SIL - Driftserfaringer fra Kristin
ESRA 29.01.2014

Bjørnar Berg Teknisk Sikkerhet - Kristin

Espen Sørensen Automasjon – Kristin

Innhold i presentasjon -

- Innhold
- Bakgrunn og basis for SIL arbeidet vårt på Kristin
- Oppfølging i driftsfase og årlig gjennomgang
- Hva kan vi bli bedre på / erfaringer

Bakgrunn og basis for SIL arbeidet vårt

Kristin

- **Trykk: 910 barg**
- **Temp: 170 °C**

- **Produksjonskapasitet:**
- **Gass 18.3 mill Sm3/d**
- **Kondensat 20.000 m3/d**
- **Vann 5000 m3/d**

- **104 senger**

- **Oppstart Kristin: 2005**
- **Oppstart Tyrihans: 2009**
- **Oppstart LPP: 2014**

- **Tie back Maria**
- **Erlend/Lavrans/Kristin Sør???**

Kristin og SIL - historisk tilnærming

- Brukte OLF 070 hvis mulig. Ellers ble allokering gjort pr funksjon.
- 13 SRS'er og drøyt 30 SAR'er utarbeidet i prosjektet
- SRS'ene ble svært detaljert og «engineering rettet», vi utarbeidet egen «drift-SRS»
  - Ett overbygg/hoved dokument med 12 underliggende appendiks
- Ikke noe «SIL-sertifisert» utstyr i 2003, stor jobb med å skaffe underlag for SIL/PFD beregninger. Tillegg til opprinnelig kontrakter i Kristin prosjektet
- Ikke noe ferdig rammeverk for «SIL i drift»
  - Ingen konsernkrav i Statoil
  - OLF 070 lite praktisk rettet mot driftsoppfølging

Kristin og SIL

- Topside ca 35 instrumenterte sikkerhetsfunksjoner
- Subsea; 7 SIL funksjoner
- Noen funksjoner ikke spesifisert i OLF
  - Romkjølere
  - "Green line" til Åsgard C
  - HVAC ventiler i skroget
  - Vanntette dører inkl klemsikring
- Tyrihans inkl topside HIPPS

	Lukke SCSSV ved lavt trykk oppstrøms undervannschoke	SIL 1	
	HIPPS: Isolate flowline from wells upon P≥280 bar	SIL 3	
19	PAS – Isolere topside fra workover riser ved å stenge SPWV ved å aktivere trykknapp	SIL 2	-ZAA-S-RB-0007
	NAS – Isolere workover riser fra reservoar ved å stenge WCP-ventiler ved å aktivere trykknapp	SIL 2	-ZAA-S-RB-0007
52	Nødstopp av ballast pumper eller ventiler	SIL 2	App B
70	Brann deteksjon	SIL 2	App C
	Gass deteksjon	SIL 2	
	Manuell aktivering fra felt til B&G-systemet	SIL 2	
71&72	Aktivering av deluge	SIL 2	App D
	Vanntåke	SIL2	
	Sprinkler	SIL2	
	Brannvanns monitor	SIL2	
	Kjøling av nødgenerator	SIL2	
77	Stenge luftinntak til rom/brannområde	SIL 1	App E
	Start av DX-enhet	SIL 2	
	Isolering av et rom i skroget	SIL 2	
79	Åpne trykkavlastningsventil	SIL 2	App F
	Åpne ESV nedstrøms høytrykksfakkel væskeutskiller (HP KO drum)	SIL 2	
	LAHH (NAS signal) i væskeutskiller (KO drum)	SIL 2	
	NAS seksjonalisering ved å benytte en nødavstengningsventil	SIL 2	
	Manuell initiering av nødavstengningssystemet	SIL 2	
	Elektrisk isolering (singel gass i prosess område)	SIL 2	
84	Start av nødgenerator	SIL 2	App G
86	Overføring av tap av signal "permit to export" fra Åsgard C til Kristin PAS	SIL 2	App H
87	Prosess seksjonalisering	SIL 1	App I
	Prosess funksjon PAHH/LALL/LAHH	SIL 2	
	Prosess funksjon TAHH/TALL	SIL 2	
	LAHH i væskeutskiller (KO drum)	SIL 2	
93	Lukke to vanntette dører	SIL 1	App J
18	NAS: Isolering av en undervannsbrønn; lukk PWV eller (PMV og XOV).	SIL 3	App K
	NAS: Isolering av strømningsrør fra stigerør, lukke SSIV	SIL 2	
	Undervanns nedstengning på topside PAS	SIL 1	
	Undervanns nedstengning på PAHH nedstrøms undervanns choke	SIL 1	
	Lukke SCSSV ved lavt trykk oppstrøms undervannschoke	SIL 1	
	Stenge annulusventil (AWV) ved høyt trykk i annulus	SIL1	
13	Isolere topside prosess mot overtrykk med HIPPS	SIL 3	App L

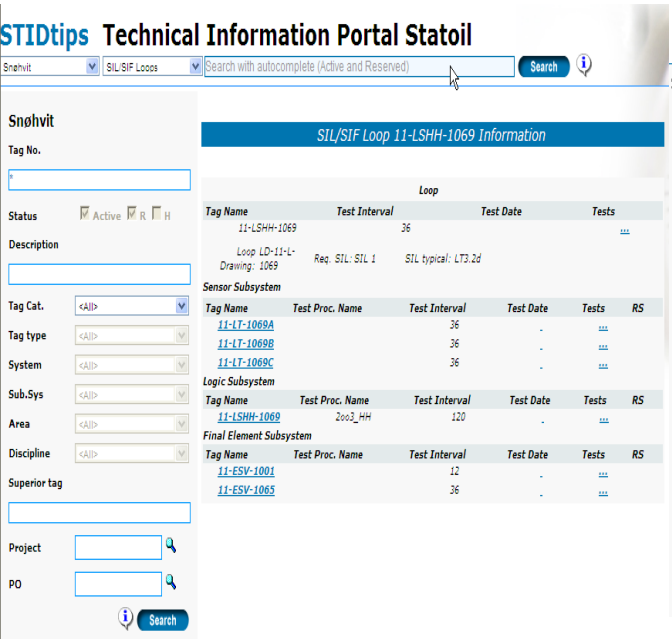
Statoil

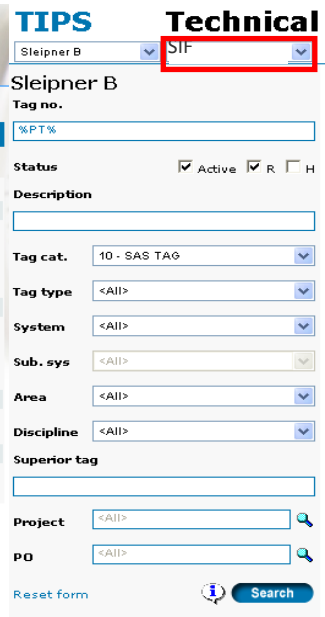
Kristin og SIL

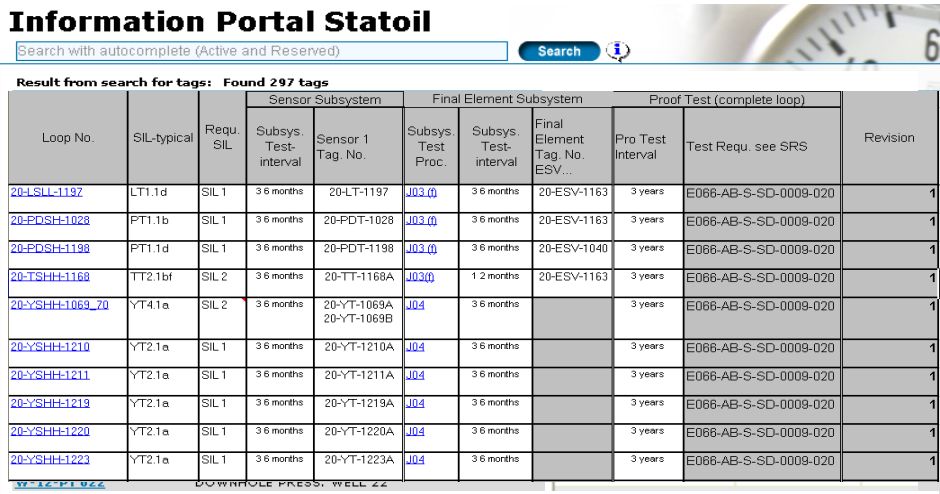
- Ikke utstrakte krav til enkeltfunksjoner, men til «typiske» funksjoner
- Dvs likt utstyr har stort sett samme SIL krav og samme krav til pålitelighet og følges opp likt.
- Eksempel: Alle LST, PST, TST følges opp som om de har SIL krav, uavhengig om de har SIL krav eller ikke.
- Stort sett samme type utstyr på de forskjellige funksjoner (samme type transmitter)
  - Gir bedre oversikt over feil på utstyrstypen (mere data)
- Oppfølging av logikk som en egen sak
- Oppfølging av «påhengt utstyr» (solenoid, grensebryter etc)
- Med dagens begrensninger (SAP, STID etc) følger vi opp enkelt komponenter og ikke funksjoner, da Statoil ikke har noe verktøy for oppfølging av funksjoner. Må da egentlig fordele PFD for funksjonen utover enkeltkomponentene.

Verktøy for funksjons-oppfølging?

- Ikke noe felles verktøy i Statoil i dag som følger opp på funksjonsnivå
- Endring i SAP – kopling av tag i funksjoner?
- Det er laget et forslag/pilot til ny STID modul for å identifisere og holde orden på SIL funksjoner.







Statoil

Statoil kravdokumentasjon for SIL

- Kristin laget selv to styrende dokumenter:
  - WR1381 Krav til oppfølging av IEC 61508 (SIL) i drift, Kristin
  - WD0688 (GL 0504) IEC61508/61511 Kristin Management of Compliance
- I ettertid har Statoil kommet med en del styrende dokumentasjon, som i hovedsak er mer generell enn de vi laget for Kristin. De viktigste er:
  - TR2041 - Safety Instrumented System (SIS) - Management of Lifecycle Requirement
  - TR3138 - Testing and inspection of safety instrumented systems including safety related valves
  - GL3137 - SIS, the follow up in operation
  - GL0114 – Safety Equipment (delvis, gir anbefalt nivå for sviktrate)
- **Det er en utfordring i konsern kravene at de skal passe både gamle og nye installasjoner på norsk og internasjonal sokkel, og da ikke blir konkrete nok!**

Lokal styrende dokumentasjon for SIL

- WD0688 – ”Management of Compliance”
  - Beskriver arbeidsprosesser og aktiviteter nødvendige for å samsvare med SIL.
  - Compliance iht 61508’s livssyklusfaser, og hvordan har vi oppfylt de enkelte faser
  - Hvordan Kristin har tilordnet SIL krav
  - Hvilke krav stilles/er stilt til utstyrsleverandører (Well proven krav)
  - Testing (kun prinsipielt)
  - Beskrivelse av arbeidsprosess for oppfølging i drift
- WR 1381 SIL oppfølging av ISS
  - Konkretisering av de ulike aktiviteter i drift og modifikasjoner
  - Hvordan gjennomføres krav gitt i WD0688
  - Hvem er ansvarlig for å utføre de ulike aktiviteter i egen organisasjon
- WD0688 er revidert og i ferd med å gis ut som GL0504, og WR 1381 er under revisjon.

Oppfølging i driftsfase og årlig gjennomgang

Oppfølging i driftsfasen

- Kristin er den første offshore Statoil installasjonen som er fullt bygget etter IEC 61508/61511 og forsøker å følge opp iht intensjon i standard også i drift/vedlikehold /modifikasjonsfaser.
- Alt ”SIL” utstyr er klassifisert som «utvalgt sikkerhetskritisk utstyr» (med noen få unntak) (på tag nivå – ikke funksjon)
- Rapportering av feil som for annet«utvalgt sikkerhetskritisk utstyr»
- Sørger derfor for at «utvalgt sikkerhetskritisk utstyr» følges opp slik at det tilfredsstiller krav for oppfølging av SIL utstyr.
- FV program er tilpasset krav til funksjonstesting (hele funksjonen)
- Oppfølging av modifikasjoner - må være med fra starten og definere oppgaven
- Oppfølging av V&M kontraktør – arbeidsprosessen inkludert kompetanse

SIL oppfølging WR1381

- Definerte aktiviterer på faste intervall, dvs hvem gjør hva når.
- Samsvarer med «krav» (should) i konsern GL3137 (Instrumented Systems, the follow-up in operation phase)

Intervall	Aktivitet	Ansvarlig
Kontinuerlig	Utføre funksjonstesting og vedlikehold gitt i vedlikeholdsprogram og testprosedyrer, og rapportere og utbedre feil på sikkerhetskritisk utstyr som spesifisert i FV og teknisk dokumentasjon.	Vedlikeholdsutøver
	Følge opp SIL mot OPS/KRI/V&M	Teknisk systemansvarlig
	Følge opp Modifikasjoner og prosjekt for «SIS» iht GL0504 og GL3137.	Teknisk systemansvarlig og SIL ansvarlig + roller fra GL0504.
	Sørge for opplæring av utførende personell om SIL styringssløyfe.	PV leder
Månedlig – kvartalsmessig	TIMP - synliggjøre og dokumentere teknisk integritet for alle fag/system/PS med oppdatert info om utvalgt sikkerhetskritisk utstyr	Teknisk fag/systemansvarlig/PS ansvarlig/Anleggsansvarlig
	Trekke ut og kvalitetssikre rapporterte feil på M2 notifikasjoner for SIL funksjoner og utvalgt sikkerhetskritisk utstyr	Vedlikeholdsstyring
	Ha kontroll på at testing og rapportering utføres iht. gjeldende prosedyrer Ha kontroll på utestående funksjonstesting ref. WD1148.	Teknisk systemansvarlig og vedlikeholdsstyring
Årlig	Utføre årlig gjennomgang av feil på utvalgt sikkerhetskritisk utstyr og øvrige SIL funksjoner Beregne feilrate for siste år Verifisere at erfarte feilrater samsvarer med akseptkriterier fra design (innenfor oppr. Feilrater) Ta relevante aksjoner ut fra funn i årlig gjennomgang Evaluere behov for og tidspunkt for neste ekspertpanelvurdering Oppdatere historikk på utvalgt utstyr, oppdatere datadossier Evaluere demandrater fra IMS applikasjon Evaluere om store avvik fra designforutsetningene har påvirket sikkerhetsfunksjonene, slik som demands/spurious trips, inhibiteringer/ overbroinger, kompenserende tiltak, utstyr som ikke er i bruk/ødelagt/utkoblet? Sjekke relevante unntak / SIS i Disp / Synergi	Automasjon/Teknisk Sikkerhet + Vedlikeholdsstyring + andre etter behov
	Planlegge og budsjettere for SIL aktiviteter i påfølgende periode.	SIL-ansvarlig
	Evaluere om testintervall kan endres ut fra gitte kriterier og anerkjente metoder. (PDS metoden)	SIL-ansvarlig med bistand ekspertpanel
	Endre testintervall ved behov, og oppdatere dokumentasjon/SAP	SIL-ansvarlig med bistand ekspertpanel
Fem-årlig eller etter behov	Oppdatere datadossier	SIL-ansvarlig
	Arrangere SIL kurs etter internt behov	SIL-ansvarlig
	Arrangere ekspertpanel gjennomgang mhp PFD og mulig justering av FV testintervall eller andre tiltak	SIL-ansvarlig med bistand fra systemansvarlig

Oppfølging i driftsfasen forts

- Feil rapporteres på M2 notifikasjon i SAP og benytter definerte feilkoder
  - Opplæring av driftsteknikere til å skrive utfyllende notifikasjoner
  - Feil rapportert blir kvalitetssikret av fagansvarlige anleggsintegritet
  - Utfordringer:
    - Langtekst/fritekst beskrivende nok til å verifisere klassifisering av feil
    - Rett klassifisert/kodifisert
    - Tid/ressurser til oppfølging/kvalitetssikring

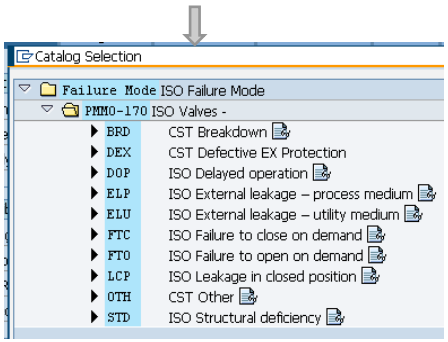
- SAP A10 rapport: farlige feil på utvalgt sikkerhetskritisk utstyr funnet ved testing

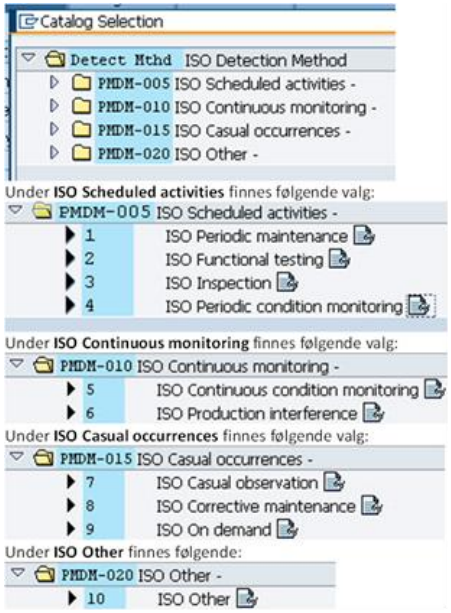
Rapportering av feil

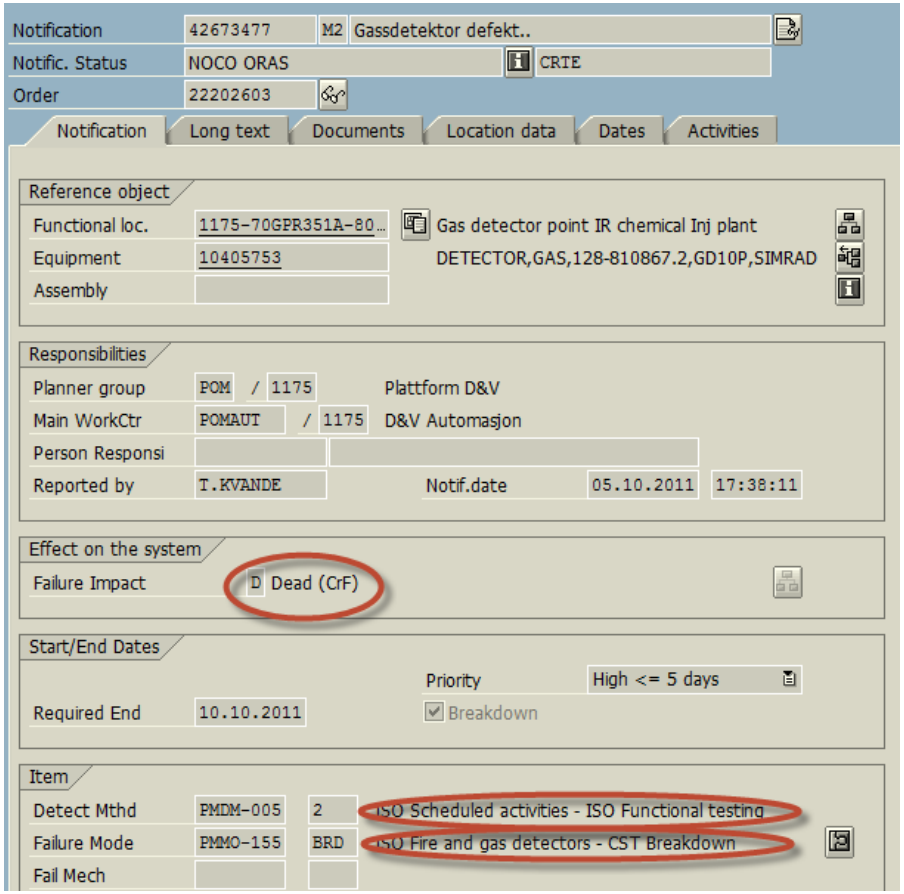
- Failure impact

- **Hvordan virker svikten inn på systemet/funksjonen**
- U Uvel — Mindre feil som ikke direkte truer utstyrets evne til å utføre tiltenkte funksjoner
- S Syk — Brukes når en har oppdaget en alvorlig degradering eller feilutvikling.
- D Død — Utstyret har sviktet eller satt ut av drift.

- Detection method
- Failure mode







Statoil

Årlig gjennomgang

- Kristin gjør en årlig gjennomgang av rapporterte feil på alt sikkerhetskritisk utstyr
- Gjennomgangen utføres av Automasjon, Teknisk sikkerhet, Vedlikeholdsstyring samt andre etter behov
- Erfarer at dette er noe av det som gis mest igjen
  - Tverrfaglig gruppe
  - Ser på tvers av fag
  - Ser på tvers av systemer
  - Over et helt år
  - Sammenlikner mot tidligere år
  - Komplett historikk med årlig gjennomgang/status siden oppstart 2006
- Har jobbet fram arbeidsmetodikk sammen med SINTEF / NTNU.
- Alle kvalitetssikrede data fra oss er gjort tilgjengelig for PDS forum.

Omfang for gjennomgangen

- Den tar utgangspunkt i SAP A10 rapport, i tillegg har vi noe SIL utstyr som ikke er kategorisert som utvalgt sikkerhetskritisk i SAP (eks telemetri, APS kjøleenheter, HVAC ventiler i skroget)
- Gjennomgangen verifiserer:
  - utfylling, kodifisering og klassifisering av alle notifikasjoner
  - utført vedlikehold
  - antall tester utført på utstyret
  - klassifisering av tag
  - knytning mot standard tekster
  - Ser separat på feil rapportert på sentralutstyr (ESD/PSD/B&G)
- Det utføres en evaluering og vurdering av utstyret på bakgrunn av tilgjengelig informasjon
- Totalt er 386 M2 og M4 notifikasjoner manuelt verifisert i gjennomgang for 2012, i tillegg til at FV program, tag klassifisering, kritikalitet og standardtekster er verifisert.

Utklipp fra årlig gjennomgang

A.1 A10 26 Blow down valve (33 stk.)

Class	No of funct loc.	No of tests	No of failures	Target
26 Blow down valve	33	31	1	3

To nye LPP ventiler er ikke driftsatt eller testet enda.
Target verdi er feil, GL0114 sier 0,5% tillatt feil, A10 benytter 10%

Notification	Description	Functional Loc.	Fail mode	Det meth	Failure Imp	Created on	Klass
42777939	23ESV1023 hakker veldig og aktuator er l	1175-23ESV1021	OTH	1	S	29.01.2012	SU
42801432	Ventil går rykkvis.	1175-23ESV1021	OTH	2	S	24.02.2012	NA
42801594	Ventil går rykkvis.	1175-23ESV1021	OTH	2	S	24.02.2012	NA
43101945	Defekt hydraulikkslange	1175-45ESV1009	BRD	1	S	03.11.2012	SD
43114313	Korrosjon på hovedbolter og drenstusser	1175-13ESV2506	OTH	3	U	08.11.2012	SU
42893696	Alarm ved test av blowdown ventil	1175-20ESV1412	DOP	2	U	02.06.2012	DU
42972029	Utvendig korrosjon på aktuator 43ESV4102	1175-43ESV4102	STD	7	U	26.08.2012	NA

Registrerte feil (7 notifikasjoner)

- 1 SD feil på slitte hydraulikkslanger
- 2 SU rykkete gange (men innenfor krav) samt rust.
- 1 DU, ventil bruker for lang tid på å åpne, OK etter justering av flow controller
- 4 NA feil, forbedringsforslag eller uklare notifikasjoner med uidentifiserbare ukritiske feil

Vurdering:

- Kun en M2 på slitte hydraulikk-slanger, dette er en vesentlig nedgang fra foregående år.
- Relativt få feil i forhold til tidligere år.
- Ingen feil på grensebrytere eller solenoid ventiler

Det gjøres en kvalitetssikring av resultatene sammen med relevante fag-/systemansvarlige. Videre aksjoner avtales med disse.

Statoil

Feil oppdaget ved test vs feil oppdaget i drift

- For noen typer utstyr er testing dominerende demand rate og SAP A10 rapport vil gi et riktig bilde, da de fleste feil oppdages ved testing. (f.eks B&G detektorer)
- For annet type utstyr vil ”normal bruk” være dominerende demand, for eksempel branndører. Dørene har 4mnd test intervall, men opereres flere ganger daglig. De fleste farlige feil vil oppdages ved normal bruk.
- I henhold til definisjon i IEC 61508/61511 skal farlige feil både fra testing og ved reelt behov vurderes. SAP A10 synliggjør kun farlige feil funnet ved testing, og følger altså ikke definisjon fra IEC 61508/61511.
- TR3138 (Testing and inspection of safety instrumented systems) stiller krav om vurdering og oppfølging av feil iht IEC61511
- Å kun benytte A10 som mål på farlige feil /feilrate (DU) på utstyr er ikke tilstrekkelig.
- Dersom man tar med feil oppdaget i drift, kan det være en utfordring å beregne feilrate, vi må da vite demand rate.

Feil ved test vs feil i drift for 2012

- I A10 rapport direkte fra SAP vises 9 farlige udetekterte feil funnet under testing av sikkerhetskritisk utstyr. Etter manuell gjennomgang av alle notifikasjoner på sikkerhetskritisk utstyr, finner vi at det ved test eller reell demand er 19 farlige feil.
- Det vil si at mindre enn halvparten av de farlige feilene oppdages ved testing.
- Vi ser ellers at totalt antall farlige feil (19 stk) ligger i samme størrelsesorden som for tidligere års gjennomganger. Det vil si at vi ikke ser noen tendenser for økt feilrate for installasjonen samlet sett.

Funn og vurderinger

- Feil funnet ved testing viser at 2 klasser er over akseptkriterie på max tillatte feil.
- Om man tar med feil funnet i drift, samt SIL utstyr som ikke er definert som «utvalgt sikkerhetskritisk utstyr»:
  - To klasser over krav pga feil oppdaget i drift.
  - En klasse SIL utstyr som ikke er definert «utvalgt sikkerhetskritisk» over akseptkriterie.
- Dvs totalt 5 klasser over krav til max antall tillatte feil

- Vi har så langt holdt oss til opprinnelig planlagt test intervall og omfang for ”SIL” utstyr fra design fasen, med unntak av noen mindre forbedringer/endringer i test intervall for røyk deteksjon. Dette viser at konseptet som ble valgt er en god og forutsigbar metodikk for å følge opp utstyret.

Farlige feil funnet i drift

- Hvilke farlige feil fant vi i drift?

- 1 stk PSV feil forsvant (åpnet for tidlig, ikke «farlig»)
- Brannspjeld, 2 feil (feil registrert)
- Branndør, 1 feil (feil registrert, gulvteppe imellom)
- PSD ventil, 2 feil (ventil lukket ikke i drift)
- PSD/ESD transmitter 6 feil (2 stk PST viser 8 bar trykkløst, LL på 5 bar, 4 LST målefeil)

- Dvs 4 stk feil-registrert (mot vedlikehold og ikke testing), 2 ventiler lukket ikke ved reelt behov, avvik mellom seglass/LT og LST for 4 nivåmålere

Samlet statistikk fra 2006 til i dag

- Siden vi har kjørt dette siden 2006 begynner vi å få et godt datagrunnlag

- Noen gjengangere, men også noen «tilfeldige»

KRISTIN						No of failures						
Hidden Failure (Class)	No.of.Func.Loc.	No. of tests	No.of failures	Target	SIL krav	2006	07	08	09	10	11	12
nn1	328	1815	22	73		6	0	6	1	5	3	1
nn2	207	1464	3	15	SIL2	0	1	0	1	1	0	0
nn3	585	3532	4	33	SIL2	0	1	2	0	0	1	0
nn4	306	1811	4	18	SIL2	0	0	1	0	3	0	0
nn5	821	5639	12	56	SIL2	4	4	2	1	1	0	0
nn6	39	262	1	1	SIL2	1	0	0	0	0	0	0
nn7	65	429	0	7	SIL2	0	0	0	0	0	0	0
nn8	12	81	0	0	SIL2	0	0	0	0	0	0	0
nn9	8	44	6	1		0	0	5	0	0	0	1
nn10	65	995	33	19	SIL1	0	3	1	7	7	8	7
nn11	12	391	1	39	SIL1	0	1	0	0	0	0	0
nn12	1	84	0	0	SIL2	0	0	0	0	0	0	0
nn13	11	33	0	0		0	0	0	0	0	0	0
nn14	0	33	0	0		0	0	0	0	0	0	0
nn15	3	546	4	7		0	0	4	0	0	0	0
nn16	3	122	3	0		0	0	3	0	0	0	0
nn17	2	42	0	0		0	0	0	0	0	0	0
nn18	196	3798	21	39		7	1	1	2	9	0	1
nn19	12	1143	0	9	SIL2	0	0	0	0	0	0	0
nn20	10	153	5	1	SIL2	3	1	1	0	0	0	0
nn21	1511	0	0	0	SIL 2	0	0	0	0	0	0	0
nn22	33	206	1	18	SIL2	0	0	0	0	0	0	1
nn23	94	628	7	13	SIL1	0	1	0	1	0	3	2
nn24	13	91	0	0	SIL2	0	0	0	0	0	0	0
nn25	1	182	3	0		0	0	1	0	2	0	0
nn26	8	654	0	8	SIL2	0	0	0	0	0	0	0
nn27	62	1222	0	13	SIL2	0	0	0	0	0	0	0
nn28	32	851	0	8	SIL2	0	0	0	0	0	0	0
nn29	20	140	0	0	SIL2	0	0	0	0	0	0	0
nn30	1	7	0	0	SIL2	0	0	0	0	0	0	0
nn31	4	26	0	0	SIL2	0	0	0	0	0	0	0
nn32	1381	8202	2	165		0	0	2	0	0	0	0
nn33	236	1396	18	13	SIL2	4	1	0	4	2	1	6
nn34	0	158	0	0	SIL2	0	0	0	0	0	0	0
nn35	30	2507	1	27	SIL1	0	1	0	0	0	0	0
nn36	18	72	0	0		0	0	0	0	0	0	0
nn37	13	300	0	4	SIL2	0	0	0	0	0	0	0
nn38	4	12	0	0		0	0	0	0	0	0	0
nn39	16	138	0	0	SIL3	0	0	0	0	0	0	0
nn40	56	491	1	5	SIL2	0	0	0	0	1	0	0
TYRIHANS (FRA OG MED 2010)												
nn1	12	72	0	0	SIL 1					0	0	0
nn2	2	5	0	0	SIL 1					0	0	0
nn3	18	98	2	2	SIL 2					0	2	0
nn4	12	92	1	2	SIL 2					1	0	0
						25	15	29	17	32	18	19

Statoil

Samlet statistikk fra 2006 til i dag

- Vi har også tilsvarende oversikt med ytterligere klassifisering i sikre/farlige og detekterte/udetekterte feil for alle SIL funksjoner

		KRISTIN										
System	Sikkerhetsfunksjon	SIL	Ant tag	Ant test	DU feil	SIL krav ant.	DD feil	SD feil	SU	Spurious	Ikke	N
	Isolering av et rom i skroget (butterfly ventiler)	2	291	291	0	2,91	0	4	2	0	1	
79	26 - Åpne trykkavlastningsventil	2	180	175	0	1,75	0	15	1	0	7	
	Åpne ESV nedstrøms høytrykksfakkel væskeutskiller (HP KO drum)	2	6	6	0	0,06	0	0	0	0	0	
	LAHH (NAS signal) i væskeutskiller (KO drum)	2	6	6	0	0,06	0	2	0	0	0	
	24 – ESD riser valve test	2	107	75	2	1,33	2	16	14	0	32	
	49 - NAS seksjonalisering ved å benytte en nødavstengningsventil	2	307	458	1	4,59	0	46	7	1	20	
	9 - Manuell initiering av nødavstengningssystemet (79ES)	2	334	319	0	3,27	0	0	0	0	3	
	Elektrisk isolering (singel gass i prosess område)	2	70	70	0	0,7	0	0	0	0	0	
	ESD logikk	2	18	27	2	0,12	3	1	0	0	2	

Sum | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | Sheet2 | Sheet1

Statoil

Aksjonsliste eksempel fra 2012

- A10 teller med inaktive (historiske) tagger som er klasset, slik at det i enkelt klasser kommer med flere tagger en det skulle ha vært.
- A10 teller feil for flere klasser i år også, som den har gjort i alle tidligere år.
- En HIPPS ventil er utkoplet i 2012 der potensiale for overtrykking ikke lengre er tilstede. Dokumentasjon må oppdateres.
- FV for livbåtradio ligger ikke mot utstyret, men mot administrativt tag. Rapporterte feil knyttes da ikke mot sikkerhetskritisk utstyr og kommer ikke i A10 rapport.
- Mange feil som er funnet og rapportert under testing er rapportert med «Detection method: ISO Periodic Maintenace» istedet for «ISO Functional Testing».
- 8 stk PSV'er på system 29 mangler klassifisering, 3 stk PSV'er på system 53 mangler klassifisering
- Klasse 37, PA: Det er gjort både 12mnd og 24 mnd FV i fjor. Dette skyldes at de ikke ligger på samme plan. FV'ene må legges inn mot samme maint plan.
- En del røykdetektorer som har gått i feil grunnet dårlig tildekking/sikring ved maling.

Aksjonsliste eksempel forts.

- Funksjon «stopp brannpumper» har ikke SIL krav, men skal i henhold til SRS følges opp på samme måte som øvrige instrumenterte sikkerhetsfunksjoner 12 stk 56LT* transmittere stopper brannpumpene ved vann i pumperom. Det er 60mnd FV, ikke dokumentert utført. Og funksjonen «stopp brannpumper på høyt nivå i pumperom» ser ikke ut til å ha eget FV program.
- 56LT* er absolutt transmittere med 2/3 votering. Korrigeres for atmosfæretrykk med referanse trykktransmitter. Feil på referanse trykk transmitter (brudd) fører til stopp av brannpumper, også i fire mode. God løsning?
- Trykk transmitter i deluge skid som gir NAS 2.1 ved bekreftet utløst deluge er ikke klasset som «utvalgt sikkerhetskritisk utstyr» (71PIT*). Bør klasses som utvalgt sikkerhetskritisk utstyr.
- Trykktransmitter som gir bekreftet vanntåke utløst og igjen stans/blokkering av nødgenerator, essential generator, hovedgeneratorer, brannpumper og eksport kompressor, ikke er klasset som «utvalgt sikkerhetskritisk utstyr» (72PIT...)

Suksesskriterier for årlig gjennomgang

- Det er viktig at det er et ledelses fokus på dette med å gjennomføre denne typen gjennomganger av feil på sikkerhetskritisk utstyr.
- Kompetanse til deltakere i gjennomgangen er viktig for å få utnyttet den tverrfaglige kunnskapen. Denne tverrfaglige prosessen gir en kvalitet som langt overgår det som fagpersonene ville ha fått til hver for seg. Mange av funnene kommer som en følge av dette.
- Kvaliteten på datagrunnlaget for gjennomgang av feil på sikkerhetskritisk utstyr er helt avgjørende for at man skal få til en effektiv gjennomgang. Essensielt at notifikasjoner har riktig tilbake melding og er utfylt korrekt.
- Kontinuitet for nøkkelpersonell i AI og vedlikeholdsstyring samt offshore hos fagarbeidere.
- Prioritere og sette av tilstrekkelig tid. Ca fire ukeverk i omfang
- Årlig gjennomgang er tatt inn i vedlikeholdsstrategien i selskapet.
- Vi har valgt å justere FV intervall på bakgrunn av disse gjennomgangene.

PETROLEUMSTILSYNET

Revisjonsrapport

Rapport	
Rapporttittel **Rapport etter tilsyn med elektriske anlegg og instrumenterte sikkerhetssystemer - Kristin**	Aktivitetsnummer 001199004

6 Andre kommentarer

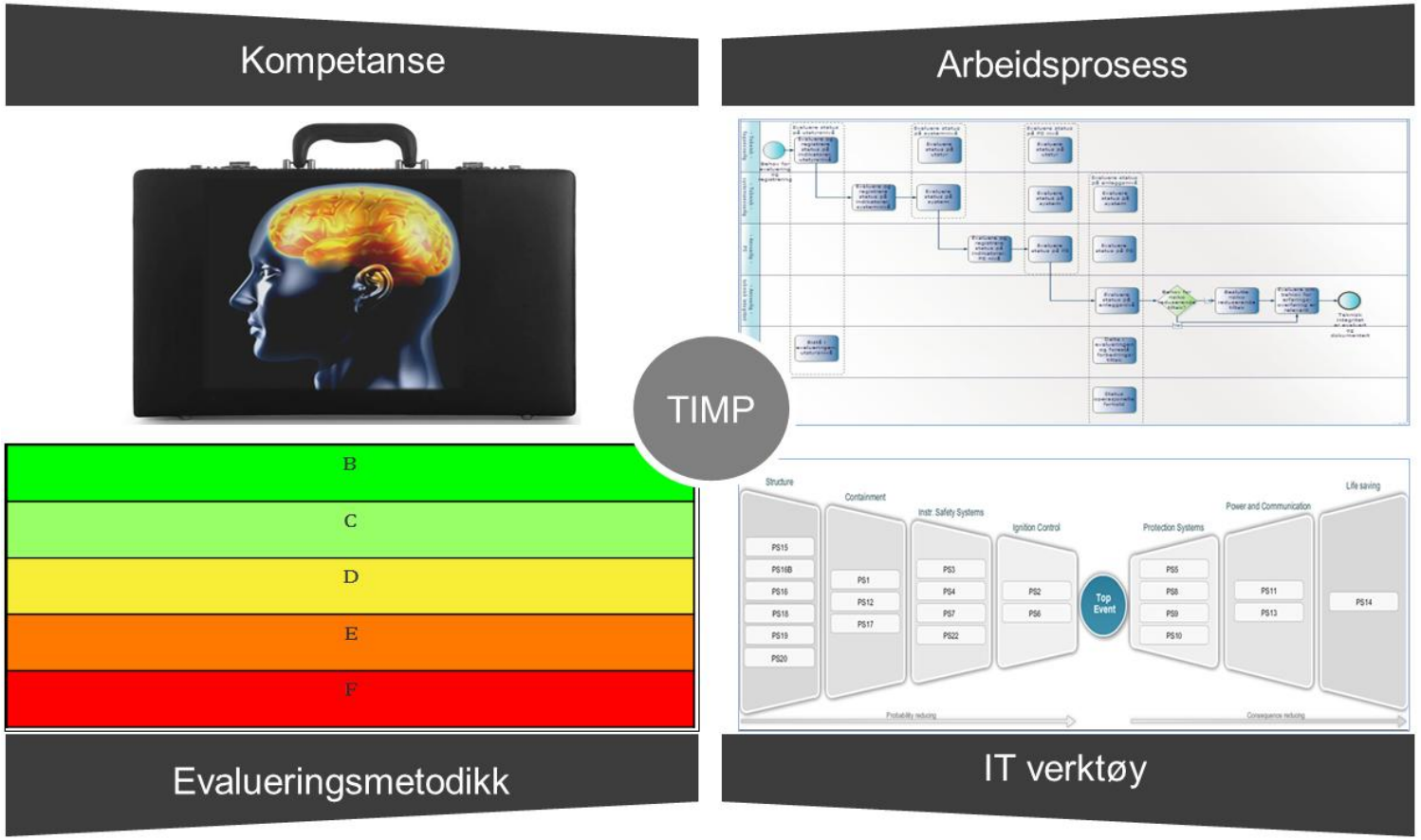
6.1 Oppfølging av SIL krav i drift

Innenfor temaet instrumenterte sikkerhetssystemer ble vi forelagt en rapport som tar for seg årlig gjennomgang og vurdering av feil for instrumenterte sikkerhetsfunksjoner. Målet med dokumentet er å verifisere at SIL kravene som er satt til instrumenterte sikkerhetsfunksjoner er oppfylt i drift. Rapporten danner videre grunnlag for eventuell justering av testintervall for instrumenterte sikkerhetsfunksjoner. Vi fikk også inntrykk av at resultatene fra kartleggingen ble fulgt opp, eksempelvis var det besluttet at brannspjeld skulle byttes grunnet flere feil enn akseptkriteriet.

Vår vurdering er at dette er en god måte å følge opp krav til instrumenterte sikkerhetssystemer i drift.

Statoil

Technical Integrity Management Program



Technical Integrity Management Programme (TIMP) er et konsept som er utviklet i Statoil, for å standardisere og forenkle arbeidet med å følge opp og styre teknisk integritet på Statoils anlegg og installasjoner.

TIMP, Technical Integrity Management Programme

- Konsept som er utviklet i Statoil, for å standardisere og forenkle arbeidet med å følge opp og styre teknisk integritet på Statoils anlegg og installasjoner.
  - Gir oppsummering av status på barrierer på 2 månedlig status ut fra et sett av indikatorer.
  - Dokumenteres i etablert verktøy
  - Brukes for synliggjøring, prioritering & beslutning, risikostyring
- Vi mener at årlig gjennomgang utfyller dette på en svært god måte:
  - Bedre samhandling og tverrfaglighet
  - Ser flere fag/systemer/indikatorer i sammenheng
  - Ser trender over lengre tid, i mange tilfeller flere år
  - Setter av tilstrekkelig tid (TIMP prioriteres ofte etter daglig brannslukking av drifts utfordringer)
  - Mulighet til å gå grundigere inn på spesielle problemområder og utfordringer
  - Vi erfarer at vi gjør veldig mange funn til tross for mer enn 3 år med TIMP!

Hva kan vi bli bedre på ?

Erfaringer fra Kristin / Tyrihans

- Suksessformel for lokalt arbeid med SIL er å bruke i størst mulig grad de etablerte systemene og rollene (SAP, Timp.) og inkludere nødvendige aktiviteter der en allikevel samles/møtes.
- Bevisstgjøring om at det finnes krav til system gir endringskontroll !
- Kvalitet på arbeid/prosedyrer knyttet til endringer har betalt seg ift høy regularitet. (Best i UPN i 2012, ikke i 2013 ☹)
- Kristin har hatt få uplanlagte stans og tripper pga SIL/SIS, men hatt utfordringer med ikke instrumenterte systemer / utstyr (stigerør, livbåter, eksoskanaler, uheldig rørdesign med materialvalg osv)
- Kontinuitet i oppgaver knyttet til oppfølging og kunnskap til anlegg har vært en nøkkelsak for å få kvalitet i driftsoppfølgninga.

Forbedringer – lokalt

- Fortsette å være «tett på» de etablerte arbeidsprosesser med å kjøre de lokale aktivitetene etter egen styringssløyfe med lokale styrende dokumenter.
- Fortsette endringskontroll på SIS og årlige gjennomganger.
- Lande kompetansekrav iht PTIL forventninger, ref tilsyn 2012. (neste slide)
- Selge inn lokalt arbeid til «Plant Integrity – forbedet vedlikeholdsstyring» slik at det vi gjør bra blir beste praksis
- Sluttføre oppdatering av lokal styrende dokumentasjon
- Utvide de lokale dokumentene med krav til kompetanse / kursing ift definerte SIL oppgaver
- Kjøre SIL kurs med eksern støtte for å bedre kompetanse og flerfagligheten.
- Tett oppfølging i tidlig fase på studier / prosjekter
- Hjelpe sentrale aktører med nødvendige endringer basert på Kristin opplegget.

Revisjonsrapport

Rapport	
Rapporttittel **Tilsyn med drift av alarmsystemer – Kristin**	Aktivitetsnummer 001199005

5.1.3 Manglende krav til kompetanse knyttet til arbeid med instrumenterte sikkerhetssystemer

Avvik:

Det er ikke dokumentert krav til spesiell kompetanse knyttet til arbeid med de instrumenterte sikkerhetssystemene.

Begrunnelse:

Vi fikk forelagt kompetansekrav for personell som arbeider med de instrumenterte sikkerhets-systemene. På Kristin er disse systemene bygget for å være i samsvar med IEC 61511 og drift av disse krever spesialkompetanse. Vi finner ikke i gjennomgangen av kompetansekravene at det er noen referanse knyttet til de kompetansekravene som gjelder for disse systemene.

Krav:
Aktivitetsforskriften § 21 – om kompetanse og § 47 – om vedlikeholdsprogram
Innretningsforskriften §§ 32 - 34. – om brann- og gassdeteksjonssystemet, nødavstengningssystem og prosessikringssystem

Forbedringsområder – sentralt basert på Kristin erfaringer

- Etablere tydeligere kravdokumenter sentralt og synliggjøre Statoil's oppgaver i LCM / LCI setting
- Definere hva vi må ha hjelp til og hva vi må gjøre sjøl!
- Standardisering av løsninger og allokeringsmåter – vi trenger ikke 10 måter å lande et SIL nivå på …
- Forbedre fagoppfølging med involverte nøkkelfag og leverandører
- Forbedre sporbarhet av opprinnelig SIL klassifisering og PFD beregninger
- Underlag for krav til testintervall fra design(krav til endring/populasjon av tester)
- Synliggjøring og bevisstgjøring av farlige feil oppstått i drift
- Oppdaterte krav til SIL kompetanse for personell involvert på alle felt med eksisterende og nye SIL funksjoner.
- Fagfolk i havet har individuelle kompetanse krav/mål. Hvordan sikre tilstrekkelig kompetanse?

Forbedringsområder – Statoil forts.

- Eget verktøy for oppfølging av SIL funksjoner i konsernet?
- Definere alt SIL utstyr som utvalgt sikkerhetskritisk utstyr
- Vurdering av demand rater til funksjonene (IMS gir mulighet for dette)
- Deling av utstyrsinformasjon / historikk til leverandører
- Synliggjøring av SIS med Statoil sin Modifikasjonsprosessen mangler. En oppgavestyrt organisasjon er utfordrende da sluttkunden blir borte underveis!
- Oppfølging av SIL i modifikasjoner. Må beskrives bedre i styrende dokumentasjon og følges opp i detalj prosjekter.
- Oppfølging av SIL arbeid hos V&M kontraktør - trenger mye oppfølging.

SIL og levetid

- Hvor lenge er SIL funksjon intakt og tilfredsstiller krav?
  - Erfaring på Kristin – en god del utstyr (også SIL sertifisert) er utgått fra leverandør nå etter 8 år i drift, og kan ikke engang repareres. Hva da med SIL-nivå? Eksempel:
    - LST
    - SAS power komponenter
    - Barrierer/isolatorer --->

The module has been analyzed in detail in our service lab in Germany. The reason for the malfunction of this device is an electrolytic capacitor that failed. The capacitor dried out and lost its function. The dry out process of such capacitors depends on overall lifetime and on the ambient temperature. A high temperature – even for a short time – leads to a reduced lifetime. In this case the devices achieved a life time of 8+ years according to our records. In general our products are designed to achieve a lifetime of 10 years minimum.

We would like to apologize for the inconvenience the failing have caused. We admit that it is very likely that all isolators of this type which are installed and used under the same conditions at your premises are effected in the way described above. Hence we recommend to exchange all isolators of this type installed at the time 8 years ago (revision A and B) in order to ensure a high availability of your manufacturing.

- Er pålitelighet uavhengig av klimatiske forhold, værhus/beskyttelse, innendørs/utendørs? Har en transmitter eller ventil som har stått 10 år ubeskyttet utendørs samme pålitelighet som en som har stått tørt og varmt inne i et utstyrsrom?
- SIL krav på temperatur i utstyrsrom? Høy temperatur forkorter levetid drastisk, er 40+ grader inne i skap OK?
- Høy temperatur i inne i utstyrspakker, når bør utstyr byttes?

Har vi rett fokus?

- Erfaring med feil på instrumenterte sikkerhetsfunksjoner viser at vi har mange feil som ikke dekkes av «SIL-beregning» Er det rett å bruke store ressurser på design av SIL funksjoner med PFD beregninger på promillenivå når en har utfordringer som:
  - Feil på solenoid ventil grunnet uren olje. SIL krav på hydaulikk olje/flushing etc?
  - Feil kalibrering av transmitter (operatørfeil eller feil på datablad))
  - Feil på C&E logikk (kan være både design feil, sw feil og andre årsaker)
  - Feil dimensjonering av aktuator
  - Transmitter frys eller feil pga scale/avleiringer
  - Feil montering (eks blokkventiler ifm radar målere, feil i jordingskopling)
  - Jordfeil kan forhindre aksjon (ikke nok strøm). Pålitelighet av jordfeildeteksjon/isolasjonovervåking?
  - Krav til power på 230V instrumentering (singel forsyning på Kristin)
  - Det er valgt måler/måleprinsipp som fungerer dårlig på mediet?
  - Krav om forskjellig måleprinsipp på kontroll og trip instrumentering: Når man har et godt og fungerende måleprinsipp på regulering, hvor da velge noe annet på Trip?
  - Nye instrumenter har mange titalls justerbare parametre (eks radar, gamma). Feil på en av parametrene vil kunne medføre store målefeil selv om måler har promille nøyaktighet og er SIL sertifisert.
  - Får leverandør tilbakemelding på oppståtte feil (proven in use) eller er PFD kun satt ut fra teoretiske beregninger?

There's never been a better time for good ideas

Presentation title:

Espen Sørensen / Bjørnar Berg
ESPENS / BBERG AT STATOIL.COM

www.statoil.com

Statoil