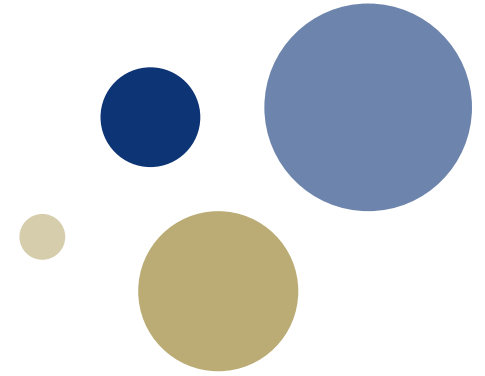




Metodikk og erfaringer – oppfølging av SIL i drift

- Introduksjon v/ Mary Ann Lundteigen (NTNU)
- Erfaringer og praktisk gjennomføring v/ Solfrid Håbrekke (SINTEF)

Agenda (1 del - introduksjon)

- Innledende refleksjoner
- Krav
- Metodikk
- Oppsummerende refleksjoner

Mary Ann Lundteigen

Professor i Pålitelighetsvurdering, NTNU

Mary.a.lundteigen@ntnu.no

www.ntnu.edu/ross/rams

Kontaktinformasjon

Innledende refleksjoner



- Instrumenterte sikkerhetssystemer (SIS) er i **økende grad** benyttet som sikkerhetsbarrierer i olje og gassvirksomheten
- Instrumenterte sikkerhetssystemer kjennetegnes av følgende egenskaper:
 - Aktive (aktiveres på kommando/demand)
 - Komplekse (interaksjon hardvare og programvare)
 - Ytelsen er **til dels** bestemt av design **og til dels** av ytelsespåvirkende faktorer i drift:
 - Teknisk løsning (redundansnivå, type utstyr, programvare)
 - Miljø og driftsforhold
 - Drifts- og vedlikeholdsaktiviteter
 - Testintervall

Innledende refleksjoner (II)



Sentrale spørsmål:

- Hvordan påvirkes ytelsen i driftsfasen?
- Er den (fortsatt) tilstrekkelig?
- Hvordan avdekker vi om ytelsen er svekket?

Innledende refleksjoner (III)



- **Barrierestyring:**

Koordinering av aktiviteter for å etablere og opprettholde barrierer slik at de til en hver tid opprettholder sin funksjon [Ptil Prinsipper for barrierestyring, 2013]

- **Oppfølging av SIS i drift:**

Praktisk gjennomføring av barrierestyring (drift, vedlikehold, feilrapportering, SIL-oppfølging ++) for SIS og i henhold til krav i IEC 61508, IEC 61511 og GL 070.

- **SIL oppfølging i drift:**

Analyse av rapporterte hendelser for utstyr som inngår i SIS i forhold til SIL krav og *identifisering* av kompenserende tiltak

(**Driftsgjennomgang** benyttes av og til som begrep dersom man analyserer rapporterte hendelser for sikkerhetskritisk utstyr generelt)

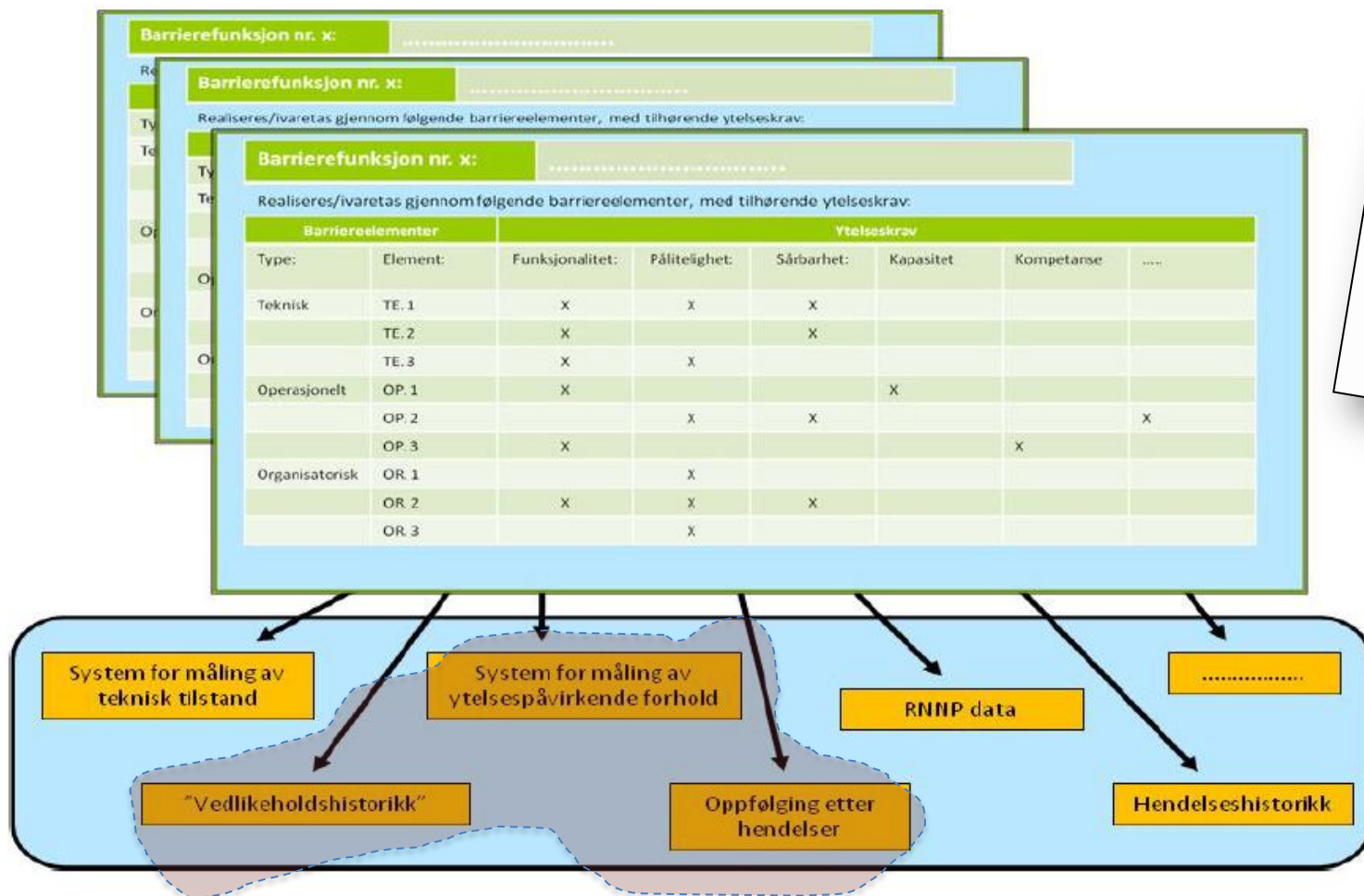
Overordnede krav (og forventninger)

Styringsforskriften § 5 (utvalg)

- Krav til ytelse skal være **satt og gjort kjent**
- **Status** på barrierer skal være kjent til enhver tid
- Det skal være kjent hvilke barrierer som er **ute av funksjon eller er svekket**. Den ansvarlige skal sette i verk **nødvendige tiltak** for å rette opp eller kompensere for manglende eller svekkede barrierer.
- **Data** skal samles inn, bearbeides og brukes til overvåkning, analyser, identifisere forbedringer, OSV



Krav og forventninger: Overordnet



Figur 16 Verifikasjon av ytelse til barrierefunksjoner og tilhørende barriereelementer



Detaljerte krav (SIS)

- Petroleumstilsynets regelverk refererer til standarder som IEC 61508 og Norsk Olje og Gass (NOG) retningslinje 070 for **design, bygging og drift/vedlikehold** av SIS.

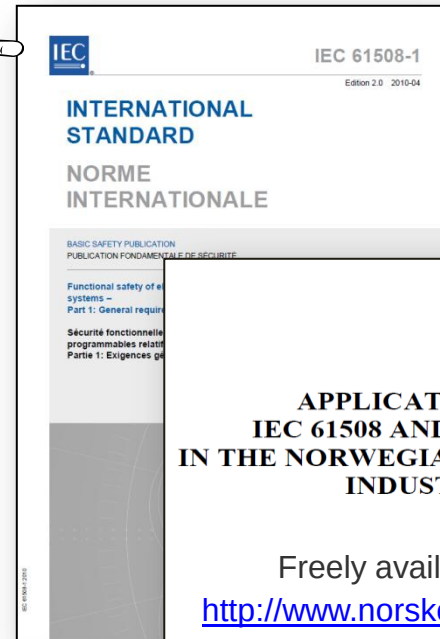
Styringsforskriften §5

Innretningsforskriften § 8

Aktivitetsforskriften § 26 & 47



IEC 61508
GL 070



**APPLICATION OF
IEC 61508 AND IEC 61511
IN THE NORWEGIAN PETROLEUM
INDUSTRY**

Freely available from

<http://www.norskoljeoggass.no/>

Implementering av krav (SIS)



Regelverkskrav (SF, §5)

- Krav til ytelse skal være satt og gjort kjent
- Status på barrierer skal være kjent til enhver tid

- Det skal være kjent hvilke barrierer som er ute av funksjon eller er svekket. Den ansvarlige skal sette i verk nødvendige tiltak for å rette opp eller kompensere for manglende eller svekkede barrierer.

- Data skal samles inn, bearbeides og brukes til overvåkning, analyser, identifisere forbedringer, osv.

Anvendt på SIS

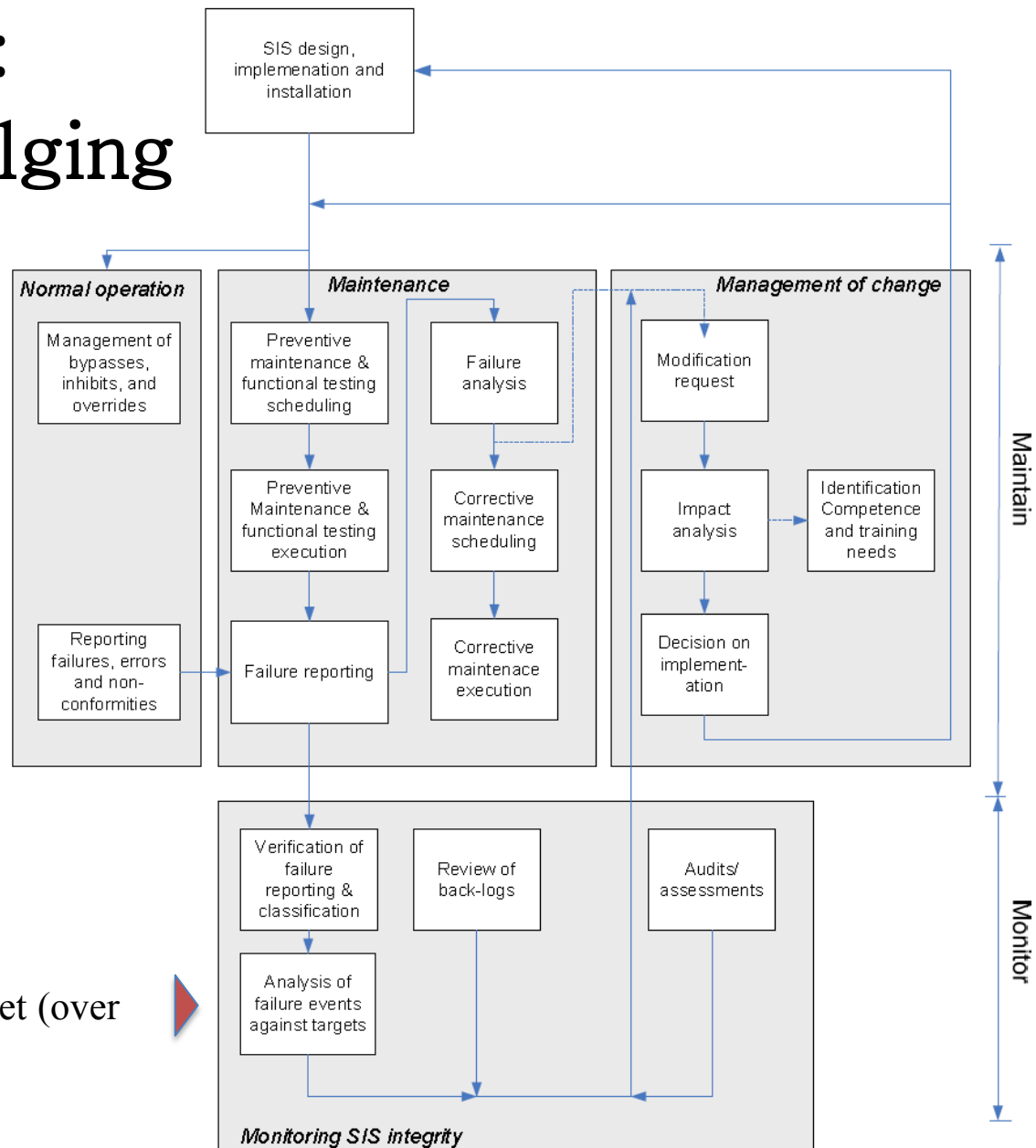
Utlede funksjonelle krav og SIL krav

SIS oppfølging, inkludert SIL oppfølging

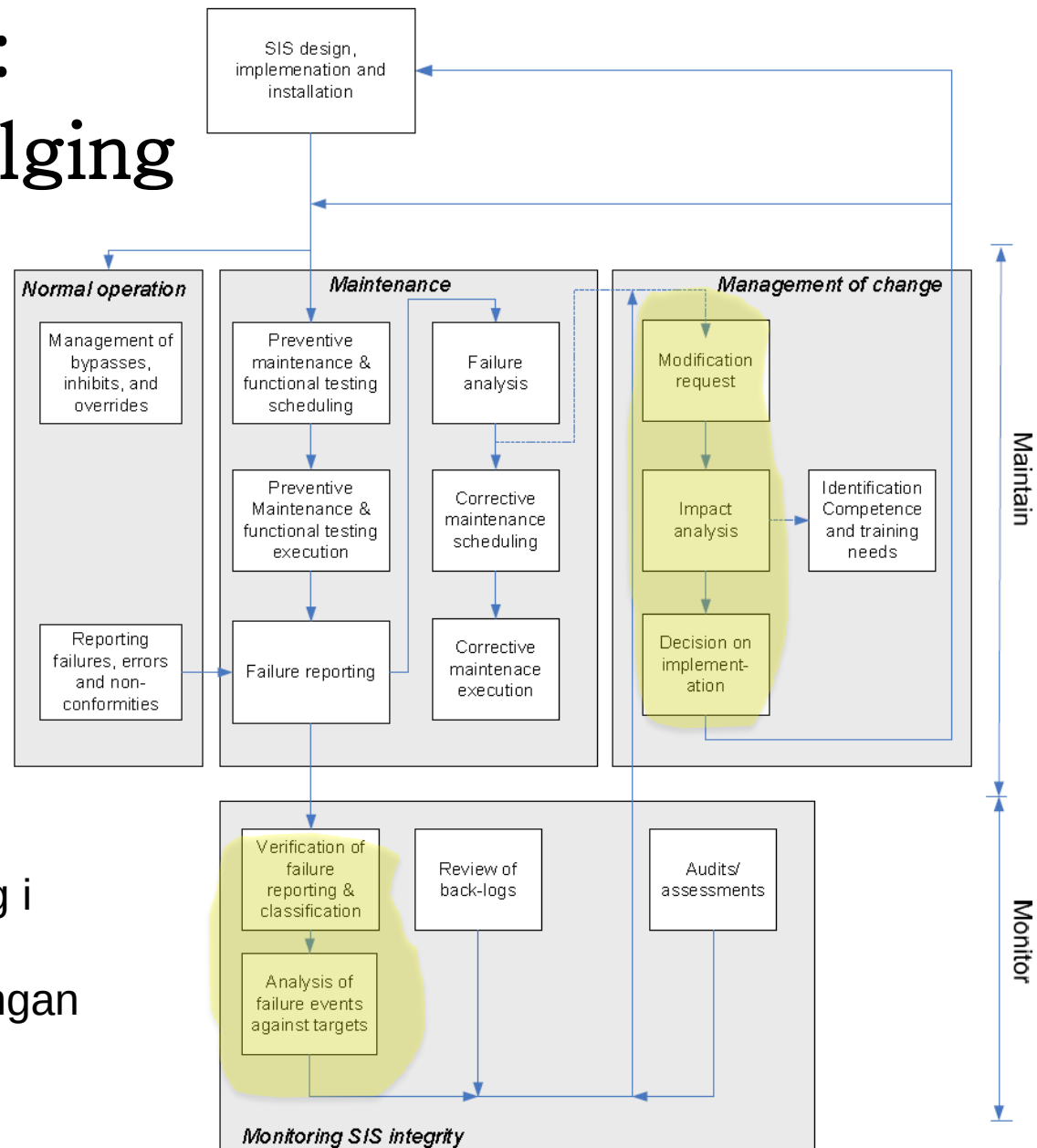
Metodikk: SIS oppfølging

Overvåkning
av *dag-til-dag*
barrierestatus

Overvåkning av
barrierenes integritet (over
tid)



Metodikk: SIS oppfølging



SIL oppfølging i driftsfasen (driftsgjennomgang)

Metodikk (SIS oppfølging)

Generelle krav:

- IEC 61508/IEC 61511

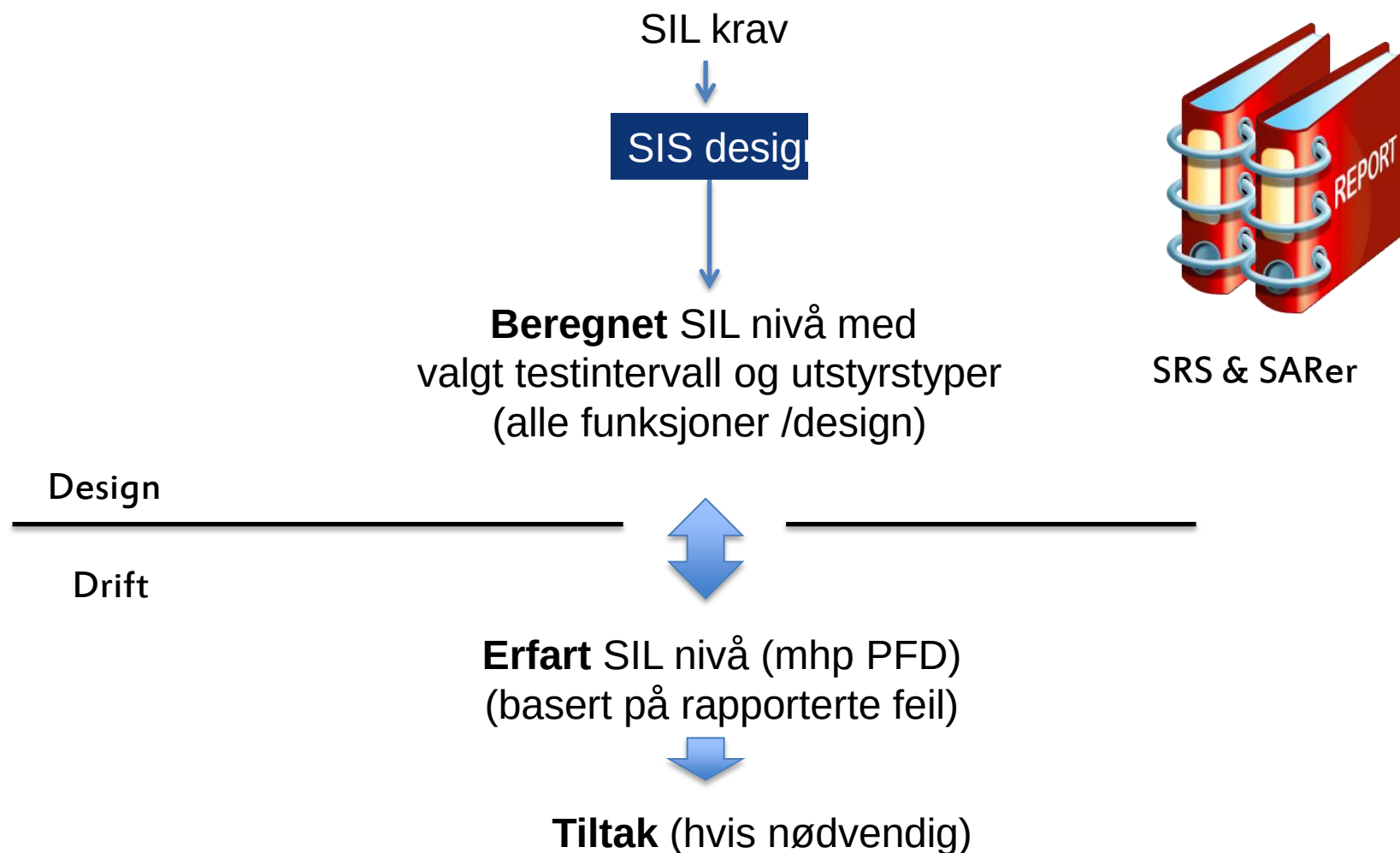
Veiledninger:

- GL 070 kapittel 10 & 11, pluss appendiks F
- *Guidelines to the follow-up of Safety Instrumented Systems (SIS) in the operating phase (SINTEF/PDS)*
- Selskapsspesifikke retningslinjer

10	SIS OPERATION AND MAINTENANCE.....	44
10.1	OBJECTIVE.....	44
10.2	OPERATION AND MAINTENANCE PLANNING.....	44
10.3	OPERATIONS AND MAINTENANCE PROCEDURES.....	44
10.4	COMPETENCE AND TRAINING.....	45
10.5	MAINTENANCE.....	45
10.5.1	Functional testing.....	45
10.5.2	Maintenance reporting.....	46
10.6	COMPENSATING MEASURES UPON OVERRIDES AND FAILURES.....	47
10.6.1	Compensating measures procedures.....	47
10.6.2	Dangerous Detected Failure.....	47
10.6.3	Override/Inhibit/Disable.....	47
10.7	REPORTING OF NON-CONFORMITIES AND DEMANDS.....	48
10.8	CONTINUOUS IMPROVEMENT OF OPERATION AND MAINTENANCE PROCEDURES.....	48
11	SIS MODIFICATION.....	49
11.1	OBJECTIVE OF MANAGEMENT OF CHANGE (MOC).....	49
11.2	MOC PROCEDURE.....	49
11.3	MOC DOCUMENTATION.....	51
APPENDIX F SIL FOLLOW UP..... 135		
F.1	OVERVIEW OF OPERATION AND MAINTENANCE ACTIVITIES FOR SIL WORK.....	137
F.2	PROCEDURES FOR UPDATE OF TEST INTERVALS.....	141
F.3	ACTUAL SHUTDOWNS AS TEST.....	144

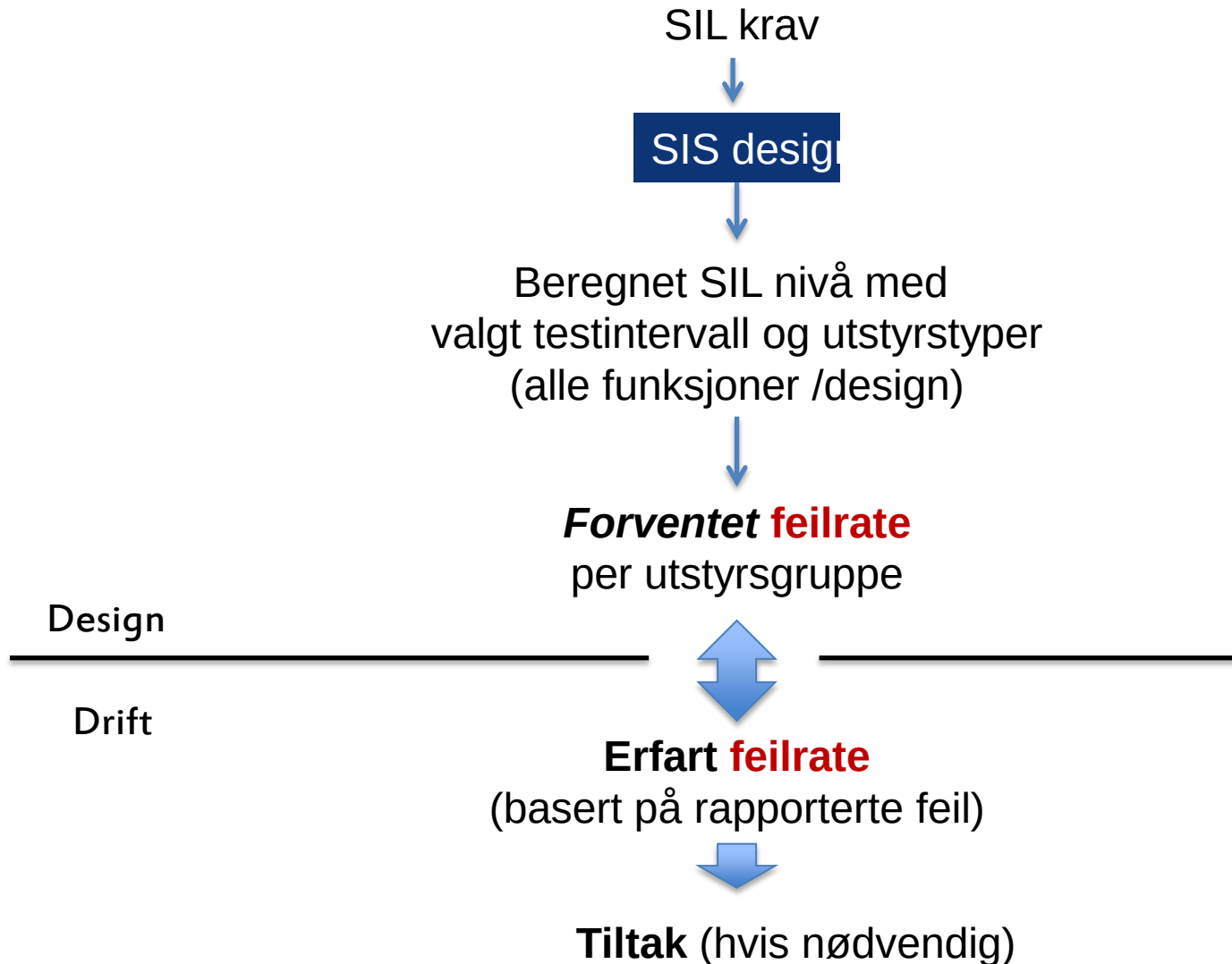
 SINTEF SINTEF Technology and Society Safety and Reliability Address: NO-7465 Trondheim, NORWAY Location: S P Andersens veg 5 NO-7031 Trondheim Telephone: +47 73 59 27 56 Fax: +47 73 59 28 96 Enterprise No.: NO 948 007 029 MVA		SINTEF REPORT	
		TITLE Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase	
AUTHOR(S) Stein Hauge, Mary Ann Lundteigen		CLIENT(S) PDS - multiclient	
REPORT NO. SINTEF A8788	CLASSIFICATION Unrestricted	CLIENTS REF. Håkon S. Mathisen, Kongsberg Maritime	
CLASS. THIS PAGE 978-82-14-04601-4	ISBN 978-82-14-04601-4	PROJECT NO. 504091.12	NO. OF PAGES/APPENDICES 38
ELECTRONIC FILE CODE PDS Report-SIS_follow_up_guideline_final_v01		PROJECT MANAGER (NAME, SIGN.) Stein Hauge	CHECKED BY (NAME, SIGN.) Tor Onshus

SIL oppfølging (generelt)

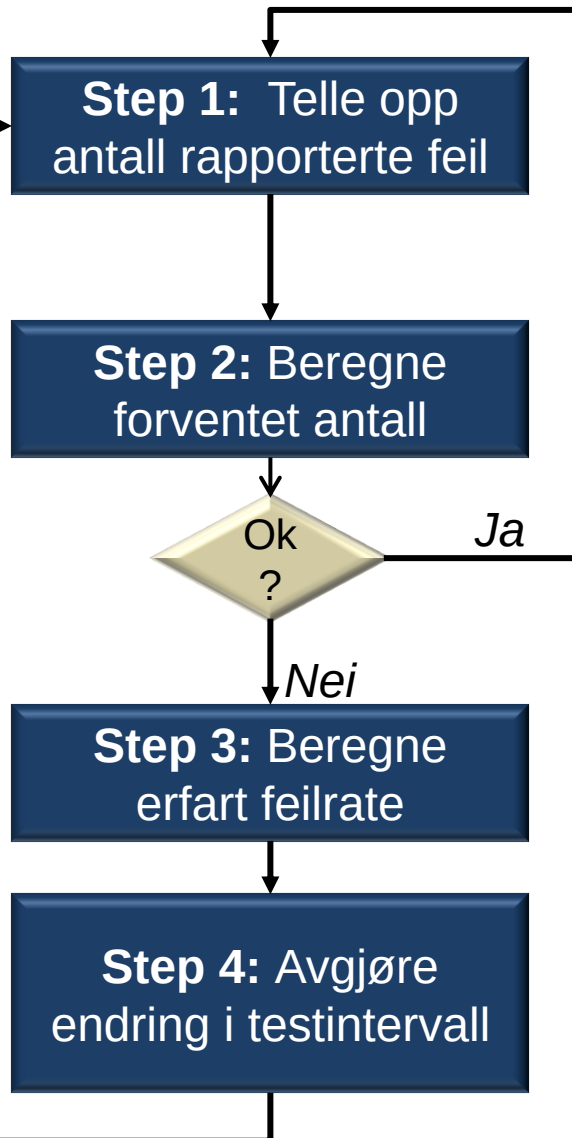


SRS: Safety requirements specification
SAR: Safety analysis report (GL 070)

SIL oppfølging (SINTEF/PDS)



Metodikk (SINTEF /PDS)



- x_1
- Med fokus på farlige udetekterte (DU)
 - Avdekket både under test og i drift
 - Innkjøringsfeil utelatt

$$x_0 = \lambda_{des} \cdot n \cdot t$$

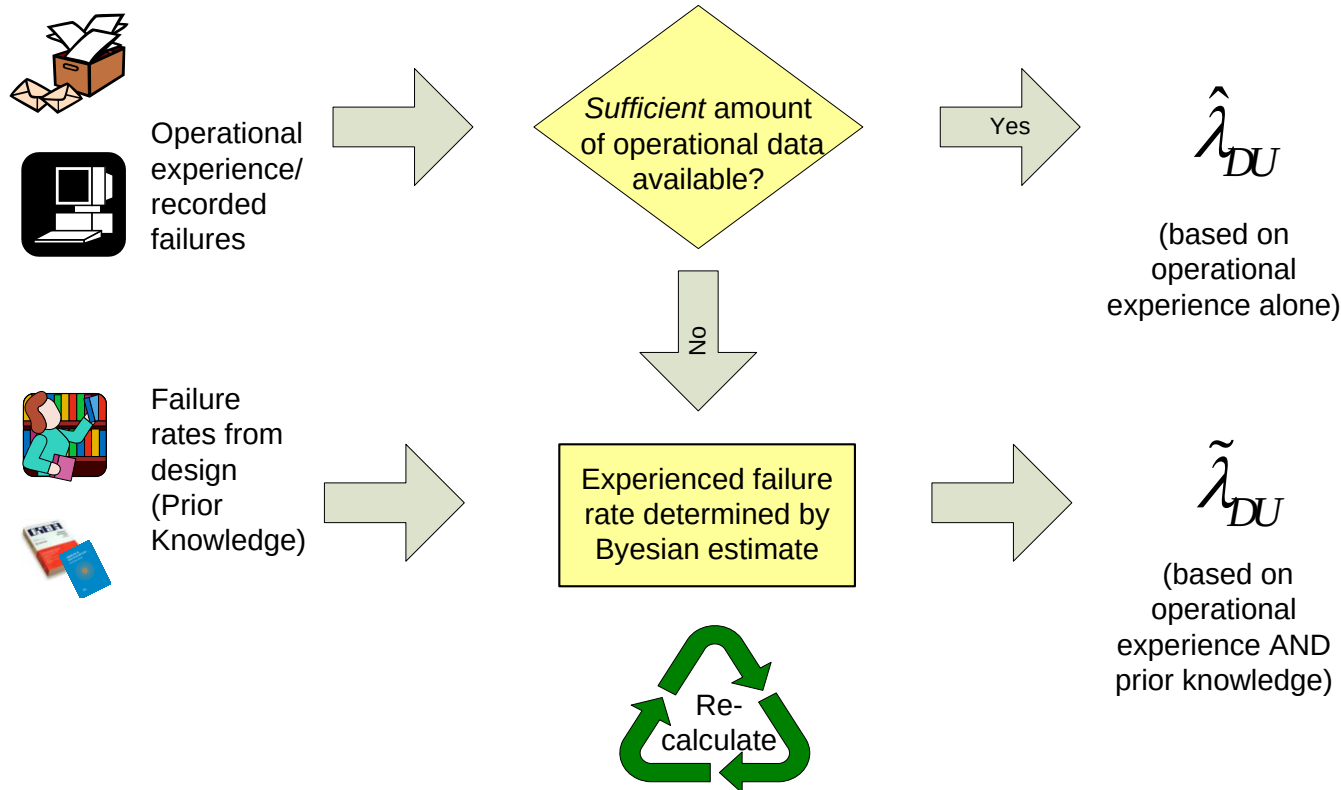
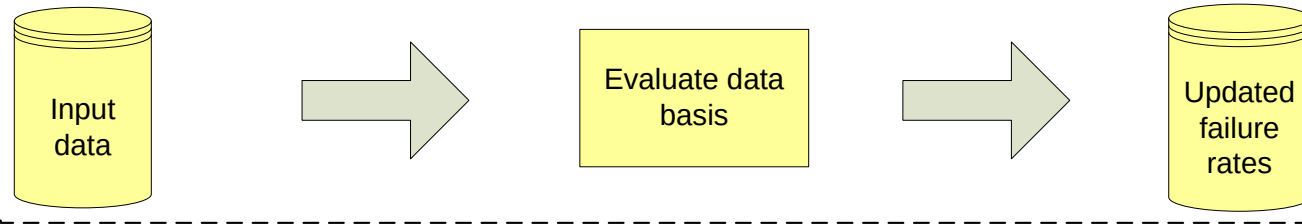
$$x_0 \Leftrightarrow x_1 ?$$

$$\hat{\lambda}_{op} = \frac{x_1}{n \cdot t}$$

(alternativ formel hvis <2 feil
eller liten (total) driftstid)

$$\tau_{op} \cdot \hat{\lambda}_{op} \leq \lambda_{des} \cdot \tau_{des} \quad + \text{ sjekkliste}$$

Metodikk for SIL oppfølging (SINTEF/PDS)



Endring av testintervall



Kvantitativ analyse:

- Endres slik at forholdet mellom feilrate og testintervall beholdes konstant
- Ved dobling/halvering er det egne tilleggskrav

Kvalitativ analyse:

- Praktiske konsekvenser for endring av testintervall?
- Leverandøranbefalinger
- Kvaliteten i feildataene; (komplett, rett kvalifisert?)
- Relevans i forhold til utstyret; (utstyr blitt skiftet ut? Ny type)
- Kvalitet/coverage på funksjonstesting;
- Skyldes feilene samme årsak/fellesfeil?
- Sekundæreffekter av hypigere/skjeldnere testing?

Eksempel



Situasjon:

- 600 røykdetektorer med antatt feilrate fra design:
 $\lambda_{DU} = 0.8 \cdot 10^{-6} / \text{time}$
- I løpet av *ett år* forventes følgende antall feil:
 $0.8 \cdot 10^{-6} \cdot 8760 \cdot 600 \approx 4 \text{ feil}$
- Erfarer 3 feil på 2 år. Gir en *erfart feilrate*:
 $\lambda_{DU} = 3 / (600 \cdot 8760 \cdot 2) \approx 0.3 \cdot 10^{-6} / \text{time}$

(Foreløpig) konklusjon:

- Færre svikt (og lavere DU feilrate) enn forventet.
- Brukes videre for vurdering av lengde på testintervall (kvantitativ + kvalitativ sjekk)

Avsluttende refleksjoner



- **Oppdatering av PFD/feilrater i drift...**
 - *Er*: Et mål for gjennomsnittlig integritet i en periode som har passert
 - *Er ikke*: Et øyeblikksbilde av integriteten
- **Dag-til-dag kontroll/overvåkning av status på barrierer må ikke «glemmes»:**
 - En alarm kan varsle om en degradert eller ikke-tilgjengelig barriere
 - En barriere kan svekkes pga feil under vedlikehold
 - En forsinket test kan bidra til at feil forblir uoppdaget
 - En modifisering kan introdusere en svekkelse

Del 2...

