikasjon av brukerprogramvaren benytte andre programvaremoduler enn de som er testet og sikkerhetsgodkjente, noe som fører til redusert sikkerhet.

For å gjøre et slikt dokument oversiktlig kan det være en idé å referere i sikkerhetsmanualen til andre prosjektdokumenter. For eksempel kan begrensningene til verktøy som blir brukt i

utvikling av brukerprogramvare stå i SAR, men bli referert til i en sikkerhetsmanual. Det samme gjelder for operatørdokumentasjon da det er en fordel å ha begrensningene til den jobben som skal utføres i samme dokument hvor beskrivelsen står.

Konfigurasjonsmanualen

Denne generiske manualen er et godt verktøy for å finne informasjon om hvordan ting skal gjøres. Men siden den er et generisk dokument så mister man sporbarheten til spesifikke krav, beskrevet i SRS eller andre kravdokumenter. Man har derfor ingen oversikt over hvilke verktøy, programvarearkitektur og brukerprogramvaremoduler som er benyttet i det konkrete prosjekt og den konkrete SIF. Manualen er også ment som et internt dokument som kan gis ut etter ønske fra kunden.

Forslaget er derfor å beholde det som det er, som et internt generisk dokument, og heller bruke informasjon fra dokumentet til å generere en SAR for programvaren.

Programvare-SAR

Dette dokumentet er noe som mangler i dokumentasjonen fra Kongsberg Maritime. SAR [52] inneholder i dag stort sett maskinvare og SIL-beregninger og har ikke så stor fokus på programvaredelen, men henviser isteden til konfigurasjonsmanualen [59].

For å kunne dokumentere at alle kravene til brukerprogramvaren er oppfylt, er det derfor nødvendig å ha en programvare-SAR. En annen mulighet er å utvide den eksisterende SAR slik at all nødvendig informasjon om programvaren blir dokumentert i prosjektdokumentasjonen. Da kan man konkret knytte brukerprogramvaren opp mot den enkelte SIF i prosjektet. Det vil si at hver SIF blant annet blir beskrevet med programvaremodulene som programvaren er oppbygd med, hvilke diagnostiske funksjoner den har, hvordan de skal testes og hvilket verktøy som blir brukt.

Safety Analysis Report

For få tilpasset SAR til hvert prosjekt, slik at sporbarheten blir bedre, er det viktig at hver SIF blir beskrevet med hvilket utstyr/ moduler de forskjellige funksjonene er bygd opp med. Det kan gjøres med at de forskjellige SIF i SIS blir listet opp med referanse til den løsningen de benytter. I SAR er det i dag listet opp alle de løsningene som K-Safe har, som ulike redundante løsninger, men de er ikke knyttet opp mot konkrete SIF. Ved å ha en oversikt over hvilken K-Safe-løsning de forskjellige SIF har, øker man sporbarheten tilbake til SRS.

Faren ved å bruke en generisk SAR er at den kan inneholde mye unødvendig informasjon som ikke er relevant for det aktuelle prosjektet. En generisk SAR er bra å ha som et utgangspunkt og som informasjonskilde, men i prosjektet sin SAR må kun relevant informasjon stå. Å ha en SAR

som er oversiktlig med en god struktur er viktig for lett å kunne verifisere at utstyret og løsningen oppfyller kravene som er gitt.

Kongsberg Funksjonal Design Document

Formålet med dokumentet er å beskrive funksjonalitetene og grensesnittene til kontrollsystemet i henhold til gitte krav. Det skal også virke som et operasjonsdokument sammen med Kongsberg Maritime sin standard operasjonsdokumentasjon og vedlikeholdsmanual.

Her må man passe på at man ikke har mye informasjon som allerede står i andre prosjektdokumenter. Å ha samme informasjon i flere dokumenter gjør det vanskelig å oppdatere alle dokumentene med rett informasjon hvis det kommer endringer. Det kan derfor ikke være nødvendig med en F&G-KFDD da informasjonen i den kan bli dekket av de andre prosjektdokumentene.

En annen løsning vil være å kun ha informasjon i F&G-KFDD som går på operasjonelle forhold, og som ikke direkte er knyttet til oppbygning og design. Man kan da heller ha referanser til de andre dokumentene slik at den ønskede informasjonen blir enkel å finne.

5 KONKLUSJON

IEC 61511-1 [1] er en viktig standard for å sikre pålitelighet og kvalitet ved bruk av instrumenterte sikkerhetssystemer. Vi har nå sett på hva et sikkerhetssystem er, hvilke feil som kan oppstå og hvordan en typisk livssyklus ser ut. Vi har også sett på usikkerhet og antakelser rundt kvantifiserte «PFD»-verdier og en mulig løsning for å forhindre at man bruker utstyr og komponenter utover de antakelser som har blitt gjort under design. Videre har vi sett på et gjennomført leveringsprosjekt fra Kongsberg Maritime for å avdekke svakheter ved dokumentasjonen og sett på mulige forbedringsmuligheter.

PFD-tallene inneholder usikkerhet og er basert på antakelser gjort under design. Det er derfor viktig å være kritisk til de estimerte pålitelighetstallene som blir presentert og man må sjekke hva som ligger bak tallene. Pålitelighetstall som har blitt framstilt på en frekventistisk metode er basert på bakgrunnsinformasjon, det kan være feil i modellene og de kan være basert på antakelser om forhold som ikke blir de reelle. Jeg mener derfor at et merkesystem som ble presentert i kapittel 3.5 kan redusere denne usikkerheten rundt antakelser som har blitt gjort, slik at parameterne som ligger til grunn er mest mulig korrekte. Som vi så kan et slikt system også være til hjelp ved innsamling av feildata til sikkerhetsutstyr.

Å kunne dokumentere alle antakelser slik at de kommer tydelig fram og at alle krav er oppfylt er noe man må ha fokus på for å forhindre feil bruk av utstyr. I resultatet fra GAP-analysen ser vi forbedringsmuligheter her. Å ha en dokumentasjon der oppsettet er mest mulig lik i hele olje- og gassindustrien har mange fordeler, blant annet at kan ambiguitetsusikkerhet reduseres ved at man har en felles forståelse av prosessen. Det er viktig å ha god dokumentasjon som klart viser at kravene er oppfylt og hva som skal til for at de skal være oppfylt gjennom hele levetiden. Å ha en SAR som også inneholder programvare er også viktig. En uoversiktlig programvarestruktur kan øke faren for systematiske feil og det kan være vanskelig å forstå hvordan brukerprogramvaren er oppbygd. Derfor er det viktig at denne blir godt dokumentert med sporbarhet tilbake til kravene slik at også valideringsfasen blir enklere. Med en oversiktlig og godt strukturert dokumentasjon med sporbarhet tilbake til kravet, kan diskusjoner rundt oppfyllelse av krav reduseres, valideringsarbeidet blir enklere og man har dokumentert hvordan sikkerheten til SIS skal opprettholdes igjennom hele livstidsløpet.

6 REFERANSER

[1] International Electro-technical Committee, «IEC 61511-1, Functional safety - Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements,» 2003-01.

[2] Petroleumstilsynet, «Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (Styringsforskriften),» 29.04.2010.

[3] International Electro-technical Committee, «IEC 61508, Functional safety of electrical/electronic/programmable electronic safety related systems,» 1998.

[4] Kongsberg Maritime, «1086010, Kongsberg Functional Design Document - ICMS General System, Jurong Shipyard H:11-1092,» Revisjon F.

[5] Kongsberg Maritime, «1086054, CAT Procedure: Fire&Gas System, Jurong Shipyard H:11-1092,» Revisjon E.

[6] Kongsberg Maritime, «1086024, Kongsberg Functional Design Document - Fire & Gas System, Jurong Shipyard H:11-1092,» Revisjon G.

[7] T. Aven, Pålitelighets- og risikoanalyse, Universitetsforlaget, 2006.

[8] S. Sklet, «Safety barriers: Definition, classification, and performance,» Journal of Loss Prevention in the process industries 19(5):494-506, 2006.

[9] M. A. Lundteigen, «Safety instrumented systems in the oil and gas industry: Consepts and methods for safety and reliability assessments in design and operation.,» NTNU, Trondheim, 2009.

[10] B. Gordon, «Mapping Fixed Gas Detectors and Flame Detectors,» November 2011. [Internett]. Available: http://www.petro-online.com/search/articles/. [Funnet 16 Juni 2011].

[11] Petroleumstilsynet, «Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (Rammeforskriften),» 2011-01.

[12] Petroleumstilsynet, «Forskrift om utføring av aktiviteter i petroleumsvirksomheten (Aktivitetsforskriften),» 29.04.2010.

[13] Petroleumstilsynet, «Forskrift om utforming og utrustning av innretninger med mer i petroleumsvirksomheten (Innretningsforskriften),» 29.04.2010.

[14] OLF-GL-070, «Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry,» The Norwegian Oil Industry Association, 2004.

[15] Angela E. Summers, Kimberly A. Ford, Glenn Raney, «Estimation and Evaluation of Common Cause Failures in SIS,» “Safeguard Safety Instrumented Systems,” Chemical Engineering Progress, pages 85-90, 1999.

[16] Lundteigen, Mary Ann; Rausand, Marvin, «Assessment of hardware safety integrity (Pages 185-198),» i *European Commission, Joint Research Centre*, Ispra, Italy, 2006.

[17] Kongsberg Maritime, «1257669: SIS Management Plan for the Heidrun Floating and Storage Unit (FSU),» Revisjon A.

[18] SINTEF, Reliability Prediction Methods for Safety Instrumented Systems - PDS Method Handbook, Trondheim: SINTEF, 2010.

[19] SINTEF. [Internett]. Available: http://www.sintef.no/. [Funnet 13 6 2013].

[20] Angela Summers, Michela Gentile, «Random, Systematic, and Common Cause Failure: How do you manage them?,» 30 October 2005. [Internett]. Available: http://sis-tech.com/paper/random-systematic-and-common-cause-failure-how-do-you-manage-them. [Funnet 16 Juni 2013].

[21] Bukowski, J. V. and Goble, W. M., «Common Cause - Avoiding Control System Failures,» Instrument Society of America, 1997.

[22] Marvin Rausand, Arnljot Høyland, System Reliability Theory: Models, Statistical Methods, and Application, John Wiley & Sons, 2004.

[23] Lundteigen, Mary Ann; Rausand, Marvin, «Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing.,» *Journal of Loss Prevention in the Process Industries*, pp. 20: 218-229, 2007.

[24] A. E. Summers, «Introduction to Layer Of Protection Analysis,» Journal of Hazardous Materials, Houston, 2002.

[25] T. Aven, Misconceptions of risk, Wiley, 2010.

[26] E. S. Andersen, Prosjektledelse, et organisasjonsperspektiv, NKI, 2005.

[27] Armen Der Kiureghian, Ove Ditlevsen, «Aleatory or epistemic? Does it matter?,» Stanford University, 2007.

[28] T. Aven, «It is meaningful and useful to distinguish between stochastic and epistemic uncertainties,» i *Misconceptions of Risk*, Wiley, 2010, pp. 145-148.

[29] D. P. Thunnissen, «Uncertainty Classification for the Design and Development of Complex Systems,» i *Proceedings of the 3 rd Annual Predictive Methods Conference, Veros Software*, 2003.

[30] F. Redmill, «Understanding the Use, Misuse and Abuse of Safety Integrity Levels,» i *Eighth Safety-critical Systems Symposium*, Southampton, 2000.

[31] M. Vintr, «Reliability Assessment for Components of Complex Mechanisms and Machines,» i *12th IFToMM World Congress*, Besançon, 2007.

[32] US Department of Defense, «MIL-HDBK-217F: Military Handbook, Reliability Prediction of Electronic Equipment,» 1991.

[33] Reliability Information Analysis Center, «Electronic Parts Reliability Data,» RIAC, 1997.

[34] Reliability Information Analysis Center, «Nonelectronic Parts Reliability Data,» RIAC,

2011.

[35] Advanced Logistics Development, «SN 29500 - Siemens,» Advanced Logistics Development, [Internett]. Available: http://www.aldservice.com/en/reliability-prediction/sn-29500-siemens.html. [Funnet 29 05 2013].

[36] Ordea.com, «ORDEA, Offshore REliability DAta,» [Internett]. Available: http://www.oreda.com/. [Funnet 06 06 2013].

[37] T. Lilleheier, «Analysis of common cause failures in complex safety instrumented systems,» Norwegian University of Science and Technology, Trondheim, 2008.

[38] S. Hauge, P. Hokstad, H. Langseth and K. Øien, Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook., NO-7465 Trondheim, NORWAY: SINTEF, 2006a.

[39] M. Finkelstein, Failure Rate Modelling for Reliability and Risk, Springer, 2008.

[40] W. Goble, «"SIL verification" in Hydrocarbon Processing,» 2001.

[41] Terje Aven, Willy Røed, Hermann S. Wiencke, Risikoanalyse; Prinsipper og metoder, med anvendelser, Oslo: Universitetsforlaget, 2008.

[42] Helton, J.C., Johnson, J.D., Sallaberry, C.J. and Storlie, C.B., «Survey of Sampling-Based Methods for Uncertainty and Sensitivity Analysis, 91,» i *Reliability Engineering & System Safety*, 2006, pp. 1175-1209.

[43] Eirik Bjorheim Abrahamsen, Willy Røed, «A semi-quantitative approach for verification of Safety Integrity Level requirements,» i *SSARS*, Gdańsk-Sopot, 2010.

[44] TÜV Rheinland Group, «TÜV Certificate for K-Safe, No. 968/ EL 161.00/ 02/08,» TÜV Rheinland Group.

[45] Exida, Certificatoin Services, «Certificate AUT 1108054 C002, AutroFlame X33AF, X32AF Multispectrum IR Flame Detectors,» Exida, 2011-03.

[46] Nemko, «ATEX- og IECEx-merking,» Nemko, [Internett]. Available: http://www.nemko.com/no/services/atex-and-iecex-certification/atex-iecex-marking. [Funnet 7 Juni 2013].

[47] «GAP analyser,» Det Norske Veritas, 2013. [Internett]. Available: http://www.dnv.no/tjenester/konsulenttjenester/drifts_vedlikeholdsoptimalisering/driftsoptimalisering/driftsoptimalisering_ikt/gap_analyser.asp. [Funnet 11 6 2013].

[48] Offshore.no, «Rigg Informasjon,» 25 02 2013. [Internett]. Available: http://www.offshore.no/Prosjekter/rigg-informasjon.aspx?navn=West+Elara.

[49] Jurong Shipyard Pte Ltd, «J001-LOG-J-FH-101, Fire and Gas Design Philosophy,» Revisjon 03.

[50] Kongsberg Maritime, «163875, Kongsberg Maritime AIM Safe Safety System. Revisjon D».

[51] TÜV Rheinland Group, «TÜV Report for K-Safe, No. 968/ EL 161.02/08».

[52] Kongsberg Maritime, «1086102, Safety Analysis Report - Fire & Gas and ESD system. Jurong Shipyard H:11-1092,» Revisjon C.

[53] Kongsberg Maritime, «1086101, FMEA Document - Fire & Gas and ESD System,» Revisjon C.

[54] Kongsberg Maritime, «1086035, FAT Procedure: Fire&Gas System, Jurong Shipyard H:11-1092,» Revisjon D.

[55] Kongsberg Maritime, «10860007, Maintenance Manual - CJ70 PetroProd Jackup (JSL H11-1092), 50373,» Revisjon C.

[56] Kongsberg Maritime, «1059485: Operator Manual - Safety Systems.,» Revisjon C.

[57] Kongsberg Maritime, «1086000, Quality Plan,» Revisjon D.

[58] Kongsberg Maritime, «C&E - Fire & Gas System, As Built,» 06.08.2011.

[59] Kongsberg Maritime, «378006, Safety Configuration Manual (SW), ESD, PSD and F&G, K-Safe,» Revisjon B.

[60] Kongsberg Maritime, «TMPL-3061. Training & Certification of AIM SW Safety Engineer, Kongsberg Safety System (K-Safe),» Template.

[61] Kongsberg Maritime, «PRO-0001, Preventive Action,» 2012.

[62] Kongsberg Maritime, «PRO-0002, Procedure for Control of Documents,» Revisjon A.

[63] Kongsberg Maritime, «PRO-0003, Handling of Nonconforming Products and Corrective Action,» 2012.

[64] Kongsberg Maritime, «PRO-0004, Procedure for Quality Audits, Internal and Supplier for KM,» 2013.

[65] Kongsberg Maritime, «PRO-0021: Delivery Process Start-up,» Revisjon A.

[66] Kongsberg Maritime, «PRO-0022, Delivery Project Planning,» 2012.

[67] Kongsberg Maritime, «PRO-0023, Engineering,» 2011.

[68] Kongsberg Maritime, «PRO-0024, Production Assembly Test,» 2011.

[69] Kongsberg Maritime, «PRO-0025, Commissioning,» 2011.

[70] Kongsberg Maritime, «PRO-0026, Delivery Project Closing,» 2011.

[71] Jurong Shipyard, *J001-LOG-810-J-XE-0001, C&E diagram for F&G System.*

[72] Kongsberg Maritime, «1032539, Design Manual: Safety Configuration Manual, ESD, PSD and F&G. Revisjon A,» 2007.

[73] «Norsok S-002, Working Environment,» Norwegian Technology Centre, Lysaker, Rev. 4, August 2004.

[74] Autronica Fire and Security AS, «116-P-X33AF Addendum/YGB, DEC P/N 95-8624,» 2007-11-12.

[75] Autronica Fire and Security AS, «116-P-X33AF Addendum/YGB, DEC P/N 95-8624,»

Autronica Fire and Security AS, 2007-11-12.

[76] Kongsberg Maritime, «1086025, Technical Specification: Mimics Fire&Gas System, Jurong Shipyard H:11-1092. Revisjon C,» 15.08.2011.

[77] Kongsberg Maritime, «Module User Manual, AIM Function Modules,» February 13, 2013.

[78] Jurong Shipyard Pte Ltd, «J001-LOG-J-Lj-003: I/O list».

[79] Kongsberg Maritime, «PRO-2105, IAS Change Register.,» Revisjon B.

[80] Kongsberg Maritime, «1088506, Alarm System Philosophy. Jorung Shipyard H:11-1092,» Revisjon A.

[81] Kongsberg Maritime, «PRO-0005, Control of Records,» Revisjon B.

[82] Kongsberg Maritime, «Quotation: Vessel Management System,» SGSGP00263-C-2.

[83] International Electro-technical Committee, «IEC 61511-2, Functional safety - Safety instrumented systems for the process industry sector. Part 2: Guidelines for the application of IEC 61511-1,» International Electro-technical Committee, 2003-07.