# SINTEF RAPPORT

**SINTEF Teknologi og samfunn**

Postadresse: 7465 Trondheim
Besøksadresse: S P Andersens veg 5
7031 Trondheim
Telefon: 73 59 03 00
Telefaks: 73 59 03 30

Foretaksregisteret: NO 948 007 029 MVA

TITTEL

**Pålitelighet av instrumenterte sikkerhets-systemer**
**- Årsrapport for 2004 -**

FORFATTER(E)

Helge A. Sandtorv

OPPDRAGSGIVER(E)

Norges Forskningsråd / Statoil

| RAPPORTNR. | GRADERING | OPPDRAGSGIVERS REF. | |
|---|---|---|---|
| STF50 A05050 | Åpen | Runar Østebø, Statoil | |
| GRADER. DENNE SIDE | ISBN | PROSJEKTNR. | ANTALL SIDER OG BILAG |
| Åpen | 82-14-03571-6 | 384620.01 | 10/5 |
| ELEKTRONISK ARKIVKODE | | PROSJEKTLEDER (NAVN, SIGN.) | VERIFISERT AV (NAVN, SIGN.) |
| S:\3840\PRO\384620\Rapport\Årsrapport 2004(helg_runar3 ).doc | | Helge Sandtorv (sign.) | Runar Østebø (sign.) |
| ARKIVKODE | DATO | GODKJENT AV (NAVN, STILLING, SIGN.) | |
| | 2005-03-14 | Lars Bodsberg, forskningssjef (sign.) | |

SAMMENDRAG

Rapporten summerer aktiviteter og resultater fra Forskningsråd-prosjektet ”Pålitelighet av instrumenterte sikkerhetssystemer” for år 2004. Prosjektet er finansiert av Norges Forskningsråd (NFR) og ledes av Statoil. SINTEF er utøvende prosjektpart. Prosjektet skal gå over 3 år og avsluttes i løpet av 2006.

| STIKKORD | NORSK | ENGELSK |
|---|---|---|
| GRUPPE 1 | Instrumentering | Instrumentation |
| GRUPPE 2 | Pålitelighet | Dependability |
| EGENVALGTE | Sikkerhetsutstyr | Safety equipment |
| | | |
| | | |

## INNHOLDSFORTEGNELSE

# 1 Prosjektets formål

## 1.1 Generelt

Olje og gassvirksomheten til havs og på land setter stadig sterkere krav til ytelsesfaktorer som tilgjengelighet og pålitelighet for utstyr og operasjoner. Prosjektet er rettet mot forskningstema tilknyttet: Instrumenteringspålitelighet.

Det er i dag en mangel på strukturering av data for pålitelighetsanalyse tilknyttet detaljer innen instrumenteringspålitelighet. Forskningsundersøkelse av ekspert-metodikk ønskes også fokusert i dette prosjektet, da dette kan akselerere tilgang på data og representerer noe nytt i forhold til tradisjonell pålitelighetsteori. Ettersom FoU-aktivitene gjennomføres over en 3-års periode 2004-06 planlegges det løpende industridialog for å ajourføre/komplettere viten som bygges opp i prosjektperioden.

## 1.2 Spesifikke mål

Analyse og vurderinger av instrumenterte sikkerhetssystemer iht såkalte SIL-analyser[1] (IEC61508), NORSOK Z-016[2] og nytt HMS-regelverk krever tilgang til pålitelighetsdata av slikt utstyr. Disse analyser har vital betydning for sikkerhetsnivå og regularitetseffekter for de anlegg som vurderes. Bransjesituasjonen mhp kvalifiserte pålitelighetsdata er ikke tilfredstillende på dette området, og det er et behov for å foreta en mer forskningspreget vurdering av data som i dag ikke dekkes tilfredsstillende for å danne metodisk grunnlag for å få nye data. Ettersom SIL-analyser vil kreve mange typer data som ikke på kort sikt vil dekkes av OREDA®-databasen, foreslås i dette prosjekt å kartlegge databehovene, identifisere tilgjengelige dataformater og etablere en datastruktur for at industrien kan ha bedre konsistens og bedre kvalifiserte data i slike analyser. Dette er også viktig mhp bruk av slike pålitelighetsdata for måltall/indikatorer.

I prosjektet vil vi i første omgang se på sikkerhetskritisk utstyr som brukes på olje/gass-plattformene så som brannvarsling/slokking og nødavstengning[3], men ikke utstyr brukt i undervannsinstallasjoner[4]. Slikt utstyr vil eventuelt bli vurdert i en senere fase av prosjektet. (En mer detaljert definisjon av instrumenterte sikkerhets-systemer finnes i IEC 61508, part 4, kap. 3.4.1).

Prosjektet gjennomføres som et samarbeid med forskningsmiljø, operatører, fabrikanter og engineering-firma. Sikkerhetskritisk utstyr som ventiler, brann & gassdetektorer, og prosess-sensorer vil vurderes mhp type inventar-data (OREDA) som kreves, og som et nært samarbeid med aktuelle leverandørerer. Pålitelighets-estimering basert på ekspertvurderinger planlegges, for å komplettere kvantitative data (se Appendiks E).

Spesiell metodikk tilknyttet dette område vil undersøkes for uttesting i SIL-sammenheng. Deriblant vil et utvalg av utførte SIL-analyser vil bli gjennomgått for å avdekke behov for forbedring av datakvalitet og foreslå en "beste praksis" vedr. fremskaffelse, kvalifisering og bruk av data for slike SIL-analyser.

---

[1] SIL = Safety Integrity Level (ref. IEC 61508)
[2] Vil i løpet av 2005 bli utviklet til ISO – Standard (ISO 20815)
OREDA® = Offshore Reliability Data
[3] Se også ”Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry”, table 1.1, for opplisting av sikkerhetskristisk utstyr
[4] Dette utstyret blir nå forholdsvis godt dekket i OREDA-prosjektet.

### 1.3 Behov for pålitelighetsdata for sikkerhetskristisk utstyr

Såkalte SIL-analyser basert på IEC standarden 61508 er blitt et krav i Olje & Gassindustrien for sikkerhetskritisk utstyr. For slike analyser trengs det erfaringsdata for påliteligheten av slikt utstyr for å kunne gjøre best mulige estimater av feilsannsynlighet, og dermed få grunnlag for å velge en design-løsning som tilfredsstiller egne selskaps-krav samt krav fra myndighetene. Selv om det finnes en del pålitelighetsdata for dette utstyret[5] er det ulike mangler i disse dataene prosjektet vil adressere:

- Klassifisering av utstyret (såkalt taksonomi-beskrivelser)
- Type og klassifisering av informasjon om utstyrssvikt (feildata)
- Hvor gamle data er ift utvikling av teknologien
- For hvilket utstyr det mangler eller er for få data
- Kvalitet av data (hvor dekkende og detaljert data er)

Prosjektet skal således både legge grunnlag for å forbedre *datakvaliteten* samt identifisere *manglende* data.

### 1.4 Anvendelser

Det pågår også andre aktiviteter/anvendelser der prosjektet er tenkt å bidra både med innspill og som komplementær aktivitet:

**Tabell 1 – Brukere av prosjektresultatene**

| Aktivitet/ produkt | Anvendelse |
|---|---|
| ISO 14224 ISO/TC67/WG4 | Det har siden 2002 pågått et arbeid med å revidere denne standarden og de beskrivelser av taksonomi og feilkoder i dette NFR-prosjektet vil formidles til å bli en del av denne standarden |
| OREDA JIP | OREDA er et JIP-prosjekt med bred deltagelse fra oljeindustrien der det bl.a. samles inn data for instrumenterte sikkerhetssystemer. NFR-prosjektet vil tilsvarende som for ISO 14224 gi verdifullt grunnlag for å forbedre måten man definerer og samler inn feildata på for dette utstyret. NFR-prosjektet vil tilføre OREDA JIP forskningsinnsats og vurdering av analyse av OREDA-type data. |
| PDS-forumet | PDS-forumet er et samarbeidsforum for industrien, konsulenter og FoU der bruken av data i ulike analyse-sammenhenger er i fokus. PDS-forumet jobber også med å få tilgang til bedre data bl.a. fra OREDA. |
| SIL-analyser | Er i dag den aksepterte metode for analyse av instrumentert sikkerhets-kritisk utstyr. Som nevnt over inngår pålitelighets-data i slike analyser og kravene til disse dataene er bl.a. definert i IEC 61508 samt den norske rettledningen til IEC 61 508 utgitt av OLF. |
| Industrigruppen etablert i dette prosjektet | Denne gruppen med representanter fra ulike industrier har både bidratt inn i prosjektet samt fått ta del i den felles kunnskap som er fremkommet i prosjektet. |
| Myndighetene (OD) | Regelverket for norsk sokkel krever at det skal samles inn og følges opp data som beskriver påliteligheten av nevnte utstyr. |

[5] OREDA + PDS Handbook

Som ovennevnte oversikt viser er det mange dels komplementære behov for disse data, men det er ingen av disse aktivitetene som spesifikt jobber med å definere grunnlaget for klassifisering og innsamling av slike data på det detalj-nivået dette prosjektet har som mål.

# 2 Prosjektorganisering

Prosjektet er organisert med en forholdsvis bred industrideltagelse fra oljeselskaper, fabrikanter/leverandører og konsulenter som vist i vedlagte tabell:

**Tabell 2 - Deltagere i NFR-prosjektet instumenterte sikkerhetssystemer**

| Navn | Firma |
|---|---|
| | ***Prosjektledelse*** |
| Runar Østebø (prosjektleder) | Statoil |
| Helge Sandtorv (delprosjektleder) | SINTEF |
| | ***Oljeselskaper*** |
| Frank Firing | Statoil |
| Gunhild Holtet Eie | Statoil |
| Jan Ståle Austbø | Statoil |
| Håkon Løvåsen | Statoil |
| Atle Hjorteland | Statoil |
| Turid M. Haugerød | Hydro |
| Arnt Kr. Viland | ConocoPhillips |
| | ***Fabrikanter/Leverandører*** |
| Jarle Øygarden | Bjørge SAAS System |
| Erik Korssjøen | Kongsberg Simrad |
| John Dawes | Siemens |
| Arvid Bjerkestrand | Simrad Optronics |
| Fahrad Pakshad | VetcoAibel (ABB) |
| Odd Magne Andersen | VetcoAibel (midlertidig erstatter for Pakshad)) |
| | ***Engineering*** |
| Mette Pettersen | AkerKvaerner |
| Ivar Skjeldal | AkerKværner Offshore Partner (AKOP) |
| | ***Konsulenter*** |
| Gjermund Våge | DnV |
| Roar Renton | Lilleaker Consulting |
| Frank Hansen | Safetec Nordic |
| Henriette Hall | Scandpower Risk Management |

Statoil v/ Runar Østebø er prosjektleder mens SINTEF v/ Helge Sandtorv er den utførende part vedrørende håndtering og bearbeiding av teknisk materiale samt diverse administrative oppgaver (møtereferater, administrering av eROM, m.m.)

# 3 Aktiviteter 2004

Oppgavene i prosjektet vil til en viss grad bli utformet underveis, men i utgangspunktet er flg. planlagt:

1. Beskrivelse av egnet dataformat, definisjoner og taksonomi for innsamling av pålitelighets-data for instrumenterte sikkerhets-systemer

2. Innspill til ISO-standardiseringsarbeid (ISO TC67/WG4) og industri-JIP (OREDA)
3. "Beste praksis" for estimering og bruk av pålitelighetsdata i såkalte SIL-analyser inkludert kvalifisering av godheten av data
4. Gjennomgang av aktuelle "case" for å klarlegge databehovet og datakvalitet for SIL-analyser

I 2004 har hovedfokus vært arbeid knyttet til pkt. 1 og 2 nevnt over. En vesentlig del av prosjektarbeidet har pågått som arbeidsmøter i ovennevnte industrigruppe. I alt har det vært avholdt 5 heldags-møter i 2004. Oppmøtet fra industrien har vært godt med deltakelse fra 8 – 12 selskaper per møte. En vesentlig del av resultatet for 2004 har vært en gjennomgang og total revisjon av taksomi-beskrivelsene for utstyr som flg.(se også Appendiks A):

- F & G detektorer
- Prosess sensorer
- Kontroll-enheter
- Ventiler
- Nozzles (FiFi)
- UPS (Uninterruptable Power Supply)

Arbeidet med bruk av ekspertvurderinger, samt gjennomgang av en "case" fra SIL-analysen for Kristin-feltet, er påbegynt og vil bli videreført i 2005.

# 4 Resultater

1. Resultatet av gjennomgangen og revisjon av taksonomibeskrivelsen for utstyret referert over er gjengitt i Appendix A. Dette arbeidet har gitt direkte innspill til revisjons-arbeidet med ISO 14224[6] og vil etter hvert også bli innpasset i en bedre modell for å samle inn data i OREDA samt harmonisere kravene til data med behovet definert i nevnte SIL-analyser.

2. I flere av arbeidsmøtene har det vært diskutert hvilket utstyr det i dag er dårlig/lite datagrunnlag på. Herunder er det også definert databehovet for "nye" utstyrsklasser, dvs. utstyrsklasser det per i dag ikke samles data på eller finnes taksonomibeskrivelser for. Dette er summert i tabell 3 og 4

3. I prosjektet har vi også samlet en oversikt over hvilke fabrikanter/leverandører som leverer relevant instrumentert utstyr der disse er norske eller er representert i Norge Dette er vist i Tabell 5.

4. For videre arbeid i 2005 har det også blitt definert behov for bedre data om:

   - Demand rate (relle demands samt test-demands)
   - Test-intervall for å beregne PFD-tallene med mindre usikkerhet. Planlagte/virkelige testintervaller kan variere mellom oljeselskapene som har bidratt med historiske data.

[6]Resultatene fra prosjektet ble implementert i ISO 14224 i den utgaven (DIS-versjon) som ble utgitt 2/12-2004. Senere arbeid gjort i prosjektet vil bli tatt med i endelig versjon av ISO 14224 i den grad det blir vurdert som relevant.

- ”Coverage” faktor. Denne inkluderer andel farlige feil detektert automatisk ved selvtest.

5. For å bedre datakvalitet har følgende tiltak blitt identifisert som viktige (for 2005):

   - Styrke ISO ved å gi kommentarer til ISO/DIS 14224 til mai 2005
   - Samle inn flere og nyere data bl.a. via OREDA
   - Evaluere metoder for bruk av ekspertmetodikk på utvalgt utstyr
   - Vurdere prioritet av databehov

6. Analysemetodikk

I prosjektet vil vi også vurdere bruk av ekspertmetodikk for fastleggelse av data. En start på dette arbeidet er et resultat av et Dr.ing. studium utført av Atle Hjorteland ved Universitetet i Stavanger (se Appendiks C).

I prosjektet planlegges for øvrig ikke å gå inn på analysemetoder for data i noe omfang, idet dette feltet bl.a. dekkes i det arbeidet som utføres i det såkalte PDS-forumet (PDS-metoden). Siden SINTEF er deltager begge steder vil vi sørge for at synergi-effekten mellom de 2 aktivitetene blir best mulig utnyttet.

**Tabell 3 - Utstyrsklasser som helt eller delvis har en sikkerhetskristisk funksjon og som i dag er dekket med taksonomi-beskrivelse i ISO 14224**

| Utstyrs-klasse | Beskrivelse | Instrumentert sikkerhetsutstyr fokusert i dette prosjektet | Annet sikkerhets-kritisk utstyr[7] | Kommentarer |
|---|---|---|---|---|
| FG* | Brann & Gass detektorer | X | | |
| CLU* | ”Control Logic Units” (CLU) | X | | Tilgjengelige data (OREDA) er noe utdaterte |
| CE | Forbrenningsmotorer | | X | |
| PS* | Prosess sensorer (”Input devices”) | X | | Prosess-sensorer er blitt gitt nytt navn: ”Input devices” |
| PU | Pumper | | X | Brannvannspumper har begrenset fokus i NFR prosjekt nå. |
| VA* | Ventiler | X | | Fokuserer på ESV/ESD inklusiv HIPPS samt pilot-ventiler |
| UPS* | ”Uninterruptable Power supply” | | X | Begrenset fokus i NFR prosjekt nå. |
| EG | Electric generator | | X | |
| EM | Electric motor | | X | |
| HPU | HPU hydraulic safety valve | | | |

[7] Det kan bli aktuelt å inkludere noe av dette utstyret i prosjektet på et senere tidspunkt

| | | | | |
|---|---|---|---|---|
| | X-mas tree topside/onshore | | X | |
| | DHSV | | X | |
| | SSIV | | X | |
| | Other subsea equipment | | X | |

**Tabell 4 - Utstyr der det i dag mangler taksonomi-beskrivelser og/eller der det er sparsomt med, eller for gamle, data**

| **Utstyrskategori** | **ISO 14224 utstyrsklasse** | **Utstyr med manglende/lite data** |
|---|---|---|
| Electrical | Switchgears/switchboards and distribution boards | Brytere (circuit breakers) |
| | | Releer (relays) |
| | Power cables and terminations | Kabler (høyspent/lavspent & signal) |
| Marine | Dynamic position equipment | DP systemer |
| | To be defined | Ballastering (pumper, styring) |
| Utilities | HVAC | Brannspjeld |
| | (Not covered as an equipment class in ISO 14224) | Telemetri-systemer |
| Safety and Control* | To be defined | Deluge systemer |
| | | |

* Vanntåke og sprinkler-utstyr ble vurdert til normalt ikke å være sikkerhetskristisk til storulykker relatert til hydrokarbonlekkasjer/-branner

**Tabell 5 – Oversikt over utstyrsleverandører av instrumentert sikkerhetskritisk utstyr**

| **Equipment class / element** | | | | |
|---|---|---|---|---|
| **F & G**<br>(Sensoring element) | **Input device**<br>(Sensoring element) | **CLU**<br>(Logic solver) | **Valves**<br>(Final element) | **Circuit breakers**[8]<br>(Final element) |
| Siemens<br>Simrad Optronics<br>Autronica<br>Dräger | Siemens<br>Simrad Optronics<br>ABB<br>Emerson<br>Rosemount | Siemens<br>Simrad Optronics<br>ABB<br>Kongsberg Maritime<br>Autronica<br>Honeywell<br>Tricon<br>HIMA<br>Bailey Norge<br>Bjørge SAAS | Bjørge SAAS<br>Håkon Ellingsen<br>Håland Instruments<br>Scana Rotator | Siemens<br>ABB<br>Aker Elektro |

[8] ”Circuit breakers” er pr i dag ikke egen utstyrsklasse i verken OREDA eller ISO 14224 DIS, men dette er til vurdering hos SINTEF ifm OREDA JIP prosjektet og ifm ISO-arbeid.

# 5 Formidling av resultater/industridialog

Følgende fora er brukt for formidling av resultatene så langt:

a. Innspill til ISO/TC67 arbeidsgruppe WG4 for revisjon av ISO 14224
b. Innspill til OREDA-prosjektet for forbedring av krav til datainnsamling
c. Presentasjon av prosjektet i det såkalte PDS-forum (2 PDS-forum møter i 2004)
d. Info om prosjektresultatene til deltagerne i industrigruppen
e. Oppretting av eget e-ROM der industrigruppen får tilgang til alle prosjektresultater
f. Det har vært avholdt 5 møter/workshops, der totalt 29 personer fra 15 selskap har deltatt. I gjennomsnitt har det deltatt 8 – 10 personer per møte med deltagelse fra oljeseskaper, fabrikanter/leverandører, engineering, konsulenter og FoU-institusjoner.

# 6 Planer for videre arbeid i 2005/06

1) Gjennomføre en ”mapping”-analyse med oversikt over instrumenterte sikkerhets-systemer som anvendes i SIL-analyser og tilgjengelighet og kvalitet på data for dette utstyret

2) Jobbe videre med bruk av ekspertmetodikk for å estimere pålitelighetstall der datagrunnlaget er tynt. Gjennomføre ekspertdata-sesjoner planlegges i 2005.

3) Gjennomgå et utvalg ”cases” med SIL-analyser. Flg. er vurdert som aktuelle:

| **Selskap** | **Installasjon/anvendelse** | **Utbygging** | **Drift** |
|---|---|---|---|
| Statoil | Kristin | x | |
| COPCO-Statoil-Hydro | Anneks F i ISO 14224 basert på ”Samarbeids-forum vedr. sikkerhetskristisk utstyr” | | x |
| Norsk Hydro | Ormen Lange landanlegg | x | |
| Statoil | Snøhvit landanlegg | x | |
| ConocoPhillips | 2/4-M | | |

4) Ta opp problemstillinger knyttet til pålitelighet av instrumenterte sikkerhets-systemer basert på innspill fra industrigruppen. Et eksempel på temaer som vil bli nærmere vurdert vil være kompatibilitet mellom hvordan data registreres i dag iht. ISO 14224 og de behov som kreves for å utføre såkalte SIL-analyser. Mer spesifikt er det ønskelig å kunne samle data på såkalte *”dangerous failures”* og ”*safe failures*” samt skille mellom såkalte *detekterbare* og *udetekterbare* feil. Det er vanskelig med dagens taksonomi slik som beskrevet i OREDA og ISO 14224 å få fatt i denne informasjonen på en *direkte* måte. (Se også [2]).

# 7 Referanser

## 7.1 Standarder og retningslinjer

[1] ISO 14 224 ”Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data”. DIS-version issued 02.12.2004

[2] NORSOK Z016 (ISO 20815 is under development…)  se http://www.standard.no

[3] IEC 61508 ”Functional safety of electrical/electronic/programmable electronic safety-related systems”

[4] IEC 61511 “Functional safety: Safety instrumented systems for the process industry sector”

[5] OLF GL070 http://www.itk.ntnu.no/sil/

## 7.2 Datakilder

[6] OREDA JIP (Joint Industry Project)

[7] OREDA 2002 Reliability Data Handbook (4. ed.)

[8] PDS Data Handbook, 2004 edition

## 7.3 Annet

[9] Hjorteland, A. & Aven, T., How to use expert judgement in regularity analyses to obtain good predictions. Accepted for publication in the 16th European Safety and Reliability Conference (ESREL), 2005 (see Appendiks E)

[10] Jean-Pierre Signoret: “High integrity protection systems (HIPPS) – Difficulties in SIL-calculations”. Presentation given at the Regularity Management Conference in Stavanger 2004

# VEDLEGG A

## Taksonomi-beskrivelser for sikkerhetsutstyr

Denne taksonomibeskrivelser er i hovedsak identisk med ISO 14224 (DIS-versjon) utgitt 02.12.2004. Der det er forskjeller er dette merket med gult samt kommentert i tilhørende fotnoter. Endringene er kun i tabell A.8 og Figur A.4. (Henvisning til korresponderende kapitel i ISO 14224 er gitt i overskriften til kapitlene/tabellene).

## A.1 Safety & Control equipment (ref. ISO 14224, Annex A kap. A.2.5)

### A.1.1 Fire and gas detectors

**Table A 1 — Taxonomy classification — Fire and gas detectors**

| Equipment class | | Type | |
|---|---|---|---|
| Description | Code | Description | Code |
| Fire and gas detectors | FG | *Fire detection:* | |
| | | Smoke/Combustion | BS |
| | | Heat | BH |
| | | Flame | BF |
| | | Manual pushbutton | BM |
| | | Others | BA |
| | | *Gas detection:* | |
| | | Hydrocarbon | AB |
| | | $H_2S$ | AS |
| | | Others | AO |

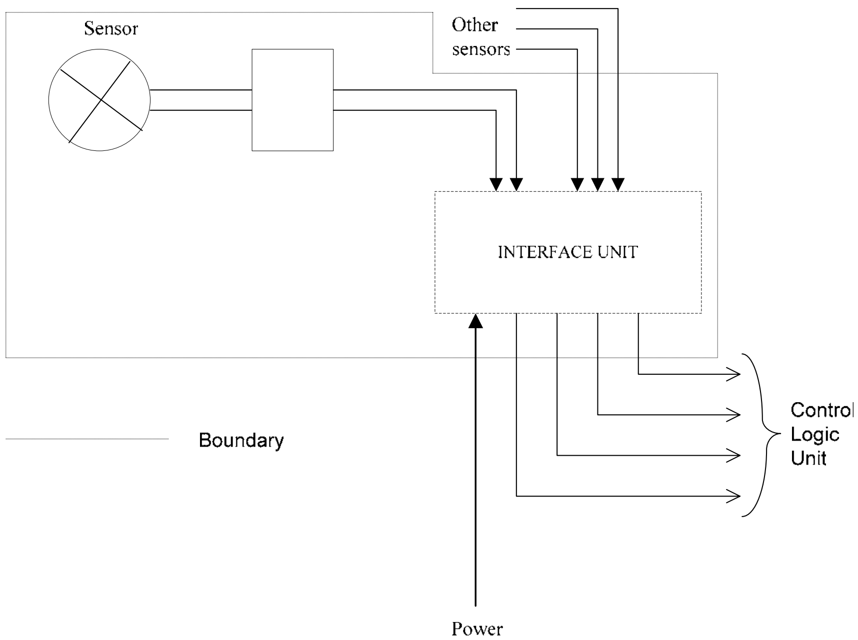


**Figure A 1 — Equipment boundary — Fire and gas detectors**

*Interface Unit will not be applicable for all F & G sensors

<u>NOTE on "Interface Unit"</u> (see Boundary Drawing F & G detector above):

Field input devices such as fire and gas detectors are usually connected to Fire and Gas logic solver (node) which is not included in the boundary of F & G detectors (ref. Fig. A3). Monitoring/interface units may be used between detector and LS and this will be part of F & G detectors. The purpose of these units is, among others, to monitor the detectors, their interface connections and cables, analyzing the incoming data by different algorithms and initiating fault or alarm signals. The basic principle of data communication between field equipment and such interface systems might be based on multiplexing and sequential polling of data.

**Table A 2— Equipment unit subdivision — Fire and gas detectors**

| **Equipment unit** | **Fire and gas detectors** | | |
|---|---|---|---|
| Subunit | Sensor | Interface unit * | Miscellaneous |
| Maintainable items | Cabling<br>Cover<br>Detector (incl. head and associated electronics)<br>Mounting socket | Cabinet<br>Control card<br>Display | Others |

*Not applicable for all F & G sensors

**Table A 3— Equipment unit specific data — Fire and gas detectors**

| **Name** | **Description** | **Unit or code list** | **Prior.** |
|---|---|---|---|
| | *Functional characteristics:* | | |
| Location on installation | Where installed | Drill floor, wellhead, process, auxiliary, mud processing, power generation, utility, control room, auxiliary room, living quarter | H |
| Environment | Exposure | Severe, Moderate, Low, Unknown* | H |
| | *Item characteristics:* | | |
| Sensing principle | Type | *Fire*: Ionization, optical, IR, UV, IR/UV, rate rise, rate comp, fixed temp, fusible plug, camera, multisensor (optical/heat)<br>*Gas*: Catalytic, electrochemical, photoelectro-chemical, photoelectric beam, IR, UV, acoustic, camera, aspirating, optical beam, solid state | H |
| Detector communication | Type | Conventional, addressable (one-way), smart (two-way) | M |
| Fault tolerance** | Respons at failure | Yes/No | M |
| Self-test feature | Degree of self-testing | No self-test, automatic loop test, built-in test, combined | M |
| Safety class | Ex standard | Ex(d), Ex(e), Ex(i), None | L |

*Environment classification:
SEVERE: Not enclosed and/or outdoor. Heavily exposed (vibration, heat, dust, salt).
MODERATE: Partly enclosed and or moderately exposed (vibration, heat, dust, salt). Naturally ventilated.
LOW: Enclosed and/or indoor. Minor exposure (vibration, heat, dust, salt). Mechanically ventilated.

** Design based on de-energized principle is compatible with Fail-Safe philosophy. A safety instrumented system operating in "normally-energized" mode can be designed to fail-safe on loss of power or signal.

**H** = High, **M** = Medium, **L** = Low Importance

### A.1.2 Input devices

Input devices are in general sensors that converts process parameters into an electric signal that can be monitored. Typical main categories of Input devices are:

- *Transmitter* (converts process parameter, e.g. pressure, into proportional electrical signals – typical 4 mA to 20 mA or 0 V to 10 V (ref. IEC 60381-2);
- *Transducer* (converts process parameters, e.g. pressure, into proportional electrical signals – typical unamplified output);
- *Switch* (converts process parameters, e.g. pressure, typical into on/off electrical signals)

**Table A 4 — Taxonomy classification — Input devices**

| Equipment class | | Equipment Type | |
|---|---|---|---|
| Description | Code | Description | Code |
| Input devices | IP | Pressure | PS |
| | | Level | LS |
| | | Temperature | TS |
| | | Flow | FS |
| | | Speed | SP |
| | | Vibration | VI |
| | | Displacement | DI |
| | | Analyser | AN |
| | | Weight | WE |
| | | Corrosion | CO |
| | | Limit switch | LP |
| | | On/off (pushbutton) | PB |
| | | Others | OT |

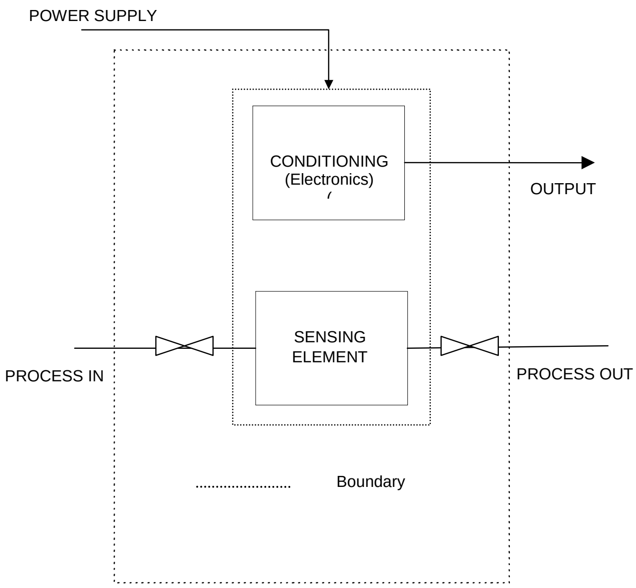


**Figure A 2 — Equipment boundary —Input devices**

(Do not apply for switches and pushbuttons)

**Table A 5 — Equipment unit subdivision, Input devices**

| Equipment unit | Input devices | |
|---|---|---|
| Subunit | Sensor and electronics | Miscellaneous |
| Maintainable items | Sensing element<br>Conditioning (electronics) | Cabling<br>Piping<br>Others |

### Table A 6 — Equipment unit specific data — Input devices

| Name | Description | Unit or code list | Prior. |
|---|---|---|---|
| *Functional characteristics:* | | | |
| Location on installation | Where installed | Drill floor, wellhead, process, auxiliary, mud processing, power generation, utility, control room, auxiliary room, living quarter | H |
| Application | Where applied | Process control, emergency shutdown, process shutdown, pressure reduction, by-pass, blowdown, monitoring, combined | H |
| Fluid/gas corrosive-/erosiveness | Classify as explained at end of table | Benign, moderate, severe (see Note below) | M |
| *Item characteristics:* | | | |
| Category | Main category | Transmitter, transducer, switch, pushbutton | H |
| Sensing principle | Applicable for pressure sensors only | Bonded strain, semiconductor, strain, piezoelectric, electromechanical, capacitance, reluctance, oscillating wire | H |
| | Applicable for level sensors only | Differential pressure cell, capacitance, conductive, displacement, diaphragm, sonic, optical, microwave, radio frequency, nuclear | H |
| | Applicable for temperature sensors only | Resistance temperature detector (PT), thermocouple, capillary | H |
| | Applicable for flow sensors only | Displacement, differential head (closed conduit/pipe, open channel), velocity, mass | H |
| | Insert additional types as relevant (e.g. speed, vibration) | To be defined by user as needed | H |
| Sensor voting, *k* out of *n* (only as relevant) | At least *k* out of *n* sensors shall provide signal to initiate control/safety action. *K* and *n* shall be entered; if no voting, leave blank | *k* = '*nn*' (integer) *n* = '*nn*' (integer) | L |
| Fault tolerance | Response at failure | Yes/No | H |
| Detector communication | Type | Conventional, addressable (one-way), smart (two-way) | M |
| Self-test feature | Degree of self-testing | No self-test, automatic loop test, built-in test, combined | H |
| Safety class | Ex standard | Ex(d), Ex(e), Ex(i), None | L |
| *Benign* (clean fluids, e.g. air, water, nitrogen)<br>*Moderately* corrosive/erosive (oil/ gas not defined as severe, sea water, occasionally particles)<br>*Severe* corrosive/erosive (sour gas/oil (high $H_2S$), high $CO_2$ content, high sand content) | | | |

**H** = High**, M** = Medium, **L** = Low Importance

### A.1.3 Control Logic Units

**Table A 7 — Taxonomy classification — Control Logic Units**

| Equipment class | | EquipmentType | |
|---|---|---|---|
| Description | Code | Description | Code |
| Control logic units | CL | PLC | LC |
| | | Computer | PC |
| | | Distributed control unit | DC |
| | | Relay | RL |
| | | Solid state | SS |
| | | Single loop controller | SL |
| | | Programmable Automation Controller (PAC) | PA |

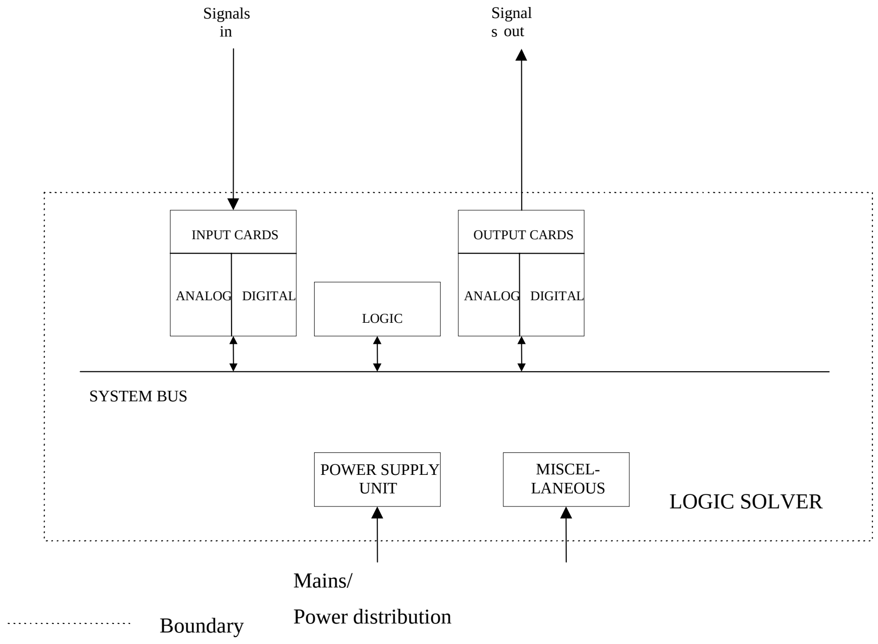


**Figure A 3— Equipment boundary — Control Logic Units**

## Table A 8 — Equipment unit subdivision — Control Logic Units

| **Equipment unit** | **Control Logic Unit** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Subunit | Analog input cards | Digital input cards | Analog output cards | Digital output cards | Logic[9] | System bus | Power supply | Miscellaneous |
| Maintainable items | Input card<br>Connec-tion unit | Input card<br>Connect-ion unit (X-wiring) | Output card<br>Connect-ion unit (X-wiring)<br>Relay | Output card<br>Connect-ion unit (X-wiring)<br>Relay | Processing card[10]<br>Random access memory (RAM)<br>Watchdog/ diagnostics<br>Software | No sub-division | No sub-division | Others<br>Galvanic barriers |

## Table A 9 — Equipment unit specific data — Control Logic Units

| **Name** | **Description** | **Unit or code list** | **Prior.** |
|---|---|---|---|
| Application - control logic | Where used | Centralised, distributed, man-machine interface | M |
| CLU redundancy configuration* | Specify if there are redundant (parallel) CLUs installed[a] | Yes/No | L |
| Fault tolerance | Response at failure | Yes/No | H |
| Selftest feature | Degree of self-testing | No self-test, automatic loop test, bult-in test, combined | H |
| [a]Redundant CLUs shall comprise the complete CLU, not just sub-items (e.g. CPUs) | | | |

**H** = High, **M** = Medium, **L** = Low Importance

[9] ISO 14224 DIS: Logic Solver
[10] ISO 14224 DIS: Central Processor Unit (CLU)

### A.1.4 Valves

**Table A 10— Taxonomy classification — Valves**

| Equipment class | | Equipment Type | |
|---|---|---|---|
| Description | Code | Description | Code |
| Valves | VA | Ball | BL |
| | | Gate | GT |
| | | Globe | GB |
| | | Butterfly | BU |
| | | Plug | PG |
| | | Needle | NE |
| | | Check | CH |
| | | Diaphragm | DM |
| | | 3-way | WA |
| | | PSV-conventional | SC |
| | | PSV-conventional with bellow | SB |
| | | PSV-pilot operated | SP |
| | | PSV-vacuum relief | SV |
| | | Plug & Cage | PC |
| | | External sleeve | ES |
| | | Disc | DI |
| | | Axial flow | AF |
| | | Pinch | PI |
| | | Others | OH |
| NOTE *Pilot valves* are normally non-tagged components used for self-regulation. *Pilot solenoid valves* are normally a sub-tag of a valve tag used for all ESD/PSD. *Quick exhaust dump valves* are specific valves used if quick response is required (e.g. HIPPS function). *Relief valves* are normally PSV-valves | | | |

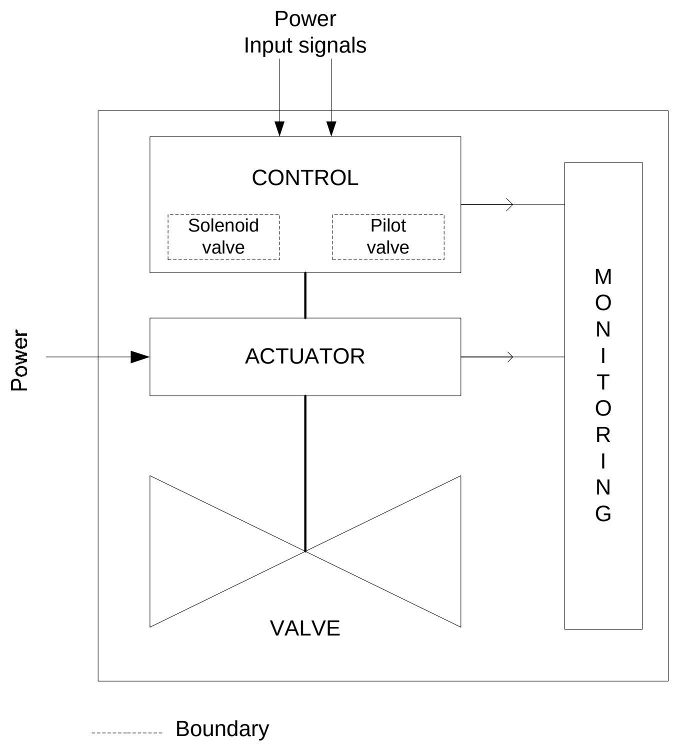


**Figure A 4 – Equipment boundary – valves**[11]

**Table A 11— Equipment unit subdivision — Valves**

| **Equipment unit** | **Valves** | | | |
|---|---|---|---|---|
| Subunit | Valves | Actuator[A] | Control and monitoring* | Miscellaneous |
| Maintainable items | Valve body<br>Bonnet<br>Flange joints<br>Seat rings<br>Packing/Stem seal<br>Seals<br>Closure member<br>Stem | Diaphragm<br>Spring<br>Case<br>Piston<br>Stem<br>Seals/gaskets<br>Electrical motor [C]<br>Gear | Cabling and junction boxes<br>Indicator<br>Instrument, general<br>Instrument, position<br>Monitoring<br>Solenoid valve<br>Pilot valve [B]<br>Quick exhaust dump valve<br>Internal power supply<br>Limit switch | Accumulator<br>Others |

A Not applicable for all valve categories

B Applicable for hydraulic/pneumatically actuated valves.

C Electric motor actuator only.

[11] The boundary drawing for valves has been significantly revised in this NFR-project to e.g. better explain the role of pilot- and solenoid valves. In ISO 14224 DIS the "old" boundary drawing is being used.

## Table A 12— Equipment unit specific data — Valves

| Name | Description | Unit or code list | Prior. |
|---|---|---|---|
| Main function | Main functional category | Flow control, non-return (check), pressure safety valves, instrument or hydraulic control, on/off | H |
| Application | Specify function in the process | Annulus (X-mas tree), blowdown, by-pass, injection, X-over, Deluge, ESD, ESD/PSD, PSD, HIPPS, swab, wing, pilot, relief*, control, choke, | H |
| Where mounted | Equipment on which the valve is installed | Wellhead, X-mas tree, wellhead flow line, wellhead injection line, pump, turbine, generator, separator, heat exchanger, vessel, header, electric motor, diesel motor, turboexpander, drilling, pipeline, mud process, utility, living quarter, air inlet, riser | H |
| Size | Internal diameter | mm (inches) | M |
| Fluid handled | Main fluid only | Oil, gas, condensate, freshwater, steam, sea water, crude oil, oily water, flare gas, fuel gas, water/glycol, methanol, nitrogen, chemicals, hydrocarbon combined, gas/oil, gas/condensate, oil/water, gas/oil/water, NGL, LPG, slurry, etc. | H |
| Fluid corrosive-/ erosiveness | Classify as shown at end of table | Benign, moderate, severe | M |
| Flowing pressure | Normal operating pressure (inlet) | pascal (bar) | M |
| Shut-off pressure | Maximum differential pressure when valve closed (design)<br>For PSVs: Set-point opening pressure | pascal (bar) | L |
| Valve material | Specify | Carbon steel, stainless steel, alloy type, composite, titanium | M |
| Stem sealing | Specify | Indicate type | H |
| Actuation-opening | Type | Electrical, hydraulic, pneumatic, self-acting (spring), self-acting/pilot, manual, | H |
| Actuation-closing | Type | Electrical, hydraulic, pneumatic, self-acting (spring), self-acting/pilot, manual | M |
| Manufacturer - actuator | Name actuator manufacturer | Specify | L |
| Manufacturer - pilot valve | Name of pilot valve manufacturer | Specify | L |
| Manufacturer - solenoid valve | Name of solenoid valve manufacturer | Specify | L |
| Pilot valve configuration | No. of and configuration<br>(Applicable for pilot -operated valves only) | Specify; e.g. 1×3/2 (= Single 3/2 pilot valve), 2×4/3 (= Double 4/3 pilot valve). | L |
| Solenoid valve configuration | No. of and configuration<br>(Applicable for solenoid-operated valves only) | Specify; e.g. 1×3/2 (= Single 3/2 pilot valve), 2×4/3 (= Double 4/3 pilot valve). | L |
| Trim type | Type<br>(Applicable Control valves only) | Noise reduction, anti cavitation, multi-stage, single stage | H |
| Valve leakage class | Type<br>(Applicable for control valves, ESD or HIPPS only) | II, III, IV, V, VI, VII | H |
| *Benign* (clean fluids, e.g. air, water, nitrogen)<br>*Moderately* corrosive/erosive (oil/ gas not defined as severe, sea water, occasionally particles)<br>*Severe* corrosive/erosive (sour gas/oil (high $H_2S$), high $CO_2$ content, high sand content) | | | |

**H =** High, **M** = Medium, **L** = Low Importance

### A.1.5 Nozzles

### A.1.6 Table A 13— Taxonomy classification — Nozzles

| Equipment class | | Type | |
|---|---|---|---|
| Description | Code | Description | Code |
| Nozzles | NO | Deluge<br>Sprinkler<br>Water mist<br>Gaseous | DN<br>SR<br>WM<br>GA |

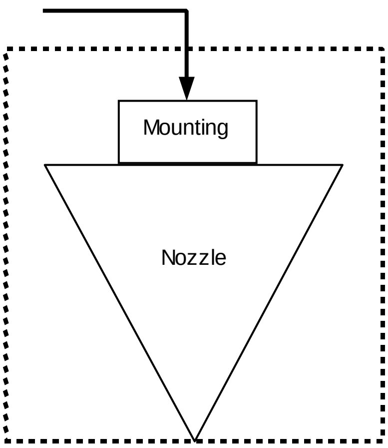


**Figure A 5— Equipment boundary — Nozzles**

**Table A 14— Equipment unit subdivision — Nozzles**

| Equipment unit | Nozzles | | |
|---|---|---|---|
| Subunit | Nozzle | Mounting assembly | Miscellaneous |
| Maintainable items | Fusible bulb<br>Nozzle body w/ internals<br>Nozzle head<br>Protective coating<br>Screen<br>Solder | Mounting connector<br>Seals | Others |

**Table A 15— Equipment unit specific data — Nozzles**

| Name | Description | Unit or code list | Prior. |
|---|---|---|---|
| Application | Where in the process applied | Deluge, sprinkler | H |
| Hazards protection | Type of protection | Electrical, Ex, fuel oil, glycol, HC gas, hydrogen gas, lubricants, methanol, combustibles, radioactivity, toxic gas, toxic liquid | H |
| Location on installation | Where installed | Drill floor, wellhead, process, auxiliary, mud processing, power generation, utility, control room, auxiliary room, living quarter | H |

| | | | |
|---|---|---|---|
| Nozzle material | Specify | Brass, chrome plated, electroless nickel plated, lead coated, stainless steel | H |
| Nozzle length | Specify | mm | H |
| Nozzle width | Specify | mm | H |
| Installation category | How installed | Concealed, horizontal sidewall, pendent, recessed, upright, vertical sidewall | L |
| Fluid handled - Nozzles | Main fluid only | Potable water, sea water | M |
| Fluid corrosive-/ erosiveness | Classify as shown at end of table | Benign, moderate, severe | M |
| Discharge temp. | At operating condition | °C | L |
| Flowing pressure | | pascal (bar) | M |
| Flow rate | | L/min. | M |
| Shut-off pressure | Maximum differential pressure when valve closed (design)<br>For safety pressure-relief valves: Set-point opening pressure | pascal (bar) | L |
| Fluid temperature | Specify | °C | L |
| Connection size | Specify | mm (inches) | H |
| Type of nozzle end | Specify | Bolted flange, clamped flange, screwed, welded | M |
| Spray angle | Specify | degrees | M |
| Spray type | Specify | Droplets, mist | M |
| Actuation | Specify | Fusible bulb, solder, external | M |
| Nozzle screen | If installed or not | Yes/No | L |
| *Benign* (clean fluids, e.g. air, water, nitrogen)<br>*Moderately* corrosive/erosive (oil/ gas not defined as severe, sea water, occasionally particles)<br>*Severe* corrosive/erosive (sour gas/oil (high $H_2S$), high $CO_2$ content, high sand content) | | | |

**H =** High, **M** = Medium, **L** = Low Importance

## A.2 Electrical Equipment

This section presents examples of typical plant / unit level application for Electrical equipment.

### A.2.1 Uninterruptible power supplies (UPS)

**Table A 16 — Type classification — UPS**

| Equipment class (level 6) | | Equipment Type | |
|---|---|---|---|
| Description | Code | Description | Code |
| UPS | UP | Dual UPS w/ standby bypass. | UB |
| | | Rectifier supplied from emergency power. Bypass from main power system. | |
| | | Dual UPS without bypass. | UD |
| | | Rectifier supplied from emergency power. | |
| | | Single UPS w/ bypass. | US |
| | | Rectifier supplied from emergency power. Bypass from main power system. | |
| | | Single UPS without bypass. | UT |
| | | Rectifier supplied from emergency power. | |

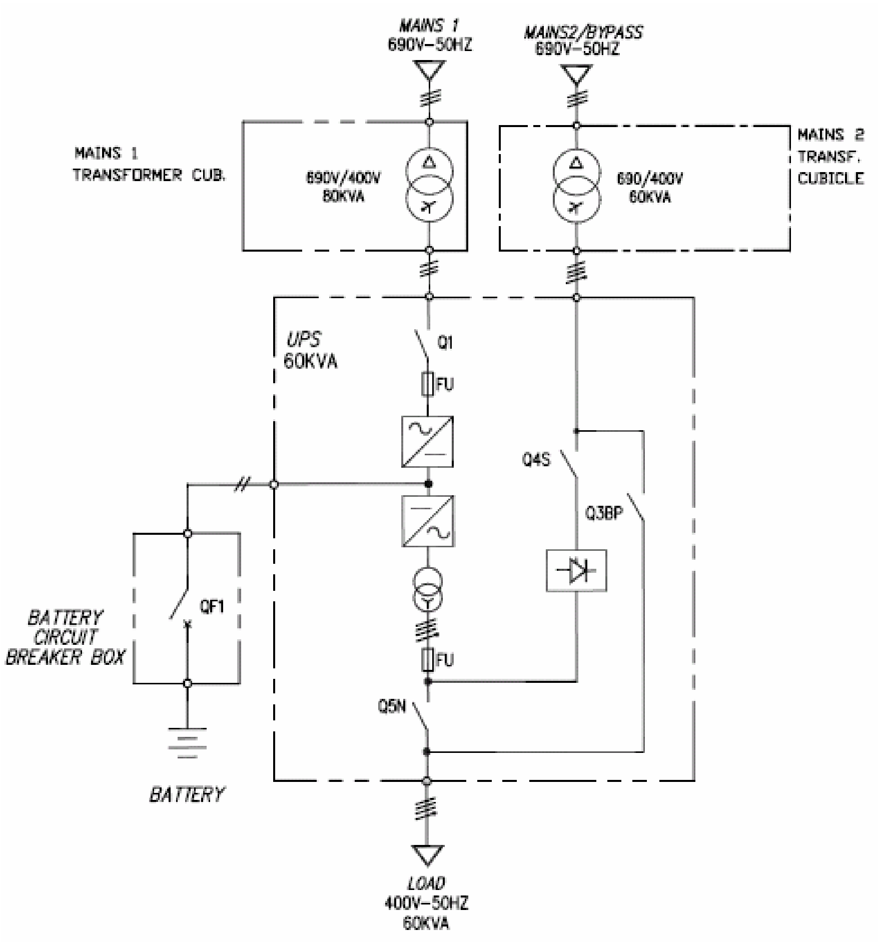


**Figure A 6 — Boundary definition — UPS**

**Table A 17 — Equipment subdivision — UPS**

| Subunit | Battery unit | Bypass unit | Inverter unit | Rectifier unit/ DC supply | Control and monitoring | Miscellaneous |
|---|---|---|---|---|---|---|
| Maintainable items | Battery breaker<br>Battery bank<br>Cabling<br>Circuit breaker<br>Connection/ socket<br>Instrument | Bypass switch<br>Bypass transformer<br>Contactor feeder[a]<br>Fuse(s)<br>Instrument<br>Static switch | Bypass switch<br>Cabling<br>Connection/ socket<br>Fuse(s)<br>Instrument<br>Inverter<br>Static switch<br>Inverter transformer | Cabling<br>Contactor feeder[a]<br>Fuse(s)<br>Fused switch<br>Instrument<br>Rectifier<br>Rectifier transformer | Control<br>Actuating device<br>Monitoring<br>Internal power supply | Cabinet<br>Insulation<br>Cooling fans<br>Others |

[a]Normally located in the supplying switchboard

**Table A 18 — Equipment specific data — UPS**

| Name | Description | Unit or code list | Prior.* |
|---|---|---|---|
| Application | What equipment the UPS is applied for | Circuit breaker, control systems, safety systems, telecommunication | H |
| System voltage | Input voltage | Volt | H |
| Input frequency | Rated input | 50 or 60 Hz | H |
| No. of phases input voltage | 1 phase or 3 phase | # | H |
| Voltage variation | Input voltage | pct. | L |
| Frequency variation | Input frequency | pct. | L |
| System voltage | Output voltage | Volt | H |
| Output frequency | Rated output | 50 or 60 Hz | H |
| No. of phases output voltage | 1 phase or 3 phase | Number | H |
| Rated output load and power factor | Apparent power and power factor in nominal operations | kVA/cos phi | H |
| Degree of protection | Protection class according to IEC 60529 | IP code | M |
| Ambient temperature | Operating temperature range | Maximun and minimum temperature in deg. C | L |
| Cooling method | Specify | Water, air, others | M |
| UPS string system | The numbers of UPS systems which are working in parallel. | Dual, single, triple | M |
| UPS string system | The number of UPS that are working in parallel | Dual, single, tripple | M |

| | | | |
|---|---|---|---|
| Rectifier/inverter bypass system | Type of bypass switch | Manual, static | M |
| Battery back-up time | The time in which the battery can supply rated output power to the inverter | min. | M |
| Recharge time | The time to recharge the battery to 90% capacity | min. | M |
| Battery technology | Type of | NiCD, Pb acid, other | M |
| Battery earth fault monitoring | Specify | Common, individual, N.A. | L |
| Method of ventilation | Specify | Forced, natural | L |
| No. of battery banks | Specify | Number | M |
| ***) H** = High, **M** = Medium, **L** = Low Importance | | | |

# VEDLEGG B

**Klassifisering av utstyr** (fra ISO Standard 14224 Standard DIS-versjon utgitt desember 2004)

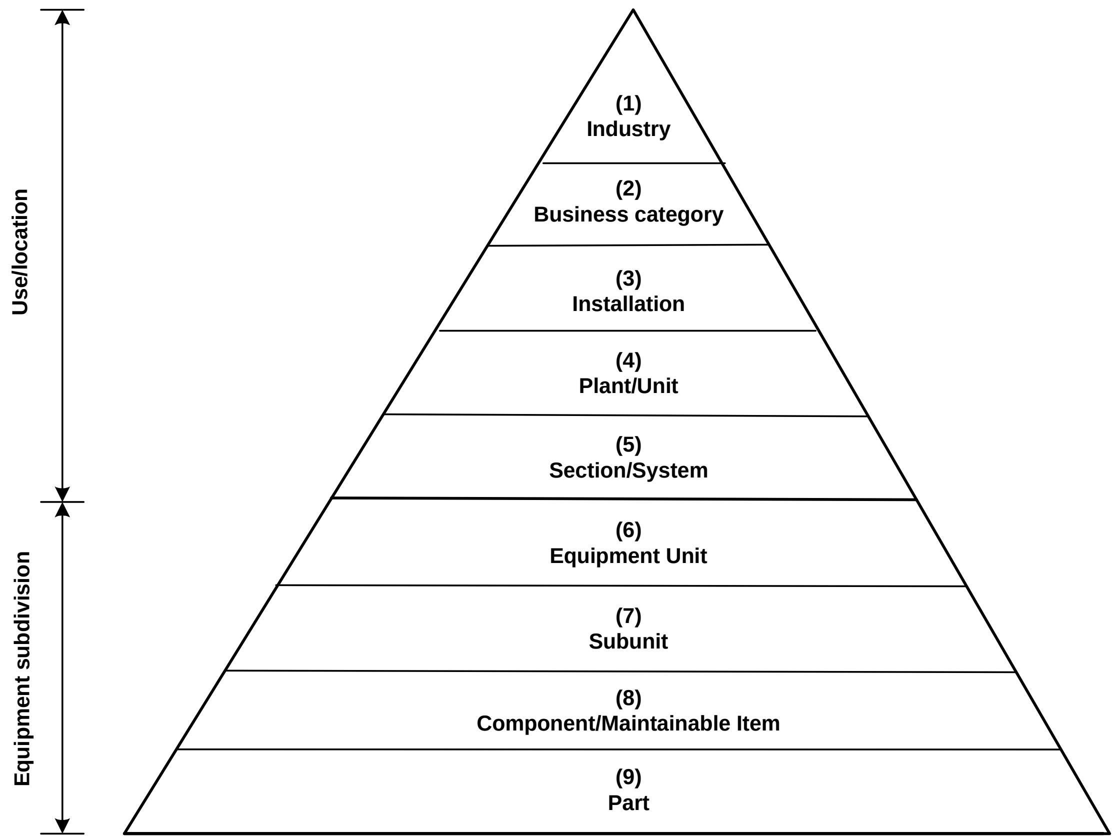


**Figure B.1 – Taxonomy** (ISO 14224 Figure 4)[12]

**Table B.1 — Equipment classes (level 6)** (ISO 14224 Annex A, Table A.4)[12]

| Equipment category | Equipment class (level 6) | Example included in Annex A |
|---|---|---|
| *Rotating* | Combustion engines | Yes |
| | Compressors | Yes |
| | Electric generators | Yes |
| | Electric motors | Yes |
| | Gas turbines | Yes |
| | Pumps | Yes |
| | Steam turbines | Yes |
| | Turboexpanders | Yes |
| | Blowers and Fans | No |
| | Liquid expanders | No |
| | Mixers | No |
| | *etc.* | |
| *Mechanical* | Cranes | Yes |
| | Heat exchangers | Yes |
| | Heaters and boilers | Yes |
| | Vessels | Yes |
| | Piping | Yes |

[12] DIS-versjon utgitt 2004

| Equipment category | Equipment class (level 6) | Example included in Annex A |
|---|---|---|
| | Winches | Yes |
| | Swivels | Yes |
| | Turrets | Yes |
| | Storage tanks | No |
| | Loading arms | No |
| | Filters and strainers | No |
| | Steam ejectors | No |
| | X-mas trees (topside/onshore) | No |
| | *etc.* | |
| *Electrical* | Uninterruptible power supply | Yes |
| | Switchgears /switchboards and distribution boards | No |
| | Power transformers | No |
| | Frequency converters | No |
| | Power cables and terminations | No |
| | *etc.* | |
| *Safety and control* | Fire and gas detectors | Yes |
| | Input devices | Yes |
| | Control units | Yes |
| | Valves | Yes |
| | Nozzles | Yes |
| | Evacuation equipment | No |
| | Fire fighting equipment | No |
| | Inert gas equipment | No |
| | *etc.* | |
| *Subsea* | Subsea production control | Yes |
| | X-mas trees | Yes |
| | Risers | Yes |
| | Subsea pumps | Yes |
| | Subsea processing equipment | No |
| | Templates | No |
| | Manifolds | No |
| | Pipelines | No |
| | Subsea isolation equipment | No |
| | Intervention tools | No |
| | Electric power distribution | No |
| | *etc.* | |
| *Drilling* | Blowout preventer [a] | Yes |
| | Top Drive | Yes |
| | Derrick [b] | No |
| | Drawworks | No |
| | Mud pumps | No |
| | Mud treatment equipment | No |
| | Diverter | No |
| | Choke manifold | No |

| Equipment category | Equipment class (level 6) | Example included in Annex A |
|---|---|---|
| | String motion compensator | No |
| | Riser compensator | No |
| | Cementing equipment | No |
| | Drilling and completion risers | No |
| | Crown and travelling blocks | No |
| | *etc.* | |
| *Well completion (downhole)* | Downhole safety valves | Yes |
| | Casing | Yes |
| | Tubing | Yes |
| | Hangers | No |
| | Packers | No |
| | Electrical submersible pumps | No |
| | Downhole sensors | No |
| | Wellheads | No |
| | *etc.* | |
| *Well intervention* | Coiled Tubing, surface equipment | No |
| | Coiled Tubing, BOPs and control systems | No |
| | Coiled Tubing, other pressure control equipment and systems | No |
| | Coiled Tubing, string and mechanical bottom hole assembly bottom | No |
| | Coiled tubing, string and electrical bottom hole assembly | No |
| | Wireline, surface equipment | No |
| | Wireline, BOPs and control systems | No |
| | Wireline, other pressure control | No |
| | Wireline, slickline/braided cable and bottom hole assembly | No |
| | Wireline, electric cable and bottom hole assembly | No |
| | Rig Assisted (RAS) Snubbing, surface equipment | No |
| | Rig Assisted (RAS) Snubbing, BOPs and control systems | No |
| | Rig Assisted (RAS) Snubbing, other pressure control equipment | No |
| | Rig Assisted (RAS) Snubbing, tubing and bottom hole assemblies | No |
| | etc. | |
| *Marine* | Anchor windlasses and mooring equipment | No |
| | Thrusters | No |
| | Dynamic positioning equipment | No |
| | Towing equipment | No |
| | Jacking equipment | No |
| | De-icing equipment | No |
| | Helicopter deck with equipment | No |
| | etc. | |
| *Utilities* [c] | Hydraulic power units | No |
| | Air supply equipment | No |
| | De-superheaters | No |
| | Nitrogen supply equipment | No |
| | Heating/cooling media | No |
| | HVACs | No |

| Equipment category | Equipment class (level 6) | Example included in Annex A |
|---|---|---|
| | *etc.* | |

[a] Subsea blowout preventer.

[b] Including heave compensation.

[c] Utilities may comprise a number of equipment classes in this International Standard (e.g. pumps, valves, instrumentation).

# VEDLEGG C

**Feilmode definisjoner for sikkerhetsutstyr**
(fra ISO Standard 14224, DIS-versjon 2004, Annex B + C)

**Table C 1 - Safety & Control Equipment - Failure Modes** (ref. ISO 14224 Annex B Table B.8)[12]

| Equipment | | | | | | Failure mode | | | |
|---|---|---|---|---|---|---|---|---|---|
| Fire & Gas detectors* | Input devices | Control Logic Units | Valves | Nozzles | UPS | Description | Examples | Code[a] | Type[b] |
| X | X | X | X | | X | Fail to function on demand | Doesn't start/open on demand | FTF | 1 |
| | | | X | | | Fail to stop/close on demand | Doesn't stop/close on demand | STP | 1 |
| | | | X | X | | Delayed operation | Opening time below sepc. | DOP | 2 |
| | | | X | | | Spurious stop | Unexpected closure | UST | 2 |
| | X | X | | X | | Spurious operation | E.g. false alarm | SPO | 2 |
| X | X | X | X | | | High output | Overspeed/output above acceptance | HIO | 2 |
| X | X | X | X | | X | Low output | Delivery/output below acceptance | LOO | 2 |
| X | X | X | | | X | Erratic output | Oscillating, hunting, instability | ERO | 2 |
| X | X | | | | X | No output | No output | NOO | 1 |
| | | | | | X | Faulty output frequency | Wrong/unstable frequency | FOF | 2 |
| | | | | | X | Faulty output voltage | Wrong/unstable output voltage | FOV | 2 |
| X | | | | | | Spurious high alarm level | E.g. 60% LEL | SHH | 2 |
| X | | | | | | Spurious low alarm level | E.g. 60% LEL | SLL | 2 |
| | | | | | X | Loss of redundancy | One or more redundant units not functioning | LOR | 3 |
| | | | X | X | | Plugged/choked | Partly or fully flow restriction | PLU | 1 |
| | | | | | X | Overheating | Machine parts, fluids etc. | OHE | 3 (2) |
| | X | | X | | | External leakage process medium | Oil, gas, condensate, water | ELP | 3 |
| | X | | X | | | External leakage utility medium | Lubricant, cooling water | ELU | 3 |
| | | | X | | | Internal leakage | Leakage internally process or utility fluids | INL | 1 - 3 |
| | | | X | | | Leakage in closed position | Leak through valve in closed position | LCP | 1 - 3 |
| | | | X | | | Abnormal instrument reading | False alarm, faulty instrument indication | AIR | 2 (3) |
| | | | X | X | | Structural deficiency | Material damages (cracks, wear, fracture, corrosion) | STD | 3 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| X | X | X | X | X | X | Minor in-service problems | Loose items, discoloration, dirt | SER | 3 |
| X | X | X | X | X | X | Other | Failure modes not covered above | OTH | - |
| X | X | X | X | X | X | Unknown | Too little information to define a failure mode | UNK | - |

a A proposed abbreviated code for the failure mode.

b Three types of failure modes are shown as follows:

8 desired *function is not obtained* (e.g. fail to start);

9 *specified function lost or outside* accepted operational limits (e.g. spurious stop, high output);

1. *failure indication* is observed, but there is no immediate and critical impact on equipment unit function. These are typical *non-critical* failures related to some degradation or incipient fault condition

c The codes shown apply to equipment classes marked with X

## * NOTE on F & G detector failure modes :

For F & G detectors it is important that all failures are recorded also those detected during scheduled testing and those detected in operation. E.g. replacement of a detector head should be recorded even if this is done as part of the preventive maintenance program. Note that a failure recorded on a F&G detector may sometimes be caused by failure in other parts of the loop (e.g. Central Unit, Logic Solver).

Typical failure modes are:

*Fail to function:*

The detector does not respond when exposed to its relevant stimulus (e.g. gas or heat). This failure mode is normally observed during functional testing.

*Spurious operation:*

The detector gives an alarm signal when it is not exposed to relevant stimulus. This failure mode is normally observed during operation and logged by control room personnel.

*Others:*

Additionally, some failure modes related to low/high output, adjustments and overhauls will typically be found in the log-books.

SINTEF

**Table C 2 — Failure definitions in relation to reliability and availability/application**

(ref. ISO 14224 Annex C, table C.1)[12]

| **Type of failure/maintenance to record** | **Relia-bility** | **Avail-ability** |
|---|---|---|
| Failures that require some corrective maintenance action to be carried out (repair, replacement) | Yes | Yes |
| Failure discovered during inspection, testing, and/or preventive maintenance that requires repair or replacement of typically non-wear items (seals, bearings, impellers, etc.) | Yes | Yes |
| *Failure of* safety devices or control/monitoring devices that necessitates shutdown (trip), or reduction of the items capability below specified limits. | Yes | Yes |
| Shutdown (trip) of the item (whether automatically or manually controlled) due to external conditions or operating errors, where no physical failure condition of the item is revealed. | No | Yes |
| Failure on the equipment that are caused by external impact (e.g. lack of power supply, structural impact, etc.) | No | Yes |
| Periodic replacement of consumables and normal wear parts | No | No |
| Minor planned maintenance services like adjustments, lubrication, cleaning, oil replacement, filter replacement or cleaning, painting etc. | No | Yes |
| Testing and inspections | No/Yes[c] | Yes |
| Preventive or planned maintenance [a] | Yes/No | Yes |
| Modifications, new work, upgrades [b] | No | Yes/No |

[a] To get the full lifetime history of the equipment the actual preventive maintenance should be recorded. For recording failures only, this can be skipped.
[b] Modifications are normally not a part of maintenance but frequently done by maintenance personnel.
[c]For safety equipment normally used on demand, the no. of demands should be recorded in order to calculate PFD numbers

SINTEF

# VEDLEGG D

## Prosjektsammendrag

Olje og gassvirksomheten til havs og på land setter stadig sterkere krav til ytelsesfaktorer som tilgjengelighet og pålitelighet for utstyr og operasjoner. Prosjektet er rettet mot forskningstema tilknyttet : 1) Instrumenteringspålitelighet 2) Pålitelige dypvannsoperasjoner.
Det er i dag en mangel på strukturering av data for pålitelighetsanalyse tilknyttet detaljer innen instrumenteringspålitelighet. Forskningsundersøkelse av ekspert-metodikk ønskes også fokusert i dette prosjektet, da dette kan akselerere tilgang på data og representerer noe nytt i forhold til tradisjonell pålitelighetsteori.
Ettersom FoU-aktivitene gjennomføres over perioden 2004-6 planlegges det løpende industridialog for å ajourføre/komplettere viten som bygges opp i prosjektperioden.

**1) Fokusområde - Instrumenteringspålitelighet**
Analyse og vurderinger av instrumenterte sikkerhetssystemer iht såkalte SIL-analyser (IEC61508), NORSOK Z-016 og nytt HMS-regelverk krever tilgang til pålitelighetsdata av slikt utstyr. Disse analyser har vital betydning for sikkerhetsnivå og regularitetseffekter for de anlegg som vurderes. Bransjesituasjonen mhp kvalifiserte pålitelighetsdata er ikke tilfredstillende på dette området, og det er et behov for å foreta en mer forskningspreget vurdering av data som i dag ikke dekkes i internasjonalt OREDA-prosjekt for å danne metodisk grunnlag for å få nye data. Ettersom SIL-analyser vil kreve mange type data som ikke på kort sikt vil dekkes av OREDA-databasen, foreslås i dette prosjekt å kartlegge databehovene, identifisere tilgjengelige dataformater og etablere en datastruktur for at industrien kan ha bedre konsistens og bedre kvalifiserte data i slike analyser. Dette er også viktig mhp bruk av slike pålitelighetsdata for måltall/indikatorer.
Det vil gjennomføres som et samarbeid med forskningsmiljø, operatører, fabrikanter og engineering. Driftsmodellen for OREDA-24 Databank planlegges utnyttet etter nærmere avtale med Statoil, f.eks. driftstilganger for aktuelle parter i prosjektet. Sikkerhetskritisk utstyr som ventiler, brann&gassdetektorer, prosess-sensorer vil vurderes mhp type inventar-data (OREDA) som kreves , og som et nært samarbeid med aktuelle leverandørerer. Pålitelighets-estimering basert på ekspertvurderinger planlegges, for å komplettere kvantitative data (ref. OREDA). Spesiell metodikk tilknyttet dette område vil undersøkes for uttesting i SIL-sammenheng.

1.1 <u>Del-aktiviteter</u>

a) Datastruktur / granskning
Ved innsamling av data for såkalte SIL-analyser er det nødvendig at data blir tilpasset et format som tilfredsstiller både behovet for analyse og som er tilpasset de data man kan forvente seg finnes tilgjengelig hos operatørene. Aktuelle format, definisjoner og taksonomier for slike data vil bli vurdert og forbedringer foreslått.

b) Caser/beste praksis
Et utvalg av utførte SIL-analyser vil bli gjennomgått for å avdekke behov for forbedring av datakvalitet og foreslå en "beste praksis" vedr. fremskaffelse og bruk av data for slike SIL-analyser.

c) Tilleggsoppgaver definert etter behov som måtte bli avdekket underveis

1.2 <u>Produkter</u>

Produktene fra prosjektet vil til en viss grad bli utformet underveis, men i utgangspunktet er flg. planlagt:

- Beskrivelse av egnet dataformat, definisjoner og taksonomi for innsamling av pålitelighets-data for instrumenterte sikkerhets-systemer
- "Beste praksis" for estimering og bruk av pålitelighetsdata i såkalte SIL-analyser inkludert kvalifisering av godheten av data
- Innspill til ISO-standardiseringsarbeid (ISO TC67/WG4) og industri-JIP (OREDA)

SINTEF

# VEDLEGG E

## Foredrag (”Paper”) om hvordan man kan bruke ekspertmetoder for å prediktere pålitelighets-parametre

(Hovedinnholdet i foredraget ble presentert av A. Hjorteland, Statoil, på prosjektmøtet 6. Desember)

SINTEF

# On how to use expert judgments in regularity analyses to obtain good predictions

A. Hjorteland & T. Aven
*Stavanger University College, Stavanger, Norway*

ABSTRACT:

The purpose of regularity analysis is to assess future deliveries of production and transportation systems, such as oil and gas installations. When conducting such analysis, models are developed reflecting the performance of various equipment, for example compressors and pumps. To assess the equipment performance there is a need for relevant knowledge, including observed data and expert judgments.

One of the challenges in regularity analyses is to assess uncertainties for the large number of quantities in the models being used. These quantities are either observable quantities such as lifetimes or repair times, or statistical expected values or probabilities, such as the MTTF or MTTR. The purpose of this paper is to present and discuss a practical approach for such assessments using the combination of expert judgments and hard data. The approach is based on a Bayesian framework, with focus on prediction and uncertainty assessments of observable quantities.

# 1 Introduction

Regularity is a term used to describe how a system, for example an offshore oil and gas production and transport system, is capable of meeting demands for deliveries or performance. Production availability, deliverability or other measures can be used to express regularity. In regularity analyses these measures are assessed, and in this way the analyses support decision-making in design and operation.

Suppose that a regularity analysis is to be conducted for a gas producing offshore installation during the concept development phase. The quantities of interest are regularity measures such as gas production within a certain period of time, and to be able to predict such quantities, information is gathered to increase the knowledge about the production process. A model, reflecting the process is developed, and available information is used to express uncertainty related to the outcome of the unknown quantities in the model. The information used can be categorized as:

1. Historical (observed) data.
2. Expert judgments.

One of the challenges in regularity analyses is to assess uncertainty for a very large number of quantities. The planned offshore installations main functions are to receive rich gas from the reservoir, separation of gas and fluids, gas compression and gas export to an onshore process plant. Each of these functions contains a large number of subsystems and the subsystems contain equipment like pumps, valves, pipes and vessels. A model is developed linking the performance of the equipment. When considering the performance of equipment, quantities such as uptimes and downtimes are included. The remaining part of the regularity analysis is to assess uncertainties about the equipments future performance. When predicting regularity of such a system, it is normal that there are approximately 600 - 800 unknown quantities in the model. Clearly, assessing such large numbers of quantities can be very resource demanding.

Hence there is a need for procedures that give guidance on how to perform the uncertainty assessments. Some guidance is given by the industrial standard for regularity management and reliability technology, cf. Norwegian Technology Standard Institution (1998), which provides requirements and guidelines for planning, execution and use of regularity analyses and management. The above-presented approach to regularity analyses is based on this standard. The standard adopts a predictive, Bayesian approach to regularity in the sense that focus is on predicting observable quantities and probability is used as a measure of uncertainty, seen through the eyes of the assessors, cf. Aven (2003). However, this standard does not give detailed recommendations on how to deal with the many challenges related to uncertainty assessments, such as:

- The vast number of quantities to be assessed.
- Lack of sufficient amount of relevant hard data.
- How to incorporate expert judgments.

This paper addresses these challenges in the context of the predictive, Bayesian approach. More specifically we look at ways of compensating for lack of sufficient amount of relevant hard data, by using expert judgments. In a Bayesian context the normal procedure would be to use probability models for the uptimes and downtimes of the equipment, and specify uncertainty distributions for the parameters of these probability models. Bayesian statistics is mainly concerned about inference on parameters in probability models. Based on thought experiments, i.e. introducing 'similar' situations, the traditional Bayesian approach gives focus on fictional parameters. This means that the analyst is to express uncertainty related to an unobservable fictional quantity based on a sequence of hypothetical similar situations.

Such a full Bayesian procedure is however difficult to carry out in practice, and in this paper we discuss the use of expert judgments as a tool for simplifying this procedure. We discuss how expert judgment can be used to establish suitable uptime and downtime distributions, and avoid the problem of dependencies between consecutive uptimes (downtimes), by strengthening the background information for the uncertainty assessments. Adopting a Bayesian approach the consecutive uptimes (downtimes) are dependent as we learn by observing the uptimes (downtimes). However, it turns out that if the background information is sufficient strong, for example obtained by using expert judgments, this learning process can be ignored. The result is that we may use identical distributed, independent distributions for the uptimes (downtimes). This simplifies the analysis to large extent.

The literature presents a number of methods for uncertainty assessments utilizing expert judgments. However, most of these methods are somewhat technical and complex for application in regularity analyses. The regularity analyst will in most cases have problems when applying these procedures, concerning both technicality and the demand of resources. For the purpose of the regularity analysis there is a need for a simple approach, which can be used in an operational setting. In this paper we discuss the structure of such an approach, again in the context of the predictive, Bayesian framework. The starting points are the requirements and guidelines given by the industrial standard for regularity management and reliability technology (1998), and expert judgment elicitation methodology as presented by Cooke (1991) and others.

The rest of this paper is organised as follows: In Section 2 we formalise the challenges described above using a regularity analysis example as a starting point, emphasising the problems of dependencies. In Section 4 we give some remarks on the expert judgement elicitation process.

## 2 A regularity analysis example

Again we refer to the planning of the gas producing offshore installation. A regularity analysis is carried out during the concept development phase, supporting assessments of future gas deliveries and company profit. As a basis for such assessments, there is a need for information about key performance measures, both technical measures (related to equipment properties, system capability, future production, etc.) and financial measures (related to future exchange rate, planned and actual investments, expense budget due to equipment repair and maintenance, etc.). In this paper emphasis is put on the regularity analysis and prediction of gas production.

The main process stages of the gas producing offshore installation are illustrated in Figure 1.

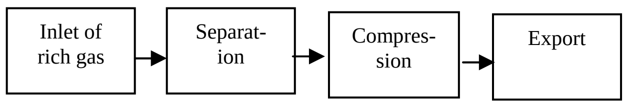


Figure 1. Illustration of the system's main process stages

Let $Y_t$ denote total production for the relevant period of time [0, $t$], for example a specific one-year period. The quantity $Y_t$ can be expressed in cubic meter of gas or normalized as a percentage in relation to the demand volume. Now in the planning phase $Y_t$ is unknown, thus we are led to prediction of this quantity. Later we can accurately measure $Y_t$; $Y_t$ is what we refer to as an observable quantity. The prediction can be done in different ways. We may compare with similar systems if available, or we could develop a more detailed model of the system reflecting the various equipment of the concept of interest, i.e. a regularity model. Using such a model, we try to reduce the complexity of the uncertainty related to $Y_t$, and thus reduce uncertainty.

But there are still some uncertainties remaining, related to the times to failure and the duration of downtimes of the various equipment included in the process stages. These are the unknown quantities of the model. By assigning probabilities related to their possible outcomes, we will arrive at an uncertainty distribution and prediction of $Y_t$.

To see in more detail what are the basic elements of this framework, we below present the details of such a regularity model. The presentation is based on the assumption that the system is a binary system of binary components.

Let $X_t(i)$ represent the state of equipment $i$, $i = 1, 2, \ldots, n$; $X_t(i) = 1$ if component $i$ is functioning at time $t$ and $X_t(i) = 0$ if component $i$ is not functioning at time $t$. We assume $X_0(i) = 1$. Let $T_{im}$, $m = 1, 2, \ldots$, represent the positive length of the $m$th operation period of component $i$, and let $R_{im}$, $m = 1, 2, \ldots$, represent the positive length of the $m$th repair time for component $i$. An overview of the unknown quantities is listed Table 1.

| Process stages | Equip. (i) | Time to failure ($T_{im}$, m= 1, 2, … ) | | | Time to repair ($R_{im}$, m= 1, 2, …) | | |
|---|---|---|---|---|---|---|---|
| | | $T_{i1}$ | $T_{i2}$ | … | $R_{i1}$ | $R_{i2}$ | … |
| Inlet of rich gas | 1 | $T_{11}$ | $T_{12}$ | … | $R_{11}$ | $R_{12}$ | … |
| | 2 | $T_{21}$ | $T_{22}$ | … | $R_{21}$ | $R_{22}$ | … |
| | … | … | … | … | … | … | … |
| Separation | … | … | … | … | … | … | … |
| Compression | … | … | … | … | … | … | … |
| Export | … | … | … | … | … | … | … |
| | n-1 | $T_{(n-1)1}$ | $T_{(n-1)2}$ | … | $R_{(n-1)1}$ | $R_{(n-1)2}$ | … |
| | n | $T_{n1}$ | $T_{n2}$ | … | $R_{n1}$ | $R_{n2}$ | … |

Table 1. The unknown quantities of the regularity model

Furthermore, let $g$ denote the relationship between $Y_t$ and the uptimes and downtimes $T_{im}$ and $R_{im}$. It is clear that $Y_t$ can be determined from the uptimes and downtimes - an explicit formula is given in Aven and Jensen (1999), p. 101, and thus we can write

$$Y_t = g(t, \boldsymbol{T}, \boldsymbol{R}), \qquad (1)$$

where $\boldsymbol{T}$ and $\boldsymbol{R}$ are the vectors of $T_{im}$ and $R_{im}$.

The function $g$ is a model. If all the uptimes and downtimes $T_{im}$ and $R_{im}$ were known, $Y_t$, could be predicted with certainty, given the assumptions of $g$. However, in practice, such information is not available, and uncertainties have to be taken into account.

Now, how should we assess the uncertainties of the vectors ($\boldsymbol{T}, \boldsymbol{R}$)? Ideally, a simultaneous distribution for all lifetimes and repair times should be provided, but this is not feasible in practice. Clearly, if we could use independence between all the quantities, the uncertainty assessments would be manageable, as we could assign a probability distribution for each quantity, and if we could apply the same distribution for the uptimes and the same distribution for downtimes, we are more or less done. However, we do not have independence and identically distributed quantities. Think of the time development process for one component, from time 0 to $t$. Having observed the four previous lifetimes (say), we have learnt about the component performance and should take this into account when assigning the probability distribution for the fifth lifetime.

The Bayesian solution to this problem is to introduce probability models, cf. e.g. Bedford & Cooke (2001) and Bernardo & Smith (1994). By conditioning on the parameters of these models, independence is obtained. Unconditionally, the random quantities are exchangeable, and not independent, but the probability models categories the components according to specific properties, and given these properties, the components may be considered independent.

As an example, an exponential distribution with parameter $\lambda$ could be utilized to express uncertainty related to $T_{im}$. Here $\lambda$ is interpreted as the long run fraction of failures when considering an infinite (or very large) number of 'similar' situations to the one analyzed. The parameter $\lambda$ is unknown; it is a random quantity, and the assessors uncertainty related to its value is specified through a prior (posterior) distribution $H(\lambda)$. Given $\lambda$, the lifetimes are independent and exponentially distributed with parameter $\lambda$.

From this set-up, we can calculate the distribution of $Y_t$, using standard probability calculus. However, running a full Bayesian analysis according to this scheme is challenging since we have to specify a high number of prior (posterior) distribution. Experience from regularity analyses applications shows that there is a need for simplifications to obtain a more practical tool. And the natural first choice for such a simplification is to question the need for assessing uncertainties of the parameters. Is it possible to justify the use of fixed parameters? Is it possible to justify independence between the random quantities?

According to the Bayesian theory, ignoring the uncertainty about $\lambda$ gives misleading over precise inference statements about $X$, cf. e.g. Bernardo & Smith (1994), p. 483. This reasoning is of course valid if we work within the standard Bayesian setting, considering an infinite number of exchangeable random quantities. However, if our focus are the observable quantities of the time interval considered, and we have a sufficient strong background information for assessing the uncertainties, the additional information gained by observing some lifetimes (repair times) are not significant, in the sense that we need not adjust the uncertainty distribution for the remaining lifetimes (repair times).

Thus, as a simplification of the uncertainty assessments, we could judge all $T_{im}$ and $R_{im}$ to be independent and use the same distribution $F$ for all lifetimes and the same distribution $G$ for all repair times for a given type of equipment.

The requirement of having strong background information is of course not always met. But the point made in this paper is that sufficient knowledge may be obtained by using expert judgments in some cases. Adding information by using expert judgment is the key to ensure independence. The result is that we may use, for selected components, identical distributed, independent distributions for the uptimes and downtimes. This simplifies the analysis to large extent.

## 3 Using expert judgment to justify independence

We return to the analysis in the previous section. The system being analyzed is in the concept development phase, and has therefore never been observed in operation. This means that no specific historical data of performance exists, either on system or on equipment level. However, similar equipment will in most cases have been observed on comparable installations and in comparable operational environment. This means that some generic observed data are normally available. In addition to generic data, some information from design, fabrication and testing of equipment will in most cases be available.

As an example, generic performance of a compressor can illustrate the collection of historical data. The equipment of interest is a centrifugal, turbine driven, compressor (8000 kW). In this case, the database OREDA (2002), provides experience data from 10 compressors, operated on four different installations. From the observed failures, the mean failure rate is 72 (per $10^6$ hours). OREDA (2002) also provide an upper and a lower failure rate, with an adjusted factor of $\pm 3$.

Now returning to the regularity analysis for the compressor in the concept development phase, and say that we for the first lifetime of the compressor use an exponential distribution with parameter $\lambda = 72$ (per $10^6$ hours). For the next lifetime, we should incorporate the information gained by observing this first lifetime, but given that the background information is strong, this is not required, as the 'error' introduced by this simplification is marginal. Thus we use the same distribution also for the second lifetime, and the two lifetimes are considered unconditionally independent. Using the same type of reasoning, we can do the same for the third lifetime and so on.

The difference by applying this approach as opposed to the traditional Bayesian framework would be insignificant in most practical cases. This is demonstrated by the example in Figure 2, where uncertainty related to the $10^{th}$ time to failure of the compressor is expressed both by assuming unconditionally independence and utilizing the traditional Bayesian approach. When applying the traditional Bayesian approach, the random quantity $T_{10}$ is assumed to follow an exponential distribution given the parameter $\lambda$. To express uncertainty related to what will be the true value of $\lambda$, a probability distribution needs to be assigned. In this case, a triangular distribution is judged to express the analysts' uncertainty of $\lambda$, utilizing the mean, upper and lower failure rate from OREDA (2002). For the exemplification in Figure 2 the $10^{th}$ time to failure for the compressor is assessed. Monte Carlo simulation is utilized to establish the uncertainty distributions.

From Figure 2, we see that the introduced 'error' when assuming independence is negligible, considering future performance in the concept development phase. The key factor influencing the 'error' is the amount of knowledge. In general there is more information available in the later project phases, and thus the 'error' will decrease.

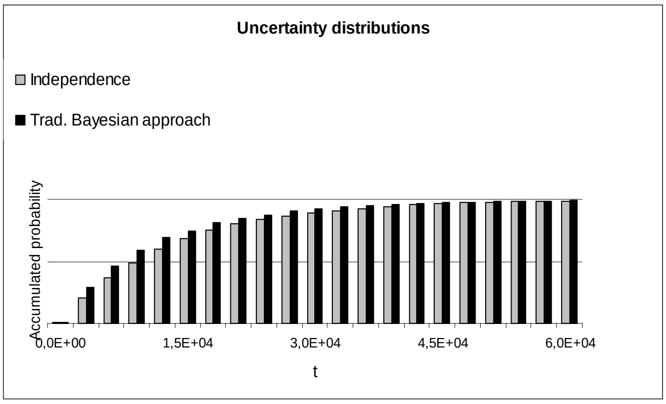


Figure 2. Uncertainty related to $T_{10}$, Example 1

If the generic data for the specific equipment provide 'sufficient knowledge', i.e. the 'error' is judged to be insignificant; an additional observation would have negligible influence on the assessed uncertainties. This means that we could justify the use of unconditional independence. Generic data will often provide sufficient knowledge, but are in some cases limited, regarding both quantity and quality/ relevance. The two key factors that have an impact on the relevance of the generic data are technology and application. In general, if the equipment being used is based on new technology or the application of the equipment is new, making use of expert judgments are needed to compensate for limited data.

To illustrate the increased difference between applying independence and the traditional Bayesian framework when having only partially relevant data, we refer to a population of electrical driven compressors with a wide upper and lower failure rate, an adjusted factor of $\pm$10. The reason for the wide boundaries is that this population of compressors is represented by a number of somewhat different models operated in different applications. Clearly, when a population is defined by equipment with varying properties, the historical observations are less relevant and contain more variance. Basically, this means that we become more uncertain when predicting the vectors (***T, R***).

As an example, an exponential distribution with parameter $\lambda$ is utilized to express uncertainty related to $T_{10}$. Analogous to the example in Figure 2, uncertainty of $\lambda$, when applying the traditional Bayesian approach, is expressed by a triangular distribution, now with boundaries given by the adjusted factor of $\pm$10. The uncertainty distributions are illustrated in Figure 3. The uncertainty distribution assuming independence remains the same as in the previous example, but the uncertainty distribution in accordance with the traditional Bayesian approach becomes wider as the uncertainty distributions are wider.

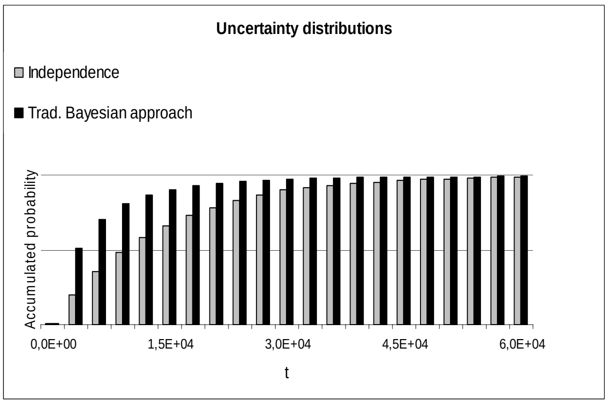


Figure 3. Uncertainty related to $T_{10}$, Example 2

As expected the differences between the two distributions are larger in Figure 3 than in Figure 2. The more uncertain the analyst is about a given parameter, the more ‘error’ is introduced. In most regularity analyses there are stronger information than assumed in Example 2, but there are cases where the background information is poor and then the difference becomes significant. The question is then how to obtain sufficient knowledge.

Sufficient knowledge is a judged amount of knowledge, when the assessor can ignore the assessment ‘error’. This point of reference is dependent on the objective of the analysis conducted and relates to the requirements to uncertainty in the various project development phases, cf. Hjorteland, Aven & Østebø (2003). In the concept development phase, the requirement is predictions with a $\pm$30% accuracy, whereas this requirement is $\pm$20% in the detailed engineering phase.

Assume that the generic data from the electrical driven compressors, with an adjusted failure rate factor of $\pm$10, where judged not sufficient by the assessor. This situation leaves the assessor with two alternatives; to apply the traditional Bayesian framework or to establish additional knowledge to ensure unconditional independence. In the following we focus on the latter case, where sufficient knowledge may be obtained by using expert judgments.

When predicting the vectors (***T, R***) the challenges are to extract the experts’ uncertainties related to the future outcome and to combine it with the generic data. The overall assessment process is illustrated in Figure 4. In the following section these challenges are discussed and recommendations are given on how to execute the expert elicitation process from a practical point of view. By conducting the expert judgment elicitation process, independence is ensured.

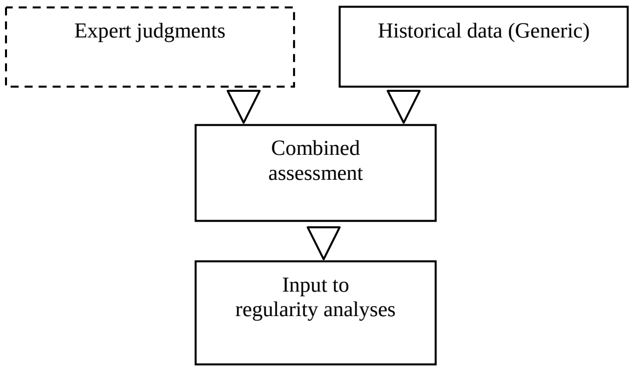


Figure 4. Main tasks of the assessments of quantities, utilizing expert judgments

# 4 Some remarks on the expert JUDGMENT elicitation process

The expert judgment elicitation process is a very resource demanding procedure if we are to assign probabilities expressing uncertainty for all the unknown quantities of the regularity model. Expert elicitation is very time demanding and expensive to carry out. The point is that if we treat all $T_{im}$ and $R_{im}$ to be dependent, the expert judgment process would in most cases not be practical feasible. Using the same reasoning as in the previous sections, given that the expert judgments provide sufficient knowledge, the quantities of ($\boldsymbol{T}$, $\boldsymbol{R}$) are supposed to be unconditional independent.

Referring to the compressor example in Section 3, Example 2, with an adjusted failure rate factor of $\pm$10, the objective of the elicitation process is to establish an uncertainty distribution with a lower adjusted factor, when combined with generic data. Reasonable resources are to be utilized to gather sufficient knowledge through expert judgments.

The challenge of the elicitation process is to extract the experts' uncertainties related to the future outcomes of the performance measures, i.e. $T_{im}$ and $R_{im}$. Such quantities are not to be interpreted as MTTF (Mean Time To Failure) and MTTR (Mean Time To Repair), but as future performance measured by $T_{im}$ and $R_{im}$ with a random selected $m$, given an equipment $i$. The selected panel of experts is to express uncertainty related to the performance of the relevant equipment, i.e. equipment judge to have an insufficient historical record.

The rest of this Section 4 will concentrate on how to establish uncertainty distributions for the future quantities of ($\boldsymbol{T}$, $\boldsymbol{R}$), based on historical data adjusted by experts. A practical, cost-effective approach to the assessment process is sought. The basis for the following discussions is mainly Cooke (1991), where basic methodologies for expert judgment elicitation processes can be found.

The following sections contains some discussions related to the two key challenges of the uncertainty assessment process:

- How to capture an experts' uncertainty.
- How to establish the final combined uncertainty distribution.

## 4.1 How to capture an experts' uncertainty

To communicate the experts' belief about the outcome of an observable quantity, for example the 10$^{th}$ operational period from Example 2, Section 3, a probability distribution is to be established through the elicitation process. This means that the regularity analysts' main challenge is to transform the experts' opinions into a probability distribution.

There are many ways of extracting an experts' opinion based on the notion of probabilities. Most people have poor intuitions regarding numerical probabilities. However, with some training in the terms and concepts of probability assignments, direct elicitation methods may be utilized. The analyst simply asks for the experts' opinion expressed in terms of probability. Clearly, training in numerical probability communication is required when extracting expert opinions, in which the analyst has confidence. The direct elicitation methods are normally supported by points of references, c.f. Lindley (1970). The idea is that the sought probabilities are assigned by comparing with other events, to which probabilities may easily be assigned.

To derive at one particular probability distribution, reflecting the experts' uncertainty, the normal procedure is to use parametric elicitation, cf. Cooke (1991). The parameters of the distribution are determined by specifying some peak value of the distribution and/or quantiles. To be more specific, and as an example, we again consider the 10th operational period from Example 2, Section 3. A probability distribution is to be established through the elicitation process utilizing the exponential distribution. This method presupposes that the experts' uncertainty is in reasonable accordance with this probability class. The experts are asked to predict the percentage *k* of the 10 lifetimes, having values exceeding *x* hours. From this we easily compute the mean of the exponential distribution, using the equation;

$$100\exp\{-x/\text{MTTF}\} = k. \quad (2)$$

We refer to Cooke (1991), De Finetti (1974), Lindley (1970) and Ramsey (1931) for other approaches and examples on how to perform the assignments.

### 4.2 How to establish the final combined uncertainty distribution

The final combined uncertainty distribution is not a distribution determined by the experts or the historical data, but uncertainty expressed by the analyst. However, the distribution is based on the expert judgements and the historical data. Clearly, the analyst must relate to all the information, consider its relevance and express uncertainty reflecting the available knowledge. The analyst has to combine information. How should this be done in a reasonable practical way?

The process is twofold, considering the opinions from the various selected experts and the observed data:

- Combining the various expert judgments.
- Combining the experts' opinion with the generic data.

Clearly, the experts' beliefs may conflict to a certain extent and the challenge for the analyst is to relate to the various statements within the panel of experts. Formal procedures exist for weighting expert judgments, but such procedures are difficult to carry out in practice. In addition, some would argue that any weighting procedure is inappropriate as all experts appointed should be given the same status, cf. Cooke (1991).

For an extensive review of literature concerning weighting procedures and combining expert opinions in general, see Cooke (1991).

As an alternative, expert panels are established with the aim of obtaining consensus. The aim is to obtain consensus among the experts and derive at one distribution reflecting the groups' judgments. This is cost-effective and practical applicable approach, but it does not function well if not properly managed.

Building consensus is of major concern when using expert judgements. Five principles are often highlighted, cf. Cooke (1991):

1. *Reproducibility*. It must be possible to reproduce all calculations.

2. *Accountability*. The basis for the probabilities assigned must be identified.

3. *Empirical control*. The probability assignments must in principle be susceptible to empirical control.

4. *Neutrality*. The methods for combining or evaluating expert opinion should encourage experts to state their true opinion.

5. *Fairness*. All experts are treated equally, prior to processing the results of observations.

We find these principles appropriate, except for ‘empirical control’. A probability expressing uncertainty cannot be verified when adopting subjective probabilities. Verification of a probability indicates that there exists a true objective probability, which is not in accordance with our interpretation of probabilities, cf. Aven (2003) and Hjorteland & Aven (2003).

The hard data may be a part of the information given to the expert panel, and then the panel way produces the relevant distributions for the analysts. However, it is also possible that the experts give their assessments without reference to the hard data. The analyst must then combine these two sources of information. This can be done in several ways, for example using a weighting procedure, reflecting the analysts’ judgments of the goodness of the information. An example of such a weighting procedure is shown in Table 2, where the goodness is categorised in three levels. Hence if the expert judgments are given the highest score, whereas the historical data the lowest, the weight distribution should be 80% on the expert panel and 20% on the hard data.

Table 2. Weighting system, E%-H%

| **E%-H%** | | **Expert judgements (E)** | | |
|---|---|---|---|---|
| | | 1* | 2* | 3* |
| **Historical data (H)** | 1* | 50%-50% | 60%-40% | 80%-20% |
| | 2* | 40%-60% | 50%-50% | 60%-40% |
| | 3* | 20%-80% | 40%-60% | 50%-50% |

** Here 1, 2 and 3 represent the judged goodness of the information*

# 5 References


Aven, T. 2003. Foundations of Risk Analysis – A Knowledge and Decision-oriented Perspective. New York, John Wiley & Sons Ltd.

Aven, T. & Hjorteland, A. 2003. A predictive Bayesian approach to multistate reliability analysis. *International Journal of Reliability, Quality and Safety Engineering*, Vol. 10., No. 3., 221-234.

Aven, T. & Jensen, U. 1999. *Stochastic Models in Reliability*. New York: Springer.

Aven, T. & Kvaløy, J.T. 2002. Implementing the Bayesian paradigm in risk analysis. *Reliability Engineering and System Safety* 78, 195-201.

Bedford, T. & Cooke, R.M. 2001. *Probabilistic Risk analysis: Foundations and Methods*. Cambridge: Cambridge University Press.

Bernardo, J.M. & Smith, A., *Bayesian Theory*. Chichester: Wiley & Sons, 1994.

Cooke, R.M. 1991. *Experts in uncertainty*. New York: Oxford University Press.

De Finetti, B. 1974. English translation, *Studies in Subjective Probability*, Wiley, New York (Original, 1937).

Hjorteland, A., Aven, T. & Østebø, R. 2004. On how to treat uncertainty in regularity analyses. Submitted for publication in *Reliability Engineering and System Safety*.

Hjorteland, A. & Aven, T. 2003. Reliability analyses and observables. The 14th *European Safety and Reliability Conference* (ESREL 2003), Vol. 1, ISBN 90 5809 551 7.

Lindley, D. 1970. Introduction to Probability and Statistics from a Bayesian Viewpoint, Cambridge University Press, Cambridge.

Norwegian Technology Standard Institution 1998, NORSOK Z-016 Regularity management & reliability technology, Rev. 1.

OREDA 2002. Offshore Reliability Data, 4th Edition. OREDA Participants.

Ramsey, F. 1931. ‘Truth and Probability’, in Braithwaite (ed.), *The Foundations of Mathematics*, Kegan Paul, London.