

SINTEF A26001 - Åpen

# Rapport

## Vedlikeholdets plass i barrierestyringen

### Forfattere

Knut Øien og Stein Hauge





# Rapport

## Vedlikeholdets plass i barrierestyringen

EMNEORD:  
Vedlikehold  
Vedlikeholdsstyring  
Barrierestyring

**VERSJON**

1.0

**DATO**

2014-03-12

**FORFATTERE**

Knut Øien og Stein Hauge

**OPPDRAGSGIVER**

Petroleumstilsynet

**OPPDRAGSGIVERS REF.**

Hans Kjell Anvik

**PROSJEKTNR**

102005812

**ANTALL SIDER OG VEDLEGG:**

77

**SAMMENDRAG**

Vedlikeholdets plass i barrierestyringen kan oppfattes både enkelt og vanskelig. Enkelt sagt skal vedlikeholdet bidra til å opprettholde og gjenopprette de tekniske barrierenes funksjon, samt verifisere ytelsen til barrierene. Når det er sagt er det ikke like rett frem hvordan dette skal gjøres i praksis. Heller ikke barrierestyringen i seg selv er rett frem.

I denne rapporten diskuterer vi vedlikeholdets plass i barrierestyringen både på prinsipielt grunnlag, trinn for trinn i barrierestyringsprosessen, gjennom konkrete eksempler, samt i forhold til utvalgte sentrale tema.

Vi håper denne rapporten gir et nyttig bidrag til bevisstgjøring rundt barrierestyring og vedlikeholdets plass i barrierestyringen, samtidig som vi er klar over at det kan være andre måter å betrakte dette på.

**UTARBEIDET AV**

Knut Øien

**SIGNATUR****KONTROLLERT AV**

Per Schjøberg

**SIGNATUR****GODKJENT AV**

Stian Antonsen, Forskningssjef

**SIGNATUR****RAPPORTNR**

SINTEF A26001

**ISBN**

978-82-14-05676-1

**GRADERING**

Åpen

**GRADERING DENNE SIDE**

Åpen

## Historikk

---

| <b>VERSJON</b> | <b>DATO</b> | <b>VERSJONSBEKRIVELSE</b>               |
|----------------|-------------|-----------------------------------------|
| Utkast 1       | 10-12-2013  | Første utkast                           |
| Utkast 2       | 04-02-2014  | Andre utkast etter kommentarer fra Ptil |
| 1.0            | 12-03-2014  | Endelig                                 |

# Innholdsfortegnelse

|                                                                                           |           |
|-------------------------------------------------------------------------------------------|-----------|
| <b>SAMMENDRAG .....</b>                                                                   | <b>5</b>  |
| <b>1 Innledning .....</b>                                                                 | <b>7</b>  |
| 1.1 Bakgrunn og begrunnelse .....                                                         | 7         |
| 1.2 Hensikt .....                                                                         | 8         |
| 1.3 Beskrivelse av oppgaven .....                                                         | 9         |
| 1.4 Definisjoner og begreper .....                                                        | 9         |
| 1.5 Forkortelser .....                                                                    | 12        |
| 1.6 Rapportstruktur .....                                                                 | 13        |
| <b>2 Vedlikeholdets plass i barrierestyningen – prinsipielle sammenhenger .....</b>       | <b>15</b> |
| 2.1 Overordnet betraktning .....                                                          | 15        |
| 2.2 Prinsipper og rammeverk .....                                                         | 15        |
| 2.3 Barrierestytingsprosessen .....                                                       | 16        |
| 2.4 Oppfølging i driftsfasen .....                                                        | 18        |
| 2.5 Måling og verifikasjon av barriereytelse .....                                        | 19        |
| 2.6 Kopling til vedlikeholdsstyringssløyfa .....                                          | 20        |
| 2.7 Barriere- og vedlikeholdsstyring: Prinsipper, rammeverk og prosess .....              | 22        |
| <b>3 Vedlikeholdets rolle i barrierestytingsprosessen – trinn for trinn .....</b>         | <b>25</b> |
| 3.1 Kontekst .....                                                                        | 26        |
| 3.1.1 Krav og føringer i regelverk, standarder og selskapsspesifikke retningslinjer ..... | 27        |
| 3.1.2 Definere ansvarsforhold og nødvendige interaksjoner/grenseflater .....              | 34        |
| 3.1.3 Definere metodikk .....                                                             | 34        |
| 3.1.4 Faktisk utforming og tilstand (og implikasjoner for vedlikeholdsvennlighet) .....   | 34        |
| 3.1.5 Viktige drivere og trender .....                                                    | 35        |
| 3.1.6 Oppfatninger og verdisyn hos eksterne interessenter .....                           | 35        |
| 3.1.7 Ressurser, kunnskap og kontraktsmessige forbindelser .....                          | 35        |
| 3.1.8 Krav til risikoreduksjon / kontinuerlig forbedring .....                            | 35        |
| 3.2 Risikovurderinger .....                                                               | 36        |
| 3.2.1 Identifisere fare- og ulykkessituasjoner .....                                      | 36        |
| 3.2.2 Etablere barrierefunksjoner .....                                                   | 37        |
| 3.2.3 Gjennomføre risikoanalyser og sikkerhetsstudier .....                               | 37        |
| 3.2.4 Vurdering og evaluering av risikobildet .....                                       | 38        |
| 3.3 Risikohåndtering .....                                                                | 38        |
| 3.3.1 Behov/mulighet for mer effektive barrierer .....                                    | 38        |
| 3.3.2 Etablere spesifikk barrierestrategi og spesifikke ytelseskrav .....                 | 39        |

|          |                                                                                                 |           |
|----------|-------------------------------------------------------------------------------------------------|-----------|
| 3.4      | Kommunikasjon og konsultasjon .....                                                             | 39        |
| 3.5      | Overvåking og gjennomgåelse .....                                                               | 40        |
| <b>4</b> | <b>Konkrete eksempler på vedlikeholdets betydning for god barrierestyring .....</b>             | <b>41</b> |
| 4.1      | Bakteppe .....                                                                                  | 41        |
| 4.2      | Vedlikeholdets rolle .....                                                                      | 42        |
| 4.3      | Føringer og antakelser fra design .....                                                         | 42        |
| 4.4      | Oppfølging i driftsfasen.....                                                                   | 43        |
| 4.4.1    | Fremgangsmåte og omfang .....                                                                   | 43        |
| 4.4.2    | Feilklassifisering .....                                                                        | 45        |
| 4.4.3    | Feil oppdaget ved test versus feil oppdaget i normal drift .....                                | 45        |
| 4.4.4    | Nytteverdi av driftsgjennomganger.....                                                          | 46        |
| 4.5      | Resultater og observasjoner fra driftsgjennomgangene .....                                      | 46        |
| 4.5.1    | Resultater fra gjennomgang av ventiler (ESV og BDV) .....                                       | 46        |
| 4.5.2    | Observasjoner og funn fra driftsgjennomganger .....                                             | 48        |
| 4.6      | Konklusjoner vedrørende vedlikeholdets betydning .....                                          | 48        |
| 4.7      | Oppsummeringsfigur .....                                                                        | 49        |
| <b>5</b> | <b>Diskusjon av utvalgte tema .....</b>                                                         | <b>51</b> |
| 5.1      | Viktigheten av strukturert tilnærming og kontinuerlig forbedring .....                          | 51        |
| 5.2      | Viktigheten av tverrfaglig involvering .....                                                    | 52        |
| 5.3      | Behandling av eventuelle avvik knyttet til vedlikehold av barrierer (enkeltvis og samlet) ..... | 54        |
| <b>6</b> | <b>Oppsummering.....</b>                                                                        | <b>57</b> |
|          | <b>Referanser .....</b>                                                                         | <b>59</b> |
|          | <b>Vedlegg A: Begreper og fortolkninger .....</b>                                               | <b>61</b> |
| A.1      | Generelt om definisjoner .....                                                                  | 61        |
| A.2      | Operasjonalisering av begreper .....                                                            | 61        |
| A.3      | Barrierestyring og vedlikehold .....                                                            | 62        |
| A.4      | Vedlikeholdsstyring.....                                                                        | 62        |
| A.5      | Barrierefunksjon .....                                                                          | 63        |
| A.6      | Barrieredefinisjonen .....                                                                      | 63        |
| A.7      | Sammenhenger .....                                                                              | 64        |
|          | <b>Vedlegg B: ISO 31000 .....</b>                                                               | <b>67</b> |
|          | <b>Vedlegg C: Barrierenotatets behandling av vedlikehold/vedlikeholdsstyring.....</b>           | <b>73</b> |

## SAMMENDRAG

### Innledning

Vedlikeholdets plass i barrierestyringen kan oppfattes både enkelt og vanskelig. Enkelt sagt skal vedlikeholdet bidra til å opprettholde og gjenopprette de tekniske barrierenes funksjon, samt verifisere ytelsen til barrierene. Når det er sagt er det ikke like rett frem hvordan dette skal gjøres i praksis. Heller ikke barrierestyringen i seg selv er rett frem.

### Begrunnelse

Noen av begrunnelsene for en nærmere drøfting av vedlikeholdets plass i barrierestyringen er:

- Petroleumstilsynets arbeid med barrierestyring viser at det er behov for mer kunnskap i næringen om hvordan vedlikeholdsstyring og barrierestyring er knyttet sammen.
- Vedlikeholdet er en nødvendig forutsetning for at ytelsen til en barriere skal kunne opprettholdes. Det er et avgjørende ytelsespåvirkende forhold.
- En fungerende vedlikeholdsstyringsprosess er en nødvendig forutsetning for at ytelsen til en barriere skal kunne opprettholdes og forbedres over tid.
- En del av bakteppet for nødvendigheten av denne oppgaven er også de utfordringer man står overfor både relatert til barrierestyring og vedlikeholdsstyring i petroleumsvirksomheten.
- Data fra RNNP viser at ytelsen på sentrale barriereelementer ikke opprettholdes i henhold til selskapenes egne krav.

### Hensikt

Målet med oppgaven er å utvikle kunnskap om og synliggjøre vedlikeholdets betydning for god barrierestyring og dermed bidra til at barrierer fungerer ved behov. Resultatene av oppgaven skal styrke kunnskapen om betydningen av vedlikeholdet av tekniske barrierer. Ytelsen av barrierene vil kunne bedres gjennom forbedring og optimalisering av vedlikeholdsstyringen og forbedringsarbeidet knyttet til barrierene. Resultatene fra arbeidet vil også kunne bidra til videreutvikling av tilsynsmetodikk.

### Oppgaven

I denne rapporten diskuterer vi vedlikeholdets plass i barrierestyringen både på prinsipielt grunnlag, trinn for trinn i barrierestyringsprosessen, gjennom konkrete eksempler, samt i forhold til utvalgte sentrale tema.

### Vedlikeholdets plass i barrierestyringen – prinsipielle sammenhenger

Barrierestyring inngår som en del av annen styring, bl.a. risikostyring (på selskapsnivå). Barrierestyring er ikke en separat aktivitet, men er en integrert del av bl.a. risikostyringen. Vedlikeholdet er i kraft av sitt formål (opprettholde/gjenvinne ytelsen til blant annet barriereelementene) en viktig del av barrierestyringen.

De prinsipielle sammenhengene har tatt for seg:

- Prinsippene for risiko-/barrierestyring
- Styringssløyfa for styring av rammeverket
- Rammeverket for barrierestyringsprosessen
- Selve barrierestyringsprosessen (for alle faser)
- Oppfølging i driftsfasen, inklusive måling og verifikasjon av barrierelytelse
- Vedlikeholdsstyringssløyfa og koplingen mellom vedlikeholdsstyring og barrierestyring

De prinsipielle sammenhengene med hensyn til vedlikeholdets plass i barrierestyringen viser koplingen mellom de ulike elementene i vedlikeholdsstyringssløyfa og henholdsvis rammeverket for barrierestyrings-

prosessen og selve barrierestyringsprosessen (med nærmere spesifisering av oppfølging i driftsfasen, inklusive måling og verifikasjon av barrieretelse). Sammenhengene baserer seg blant annet på vår fortolkning av ISO 31000, som er beskrevet og forklart i vedlegg B.

### **Vedlikeholdets rolle i barrierestyringsprosessen – trinn for trinn**

Vedlikeholdets rolle er drøftet for hvert av trinnene i barrierestyringsprosessen. Hoveddelene av prosessen er:

1. Kontekst
2. Risikovurderinger
3. Risikohåndtering
4. Kommunikasjon og konsultasjon
5. Overvåking og gjennomgåelse

Drøftingen har blitt understøttet med data fra RNNP, der dette har vært mulig og hensiktsmessig. Drøftingen har tatt utgangspunkt i barrierenotatet og dets behandling av vedlikehold og vedlikeholdsstyring, som er gjengitt i vedlegg C.

### **Konkrete eksempler på vedlikeholdets betydning for god barrierestyring**

Når vi har gitt konkrete eksempler på vedlikeholdets betydning for god barrierestyring har vi tatt utgangspunkt i føringer og antakelser fra design og sett på videre oppfølging i driftsfasen, spesielt gjennom driftsgjennomganger av feil i sentrale barriereelementer. Dette inkluderer beskrivelse av fremgangsmåte og omfang, feilklassifisering, diskusjon rundt feil oppdaget ved test versus feil oppdaget i normal drift, samt gjennomgang av generelle nytteverdier av driftsgjennomganger.

Avslutningsvis har vi presentert og diskutert resultatene av driftsgjennomgangene, og en hovedkonklusjon er at en betydelig andel av feilene (på utvalgte barriereelementer) kan direkte eller indirekte tilskrives manglende eller mangelfullt (ikke utført eller for dårlig utført) vedlikehold. Det er derfor et stort potensiale for å redusere antall sikkerhetskritiske feil ved å fokusere på et bedre vedlikehold.

Dessuten har vi gitt et eksempel som viser hvor "ømfintlig" og avhengig en barriere kan være for et korrekt tilpasset vedlikehold, dersom kravet til ytelse skal opprettholdes i driftsfasen i samsvar med krav stilt under design.

### **Utvalgte tema**

Vi har tatt for oss følgende utvalgte sentrale tema knyttet til vedlikeholdets plass i barrierestyringen:

- Viktigheten av strukturert tilnærming og kontinuerlig forbedring
- Viktigheten av tverrfaglig involvering
- Behandling av eventuelle avvik knyttet til vedlikehold av barrierer (enkeltvis og samlet)

Her peker vi blant annet på utfordringer med gjentakende feil og behovet for å fjerne årsaker til utstysfeil i stedet for å korrigere symptomer. Videre har vi påpekt behovet for tverrfaglig samarbeid i forbindelse med kritikalitetsklassifisering, optimalisering av testintervall, ved driftsgjennomganger av notifikasjoner, samt ved kommunikasjon rundt risikoanalyser (blant annet forutsetninger knyttet til barrierer som krever oppfølging i drift av vedlikeholdspersonell).

Når det gjelder håndtering av avvik stiller vi spørsmålet når "nok er nok". Hvor mye utestående vedlikehold og etterslep skal man få lov å ha? Hvor mange avvik? Hvor stort totalvolum av vedlikehold som ikke er utført? Svaret er at det er svært vanskelig å få et svar på når nok er nok. Spørsmålet blir da om man oppnår god nok kontroll uten å sette tydelige og målbare grenser.

## 1 Innledning

Vedlikeholdets plass i barrierestyringen kan oppfattes både enkelt og vanskelig. Enkelt sagt skal vedlikeholdet bidra til å opprettholde og gjenopprette barrierenes funksjon, samt verifisere ytelsen til barrierene. Når det er sagt er det ikke like rett frem hvordan dette skal gjøres i praksis. Heller ikke barrierestyringen i seg selv er rett frem, noe som blant annet behovet for Ptils barrierenotat /1/ er et uttrykk for.

Det vi presenterer i denne rapporten er et resultat av grundige vurderinger og systematisk arbeid, blant annet gjentatte gjennomganger av barrierenotatet til Ptil /1/ og ISO 31000 /2/ som barrierenotatet har brukt som grunnlag, samt driftsgjennomganger og resultater fra tidligere vedlikeholdsprosjekter gjennomført i samarbeid med Ptil /11-17/.

Vi håper denne rapporten gir et nyttig bidrag til bevisstgjøring rundt barrierestyring og vedlikeholdets plass i barrierestyringen, samtidig som vi er klar over at det kan være andre måter å betrakte dette på.

### 1.1 Bakgrunn og begrunnelse

Noen av begrunnelsene for oppgaven (gitt i oppgavebeskrivelsen) er:

- Petroleumsstilsynets arbeid med barrierestyring viser at det er behov for mer kunnskap i næringen om hvordan vedlikeholdsstyring og barrierestyring er knyttet sammen.
- Vedlikeholdet er en nødvendig forutsetning for at ytelsen til en barriere skal kunne opprettholdes. Det er et avgjørende ytelsespåvirkende forhold (jf. definisjoner i kapittel 1.4).
- En fungerende vedlikeholdsstyringsprosess er en nødvendig forutsetning for at ytelsen til en barriere skal kunne opprettholdes og forbedres over tid.
- En del av bakteppet for nødvendigheten av denne oppgaven er også de utfordringer man står overfor både relatert til barrierestyring og vedlikeholdsstyring i petroleumsvirksomheten.

Ut over begrunnelsene gitt i oppgavebeskrivelsen kan fokus på vedlikeholdet som en sentral del av barrierestyringen også motiveres ut fra data fra Risikonivå i norsk petroleumsvirksomhet (RNNP) og gjennomgang av årsaker til storulykker.

- Data fra RNNP (/3/-/6/) viser at ytelsen på sentrale barriereelementer ikke opprettholdes i henhold til selskapenes egne krav. Hvor mye av dette som eventuelt kan tilskrives mangler ved vedlikeholdet kommer vi nærmere tilbake til gjennom eksempler (i kapittel 4). Data fra driftsgjennomganger viser dessuten at feil som rapporteres til RNNP – test-introduserte feil – bare utgjør en del av de totale sikkerhetskritiske feilene. Situasjonen kan dermed være verre enn det RNNP viser.
- Gjennomgang og granskninger av storulykker viser dessuten at vedlikehold kan være en viktig medvirkende årsak, som følge av manglende vedlikehold av barrierene eller feilaktig vedlikehold/testing av barrierene (/7/-/10/). Noen eksempler på hendelser hvor mangelfullt vedlikehold har vært medvirkende er: Macondo utblåsningen (2010), Texas City (2005), Pasadena (1989), Piper Alpha (1984), Bhopal (1984), Three Mile Island (1979).

#### *Utfordringer ved barrierestyring*

Tall fra RNNP /6/ viser god utvikling på mange områder, men gir også grunn til uro. Bedre styring av storulykkerisiko og bedre barrierestyring er oppgaver petroleumsnæringen må ta tak i. Når det gjelder barrierestyring, kreves det et krafttak i næringen.

Barriereindikatorene viser at det er til dels store nivåforskjeller mellom innretningene på norsk sokkel, ikke bare i 2012, men de siste ti årene /6/. Flere innretninger har relativt sett dårlige resultater for enkelte barriere-systemer. De tallene vi ser i RNNP, viser at det fortsatt må arbeides med forbedringer. Det er her snakk om sikkerhetskritiske barrierer som ikke oppfyller anerkjente ytelseskriterier. Selskapene sitter således med informasjon om barrierer som ikke fungerer som de skal, uten synlig forbedring. Det er derfor viktig å se nærmere på hvordan forbedret vedlikeholdsstyring kan motvirke dette og redusere antall feil slik at ytelseskriteriene oppfylles.

### **Utfordringer ved vedlikeholdsstyring**

Myndighetenes (blant annet /11/-/17/) og aktørenes satsing på forbedring av vedlikehold viser på flere områder positive resultater, men det gjenstår betydelige problemområder. Vedlikehold er et sikkerhetskritisk område, og utfordringene på dette området bør derfor kommuniseres tydelig og bredt.

RNNP-tallene fra 2009 til 2012 (/3/-/6/) viser at flere aktører har utfordringer med vedlikeholdsstyring. Flyttbare innretninger har mangler knyttet til merking og klassifisering av utstyr, til etterslep av forebyggende vedlikehold og til utestående korrigerende vedlikehold, inkludert sikkerhetskritisk vedlikehold.

Hvordan påvirker så utfordringer ved vedlikeholdsstyringen utfordringer ved barrierestyringen? Hva er sammenhengen mellom mangelfullt vedlikehold og den manglende barrierelytelsen som en ser rapportert i blant annet RNNP? Vi har forsøkt å underbygge denne sammenhengen blant annet gjennom konkrete eksempler beskrevet i kapittel 4.

### **Utfordringer ved vedlikeholdsstyring - vedlikehold skal forebygge og forhindre**

HMS-regelverket krever at innretninger (med alt av systemer og utstyr) skal holdes ved like på en slik måte at de er i stand til å utføre tiltenkte funksjoner i alle faser av levetiden. Vedlikehold skal derfor bidra til å forhindre at det oppstår feil som får negative følger for personell, ytre miljø, driftsregularitet og materielle verdier.

Målet med vedlikeholdsstyring er blant annet å identifisere kritiske funksjoner og sikre at sikkerhetskritiske barrierer fungerer når det er behov for dem. Aktørene har således behov for anvendbare og kostnadseffektive vedlikeholdsmetoder som tar utgangspunkt i utstyrets sviktmønster (hvordan det kan svikte i ulike sammenhenger).

Det er også viktig at vedlikeholdet, i tillegg til å reparere og utbedre feil, går inn på bakenforliggende årsaker og tar tak i disse. En ser altfor ofte at feil på det samme utstyret gjentar seg gang etter gang, uten at den egentlige rotårsaken er identifisert. Her er det, som nevnt i kapittel 4, ofte en underliggende sammenheng mellom dårlig design og utilstrekkelig vedlikehold, men når en gitt design allerede er tatt i bruk er det gjennom vedlikeholdsfunksjonen at problemet med gjentakende feil må identifiseres og løses, enten dette innebærer redesign/modifikasjon eller et bedre tilpasset vedlikehold.

Det er også en utfordring at detekterte feil "blir liggende" før de blir utbedret uten at kompenserende tiltak introduseres. Dette kommer vi også nærmere inn på i kapittel 4.

## **1.2 Hensikt**

Målet med oppgaven er å utvikle kunnskap om og synliggjøre vedlikeholdets betydning for god barrierestyring og dermed bidra til at barrierer fungerer ved behov.

Resultatene av oppgaven skal styrke kunnskapen om betydningen av vedlikeholdet av tekniske barrierer. Ytelsen av barrierene vil kunne bedres gjennom forbedring og optimalisering av vedlikeholdsstyringen og forbedringsarbeidet knyttet til barrierene. Arbeidet vil også kunne bidra til videreutvikling av tilsynsmetodikk.

### 1.3 Beskrivelse av oppgaven

Oppgaven har tatt utgangspunkt i barrierenotatet /1/ og belyst interaksjonen mellom vedlikeholdsstyring og barrierestyring blant annet ved å gå gjennom trinnene i barrierestyringsprosessen, og vist/drøftet betydningen av vedlikeholdet i barrierestyringen.

Viktigheten av følgende forhold er drøftet:

- Strukturert tilnærming og kontinuerlig forbedring, både med hensyn til vedlikehold og barrierefunksjoner.
- Tverrfaglig involvering, inkludert ekspertise innenfor vedlikehold, teknisk utstyr og teknisk sikkerhet.
- Behandling av eventuelle avvik knyttet til vedlikehold av barrierer, både enkeltvis og samlet.

Oppgaven dekker både innretninger i drift så vel som nye innretninger og innretninger i prosjektfasen.<sup>1</sup>

### 1.4 Definisjoner og begreper

*Antall merket ("tagged") utstyr totalt (/17/):*

Antall merket utstyr ved utgangen av rapporteringsperioden.

*Antall "tag" som er klassifisert (/17/):*

Antall klassifisert utstyr ved utgangen av rapporteringsperioden.

*Antall "tag" klassifisert som HMS-kritisk (/17/):*

Antall HMS-kritisk utstyr ved utgangen av rapporteringsperioden.

*Barriere (/1/):*

Tekniske, operasjonelle og organisatoriske elementer som enkeltvis eller til sammen skal redusere muligheten for at konkrete feil, fare- og ulykkessituasjoner inntreffer, eller som begrenser eller forhindrer skader/ulemp.

*Barriereelement (/1/):*

Tekniske, operasjonelle eller organisatoriske tiltak eller løsninger som inngår i realiseringen av en barrierefunksjon.

*Tekniske barriereelement (/18/):*

Utstyr og systemer som inngår i å realisere en barrierefunksjon.

---

<sup>1</sup> Dette er beskrevet fortløpende underveis i rapporten der det er relevant og ikke behandlet som et separat tema.

*Operasjonelle barriereelement (/18/):*

De handlinger eller aktiviteter som personellet må utføre for å realisere en barrierefunksjon.

*Organisatoriske barriereelement (/18/):*

Personell med definerte roller eller funksjoner som inngår i realiseringen av en barrierefunksjon.

*Barrierefunksjon (/1/):* Oppgaven eller rollen til en barriere. Eksempler på barrierefunksjoner er: forhindre lekkasje, forhindre antenning, redusere brannbelastning, sikre forsvarlig evakuering, forhindre hørselsskade.

*Barrierestrategi (/1/):* Resultatet av prosess som med utgangspunkt i risikobildet beskriver og avklarer hvilke barrierefunksjoner og barriereelementer som skal implementeres for å redusere risiko.

*Barriestyling (/1/):* Koordinerte aktiviteter for å etablere og opprettholde barrierer slik at de til enhver tid opprettholder sin funksjon.

*Forebyggende vedlikehold (/6/):*

Forebyggende vedlikehold (FV) er vedlikehold som utføres etter forutbestemte intervaller eller ifølge forutbestemte kriterier, og som har til hensikt å redusere sannsynligheten for svikt eller funksjonsnedsetting (degradering).

*FV etterslep, antall timer totalt (/17/):*

Totalt antall timer forebyggende vedlikehold som ikke er utført innen fastsatt ferdigstillelsesdato, beregnet som gjennomsnittet av antall timer etterslep i FV ved utgangen av hver måned i rapporteringsperioden.

*FV etterslep, antall timer HMS-kritisk (/17/):*

Antall timer forebyggende vedlikehold på HMS-kritisk utstyr som ikke er utført innen fastsatt ferdigstillelsesdato, beregnet som gjennomsnittet av antall timer etterslep i HMS-kritisk FV ved utgangen av hver måned i rapporteringsperioden.

*HMS-kritisk (/6/):* Feil (tap av funksjon) som har konsekvenser for helse, miljø eller sikkerhet.

*Inspeksjon (/6/):* Aktivitet utført periodisk for å vurdere skadeutvikling/tilstand av en enhet.

*Klassifisering (/6/):* Plassering av et objekt i et sett av kategorier/klasser, basert på egenskaper til objektet. (En av klassene er "HMS-kritisk", eller tilsvarende).

*Kontekst (/1/):* Eksterne og interne rammebetingelser som det skal tas hensyn til i barriestyling.

*Korrigerende vedlikehold (/6/):*

Korrigerende vedlikehold (KV) er vedlikehold som utføres etter at en feil (tilstand) er oppdaget, og som har til hensikt å bringe en enhet tilbake i en tilstand som gjør det mulig å utføre en krevd funksjon.

*KV utestående, antall timer totalt (/17/):*

Totalt antall timer korrigerende vedlikehold som ikke er utført innen fastsatt tidsfrist, beregnet som gjennomsnittet av antall timer utestående KV ved utgangen av hver måned i rapporteringsperioden.

*KV utestående, antall timer HMS-kritisk (/17/):*

Antall timer korrigerende vedlikehold av HMS-kritisk utstyr som ikke er utført innen fastsatt tidsfrist, beregnet som gjennomsnittet av antall timer utestående HMS-kritisk KV ved utgangen av hver måned i rapporteringsperioden.

*Risikostyring (/1/):*

Koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko.

*Tag (/6/):*

En unik kode som definerer den funksjonelle plasseringen og funksjonen til en fysisk komponent i et anlegg. "Funksjonell plassering" henviser kun til hvor komponenten inngår i et system, ikke den presise fysiske posisjon.

*Utestående (KV)<sup>2</sup> (/6/):* Mengde KV som ikke er utført innen fastsatt tidsfrist.

*Vedlikehold (basert på /19/):*

Kombinasjon av alle tekniske, administrative og ledelsesmessige aktiviteter i levetiden til en enhet, som har til hensikt å opprettholde eller gjenopprette den til en tilstand som gjør den i stand til å utføre den krevde funksjonen.

*Vedlikeholdsevne (basert på /19/):*

Evnen til en vedlikeholdsorganisasjon til å ha riktig vedlikeholdsstøtte på riktig sted for å utføre nødvendig vedlikeholdsaktivitet på et gitt tidspunkt eller i løpet av et gitt tidsintervall.

*Vedlikeholdsmål (basert på /19/):*

Mål fastsatt og akseptert for vedlikeholdsaktivitetene.

Merknad: Disse målene kan inkludere tilgjengelighet, kostnadsreduksjon, produktkvalitet, miljøvern, sikkerhet, osv.

*Vedlikeholdsplan (basert på /19/):*

Strukturert sett av oppgaver som inkluderer aktivitetene, prosedyrene, ressursene og tidsforbruket nødvendig for å utføre vedlikeholdet.

*Vedlikeholdsstrategi (basert på /19/):*

Styringsmetode brukt for å nå vedlikeholdsmålene.

*Vedlikeholdsstøtte (basert på /19/):*

Ressurser, tjenester og ledelse nødvendig for å utføre vedlikehold.

Merknad: Støtte kan inkludere personell, testutstyr, arbeidsrom, reservedeler, dokumentasjon, verktøy, osv.

---

<sup>2</sup> Utestående KV er her regnet som overskredet KV i forhold til fastsatt ferdigstillelsesdato. Det er ikke den totale porteføljen av utestående KV (alt som skal gjøres, ikke bare det som er overskredet).

*Vedlikeholdsstyring (basert på /19/):*

Alle ledelsesaktiviteter som fastsetter vedlikeholdsmålene, strategiene og ansvar, og implementerer dem gjennom tiltak som vedlikeholdsplanlegging, vedlikeholdskontroll og tilsyn, og forbedring av metoder og organisasjon, inkludert økonomiske aspekter.

*Ytelseskrav (/1/):*

Etterprøvbare krav til barriereelementenes egenskaper for å sikre at barrieren er effektiv. Ytelseskrav kan blant annet omfatte krav til kapasitet, funksjonalitet, effektivitet, integritet, pålitelighet, tilgjengelighet, evne til å motstå laster, robusthet, kompetanse, mobiliseringstid.

*Ytelsespåvirkende forhold (/1/):*

Forhold som er av betydning for barrierefunksjoner og barriereelementers evner til å fungere som tiltenkt.

Noen av de sentrale begrepene er diskutert nærmere og gitt alternative fortolkninger i vedlegg A.

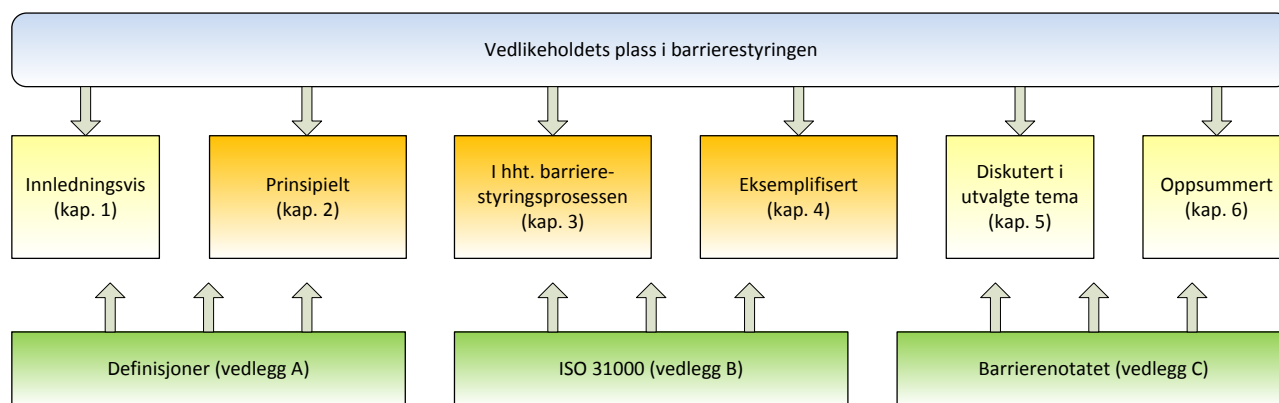
## 1.5 Forkortelser

|        |                                                                                  |
|--------|----------------------------------------------------------------------------------|
| af     | Aktivitetsforskriften                                                            |
| BDV    | Blowdown valve (avblåsningsventil)                                               |
| BOP    | Blowout preventer (utblåsningssikring)                                           |
| B&G    | Brann og gass                                                                    |
| D      | Dangerous (farlige [feil])                                                       |
| DD     | Dangerous Detected (farlig detektert [feil])                                     |
| DU     | Dangerous Undetected (farlig udetektert [feil])                                  |
| DHSV   | Downhole safety valve (nedihulls sikkerhetsventil)                               |
| ESD    | Emergency shutdown (nødavstengning)                                              |
| ESV    | Emergency shutdown valve (nødavstengningsventil)                                 |
| E(X)   | Forventningsverdi (expected value); forventede antall feil X                     |
| FV     | Forebyggende vedlikehold                                                         |
| GL     | Guideline (retningslinje)                                                        |
| HAZID  | Hazard identification (fareidentifikasjon)                                       |
| HIPPS  | High integrity pressure protection system (høypålitelig trykkbeskyttelsessystem) |
| HMS    | Helse, miljø og sikkerhet                                                        |
| IEC    | International electrotechnical commission                                        |
| I/O    | Input/output                                                                     |
| ISO    | International organization for standardization                                   |
| KV     | Korrigerende vedlikehold                                                         |
| n      | Antall komponenter i en gitt populasjon                                          |
| NA     | Not Applicable (ikke aktuell)                                                    |
| NORSOK | Norsk sokkels konkurranseposisjon                                                |
| NS-EN  | Norsk Standard – European Norm                                                   |
| NTNU   | Norges teknisk-naturvitenskapelige universitet                                   |
| OD     | Oljedirektoratet                                                                 |
| OLF    | Oljeindustriens landsforening (nå Norsk Olje og Gass – NOG)                      |

|                |                                                                             |
|----------------|-----------------------------------------------------------------------------|
| PFD            | Probability of failure on demand (sannsynlighet for feil ved behov)         |
| PSD            | Process shutdown (prosessnedstengning)                                      |
| Ptil           | Petroleumstilsynet                                                          |
| RBI            | Risk based inspection                                                       |
| RCM            | Reliability Centered Maintenance                                            |
| RNNP           | Risikonivå i norsk petroleumsvirksomhet (betegnelse fra og med 2008)        |
| RNNS           | Risikonivå på norsk sokkel (betegnelse frem til 2008)                       |
| S              | Safe (sikker [feil])                                                        |
| SAP            | Systeme, Anwendungen und Produkte in der Datenverarbeitung                  |
| SAS            | Safety automation system (sikkerhetsautomasjonssystem)                      |
| SIF            | Safety instrumented function (sikkerhetsinstrumentert funksjon)             |
| SIL            | Safety integrity level (sikkerhetsintegritetsnivå)                          |
| SINTEF         | [Forsknings-] Stiftelsen SINTEF (fullstendig navn – ikke lenger et akronym) |
| SIS            | Safety instrumented system (sikkerhetsinstrumentert system)                 |
| SRS            | Safety requirement specification (sikkerhetskravspesifikasjoner)            |
| t              | Observasjonsperioden (tid)                                                  |
| TST            | Teknisk sikkerhetstilstand                                                  |
| TTS            | Teknisk tilstand sikkerhet                                                  |
| YPF            | Ytelsespåvirkende forhold                                                   |
| $\lambda_{DU}$ | Feilrate av farlige udetekterte feil                                        |
| $\tau$         | Testintervall                                                               |

## 1.6 Rapportstruktur

Rapportstrukturen er illustrert i figur 1.1.



**Figur 1.1** Rapportstruktur

I innledningen, kapittel 1, gis bakgrunn og begrunnelse for oppgaven, målet med oppgaven og beskrivelse av selve oppgaven, samt definisjoner og forkortelser. En utdyping og diskusjon av begreper er gitt i vedlegg A.

I kapittel 2 har vi beskrevet vedlikeholdets plass i barrierestyringen ut fra prinsipielle sammenhenger. Vi har her benyttet tilsvarende figurer som i barrierenotatet, men basert på vår fortolkning av ISO 31000 /2/. Denne fortolkningen er beskrevet og forklart i vedlegg B.

I kapittel 3 har vi drøftet vedlikeholdets rolle i hvert av trinnene i barrierestyringsprosessen, og i den grad det har vært mulig og hensiktsmessig, understøttet dette med data fra RNNP (/3/-/6/). Dette bygger blant annet på barrierenotatet /1/ og dets behandling av vedlikehold og vedlikeholdsstyring, som er gjengitt i vedlegg C.

I kapittel 4 gir vi konkrete eksempler på vedlikeholdets betydning knyttet til barrierestyring, mens vi i kapittel 5 diskuterer noen utvalgte sentrale tema.

Til slutt gir vi en oppsummering i kapittel 6.

Kapitlene 2-4 utgjør hovedkapitlene (angitt med oransje farge i figur 1.1).

--- ● ---

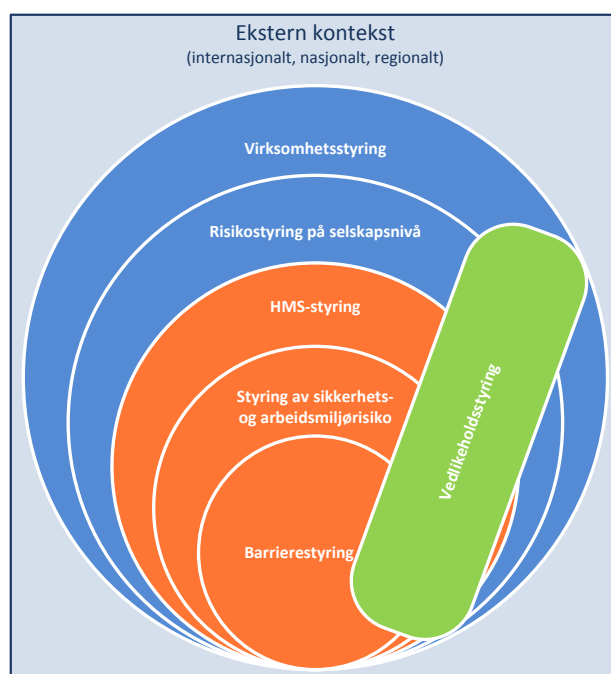
Vi starter med en prinsipiell drøfting av vedlikeholdets plass i barrierestyringen i kapittel 2.

## 2 Vedlikeholdets plass i barrierestyringen – prinsipielle sammenhenger

### 2.1 Overordnet betraktning

Barrierestyring inngår som en del av annen styring, bl.a. risikostyring (på selskapsnivå). Barrierestyring er ikke en separat aktivitet, men er en integrert del av bl.a. risikostyringen /1/.

Vedlikeholdet er i kraft av sitt formål (å opprettholde og gjenvinne ytelsen til blant annet barriereelementene) en viktig del av barrierestyringen. Styring av vedlikehold vil derfor overlappe med barrierestyring, men vedlikeholdet vil i tillegg rette seg mot utstyr som ikke defineres som barrierer, deriblant prosess- og hjelpesystemer for å opprettholde produksjonen. Figur 2.1 illustrerer denne overlappen.



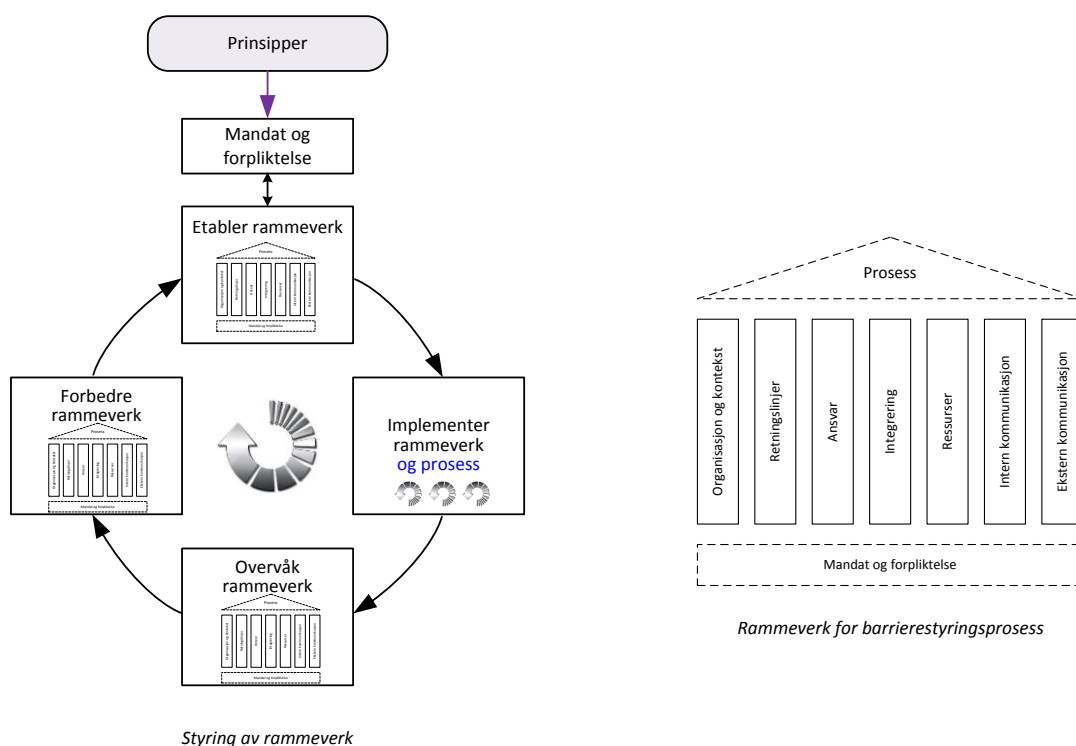
**Figur 2.1** Vedlikeholdstyring som del av annen styring (basert på /1/)

Det er også verdt å understreke viktigheten av helhetstenkning. Selv om vi nå fokuserer spesielt på vedlikeholdstyring relatert til barrierestyring, som igjen er en del av risikostyringen, så er det i denne sammenheng (dvs. vedlikeholdets plass i barrierestyringen – som del av risikostyringen) viktig å se helhetlig på risikostyringen. Dette er utfordringen ved å trekke frem barrierestyring som "egen aktivitet" i risikostyringen slik det er gjort i barrierenotatet /1/. Tilsvarende får vi den samme utfordringen når vi trekker frem vedlikeholdstyringen knyttet til barrierestyring.

### 2.2 Prinsipper og rammeverk

Prinsippene for risikostyring (og barrierestyring) gir føringer for "mandat og forpliktelse" som igjen danner utgangspunktet for etablering av rammeverket for risikostyringen (og barrierestyringen) – høyre del av figur 2.2.

## Prinsipper for risiko-/barrierestyring



**Figur 2.2** Prinsipper og rammeverk – fundament for barrierestyringen (basert på /2/)

Rammeverket må etableres, implementeres, overvåkes og forbedres, dvs. kontrolleres/styres etter en "klassisk" styringssløyfe. Styringen av rammeverket (for barrierestyringsprosessen) er altså en separat styringssløyfe, jf. /2/.

Som angitt med blå tekst i implementeringsfasen (-boksen) så skal i tillegg barrierestyringsprosessen implementeres. Denne består i seg selv av flere styringssløyfer eller iterasjonsprosesser<sup>3</sup>.

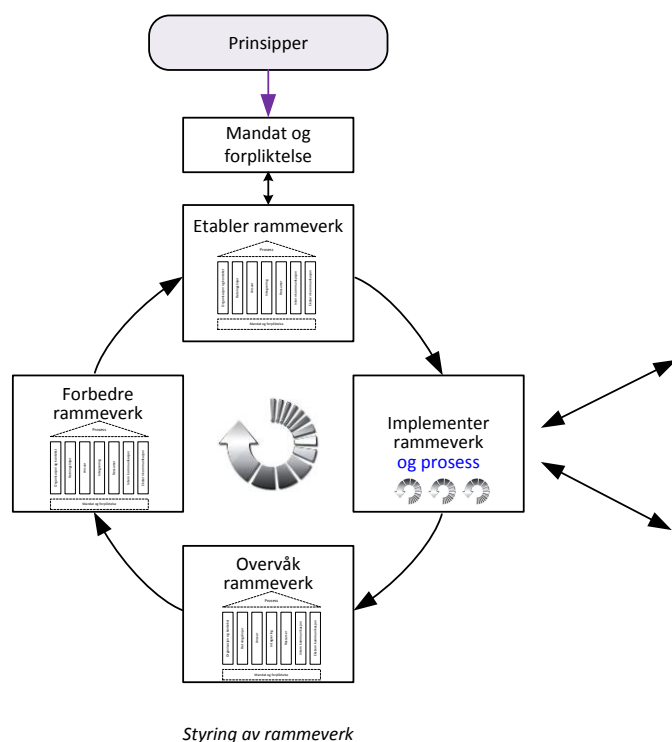
## 2.3 Barrierestyringsprosessen

Både "rammeverket for barrierestyringen" og "barrierestyringsprosessen" skal implementeres, dvs. både fundamentet for barrierestyringsprosessen og selve barrierestyringsprosessen, jf. /2/. Styringssløyfa for styring av rammeverket er vist til venstre i figur 2.3, mens styringssløyfene eller iterasjonsprosessene til barrierestyringsprosessen er vist med rødt i figur 2.3.

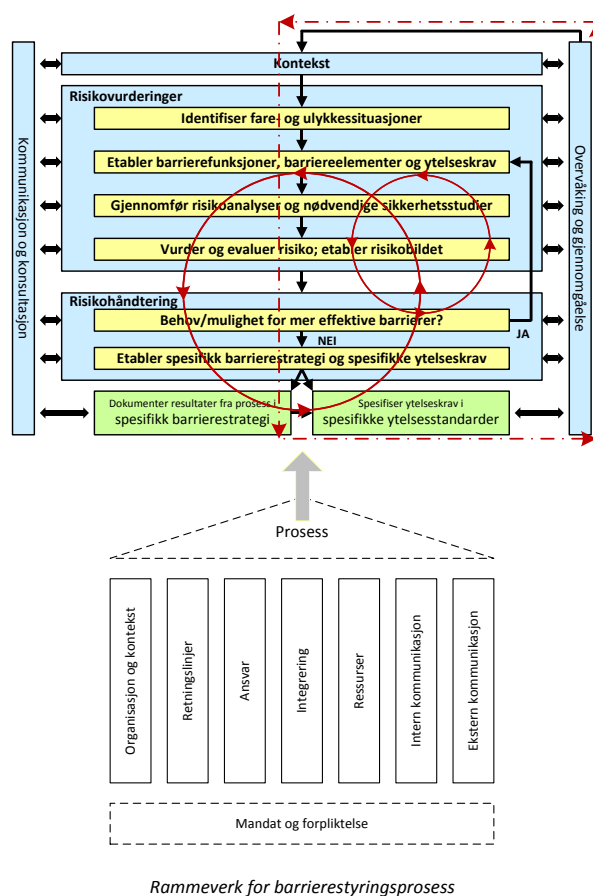
Vi skal se nærmere på disse styringssløyfene/iterasjonsprosessene med utgangspunkt i øvre høyre del av figur 2.3.

<sup>3</sup> Gjentakelser og oppdateringer.

Prinsipper for risiko-/barrierestyring



Barrierestyringsprosess (alle faser)



**Figur 2.3** Barrierestyringsprosessen relatert til prinsipper og rammeverk (basert på /1/ og /2/)

Proessen starter med å definere/klargjøre kontekst for deretter å gjøre risikovurderinger. Basert på risikovurderingene ser man i risikohåndteringen på behovet/muligheten for ytterligere eller mer effektive barrierer, som resulterer i en iterasjonsprosess som angitt i den minste røde sløyfa i figur 2.3.

Når denne første iterasjonsprosessen er ferdig etableres spesifikk barrierestrategi og spesifikke ytelseskrav (i spesifikke ytelsesstandarder). Ved etablering av spesifikke ytelseskrav vil det også inngå en vurdering av aktuelle verifikasjonsaktiviteter, herunder inspeksjon og testing. Eksempelvis vil funksjonstesting av barriereelementer som inngår i instrumenterte sikkerhetssystemer (SIS) ha krav til testintervall som beskrevet i SRS (Safety Requirement Specifications). Dette gir input til vedlikeholdsprogrammet, som også baserer seg på underlag fra utstyrsleverandører og ulike analyser og beregninger (kritikalitetsvurderinger, RCM, RBI, etc.).

Fokus i designfasen vil primært være på de tekniske barriereelementene. I byggefasen og under driftsforberedelser vil det være behov for oppdatering av barrierestrategi og ytelseskrav som også dekker alle de operasjonelle og organisatoriske barriereelementene. Denne oppdateringen, etter hvert som prosjektet går fremover, er illustrert med den største røde sløyfa i figur 2.3<sup>4</sup>.

<sup>4</sup> I noen tilfeller kan det være hensiktsmessig med kun én iterasjonsprosess jfr. den største røde sløyfa.

Det vil imidlertid være hensiktsmessig å starte arbeidet med operasjonelle og organisatoriske barriereelementer allerede i designfasen, da det kan bli fordyrende å avvente dette til senere faser (for eksempel knyttet til vurderinger og avveininger mellom manuell og automatisk trykkavlastning).

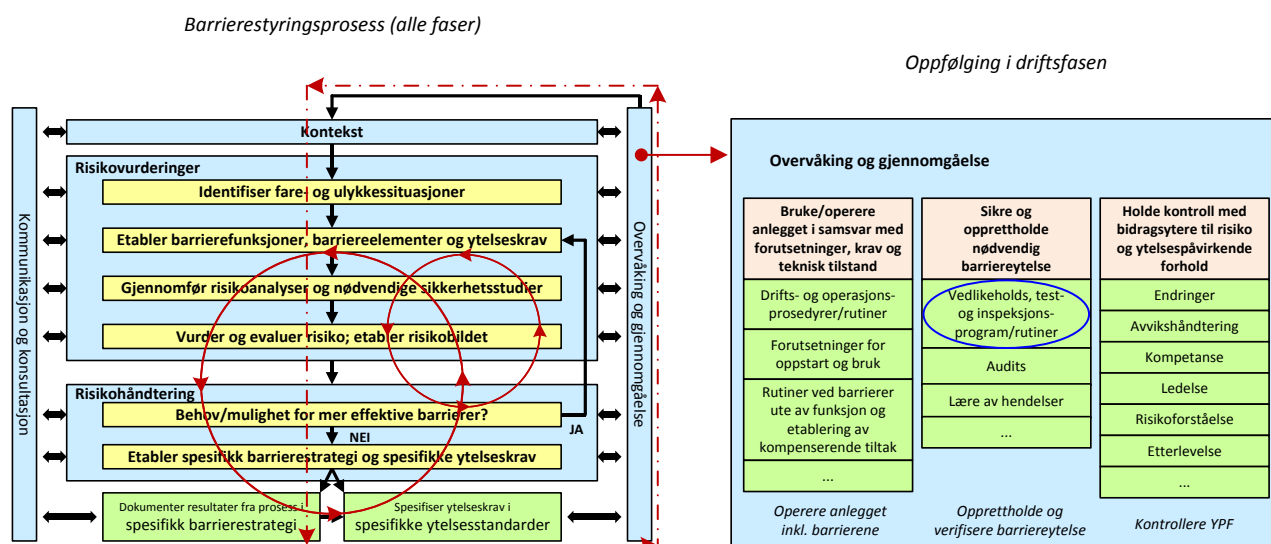
I begge tilfeller (begge iterasjonssløyfene) vil man typisk bygge på eksisterende identifikasjon av fare- og ulykkesituasjoner (HAZID) og eksisterende risikoanalyse (som også oppdateres flere ganger under design- og byggefasene).

Den tredje styringssløyfa er illustrert som et stiplet rektangel i figur 2.3. Denne dekker den boksen eller det trinnet i barrierestyringsprosessen som er kalt "overvåking og gjennomgåelse", og er i all hovedsak den kontroll som vil pågå kontinuerlig i driftsfasen når barrierestrategi og ytelseskrav/ytelsesstandards har blitt implementert. Denne oppfølgingen i driftsfasen er beskrevet mer detaljert i neste kapittel.

## 2.4 Oppfølging i driftsfasen

"Overvåking og gjennomgåelse", dvs. oppfølging i driftsfasen er illustrert til høyre i figur 2.4. Oppfølgingen består i 3 hovedelementer:

1. Drift av anlegget, inklusive barrierer, i samsvar med forutsetninger, krav og teknisk tilstand.
2. Opprettholdelse og verifikasjon av barrierereytelse.
3. Kontroll av ytelsespåvirkende forhold.



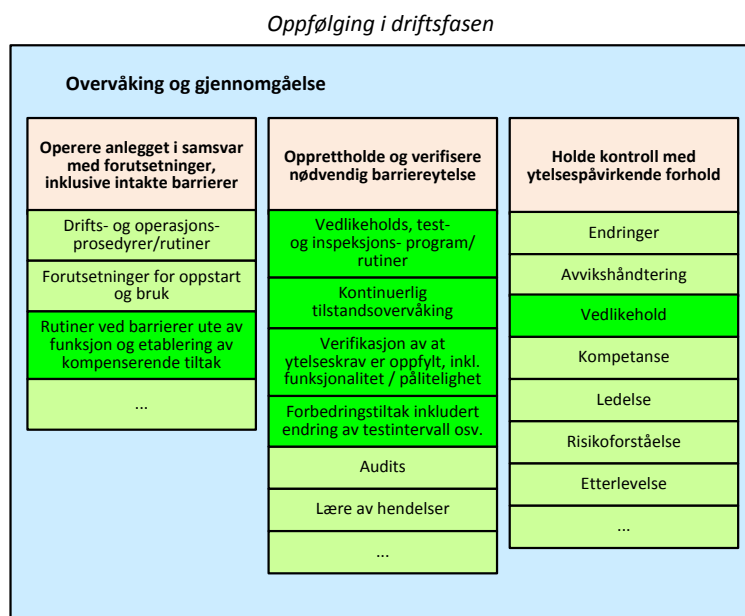
**Figur 2.4** Oppfølging av barrierene i driftsfasen (basert på /1/)

Rollen til vedlikeholdsstyringen er spesielt viktig i forhold til opprettholdelse og verifikasjon av barrierereytelse, noe som er angitt med en blå ellipse rundt "vedlikeholds, test- og inspeksjonsprogram/rutiner" i den andre kolonnen i figur 2.4.

I tillegg er vedlikeholdet i seg selv et sentralt ytelsespåvirkende forhold, selv om dette ikke inngår som eksempel i den tredje kolonnen i figur 2.4. Dermed er det også viktig å holde kontroll med vedlikeholdet, som er en bidragsyter til risiko.

Det kan argumenteres med at vedlikehold også burde synliggjøres bedre i første kolonne (og andre kolonne) i figuren da det ligger en rekke forutsetninger og input fra designfasen til drift knyttet til vedlikehold (hyppighet av testing, inspeksjonspunkter / risikobasert inspeksjon, tilstandsovervåkning av utvalgte barrierer, anvendelse av faktiske nedstenginger som erstatning for funksjonstester, osv.). Rutiner ved barrierer ute av drift griper også inn i hvordan en faktisk utfører både forebyggende og korrigerende vedlikehold knyttet til hvordan kompenserende tiltak implementeres.

Vedlikehold kunne derfor vært bedre synliggjort som et sentralt element ved oppfølging av barrierene i driftsfasen, som vist i figur 2.5.



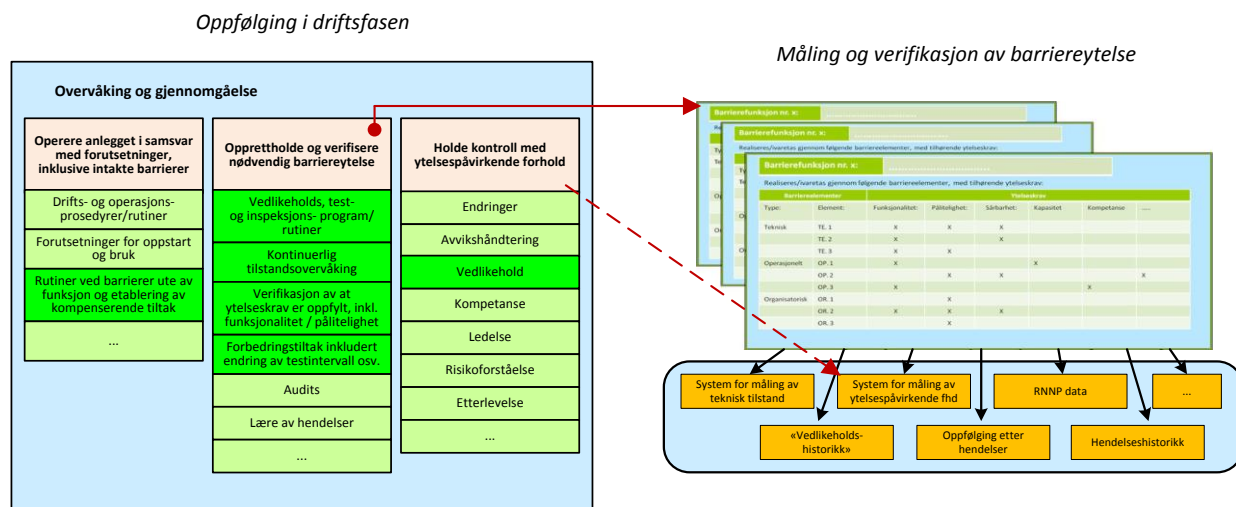
**Figur 2.5** Bedre synliggjøring av vedlikeholdets plass ved oppfølging av barrierene i driftsfasen

## 2.5 Måling og verifikasjon av barrieretytelse

Måling og verifikasjon av barrieretytelse er ytterligere illustrert gjennom figuren til høyre i figur 2.6. Den dekker også kontroll med ytelsespåvirkende forhold (YPF) som vist med den stiplede pilen, dvs. begge de to siste elementene/kolonnene i "overvåking og gjennomgåelse" (opprettholdelse og verifikasjon av barrieretytelse og kontroll med YPF).

Relevant informasjon fra vedlikehold er bl.a. vedlikeholdshistorikk, RNNP data (både testdata og vedlikeholdsdata), system for måling av teknisk tilstand og system for måling av ytelsespåvirkende forhold.

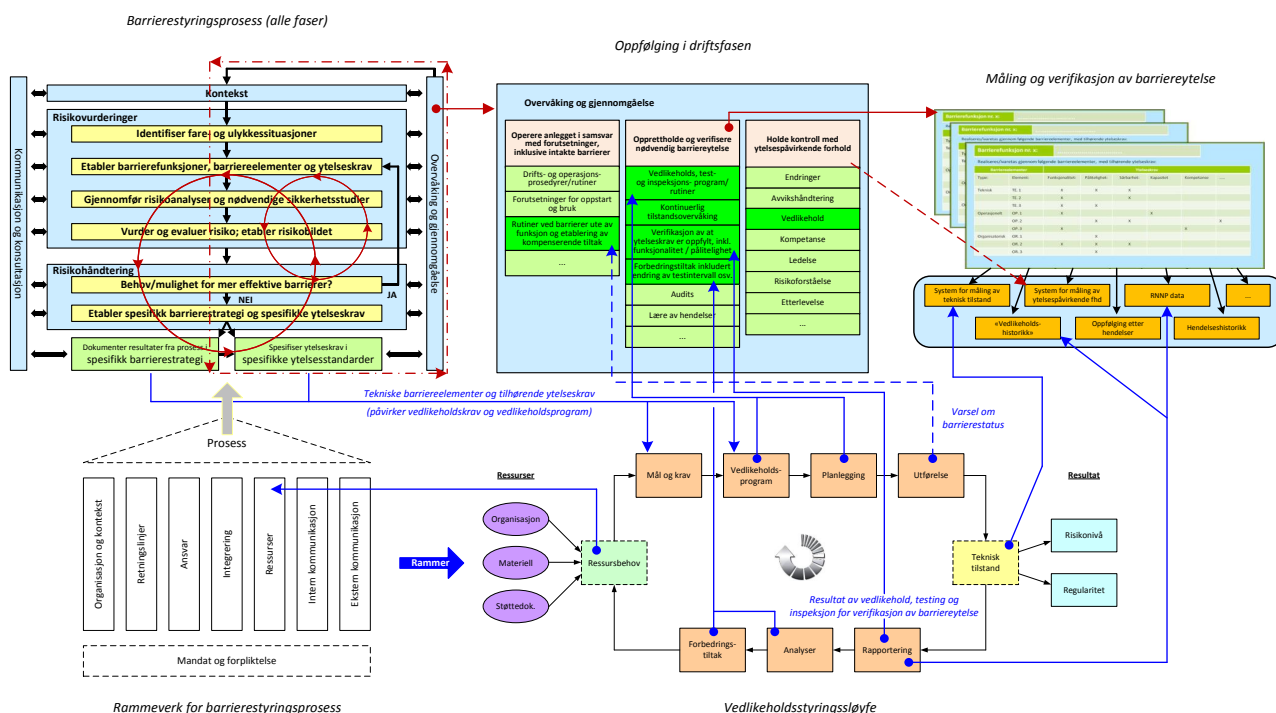
Denne informasjon er viktig underlag for å oppnå kontinuerlig forbedring.



**Figur 2.6** Vedlikeholdets rolle ved måling og verifikasjon av barriereytelse (basert på 1/)

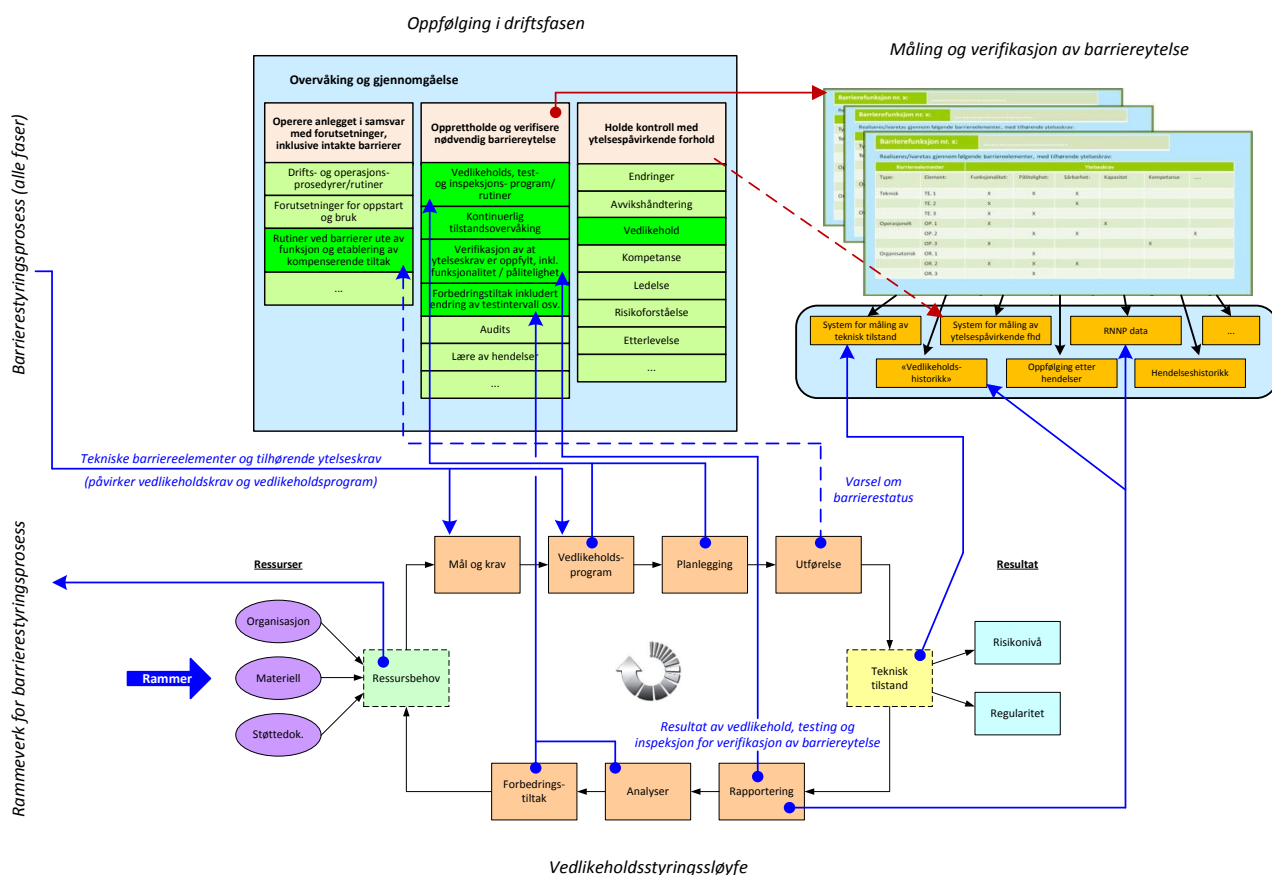
## 2.6 Kopling til vedlikeholdsstyringssløyfa

Sammenhengen mellom vedlikeholdsstyring og barrierestyring er vist ved hjelp av vedlikeholdsstyringssløyfa slik denne har blitt illustrert i norsk petroleumsvirksomhet (nede til høyre i figur 2.7). (Opprinnelig laget i forbindelse med "Basisstudien" som ble gjennomført av Oljedirektoratet i 1998 /20/).



**Figur 2.7** Sammenhengen mellom vedlikeholdsstyring og barrierestyring (basert på 1/, 2/ og 20/)

Figur 2.8 er et mindre utsnitt av figur 2.7, som er litt mer lesbar.



**Figur 2.8** Sammenhengen mellom vedlikeholdsstyring og barrierestyring – utsnitt

Noen av koplingene mellom barrierestyring /1/ og elementene i vedlikeholdsstyringssløyfa /20/ er (illustrert med blå piler og tekst):

1. Rammeverket for barrierestyringsprosessen (nede til venstre i figur 2.7) gir blant annet rammene i form av ressurser. Vedlikeholdsstyringssløyfa indikerer at det er en balanse mellom ressursbehov og ønsket resultat i form av teknisk tilstand, som igjen påvirker både risiko og regularitet. (For barrierestyring vil hovedfokus være teknisk tilstand som påvirker risikoen, ikke produksjonsregulariteten). Erfart ressursbehov gir også tilbakemelding vedrørende tilstrekkelige rammebetingelser.
2. Barrierestrategien (for tekniske barriereelementer) med tilhørende ytelseskrav gir føringer for elementene "mål og krav" og "vedlikeholdsprogram". Vedlikeholdsprogrammet (aktiviteter og intervall) vil for noen systemer (instrumenterte sikkerhetssystemer) ta inn krav fra SRS (Safety Requirement Specification), blant annet krav til responstid ("process safety time") og krav til testintervall.
3. Elementet "vedlikeholdsprogram" – det totale vedlikeholdsprogrammet – vil være de vedlikeholdsaktiviteter med tilhørende intervall som skal sørge for å opprettholde barrierereytelsen. Tilrettelegging for utførelse av vedlikeholdet inngår i elementet "planlegging".
4. Direkte knyttet til elementet "utførelse" kan det gis varsel om endret status på barrierer (eller planlagt endring i henhold til elementet "planlegging"), og behov for iverksettelse av driftsrutiner

ved barrierer ute av funksjon og etablering av kompensierende tiltak. Dette kan basere seg på online informasjon fra tilstandsovervåking, oppdagede feil under vedlikehold, testing eller inspeksjon, eller bevisst utkopling/overføring av sikkerhetssystemer/barrierer i forbindelse med vedlikehold, testing eller inspeksjon.

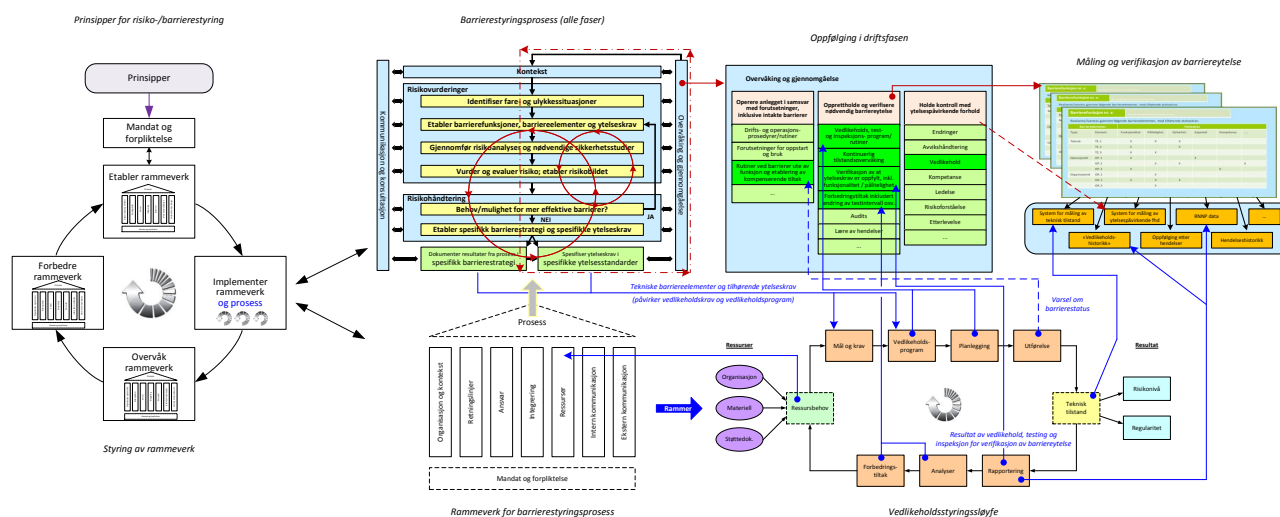
5. Fra elementet "rapportering" vil rapportering av vedlikehold, testing og inspeksjon benyttes for verifikasjon av barrierereytelse, både løpende (månedlig/kvartalsvis egenkontroll), ved halvårlig rapportering av barrierestatus i RNNP, ved årlige/femårslige tilsyn/målinger av teknisk tilstand (a la "TTS"), samt til kontroll med vedlikehold som et viktig ytelsespåvirkende forhold (vedlikeholdsindikatorer i RNNP, vedlikeholdshistorikk og system for måling av ytelsespåvirkende forhold).
6. Elementene "analyser" og "forbedringstiltak" gir input til forbedringstiltak for barrierene, inklusive behov for endring av testprosedyrer og testintervall.

## 2.7 Barriere- og vedlikeholdsstyring: Prinsipper, rammeverk og prosess

Som en oppsummering gir vi til slutt et oversiktsbilde (figur 2.9) over hele sammenhengene, dvs.:

- Prinsippene for risiko-/barrierestyring
- Styringssløyfa for styring av rammeverket
- Rammeverket for barrierestyringsprosessen
- Selve barrierestyringsprosessen (for alle faser)
- Oppfølging i driftsfasen, inklusive måling og verifikasjon av barrierereytelse
- Vedlikeholdsstyringssløyfa og koplingen mellom vedlikeholdsstyring og barrierestyring

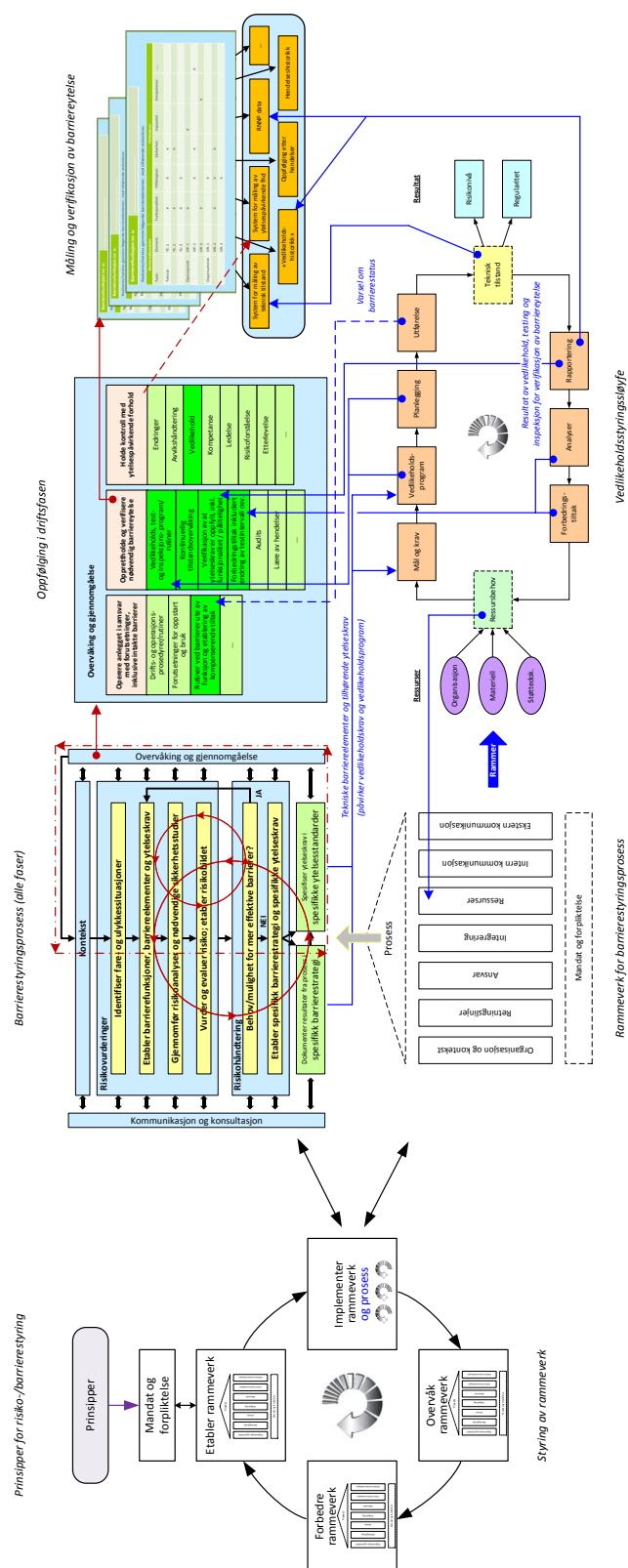
Figur 2.9a nedenfor er et liggende bilde, som gir et inntrykk av sammenhengene uten at det er særlig lesbart. På neste side er figuren (figur 2.9b) lagt på siden, og er forhåpentligvis litt mer lesbar.



**Figur 2.9a** Vedlikeholdets plass i barrierestyringen (basert på /1/, /2/ og /20/)

--- ● ---

I kapittel 3 tar vi for oss vedlikeholdets plass i barrierestyringen for hvert trinn i barrierestyringsprosessen.



**Figur 2.9b** Vedlikeholdets plass i barrierestyringen (basert på /1/, /2/ og /20/)

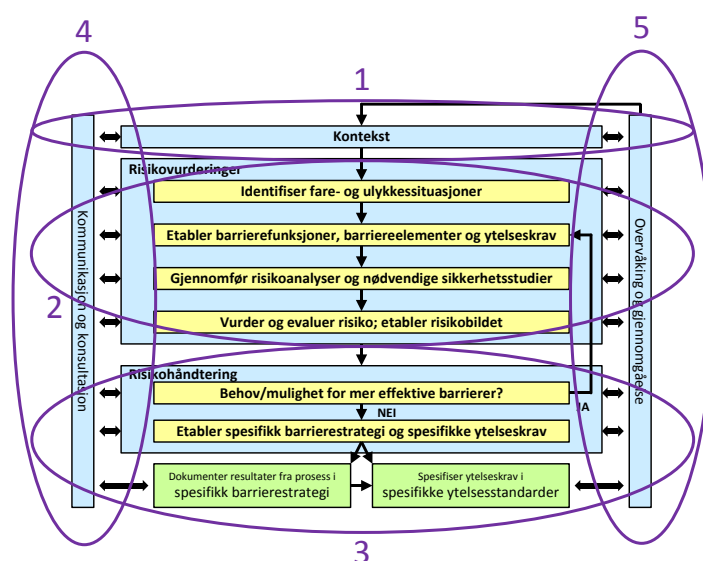


### 3 Vedlikeholdets rolle i barrierestytingsprosessen – trinn for trinn

De fem hoveddelene i barrierestytingsprosessen er:

1. Kontekst
2. Risikovurderinger
3. Risikohåndtering
4. Kommunikasjon og konsultasjon
5. Overvåking og gjennomgåelse

Disse er angitt i figur 3.1.



**Figur 3.1** De fem hoveddeler som barrierestytingsprosessen består av (basert på /1/)

I dette kapittelet belyser vi interaksjonen mellom vedlikeholdsstyring og barrierestyting for hver hoveddel og hvert trinn i barrierestytingsprosessen, samt at vi drøfter betydningen av vedlikeholdet i barrierestytingen. Trinnene er som følger (inkludert angivelse av kapitler):

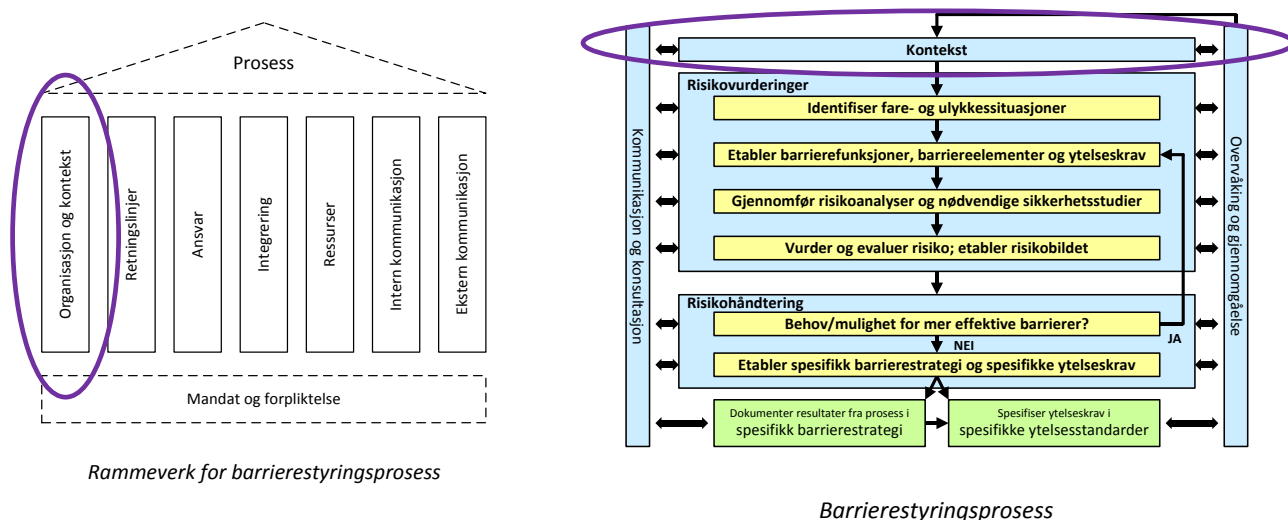
- 3.1 Kontekst
- 3.2 Risikovurderinger
  - 3.2.1 Identifisere fare- og ulykkessituasjoner
  - 3.2.2 Etablere barrierefunksjoner
  - 3.2.3 Gjennomføre risikoanalyser og sikkerhetsstudier
  - 3.2.4 Vurdering og evaluering av risikobildet
- 3.3 Risikohåndtering
  - 3.3.1 Behov/mulighet for mer effektive barrierer
  - 3.3.2 Etablere spesifikk barrierestrategi og spesifikke ytelseskrav
- 3.4 Kommunikasjon og konsultasjon
- 3.5 Overvåking og gjennomgåelse

Vedlikeholdets plass i hvert trinn er i liten grad beskrevet i barrierenotatet /1/ (jf. vedlegg C som gjengir barrierenotatets omhandling av vedlikehold/vedlikeholdsstyring). Påfølgende beskrivelser baserer seg på vår

oppfatning samt innspill fra Ptil og andre under arbeidsmøter og kommentarrunder. Vi forsøker også å eksemplifisere underveis i drøftingen, samt understøtte betydningen (og da særlig vedlikeholdets betydning) med data fra RNNP (/3/-/6/).

### 3.1 Kontekst

Hva inngår i "kontekst"? I ISO 31000 inngår kontekst både i rammeverket for risikostyringsprosessen og i selve risikostyringsprosessen (se figur 3.2).



**Figur 3.2** Kontekst som del av både rammeverk og prosess (basert på /1/ og /2/)

I tillegg til å skille mellom kontekst i rammeverket og i selve risikostyringsprosessen, skiller ISO 31000 også mellom ekstern og intern kontekst.

Det er stort sett de samme forhold som inngår i rammeverket og i prosessen, men fastleggelsen av konteksten er mer detaljert i selve risikostyringsprosessen, spesielt hvordan forholdene relateres til omfanget av den spesifikke risikostyringsprosessen /2/.

I barrierenotatet /1/ defineres kontekst som "eksterne og interne rammebetingelser som det skal tas hensyn til i barrierestyring" og det henvises til at dette samsvarer med ISO 31000 /2/. Videre beskrives det at kontekst er de rammebetingelser og føringer (eksterne, interne og prosjekt- og aktivitetsspesifikke) som er av betydning for gjennomføringen av de øvrige stegene i barrierestyringsprosessen.

I ISO 31000 /2/ er det svært mange forhold som inngår. Av de eksterne forholdene er:

- Politiske, forskriftsmessige, tekniske, økonomiske forhold, osv.
- Viktige drivere og trender som påvirker organisasjonens mål
- Oppfatninger og verdisyn hos eksterne interessenter

Av de interne forholdene inngår:

- Styling, organisasjonsstruktur, roller og ansvar
- Ressurser og kunnskap
- Form og omfang av kontraktsmessige forbindelser

Forhold relatert til risikostyringsprosessen:

- Definere ansvarsforhold
- Definere omfang, dybde og bredde av risikostyringsaktivitetene
- Definere risikovurderingsmetodikk
- Identifisere og spesifisere beslutninger som skal fattes

I barrierenotatet /1/ angis følgende forhold:

- Krav og føringer i regelverk, standarder og selskapsspesifikke retningslinjer
- Selskapsspesifikke strategier, målsettinger og prinsipper for risiko og barrierestyring
- Faktisk utforming og tilstand

Videre vektlegges det at man er bevisst *format og innhold av spesifikk barrierestrategi og spesifikke ytelseskrav* ved etablering av konteksten for å sikre at disse dokumentene blir utarbeidet og formidlet på en formålstjenlig og god måte. Det påpekes også at *kravet til risikoreduksjon (kontinuerlig forbedring)* må inkluderes som en del av konteksten. Dessuten hevdes det at etablering av *ambisiøse målsetninger og ytelseskrav* som del av konteksten kan forhindre forsinkelser, økte kostnader og mindre robuste løsninger.

Vi har her valgt å avgrense videre drøfting til følgende forhold (noen kombinerte):

- ✚ Krav og føringer i regelverk, standarder og selskapsspesifikke retningslinjer
- ✚ Definere ansvarsforhold og nødvendige interaksjoner/grenseflater
- ✚ Definere (risikovurderings-) metodikk
- ✚ Faktisk utforming og tilstand
- ✚ Viktige drivere og trender
- ✚ Oppfatninger og verdisyn hos eksterne interessenter
- ✚ Ressurser, kunnskap og kontraktsmessige forbindelser
- ✚ Krav til risikoreduksjon / kontinuerlig forbedring

### 3.1.1 Krav og føringer i regelverk, standarder og selskapsspesifikke retningslinjer

Spesielt viktig er kravene i aktivitetsforskriften /21/ kapittel IX om vedlikehold:

- Aktivitetsforskriften § 45: *Den ansvarlige skal sikre at innretninger eller deler av disse holdes ved like, slik at de er i stand til å utføre sine tiltenkte funksjoner i alle faser av levetiden.*
- Aktivitetsforskriften § 46: *Innretningers systemer og utstyr skal klassifiseres med hensyn til konsekvensene for helse, miljø og sikkerhet av potensielle funksjonsfeil. For funksjonsfeil som kan føre til alvorlige konsekvenser, skal den ansvarlige identifisere de ulike feilmodiene med tilhørende feilårsaker og feilmekanismer, og anslå feilsannsynligheten for den enkelte feilmodusen.*

Klassifiseringen skal legges til grunn ved valg av vedlikeholdsaktiviteter og vedlikeholdsfrekvens, ved prioritering av ulike vedlikeholdsaktiviteter og ved vurdering av reservedelsbehov.

- Aktivitetsforskriften § 47: Feilmodi som utgjør en helse-, miljø- eller sikkerhetsrisiko, jf. § 44, skal forebygges systematisk ved hjelp av et vedlikeholdsprogram. I programmet skal det inngå aktiviteter for overvåking av ytelse og teknisk tilstand, som sikrer at feilmodi som er under utvikling eller har inntrådt, blir identifisert og korrigert. Programmet skal også inneholde aktiviteter for overvåking og kontroll av feilmekanismer som kan føre til slike feilmodi.
- Aktivitetsforskriften § 48: Det skal utarbeides en samlet plan for utføring av vedlikeholdsprogram og korrigerende vedlikeholdsaktiviteter, jf. styringsforskriften § 12 [/22/]. Det skal foreligge kriterier for setting av prioritet med tilhørende tidsfrister for utføring av de enkelte vedlikeholdsaktivitetene. Kriteriene skal ta hensyn til klassifiseringen som nevnt i § 46.
- Aktivitetsforskriften § 49: Effektiviteten av vedlikeholdet skal evalueres systematisk på grunnlag av registrerte data for ytelse og teknisk tilstand for innretninger eller deler av disse. Evalueringen skal brukes til kontinuerlig forbedring av vedlikeholdsprogrammet, jf. styringsforskriften § 23 [/22/].
- Aktivitetsforskriften § 50: ... På rørledningssystemer der feilmodi kan utgjøre en miljø- eller sikkerhetsrisiko, jf. § 46, skal det utføres inspeksjoner for å kartlegge mulig feilmodi i rørledningssystemet. Deler av rørledningssystemet, der liggetilstanden eller andre forhold kan gi høy belastning, skal også kontrolleres. ...
- Aktivitetsforskriften § 51: Utblåsningssikringen med tilhørende ventiler og annet trykkkontrollutstyr på innretningen skal trykkprøves og funksjonsprøves, jf. § 45 og § 47. Utblåsningssikringen med tilhørende ventiler og annet trykkkontrollutstyr på innretningen skal heloverhales og resertifiseres hvert femte år.

### Aktivitetsforskriften § 45

Den ansvarlige skal sikre at innretninger eller deler av disse holdes ved like, slik at de er i stand til å utføre sine tiltenkte funksjoner i alle faser av levetiden.

Det er altså et krav om å vedlikeholde barrierer (så vel som alt annet utstyr), slik at de er i stand til å utføre sine tiltenkte funksjoner i alle faser av levetiden. Hvor enkelt er så dette? Vedlikeholdes barrierene slik at de møter ytelseskravene?

Fra RNNP /6/ finner vi følgende om ytelsen til barrierene:

Barriereindikatorene viser at det er store nivåforskjeller mellom innretningene. Noen innretninger har relativt sett dårlige resultater for enkelte barrieresystemer. Samlet sett er feilratene for stigerørs ESDV og trykkavlastningsventil over forventet nivå. På innretningsnivå observeres det at enkelte innretninger har til dels store avvik fra forventet nivå over flere år. Dette kan være en indikasjon på svekkede barrierer dersom svakheten ikke kompenseres for. Samlet sett er det mange enkeltinnretninger som for flere av barriereelementene har prestert dårligere eller betydelig dårligere enn bransjekravene, både i 2012 og i gjennomsnitt for hele perioden. Med det fokuset som bransjen den siste tiden har hatt på forebygging av storulykker, skulle en forvente at det burde være mulig å få til større forbedringer på dette området enn det dataene fra de senere årene viser.

RNNP viser at kravet i af § 45 ikke oppfylles for alle innretninger, og at noen innretninger har store utfordringer knyttet til barrierenes evne til å utføre sine tiltenkte funksjoner, enten dette skyldes vedlikehold eller andre forhold. Eksemplifisering av hvordan vedlikeholdet påvirker barrierenes ytelse er vist i kapittel 4.

### Aktivitetsforskriften § 46

*Innretningers systemer og utstyr skal klassifiseres med hensyn til konsekvensene for helse, miljø og sikkerhet av potensielle funksjonsfeil. For funksjonsfeil som kan føre til alvorlige konsekvenser, skal den ansvarlige identifisere de ulike feilmodiene med tilhørende feilårsaker og feilmekanismer, og anslå feilsannsynligheten for den enkelte feilmodusen. Klassifiseringen skal legges til grunn ved valg av vedlikeholdsaktiviteter og vedlikeholdsfrekvens, ved prioritering av ulike vedlikeholdsaktiviteter og ved vurdering av reservedelsbehov.*

Det er altså et krav om å klassifisere alle systemer og alt utstyr med hensyn på konsekvens. Blir dette gjort i tilfredsstillende grad? Hva er status?

Fra RNNP /6/ finner vi følgende om klassifisering:

*Klassifiseringen er fremdeles mangelfull for rundt 20 av de 73 [produksjons-] innretningene, men det er en liten forbedring i forhold til i fjor. Figuren [figur 104 s. 113] viser at de fleste flyttbare innretningene fremdeles har lave tall for både merking og klassifisering av systemer og utstyr. Noen har svært lave tall.*

*De fleste flyttbare innretningene kommer altså klart dårligere ut enn produksjonsinnretningene med hensyn til merking og klassifisering. Sett på bakgrunn av at systemer og utstyr skal merkes og klassifiseres med hensyn til de helse-, miljø- og sikkerhetsmessige konsekvensene av potensielle funksjonsfeil, er dette ikke tilfredsstillende.*

RNNP /6/ konkluderer altså med at systemer og utstyr ikke klassifiseres i tilfredsstillende grad for ca. en fjerdepart av produksjonsinnretningene og for mange av de flyttbare innretningene, dvs. at af § 46 trolig ikke er oppfylt for alle innretninger.

### Aktivitetsforskriften § 47

*Feilmodi som utgjør en helse-, miljø- eller sikkerhetsrisiko, jf. § 44, skal forebygges systematisk ved hjelp av et vedlikeholdsprogram. I programmet skal det inngå aktiviteter for overvåking av ytelse og teknisk tilstand, som sikrer at feilmodi som er under utvikling eller har inntrådt, blir identifisert og korrigert. Programmet skal også inneholde aktiviteter for overvåking og kontroll av feilmekanismer som kan føre til slike feilmodi.*

Det er altså krav om å overvåke ytelsen og den tekniske tilstanden til blant annet barrierene. Hva viser resultatene om overvåking av ytelsen?

Basert på RNNP /6/ kan vi avlede følgende om overvåking av ytelsen til barrierene:

Selv om ytelsen til barrierene ikke er tilfredsstillende for alle innretninger og alle barrierer (jf. drøfting av af § 45), så rapporterer alle innretninger data for overvåking av ytelsen. Ett unntak er at 8 av 41 flyttbare innretninger ikke rapporterte data for etterslep av FV og utestående KV for 2012, noe som ikke er betryggende, selv om dette ikke gjelder ytelsen direkte.

RNNP /6/ viser at ytelsen til barrierene overvåkes og rapporteres, og sånn sett oppfyller denne delen av af § 47. Det kan imidlertid stilles spørsmål ved fullstendigheten av de innrapporterte dataene, noe vi kommer tilbake til i kapittel 4.

Selv om vedlikeholdsindikatorne kun indirekte kan knyttes til barriereytelse, så bør alle innretninger evne å rapportere disse dataene i likhet med barriereindikatorne. Operatørene bør være forberedt på å rapportere inn data for alle indikatorne som RNNP etterspør.

### Aktivetsforskriften § 48

*Det skal utarbeides en samlet plan for utføring av vedlikeholdsprogram og korrigerende vedlikeholdsaktiviteter, jf. styringsforskriften § 12 [/22/]. Det skal foreligge kriterier for setting av prioritet med tilhørende tidsfrister for utføring av de enkelte vedlikeholdsaktivitetene. Kriteriene skal ta hensyn til klassifiseringen som nevnt i § 46.*

Dette er ikke direkte knyttet til data i RNNP, så vi vil drøfte dette på litt mer generelt grunnlag.

Når det gjelder prioritet, så skal det altså for det første foreligge kriterier for setting av prioritet, og dernest skal disse ha tidsfrister for utføring av vedlikehold. Dersom man først har kriterier er det liten grunn til at det ikke skal være fastsatt tilhørende tidsfrister, men det er to spørsmål som er interessante i denne forbindelse:

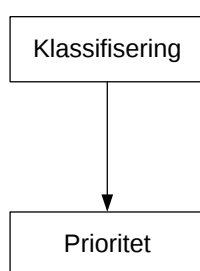
1. Har man kriterier for setting av prioritet, og dersom man har det, er "metoden" hensiktsmessig?
2. Evner man å overholde tidsfristene, dvs. unngå utestående vedlikehold knyttet til barrierene som overskrider tidsfristene?

Når det gjelder det første spørsmålet – om "metoden" for setting av prioritet er hensiktsmessig (og "sikkerhetsmessig forsvarlig") – skal vi se nærmere på hvordan i alle fall noen operatører praktiserer dette.

Svaret på spørsmål 1 har også betydning for spørsmål 2, fordi et viktig poeng her er hvordan barrierene (sikkerhetskritisk utstyr) klassifiseres og prioriteres. I RNNP rapporteres det blant annet antall timer korrigerende vedlikehold som ikke er utført innen fastsatt tidsfrist (*KV utestående, antall timer HMS-kritisk*), men inngår alle barrierer i denne kategorien (HMS-kritisk)? Eller tar man utgangspunkt i det utstyret som har høy prioritet, og blir i så fall alle barrierer gitt høy prioritet?

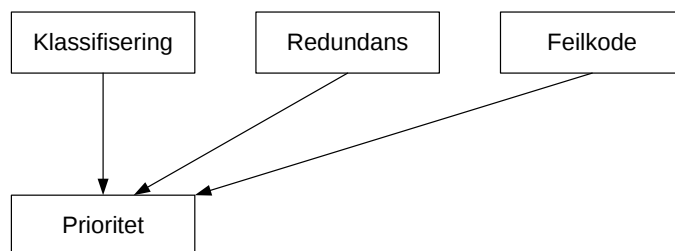
Vi starter med henvisningen til af § 46 og følgende: *Klassifiseringen skal legges til grunn ved ... prioritering av ulike vedlikeholdsaktiviteter ....*

Dette er illustrert i figur 3.3.



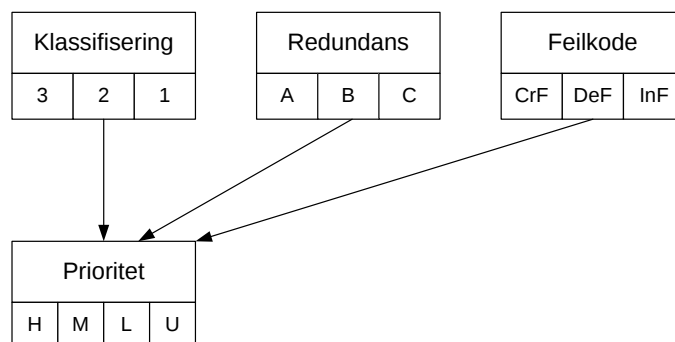
**Figur 3.3** Prioritering basert på konsekvensklassifisering

Noen operatører har imidlertid etablert en metode hvor også redundans og feilkode påvirker (og overstyrrer) klassifiseringen når det gjelder å sette prioritet på KV-jobber. Dette er illustrert i figur 3.4.



**Figur 3.4** Prioritering basert på redundans og feilkode i tillegg til konsekvensklassifisering

I figur 3.5 har vi også vist hvilke verdier klassifisering, redundans, feilkode og prioritet kan innta (mest kritisk til venstre, minst kritisk til høyre blant verdiene).



**Figur 3.5** Gradering/verdisetting av klassifisering, redundans, feilkode og prioritet

Prioritet kommer som et resultat av verdien på klassifisering, redundans og feilkode (gjennom ferdig etablerte matriser, som vi kommer tilbake til).

*Konsekvensklassifiseringen* for det aktuelle utstyret (aktuelt tagnummer) fastsettes ut fra utstyrets kritikalitet, eksempelvis ved hjelp av NORSOK Z-008 /23/, og er basert på en engangsanalyse (med eventuelt behov for senere oppdateringer). Verdien er altså her gitt for et gitt tagnummer.

*Redundans* (ekstra tilsvarende utstyrsenhet(-er)<sup>5</sup>) vil kunne medføre at prioriteringen blir lavere enn uten redundans (for eksempel fra H til M eller M til U). Fastsettelsen av redundans er, med unntak av vurderinger rundt krav, relativt enkel, og er en engangsvurdering på lik linje med konsekvensklassifiseringen. Klassifisering og redundans er dermed gitt.

Sikkerhetskritisk utstyr ("barriereelementer") skal ha konsekvensklassifisering "høy" (3) samt laveste redundansgrad A. (Redundans som er nødvendig for å oppnå påkrevd pålitelighet og tilgjengelighet for sikkerhetskritisk utstyr inkl. beredskapsutstyr skal ikke klassifiseres som redundant).

*Feilkode* ("Failure Impact") er imidlertid noe som vurderes av den enkelte hver gang det lages en notifikasjon etter at en feil har blitt oppdaget. Det skilles mellom tre grader av feil:

- |                            |   |                 |   |                       |
|----------------------------|---|-----------------|---|-----------------------|
| 1. Critical Failure (CrF)  | → | Kritisk feil    | → | "Dead" (Død)          |
| 2. Degraded Failure (DeF)  | → | Degradert feil  | → | "Seriously ill" (Syk) |
| 3. Incipient Failure (InF) | → | Begynnende feil | → | "Unwell" (Uvel)       |

<sup>5</sup> Existence of more than one means for performing a required function of an item. /36/

Feilkoden kan også "overstyre" og endre den opprinnelige prioriteten til hvilken som helst ny prioritet, det vil si at selv prioritet høy (H) kan endres til uprioritert (U). Den har derfor stor betydning, og det er svært viktig at den blir bedømt riktig, i alle fall ikke "underestimert".

Det gis ikke formelle retningslinjer for hvilke feilmøder for det enkelte utstyr som tilhører de tre feilkodene. Her er det opp til den enkelte å vurdere hvorvidt en gitt feil/feilmøde er å betrakte som kritisk, degradert eller begynnende. En liten "feil-vurdering" kan gi seg stort utslag i prioritet (som vi skal se nedenfor).

Figur 3.6 viser de matrisene som benyttes for å fastsette prioritet.

| Dead (CrF)   |   |   |   | Seriously ill (DeF) |   |   |   | Unwell (InF) |   |   |   |
|--------------|---|---|---|---------------------|---|---|---|--------------|---|---|---|
| Kritikalitet | A | B | C | Kritikalitet        | A | B | C | Kritikalitet | A | B | C |
| 3            | H | M | M | 3                   | M | L | L | 3            | U | U | U |
| 2            | M | L | L | 2                   | L | U | U | 2            | U | U | U |
| 1            | L | L | L | 1                   | U | U | U | 1            | U | U | U |

Høy (H) – tidsfrist 5 dager; Middels (M) – tidsfrist 30 dager; Lav (L) – tidsfrist 180 dager; Uprioritert (U) – tidsfrist 365 dager

**Figur 3.6** Matriser for fastsettelse av prioritet

Høy prioritet gjelder kun for det mest kritiske utstyret (kritikalitet 3), uten redundans (redundansgrad A) og med kritisk feil (CrF=Død). Kritikalitet og redundans er gitt, og vurderingen som gjenstår gjelder utelukkende feilkoden. Dersom den feilaktig blir vurdert som degradert (i stedet for kritisk) blir prioriteten middels (M) i stedet for høy (H), noe som gir 30 dager i stedet for 5 dager som tidsfrist for utbedring av feilen. Dersom den feilaktig blir vurdert som begynnende blir prioriteten uprioritert (U) i stedet for høy (H), noe som gir hele 365 dager i stedet for 5 dager som tidsfrist for utbedring av feilen. Det er altså avgjørende viktig at feilkoden ikke "undervurderes".

En underestimering kan altså redusere prioriteten betydelig, også for sikkerhetskritisk utstyr.

La oss nå returnere til de to spørsmålene vi startet med:

1. Har man kriterier for setting av prioritet, og dersom man har det er "metoden" hensiktsmessig?
2. Evner man å overholde tidsfristene, dvs. unngå utestående vedlikehold knyttet til barrierene som overskrider tidsfristene?

Når det gjelder spørsmål 1 så finnes det kriterier/metoder for setting av prioritet, og det må antas at alle operatører benytter en eller annen form for kriterium/metode, men den metoden vi har sett nærmere på her er ikke ubetinget "hensiktsmessig" fordi den er svært avhengig av en korrekt (i alle fall ikke underestimert) vurdering av feilkode (grad av feil).

Når det gjelder spørsmål 2 så fremgår det av RNNP dataene /6/ at innretningene har større eller mindre grad av utestående vedlikehold (dvs. overskridelse av tidsfristene), også det som er angitt som HMS-kritisk. Det som er minst like interessant er hvor utestående vedlikehold som følge av feil på barrierer inngår. Er dette kun i utestående vedlikehold med høy prioritet, eller fanger man også opp barrierefeil som er gitt lavere prioritet på grunn av feilkode "syk" eller "uvel".

Selv om man fanger opp barrierefeil som er gitt feilkode "syk" eller "uvel", og dermed en lavere prioritet, så er de lengre tidsfristene som er gitt for disse en utfordring i seg selv av minst to grunner. Det første er som

tidligere nevnt faren for at feilkoden er "underestimert" og at tidsfristen burde vært kortere, og det andre er muligheten for at tilstanden endrer seg i løpet av tidsfristen. Dette krever at man har god kontroll på eventuell endring fra "uvel" til "syk" eller fra "syk" til "død", mens utstyret venter på vedlikehold. Dette er en utfordring spesielt for det utstyret som er gitt feilkode "uvel" fordi de inngår i en normalt stor portefølje av uprioriterte vedlikeholdsjobber.

Konklusjonen er at af § 48 nok er oppfylt med hensyn til at operatørene har kriterier/metoder for setting av prioritet, men det skal ikke utelukkes at metoden(-e) kan gi utfordringer for barrierestyringen ved at enkelte kriterier (som for eksempel feilkode) kan overstyre kritikalitetsklassifiseringen med hensyn til prioritet på vedlikeholdsjobber.

Tidsfrister er også et krav i af § 48, men etterlevelsen av tidsfristene inngår ikke direkte som et krav i af § 48. Aktørene kan selv avviksbehandle overskridelse av egne tidsfrister, hvor det gjøres vurdering av behov for kompenserende tiltak for å opprettholde risikonivået.

Generelt kan en si at den omtalte metodikken peker mot et betydelig kompetansebehov i form av opplæring av operatører som fyller ut vedlikeholdsnotifikasjonene og tilhørende kvalitetssikring av disse.

Som diskutert andre steder i denne rapporten kan det dessuten stilles spørsmålsteget ved hvorfor det ikke er en tydelig og etablert kobling mellom de allokerede SIL kravene til utstyret og den kritikaliteten som dette utstyret får.

#### **Aktivitetsforskriften § 49**

*Effektiviteten av vedlikeholdet skal evalueres systematisk på grunnlag av registrerte data for ytelse og teknisk tilstand for innretninger eller deler av disse. Evalueringen skal brukes til kontinuerlig forbedring av vedlikeholdsprogrammet, jf. styringsforskriften § 23 [22/].*

Det er altså krav om systematisk evaluering av effektiviteten av vedlikeholdet, basert på data for ytelsen og teknisk tilstand, blant annet for barrierene.

Dersom ytelsen *ikke* er tilfredsstillende, må vedlikeholdsprogrammet tilpasses (for eksempel ved å intensivere det forebyggende vedlikeholdet) slik at ytelsen blir i henhold til kravene. Dersom ytelsen *er* tilfredsstillende, er det likevel påkrevd å forbedre effektiviteten av vedlikeholdet kontinuerlig. I tilknytning til barrierestyring er det altså ikke bare nødvendig å overvåke ytelsen til barrierene, men også evaluere og kontinuerlig forbedre effektiviteten av vedlikeholdet. Dette kan i praksis medføre at en for eksempel velger å teste utstyr mindre hyppig dersom ytelsen er bedre enn kravene, uten at dette medfører en uakseptabel endring i risikoen.

En evaluering av effektiviteten av vedlikeholdet knyttet til barrierer, på grunnlag av data for ytelsen til barrierene, inngår ikke direkte i RNNP-dataene. Dette krever nærmere analyser tilsvarende driftsgjennomgangene som er beskrevet i kapittel 4. Utvikling i barriereytelsen kan leses ut fra RNNP, men ikke i hvilken grad endringer skyldes vedlikehold.

### Aktivitetsforskriften § 50 og § 51

*... På rørledningssystemer der feilmodi kan utgjøre en miljø- eller sikkerhetsrisiko, jf. § 46, skal det utføres inspeksjoner for å kartlegge mulig feilmodi i rørledningssystemet. Deler av rørledningssystemet, der liggetilstanden eller andre forhold kan gi høy belastning, skal også kontrolleres. ...*

*Utblåsningssikringen med tilhørende ventiler og annet trykkkontrollutstyr på innretningen skal trykkprøves og funksjonsprøves, jf. § 45 og § 47. Utblåsningssikringen med tilhørende ventiler og annet trykkkontrollutstyr på innretningen skal heloverhales og resertifiseres hvert femte år.*

Her peker myndighetskravene direkte på kravet om å vedlikeholde barrierer; to sentrale barrieresystemer er trukket frem:

- 1) Rørledningssystemer som er "containment" barrierer
- 2) BOPen (som var én av flere barrierer som sviktet på Deepwater Horizon)

Disse er svært viktige med hensyn til henholdsvis å forhindre at hendelser initieres og stoppe en hendelse (utblåsning) i å utvikle seg.

### 3.1.2 Definere ansvarsforhold og nødvendige interaksjoner/grenseflater

Hvem er ansvarlig for å spesifisere barrierene? Hvem er ansvarlig for å etablere vedlikeholdsprogrammet? Det må defineres nødvendig grenseflate mellom disse miljøene.

Vi har hos selskapene sett manglende sammenheng mellom SIL nivå og kritikalitetsklassifisering for utstyr. Dette tyder på at det er mangelfull kommunikasjon mellom vedlikeholdsmiljøet og "de som holder på med SIL" (instrument/automasjon og teknisk sikkerhet). Resultatet kan for eksempel være at et HIPPS system (SIL 3) "behandles likt" med et PSD system (SIL 2 eller SIL 1).

### 3.1.3 Definere metodikk

Sikre at tilnærming/metodevalg for de som utarbeider vedlikeholdsprogram for barrierene er "kompatibelt" med andre miljø som også spesifiserer barrierer, for eksempel testintervall basert på RCM/NORSOK Z-008 versus testintervall basert på krav til SIL.

Et annet eksempel er å sikre at det utarbeides testprosedyrer som evner å teste "hele loopen" og under realistiske driftsforhold. Som nærmere diskutert og eksemplifisert i kapittel 4 ser en ofte eksempler på at ytelsen av mindre utstyr som inngår i sikkerhetsfunksjonen ikke verifiseres i forbindelse med normal funksjonstesting. Det kan også være en utfordring at utstyr testes under forhold (for eksempel trykløs prosess) som ikke representerer normal drift.

### 3.1.4 Faktisk utforming og tilstand (og implikasjoner for vedlikeholdsvennlighet)

Noen viktige forutsetninger er:

- Åpne/værutsatte områder.
- Generell tetthet av utstyr som ofte påvirker vedlikeholdsvennligheten.
- Plassering av utstyr – jf. utstyr/funksjoner som ikke lar seg teste (for eksempel høyt nivå i lagertanker hvor man ikke våger å utsette tanken for dette nivået, eller at tilkomst er umulig/vanskelig; for eksempel gassdetektorer som er plassert så høyt at en må ha stillas eller lift for å få testet dem).
- Tilstanden til en innretning (ny/gammel, godt/dårlig vedlikeholdt) generelt, og for barrierene spesielt, er del av konteksten ved at det påvirker vedlikeholdet som det må legges opp til.

### 3.1.5 Viktige drivere og trender

Blant viktige drivere og trender er eksempelvis:

- Økt bruk av tilstandsbasert vedlikehold på nye innretninger
- Økt implementering av integrerte operasjoner (IO)
- Stadige modifikasjoner av eksisterende innretninger, blanding av nytt og gammelt utstyr
- Økende omfang av subsea-/havbunnsinnretninger og utfordringer knyttet til ansvarsforhold, spesielt for interface-utstyr (topside/subsea)

### 3.1.6 Oppfatninger og verdisyn hos eksterne interessenter

En viktig ekstern interessent er Ptil og de oppfatninger og signaler Ptil gir blant annet gjennom RNNP og ved tilsyn. Fra RNNP 2012 /6/ kan man eksempelvis lese følgende:

*Det er samlet inn data om vedlikeholdsstyring i fire år. Tallene fra 2009 til 2012 viser at flere aktører har utfordringer med hensyn til det å oppfylle regelverkskravene til vedlikeholdsstyring. Flyttbare innretninger har de største utfordringene. Utfordringene er knyttet til merking og klassifisering av utstyr, til etterslep av forebyggende vedlikehold og til utestående korrigerende vedlikehold, inkludert HMS-kritisk vedlikehold.*

Utfordringene, slik RNNP viser, er en del av konteksten som selskapene må forholde seg til i sin etablering, implementering og oppfølging av barrierestyringen.

### 3.1.7 Ressurser, kunnskap og kontraktsmessige forbindelser

Dette gjelder blant annet ressurser i egen vedlikeholdsorganisasjon, kunnskap og kompetanse, samt innleide vedlikeholdsressurser og samarbeidet med disse (integrert, langsiktig, osv.).

### 3.1.8 Krav til risikoreduksjon / kontinuerlig forbedring

I rammeforskriften § 11 /24/ finner vi følgende krav:

*Skade eller fare for skade på mennesker, miljø eller materielle verdier skal forhindres eller begrenses i tråd med helse-, miljø- og sikkerhetslovgivningen, herunder interne krav og akseptkriterier som er av betydning for å oppfylle krav i denne lovgivningen. Utover dette nivået skal risikoen reduseres ytterligere så langt det er mulig.*

HMS-kritisk vedlikehold påvirker risikoen, noe som innebærer at også vedlikeholdet må forbedres kontinuerlig (så langt det er mulig). I forhold til barrierestyring er dette noe som den enkelte innretning må forholde seg til. Det må dermed etableres indikatorer som kan gi informasjon om utviklingen. Spesielt aktuelle er vedlikeholdsdata i RNNP, siden dette er noe alle innretninger uansett bes om å rapportere.

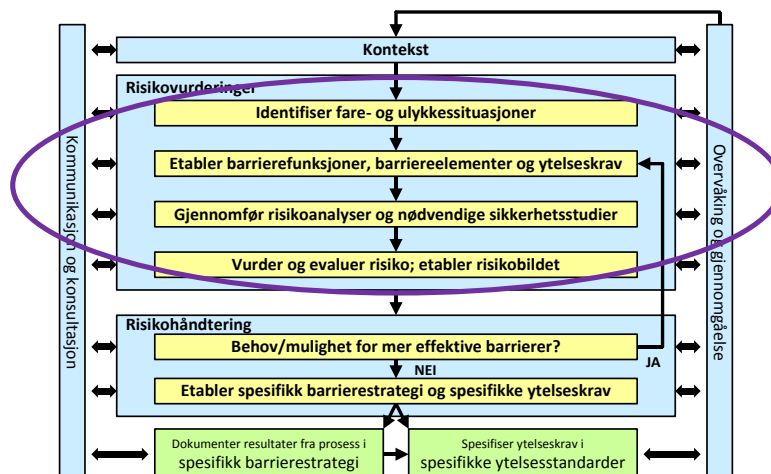
Dersom dette ikke allerede er gjort, så bør det legges til rette for innrapportering av vedlikeholdsindikatorer til RNNP.

Det er også verdt å bemerke at RNNP, som diskutert tidligere, viser at enkelte innretninger år etter år ikke oppfyller bransjestandard i forhold til ytelsen på utvalgte barriereelementer. Dette forteller noe om manglende evne til kontinuerlig forbedring.

## 3.2 Risikovurderinger

Risikovurderinger består av følgende fire trinn (som vist i figur 3.7):

1. Identifisere fare- og ulykkessituasjoner
2. Etablere barrierefunksjoner, barriere-elementer og ytelseskrav
3. Gjennomføre risikoanalyser og nødvendige sikkerhetsstudier
4. Vurdere og evaluere risiko; etablere risikobildet



**Figur 3.7** De fire trinnene som inngår i risikovurderinger

Disse er behandlet hver for seg i de påfølgende kapitlene.

### 3.2.1 Identifisere fare- og ulykkessituasjoner

RNNP statistikk /6/ viser at feil knyttet til vedlikehold (manglende eller mangelfullt utført vedlikehold) er en viktig årsak til for eksempel HC-lekkasjer; RNNP 2012 viser at 4 av 6 prosesslekkasjer kan relateres til vedlikehold (svekkelse, korrosjon, bolter som har løsnet, feilmontering). Tidligere års statistikk utfyller dette bildet ved blant annet å vise at mange lekkasjer skjer i forbindelse med inngrep i prosessanlegget /3/-/5/.

I henhold til NORSOK Z-013 /25/ skal det stilles krav til hvilke disipliner (herunder vedlikehold) som skal delta i HAZID for å sikre at alle relevante faresituasjoner identifiseres. Det er viktig at HAZID analysene inkluderer fare- og ulykkessituasjoner knyttet til forventede aktiviteter på og omkring innretningen, herunder vedlikeholdsrelaterte aktiviteter, jf. NORSOK Z-013; av aktiviteter/faser som skal dekkes inngår vedlikehold.

Det er også viktig at disse fareidentifiseringene og risikovurderingene blir innretningsspesifikke (og område-spesifikke) og ikke rent generiske, samt at det må identifiseres (av den ansvarlige) om det er spesielle/nødvendige vedlikeholdsoppgaver som for eksempel utføres med varm prosess og som krever spesielle barrierer.

### 3.2.2 Etablere barrierefunksjoner

En av målsettingene til HAZID (jf. NORSOK Z-013) er å identifisere risikoreduserende tiltak og at man dokumenterer/beskriver implementerte sikkerhetsbarrierer. Dette er i barrierestyringen (jf. barrierenotatet /1/) trukket ut som et eget trinn i prosessen. Prosessen med å etablere barrierefunksjoner, barriereelementer og tilhørende ytelseskrav vil typisk være en tverrfaglig oppgave som også dekker vedlikeholdsdisiplinen.

Det må vurderes på hvilken måte ytelseskravene til barriereelementene gir krav til testing og vedlikehold, og sørge for at dette inkluderes i vedlikeholdsprogrammet. Dette innbefatter:

- Frekvens/intervall
- Framgangsmåte - utarbeidelse av test- og vedlikeholdsprosedyrer

Det må også vurderes behov for at spesielle vedlikeholdsoperasjoner krever spesielle barrierer (jf. kapittel 3.2.1). Det bør dessuten gjøres en løpende vurdering av hvorvidt (minimums-) ytelseskrav som kommer fra standarder (og etablert praksis) er tilstrekkelig for den spesifikke innretningen og området. Er det for eksempel tilstrekkelig at en PSD ventil bruker to sekunder per tomme på å stenge?

### 3.2.3 Gjennomføre risikoanalyser og sikkerhetsstudier

Risikoanalyser som utføres som en del av beslutningsunderlaget for barrierestyring må planlegges og utføres slik at de er detaljerte nok og formålstjenlige, inklusive at de skal kunne formidles til ulike brukergrupper – inklusive vedlikeholdspersonell. Vedlikeholdspersonell må ha kjennskap til både hvilken risiko de utsettes for og hvordan de påvirker risikoen gjennom de vedlikeholdsaktiviteter de utfører, herunder oppfølging av forutsetninger relatert til vedlikehold som inngår i risikoanalysene. For eksempel forutsetter risikoanalysen av utstyr testes og vedlikeholdes i forhold til faste intervaller, noe som medfører at utsatt vedlikehold kan påvirke risikobildet negativt, og derfor bør holdes under kontroll.

Hva slags forutsetninger knyttet til vedlikehold er det egentlig risikoanalysene gjør? Man antar ofte en rekke gjennomsnittstall/-parametere som tilsvarer et eller annet "gjennomsnittlig vedlikeholds- og testeregime". Hvor realistisk er det å forutsette operasjon i henhold til prosedyrer, eller anta at detekterte feil på barrierer repareres umiddelbart og/eller medfører nedstengning?

Er det samsvar mellom forutsetninger og planlagt operasjon? Det er viktig at forutsetningene (inklusive forutsetninger knyttet til vedlikehold) formidles til drift slik at disse kan følges opp – de er krav/betingelser for sikker drift.

### 3.2.4 Vurdering og evaluering av risikobildet

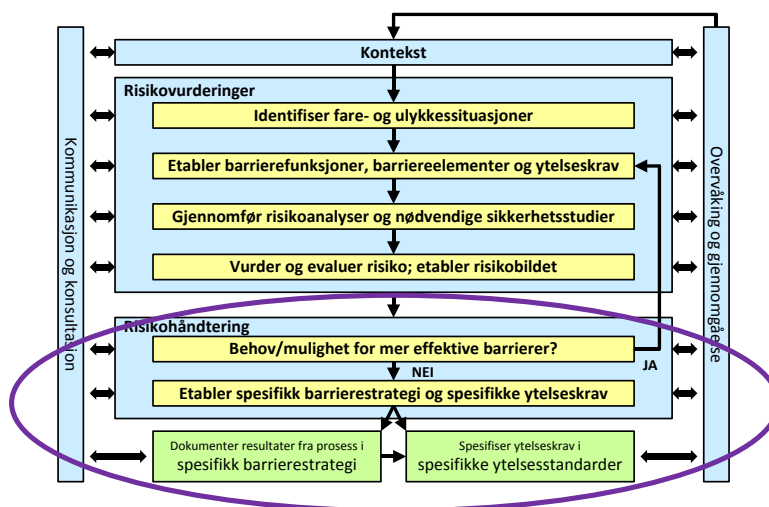
Resultatene fra gjennomførte risikoanalyser skal sammenlignes og vurderes mot etablerte beslutningskriterier. Generelt er det viktig at risikobildet etableres, nyanseres og evalueres med tanke på hva det faktisk skal brukes til (jf. barrierenotatet /1/).

Sammenligning mot beslutningskriterier/akseptkriterier kan medføre strengere (eller mildere) krav til testing av barrierene – med tilhørende justering av vedlikeholdsprogram. Det må også vurderes om de fastsatte kravene til frekvens av vedlikehold og testing er realistisk i forhold til drift sine begrensninger og ressurser (som i utgangspunktet er vurdert i kontekst, men som det kan være behov for å revurdere ved endring i kravene).

## 3.3 Risikohåndtering

Risikohåndtering består av følgende 2 trinn (som vist i figur 3.8):

1. Behov/mulighet for mer effektive barrierer?
2. Etablere spesifikk barrierestrategi og spesifikke ytelseskrav



**Figur 3.8** De to trinnene som inngår i risikohåndtering

Disse er behandlet hver for seg i de påfølgende kapitlene.

### 3.3.1 Behov/mulighet for mer effektive barrierer

Behovet for mer effektive barrierer vurderes av barriereansvarlige (for eksempel teknisk sikkerhetsmiljø), mens mulighetene (eksempelvis endring av testintervall) kan bedømmes av blant annet vedlikeholdspersonell, ut i fra at data for verifikasjon av ytelsen til barrierene kommer fra vedlikeholdsinformasjons-systemer. Det er derfor viktig med tett samarbeid mellom disse fagmiljøene.

Behovet for mer effektive barrierer må bedømmes for den enkelte innretning og den enkelte barriere, men data fra RNNP /6/ viser at i alle fall noen innretninger har et slikt behov:

*Barriereindikatorene viser at det er store nivåforskjeller mellom innretningene. Noen innretninger har relativt sett dårlige resultater for enkelte barrieresystemer.*

### 3.3.2 Etablere spesifikk barrierestrategi og spesifikke ytelseskrav

Noen av spørsmålene som må besvares i forbindelse med etableringen av spesifikk barrierestrategi og spesifikke ytelseskrav er:

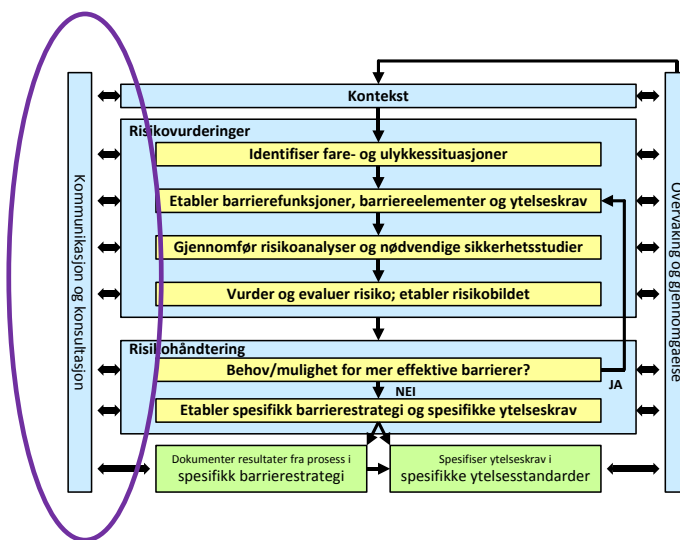
- Er det tilstrekkelig knytning og samsvar mellom barrierestrategi, ytelseskrav og det spesifiserte vedlikeholdsprogrammet?
- På hvilken måte påvirker barrierestrategien og ytelseskravene/ytelsesstandardene test- og vedlikeholdsprogrammet?
- Er utstyrshierarkiet i vedlikeholdssystemet brutt ned på et hensiktsmessig nivå, slik at krav og historikk kan knyttes til det enkelte barriereelement?
- Settes det spesielle krav knyttet til ytelsespåvirkende faktorer som påvirker vedlikeholdet? Slik som kompetanse av personell, innhold i prosedyrer, osv.?

### 3.4 Kommunikasjon og konsultasjon

Den ansvarlige skal sikre at kommunikasjon og konsultasjon (se figur 3.9), med både interne og eksterne interessenter, er formålstjenlig gjennom hele barrierestyringsprosessen.

Dette inkluderer god kommunikasjon med vedlikeholdsfunksjonen internt og eventuelt eksternt i den grad man anvender vedlikeholds-kontraktører.

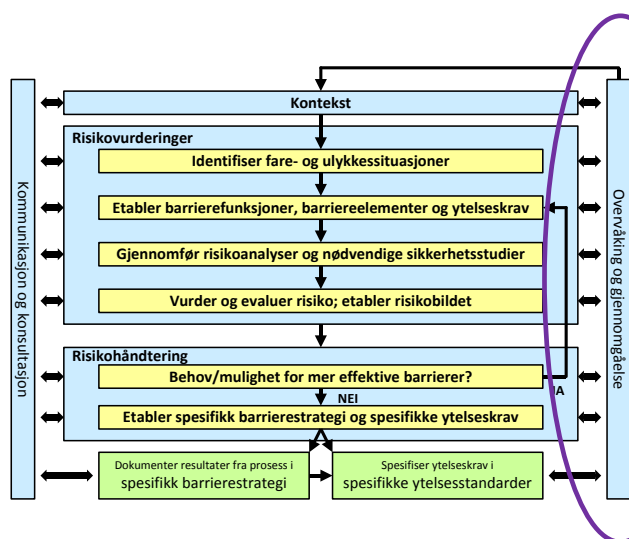
Et forhold det er satt mye fokus på i PDS<sup>6</sup> forum, er manglende kommunikasjon mellom leverandører og operatører i forhold til utveksling av feilhistorikk på utstyr. Dette er spesielt påpekt av leverandører av sikkerhetssystemer.



**Figur 3.9** Kommunikasjon og konsultasjon

<sup>6</sup> Se [www.sintef.no/pds](http://www.sintef.no/pds).

### 3.5 Overvåking og gjennomgåelse



Overvåking og gjennomgåelse er siste trinn i barriereprosessen, som vist i figur 3.10.

Barrierenes ytelse må overvåkes, følges opp og om mulig forbedres gjennom hele levetiden. Her har vedlikeholdsfunksjonen en sentral rolle i å verifisere barrierelytelsen.

I tillegg skal det holdes kontroll med vedlikeholdet som et sentralt ytelsespåvirkende forhold.

Dette er utdypet i kapittel 2.

**Figur 3.10** Overvåking og gjennomgåelse

--- ● ---

Vi har i kapittel 3 tatt for oss vedlikeholdets rolle i hvert av trinnene i barrierestyingsprosessen. I kapittel 4 gir vi konkrete eksempler på vedlikeholdets betydning for god barrierestyling.

## 4 Konkrete eksempler på vedlikeholdets betydning for god barrierestyring

Vi vil i dette kapitlet belyse vedlikeholdets rolle i barrierestyringen ved å se nærmere på et eksempel knyttet til *gjennomgang av sikkerhetskritiske feil* i driftsfasen. Målsettingene med en slik operasjonell gjennomgang er blant annet:

- 1) Å identifisere og klassifisere feil på sikkerhetskritisk utstyr.
- 2) Å sammenligne antallet sikkerhetskritiske feil med akseptabelt antall feil for de vurderte utstys-gruppene.
- 3) Å skaffe seg en oversikt over statusen på sikkerhetskritisk utstyr.
- 4) Å foreslå tiltak som kan bidra til forbedret drifts- og vedlikeholdsoppfølging, deriblant forslag til nye testintervall.

Vi bruker eksemplet til å se på hvordan vedlikeholdet påvirker hyppigheten av sikkerhetskritiske feil. Vi forsøker dessuten å knytte funn og observasjoner opp mot metode og resultater fra RNNP.

### 4.1 Bakteppe

#### *Myndighetskrav*

Ptil sitt regelverk setter krav til at barrierer skal ha ytelseskrav og at ytelseskravene skal verifiseres blant annet ved at relevante data samles inn og brukes for å vurdere ytelsen.

Myndighetene gir overordnede krav til oppfølging av sikkerhetssystemer, blant annet følgende:

- I Petroleumstilsynets regelverk sies det blant annet i innretningsforskriften /26/ § 8 (Sikkerhetsfunksjoner) at: *Det skal være spesifiserte ytelseskrav til den enkelte barrierefunksjon, barrieresystem og sikkerhetskritisk komponent.*
- Styringsforskriften /22/ § 19 (Innsamling, bearbeiding og bruk av data), samt aktivitetsforskriften /21/ § 45 (Vedlikehold) sier at *data må samles inn og brukes for å vurdere ytelsen.*
- Styringsforskriften § 5 (Barrierer) sier at *det skal utarbeides og fastsettes strategier for barrierefunksjoner/-systemer og tilhørende pålitelighets- og ytelseskrav.*
- Petroleumstilsynet refererer til IEC 61508/61511 /27-28/ («SIL») og OLF 070 /29/ som uttrykker pålitelighetskrav til instrumenterte sikkerhetssystemer (SIS).

Vi vil her bruke utvalgte SIS som eksempel på barrieresystem.

#### *RNNP statistikk*

RNNP statistikk /6/ viser at ytelsen til sentrale barriereelementer ikke opprettholdes i henhold til selskapenes egne krav. Dette er basert på statistikk fra tester av barriereelementene.

Noen eksempler fra RNNP /6/ er: Midlere andel feil for stigerørs ESV og for blowdown ventiler ligger over "bransjekravet"<sup>7</sup>. For 2012 var blant annet midlere andel feil for stigerørs ESV på 0.021 mens kravet var 0.01 og for blowdown ventiler var midlere andel feil på 0.020 mens kravet var på 0.005.

---

<sup>7</sup> Som i dette tilfellet er basert på Statoils interne GL0114; *Safety critical failures*.

Også for en rekke andre sentrale barriereelementer ser vi at enkeltinnretninger ligger over bransjekravet. Eksempler her er gassdeteksjon (10 innretninger over kravet i 2012) og DHSV (hvor 14 innretninger overstiger bransjekravet i 2012) /6/.

## 4.2 Vedlikeholdets rolle

Vedlikeholdet har tre prinsipielle roller i forhold til barriereelementer:

1. Funksjonstesting for å verifisere ytelsen til barriereelementene
2. Forebyggende vedlikehold (FV) for å forhindre at sikkerhetskritiske feil oppstår
3. Korrigerende vedlikehold (KV) for å gjenvinne funksjon

I forbindelse med korrigerende vedlikehold er det også viktig å avdekke årsaker til feilene slik at gjentakende feil kan unngås.

Fra dette kan vi avlede følgende tre spørsmål:

- Er det slik at alle kritiske feil avdekkes ved testing – eller for å si det på en annen måte: Er RNNP statistikken – som kun inneholder feil fra testing – dekkende? Eller kan situasjonen faktisk være verre enn det RNNP viser?
- Når en ser på typiske sikkerhetskritiske feil av barriereelementer – hvor stor del av dette skyldes manglende eller mangelfullt vedlikehold?
- I hvilken grad evner vedlikeholdet å forhindre gjentakende feil?

For å belyse disse spørsmålene vil vi bruke erfaringer og resultater fra *gjennomgang av sikkerhetskritiske feil* slik det er gjennomført på flere offshore-innretninger og landanlegg som en basis. Denne metodikken er noe SINTEF/NTNU har utviklet gjennom PDS prosjektet /30/ i samarbeid med én operatør (og én innretning), og har senere blitt anvendt på en rekke innretninger og anlegg. Vi vil bruke ESD ventiler og blowdown ventiler som eksempel siden dette er to av elementene som peker seg ut som spesielt problematiske, jf. RNNP /6/.

## 4.3 Føringer og antakelser fra design

IEC standardene /27-28/ krever at hver instrumenterte sikkerhetsfunksjon (SIF) skal tilordnes et SIL krav. Et SIL krav inkluderer blant annet *strukturelle krav* (som redundans og andel sikre feil), krav til *arbeidsmetodikk og tiltak* for å unngå systematiske feil og også et kvantitativt *PFD krav* (Probability of Failure on Demand). Det skal i design settes krav og vises at disse kravene kan oppnås (gitt en rekke antakelser) og det skal i drift verifiseres at krav og antakelser faktisk er oppfylt.

For å kunne oppfylle det kvantitative PFD kravet ligger det blant annet antatte feilrater (og testintervall) for utstyret til grunn. Som et eksempel kan vi anta at ESD funksjonene på en innretning har fått et SIL 2 krav. Da skal PFD for disse funksjonene være:  $10^{-2} > PFD > 10^{-3}$ . Dette kan for en gitt funksjon for eksempel oppfylles dersom den antatte kritiske feilraten ( $\lambda_{DU}$ )<sup>8</sup> for tilhørende ESD ventil er:  $\lambda_{DU} = 1 \cdot 10^{-6}$  feil per time, og testintervallet  $\tau = 8760$  timer. Dvs. en forutsetter årlig funksjonstesting som også inkluderer lekkasjetest for de ventilene som har krav om å holde tett.

<sup>8</sup> DU – Dangerous Undetected (farlige udetekterte [feil]), se kapittel 4.4.2 for feilklassifisering.

Basert på den antatte feilraten fra design kan denne nå benyttes til å stipulere antall forventede (eller akseptable) feil for en gitt populasjon og en gitt tidsperiode:  $E(X) = n \cdot t \cdot \lambda_{DU}$ . Her er  $E(X)$  forventede antall feil  $X$ ,  $n$  er antall komponenter i en gitt populasjon,  $t$  er observasjonsperioden og  $\lambda_{DU}$  er feilraten som er antatt fra design for utstyret.

Dersom vi fortsetter eksemplet med ESD ventiler og antar at  $n = 30$ ,  $\lambda_{DU} = 1 \cdot 10^{-6}$  feil per time og observasjonstid  $t = 4$  år, så blir forventede antall feil for denne populasjonen:  $E(X) = 30 \cdot 35040 \cdot 1 \cdot 10^{-6} \approx 1.1$ . Dette tilsvarer da at en kan forvente eller akseptere maksimum én DU feil hvert 4 år (for de 30 ventilene til sammen).

I RNNP og hos flere selskap benytter en *antall feil på antall tester* som akseptkriterium. Det er da verdt å merke seg følgende: (1) en tar ikke hensyn til at DU feil kan oppstå/avdekkes mellom tester og (2) det er ikke alltid samsvar mellom tillatte feilfrekvenser og SIL krav, noe som kan medføre for lave akseptkrav i forhold til nødvendige krav.

## 4.4 Oppfølging i driftsfasen

I dette kapitlet beskriver vi (deler av) framgangsmåten som benyttes i en gjennomgang av sikkerhetskritiske feil i driftsfasen. Vi har eksemplifisert dette ved å anta at operatøren benytter seg av SAP<sup>9</sup>, som er et av flere vedlikeholdssystemer i bruk i norsk petroleumsindustri.

### 4.4.1 Fremgangsmåte og omfang

Når operatøren avdekker en feil på et utstyr skal det opprettes en såkalt M2 notifikasjon ("M2 Malfunction Report") i SAP. M2 brukes til å rapportere en feilsituasjon (tilløp til feil eller svikt) samt til å rekvirere, prioritere og beskrive arbeid som ønskes utført. Foruten vanlig beskrivelse av feil, rapporteres også historikk på notifikasjon ved enkle kodevalg fra menyer.

En M2 kan resultere fra feil avdekket ved test eller feil avdekket på andre måter (tilfeldig, ved diagnostikk/overvåkning, under vedlikehold eller inspeksjon, ved behov, osv.). Hvordan feilen oppdages inngår som en del av kodevalget i M2 notifikasjonen.

Resultater fra årlige tester kan oppsummeres gjennom en egen testrapport. Dette er en rapport i SAP som gir en oversikt over antall gjennomførte tester og antall tester som feilet for utvalgte sikkerhetskritiske utstyrsgupper (innenfor en angitt tidsperiode) og som det derfor er skrevet M2 notifikasjoner for. Denne testrapporten i SAP inkluderer altså kun feil avdekket ved funksjonstesting og danner normalt grunnlaget for rapportering inn til RNNP.

Eksempel på rapportering av feil i SAP i form av en M2 notifikasjon (med "failure impact"<sup>10</sup>, "detection method" og "failure mode") er vist i figur 4.1.

Ved *gjennomgang av sikkerhetskritiske feil* går en manuelt gjennom alle M2 notifikasjonene for hver av de spesifiserte utstyrsguppene for (1) å kvalitetssikre notifikasjonene og testrapporten spesielt og (2) for å

<sup>9</sup> Vi velger å eksemplifisere med SAP, siden det er det mest brukte systemet/verktøyet for vedlikeholdsstyring.

<sup>10</sup> Betegnet som feilkode (eller grad av feil) i kapittel 3.1.1.

dekke alle kritiske feil, ikke bare de som er oppdaget ved testing. Typisk gjennomgås rundt 300-600 notifikasjoner i en årlig gjennomgang.

Gjennomgangen utføres vanligvis som en samhandling mellom fagansvarlig instrument/ automasjon, teknisk sikkerhet og fagansvarlig vedlikeholdsstyring. Dessuten deltar annet relevant personell (slik som teknisk systemansvarlig) etter behov. En slik tverrfaglig gruppe er gunstig da den kan se på tvers av fag og systemer og dermed avdekke forhold en ellers ville oversett, samt få en felles forståelse av status.

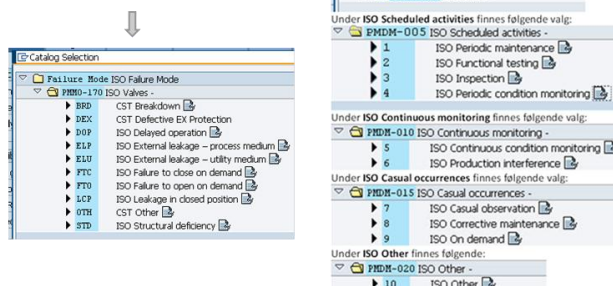
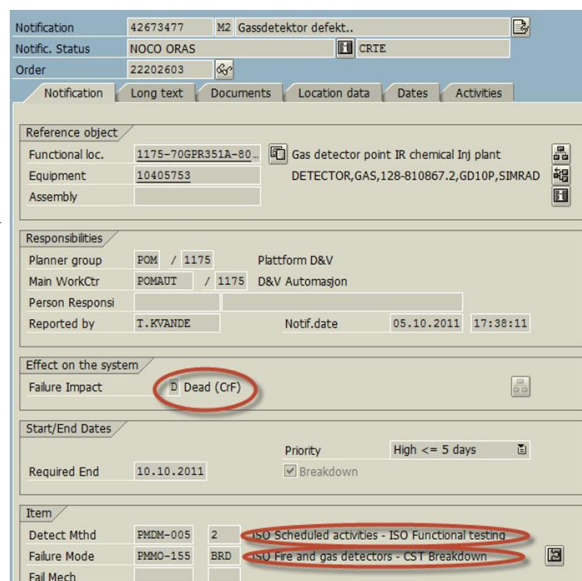
## Rapportering av feil

### • Failure impact

- Hvordan virker svikten inn på systemet/funksjonen
- U Uvel Utbedring av 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 Dad Utstyret har sviktet eller satt ut av drift for å redusere skadeomfang eller skaderisiko

### • Detection method

### • Failure mode

The image shows a SAP Notification form for a gas detector defect. The form includes fields for Notification number (42673477), Status (M2), and Equipment (10405753). It also shows the 'Effect on the system' section with 'Failure Impact' set to 'Dead (CrF)'. The 'Start/End Dates' section shows a 'Required End' date of 10.10.2011. The 'Item' section shows the 'Detect Mthd' as 'PMDM-005' and the 'Failure Mode' as 'PMDM-155'. Red circles highlight the 'Dead (CrF)' failure impact and the 'PMDM-005' and 'PMDM-155' codes.

**Figur 4.1** Rapportering av feil i SAP

Eksempler på hva en typisk avdekker:

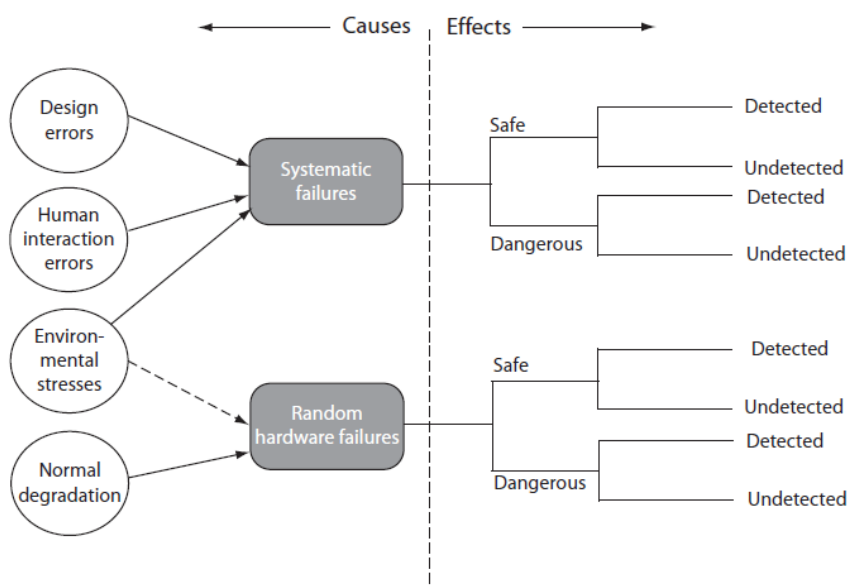
- En forholdsvis stor grad av feilrapportering. Dette fordi de anvendte kodene ikke bestandig er helt rett fram å forstå og derfor brukes feil. Dette gjelder spesielt "failure impact", "detection method" og "failure mode".
- En ser at mange kritiske feil avdekkes på andre måter enn ved testing, noe som tilsier at test-rapporten, som er basis for RNNP rapporteringen, ikke dekker hele bildet.
- Det er ofte nødvendig å gå inn i langtekst-feltet samt diskutere med fagfolk for å foreta en riktig klassifisering av rapporterte feil.

Med andre ord er det grunn til å være "konstruktivt skeptisk" til verktøy og tilnærminger som kun baserer seg på automatisk rapporterte data. En viss grad av manuell kvalitetssikring er viktig, også dersom en ønsker å avdekke bakenforliggende årsaker som basis for utarbeidelse av forbedringstiltak.

#### 4.4.2 Feilklassifisering

Feil som kan påvirke funksjonens evne til å stenge ned (eller gå til sikker posisjon) ved behov er i IEC 61508/61511 /27-28/ definert som farlige feil (Dangerous = D). Disse er igjen delt opp i udetekterte (skjulte) feil (Dangerous Undetected = DU) som kun vil oppdages ved en funksjonstest eller ved en reell anvendelse ("demand") av funksjonen, og detekterte feil (Dangerous Detected = DD) som oppdages når feilen oppstår (ved selvtest eller på annen måte via SAS systemet). I tillegg har en sikre feil (Safe = S) som ikke forhindrer selve sikkerhetsfunksjonen, men som typisk kan medføre at utstyret tripper (utløses/aktiveres) utilsiktet og som dermed kan påvirke driftstilgjengeligheten (for eksempel at en ESD stengeventil ikke åpner igjen).

Mens DU, DD og S relaterer seg til den *effekten* som en utstyrsfeil vil ha for sikkerhetsfunksjonen, så er det også interessant å se på *årsakene* til en feil. Ofte skiller en mellom *tilfeldige hardware feil* pga. aldring og slitasje og *systematiske feil* som typisk kan relateres til design, software, installasjon eller hvordan utstyret opereres og vedlikeholdes. Forholdet mellom årsak til og effekt av feil er illustrert i figur 4.2 (på engelsk).



**Figur 4.2** Feilklassifisering av instrumenterte sikkerhetsfunksjoner/sikkerhetssystem

I forbindelse med gjennomgangen av M2 notifikasjonene klassifiseres alle feilene i henhold til IEC 61508/61511 som DU, DD eller S (eller NA) og antall DU feil for hver utstyrsguppe kan deretter sammenlignes opp mot akseptkriteriet. I tillegg ser en på årsaken til feilen i de tilfeller slik informasjon er tilgjengelig.

#### 4.4.3 Feil oppdaget ved test versus feil oppdaget i normal drift

Et interessant spørsmål, blant annet knyttet til feilfrekvenser rapportert i RNNP, er å se på hvor stor andel av feilene som avdekkes under testing (jf. testrapporten) sammenholdt med det totale antall feil som en finner ved å gå gjennom alle M2 notifikasjoner.

For noen typer utstyr vil testing dominere behovsraten og testrapporten vil da være rimelig riktig, da de fleste feil oppdages ved testing (eksempelvis for brann- og gassdetektorer), mens for annen type utstyr vil "normal

bruk” kunne være dominerende behov/anvendelse ("demand"). Et eksempel er branndører som typisk testes to-fire ganger i året, men som ofte er i bruk daglig. For disse oppdages farlige feil vanligvis ved normal bruk. For utstyr slik som ventiler kan en DU feil også oppdages tilfeldig ved at en for eksempel har behov for å stenge ventilen under en vedlikeholdsjobb eller når en tilfeldig oppdager at ventilen ikke fungerer når en forsøker å operere ventilen fra kontrollrommet.

Det er derfor viktig at en i gjennomgangene ser på farlige feil oppdaget både ved testing og ved reelle behov/tilfeldig. Dette er i henhold til definisjon i IEC 61508/61511 ("SIL") og er dessuten i henhold til myndighetenes krav om å ha kontroll på anlegget og helheten.

Det er også viktig å ta hensyn til hvorvidt testene er fullstendige, om de gjøres under reelle driftsbetingelser, osv., men dette er tema vi ikke vil forfølge nærmere her.

*Eksempel fra en driftsgjennomgang i 2012(presentert på sikkerhetssystemkonferansen 2013):*

I en testrapport direkte fra SAP vises ni farlige udetekterte feil (DU feil) funnet under testing av sikkerhetskritisk utstyr. Etter manuell gjennomgang av alle notifikasjoner på sikkerhetskritisk utstyr, finner vi at det ved test eller reelt behov i normal drift er 19 farlige feil (DU feil). Det vil si at mindre enn halvparten av de farlige feilene ble oppdaget ved testing, og at mer enn halvparten ble oppdaget i normal drift.

#### 4.4.4 Nytteverdi av driftsgjennomganger

Generelt gir en slik operasjonell gjennomgang en god oversikt over status på integriteten til sikkerhetskritisk utstyr for en innretning. Med å gjennomføre en årlig gjennomgang av feil på sikkerhetskritisk utstyr, vil en indikere *svakheter ved vedlikeholdsstrategi*, mulige svakheter i design, feil bruk av komponenter og utstyr, samt om *testintervall er fornuftig*. En slik gjennomgang kan videre benyttes som basis for å identifisere nødvendige forbedringstiltak.

Gjennomgangen dokumenteres i form av en rapport som også kan benyttes til å studere trender og resultater fra år til år og se hvorvidt man har en økende feilfrekvens. I tillegg verifiserer gjennomgangen også:

- utfylling, koding og klassifisering av alle notifikasjoner
- utført vedlikehold
- antall tester utført på utstyret
- klassifisering av tag

### 4.5 Resultater og observasjoner fra driftsgjennomgangene

#### 4.5.1 Resultater fra gjennomgang av ventiler (ESV og BDV)

For å kunne si noe om vedlikeholdets betydning for hyppigheten av sikkerhetskritiske feil, er det nødvendig å se nærmere på faktiske feilårsaker. Eksempler på typiske feil på ESD ventiler (ESV), basert på feilrapporter og årsaksvurderinger, er:

- Ventiler går tregt / henger i åpen posisjon (korrosjon, forurensninger)
- Ventil stenger ikke helt pga. rust og sand i ventilhuset
- Dårlig fjær i aktuator (rust, slitasje, deformasjon, slakk)

- Ventiler stenger ikke pga. kald hydraulikkolje (manglende heat-tracing)
- Ventiler stenger ikke / går for sakte pga. forurensninger og ulike problemer med hydraulikkblokka
- Ventil stenger ikke fordi solenoiden henger ("stuck")
- Ventil stenger ikke pga. svikt i pilot til solenoiden (må rengjøres/skiftes)
- Ventiler som ikke fungerer pga. isdannelse (ikke tilstrekkelig isolasjon)
- For lang lukketid/åpningstid (f.eks. pga. feil med strupeventil, utilstrekkelig kapasitet, lekkasje i akkumulatorer, feil innstilt avblødning, osv. )
- Ventil stenger ikke pga. for lite kraft på aktuator (dobbeltvirkende) / Ventiler ikke designet for faktisk operasjonelt trykk

Vi ser av lista at dette primært er en blanding av designsvakheter og manglende/mangelfullt vedlikehold.

Eksempler på typiske feil på blowdown ventiler (BDV), basert på feilrapporter og årsaksvurderinger, er:

- BDV åpner for sakte pga. feiljustert hastighetsregulator / avblødning på luftakkumulator / begrenset kapasitet i avblødningsventil
- Diverse feil på åpningstider (ventiler åpner for sent/sakte) knyttet til utfordringer med sekvensiell blowdown
- BDV åpner ikke pga. avsetninger ("debris") på ventilkula
- BDV åpner ikke pga. hydrat/is i ventil
- BDV "setter seg" pga. for sjelden kjøring
- Ni blowdown ventiler feilet pga. lekkasjer i pneumatikkssystem som medfører utilstrekkelig lufttilførsel til ventilakkumulatorer (tre feil oppdaget ved testing og seks oppdaget i normal drift)
- Seks BDVer åpnet ikke pga. rust / værutsatt ventil. Selv etter at værbeskyttelse ble montert har rust på aktuator vært et problem for disse ventilene

Vi ser igjen av lista at dette er en blanding av designsvakheter og manglende eller mangelfullt vedlikehold. Når det gjelder designsvakheter kan en del av dette knyttes opp mot dårlig ventildesign / dårlig kvalitet eller at ventiler ikke er egnet for den bruken og det miljøet de er plassert i. Slike feil kan ikke direkte tilskrives manglende vedlikehold. På den annen side; dersom en har valgt en design som er uegnet så bør jo test- og vedlikeholdsprogrammet legges opp deretter. Vi registrerer også at mange og gjentakende feil på sikkerhetskritisk utstyr, som skyldes dårlig eller upassende design, ofte ender opp med at en bytter ut alt det relevante utstyret, men at dette gjerne tar mange år og til tider uforholdsmessig lang feilhistorikk. Dvs. at "det skurer og går med altfor mange feil altfor lenge".

En generell observasjon, som kan forklare noe av grunnen til gjentakende feil, er at ventiler svikter men ofte kjøres flere ganger til de fungerer, og deretter settes i drift igjen uten at en har funnet årsaken. Dette resulterer i gjentakende feil og notifikasjoner på samme utstyr (og gis i verste fall "godkjent test"<sup>11</sup>), og kan derfor føre til usikkerhet rundt datagrunnlaget i RNNP.

En annen observasjon er at mange feilmodi opptrer som fellesfeil og dermed slår ut flere ventiler samtidig. Dette er interessant sett i lys av krav i af § 47 (forebygging av feilmodi som utgjør et sikkerhetsproblem), og da spesielt siden slike feil fører til tap av redundans i anlegget (jf. forsvar i dybden).

---

<sup>11</sup> Jf. RNNP /6/ s.120: Datakvaliteten knyttet til enkelte av barriereelementene er ikke på det ønskede nivå. Funn tyder for eksempel på at enkelte aktører smører opp ventiler før test og at en ikke rapporterer sviktende test dersom de påfølges av en vellykket test. Denne type feil betyr at tilgjengeligheten til barriereelementet er dårligere enn testresultatene skulle tilsi.

Når en ser bort fra designsvakheter og manglende heat-tracing eller isolasjon, ser vi at øvrige feil på ventiler direkte eller indirekte kan tilskrives mangler ved selve vedlikeholdet eller styringen av vedlikeholdet og inkluderer for eksempel:

- Gjentakende feil – rotårsak ikke avdekket
- Forurenset hydraulikkolje (manglende skifte av filter, osv.)
- Rust, sand og korrosjon; manglende rengjøring, smøring og overhaling av ventilhus
- Tregheter i hydraulikkblokka – mangelfull smøring og rengjøring av deler
- Feiljustering av hastighetsregulator/strupeventiler (for sen avblødning av luft/hydraulikk)
- Feil og mangler inkl. lekkasjer i hjelpesystemer (luftsysteem) som ikke er utbedret fortløpende.

Dette indikerer at vedlikeholdets betydning for å redusere antall sikkerhetskritiske feil på ventiler er betydelig.

#### 4.5.2 Observasjoner og funn fra driftsgjennomganger

Noen øvrige observasjoner og funn fra driftsgjennomgangene er:

- i. Mange eksempler på gjentakende feil fordi rotårsak ikke har blitt avdekket og/eller fjernet.
- ii. Mange feil (for eksempel på detektorer) blir liggende uten at kompenserende tiltak blir implementert (utover at en "er klar over" feilen).
- iii. Utstyr som ikke er klassifisert som sikkerhetskritisk, men som burde vært det.
- iv. En god del feilklassifiserte notifikasjoner. For eksempel at feil funnet under testing er rapportert med «Detection method: ISO Periodic Maintenance» i stedet for «ISO Functional Testing», og dermed ikke kommer med i testrapporten.
- v. Mange feil på "diverse mindre utstyr" ligger rapportert mot tilfeldig/feil tag (av type solenoider, I/O kort, barrierer, endebrytere, transmittere, logikkfeil, osv.) og får dermed ikke en konsistent oppfølging. Dette er utstyrsfeil som ofte er kritisk for at sikkerhetsfunksjonen skal fungere. Spesielt ser vi at en del feil som kan knyttes opp mot logikk og I/O kort ikke registreres mot riktig tag, eller ikke har tilpasset tag. Siden leverandører av sikkerhetssystemer ofte opererer med særdeles optimistiske feilrater på utstyret sitt, vil det være interessant å få til en mer systematisk rapportering og innsamling av slike feil.
- vi. Andelen av *systematiske feil* (inkludert fellesfeil), dvs. designrelaterte feil samt feil som kan tilskrives bruken og vedlikeholdet av utstyret, er høy. Dette står i kontrast til de lave feilratene som ofte legges til grunn i designfasen (jf. sertifikatdata) og som gir altfor optimistiske anslag over utstyrets pålitelighet.
- vii. Det kan ofte være utfordrende å få testet hele funksjonen. Dette kan ha ulike årsaker som at en vil unngå nedstengninger, uheldig plassering av og tilkomst til utstyr, samt at fokus er på testing av definert sikkerhetskritisk utstyr (som detektorer, transmittere og ventiler) som medfører at diverse mindre utstyr (jf. punkt v.) ikke blir testet.

#### 4.6 Konklusjoner vedrørende vedlikeholdets betydning

##### *Generelt fra driftsgjennomgangene*

SINTEF/NTNU har vært involvert i omtrent ti slike gjennomganger for fem ulike innretninger/anlegg, og omtrent 8000-9000 notifikasjoner har blitt gjennomgått. Et sted mellom 500-1000 sikkerhetskritiske (DU) feil er registrert.

En hovedkonklusjon er at en betydelig andel av disse feilene direkte eller indirekte kan tilskrives manglende eller mangelfullt (ikke utført eller for dårlig utført) vedlikehold. Det er derfor et stort potensiale for å redusere antall sikkerhetskritiske feil ved å fokusere på et bedre vedlikehold, inkludert å standardisere vedlikeholdet på tvers av innretninger i forhold til aktiviteter og utførelse.

Dette kan også være en forklaring på hvorfor nivået på innretninger varierer såpass mye, jf. RNNP /6/. Det handler ikke bare om godhet på utstyr, men like mye om hvordan vedlikehold og testing utføres og hvordan funksjonsfeil følges opp. Herunder i hvilken grad man gjør en god jobb i forhold til å identifisere rot-årsaker og fjerne disse.

#### **Tilbake til eksemplet med ESD ventiler**

En slik gjennomgang kan være avgjørende for hvorvidt en bestemmer seg for å endre testintervall eller ikke. Jf. eksempelet med 30 ESD ventiler og en antatt feilrate ( $\lambda_{DU}$ ) fra design på  $1 \cdot 10^{-6}$  feil per time, samt testintervall på 12 mnd. Dette vil tilfredsstille et SIL 2 krav på stenging av ESD ventil.

Anta at en basert på tre års driftserfaring har observert seks DU feil. Justert feilrate er da omtrent  $4 \cdot 10^{-6}$  feil per time.<sup>12</sup>

Dersom en fortsetter med et testintervall på 12 mnd, blir beregnet PFD for ventil  $\approx 0.02$  som tilsvarer SIL 1. Med andre ord: hvis en ikke justerer testintervall fra 12 mnd til 6 mnd for disse ventilene opererer en ikke i henhold til designforutsetningene. Dette illustrerer hvor "ømfintlig" en barriere kan være for korrekt tilpasset vedlikehold.

## **4.7 Oppsummeringsfigur**

Figur 4.3 gir en kortfattet og stikkordsmessig oppsummering av hele kapittel 4.

Figuren viser at et typisk ytelseskrav til instrumenterte sikkerhetssystemer (SIS) er pålitelighet i form av PFD (Probability of Failure on Demand) – sannsynligheten for at systemet skal virke ved behov – og at dette påvirkes av henholdsvis feilraten og testintervallet. Ved å starte med en antatt feilrate kan testintervallet regnes ut basert på ytelseskravet (SIL nivået).

*Eksempelvis at ved antatt 1 feil per 4 år (for et antall enheter) og et krav til SIL 2, så blir testintervallet på 12 måneder.*

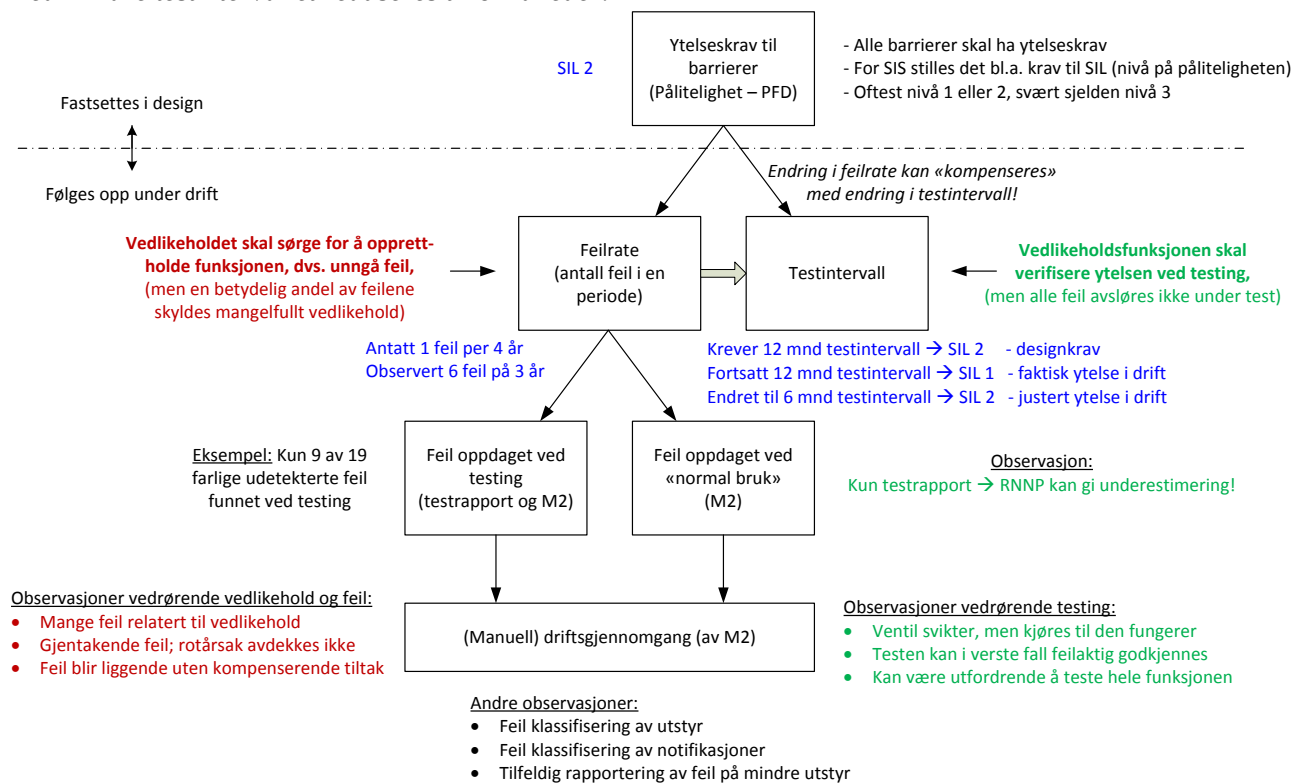
Vedlikeholdet har en rolle både i forhold til å holde feilraten nede (unngå feil) og ved å verifisere ytelsen gjennom testing (i henhold til fastsatt intervall).

Forhold som er relatert til feilraten er i figuren angitt med rødt, mens det som er relatert til testintervall er angitt med grønt. Eksemplet er angitt i blått.

I tillegg viser nederste del av figuren utfordringen med å fange opp feilene som skal inngå i feilraten.

<sup>12</sup> NB! Den justerte feilraten tar også hensyn til den opprinnelige feilraten. Dersom man bare tar hensyn til driftserfaringen ville feilraten blitt ennå høyere ( $7.6 \cdot 10^{-6}$  feil per time).

Dersom vi antar at de faktiske feilene som skal inngå i feilraten er fanget opp, og at disse eksempelvis utgjør 6 feil på 3 år (for et antall enheter) så vil ikke faktisk barrierelytelse i drift (SIL 1) tilfredsstille kravet (SIL 2), med mindre testintervallet reduseres til 6 måneder.



**Figur 4.3** Oppsummering av eksemplifisering av vedlikeholdets betydning for barrierer

--- ● ---

Vi har i kapittel 4 sett på konkrete eksempler på vedlikeholdets betydning for god barrierestyring. I kapittel 5 diskuterer vi noen utvalgte sentrale tema knyttet til vedlikeholdets plass i barrierestyringen.

## 5 Diskusjon av utvalgte tema

Følgende tema, jf. oppgavebeskrivelsen i kapittel 1.3, er diskutert i kapittel 5:

- Viktigheten av strukturert tilnærming og kontinuerlig forbedring
- Viktigheten av tverrfaglig involvering
- Behandling av eventuelle avvik knyttet til vedlikehold av barrierer (enkeltvis og samlet)

### 5.1 Viktigheten av strukturert tilnærming og kontinuerlig forbedring

*For å løse problemer, grav etter røttene i stedet for bare å hakke på bladene* [Anthony J. D'Angelo]

Styringsforskriftens § 23 (/22/) fokuserer på nødvendigheten av kontinuerlig forbedring: *Den ansvarlige skal kontinuerlig forbedre helse, miljø og sikkerhet ved å identifisere de prosessene, aktivitetene og produktene der det er behov for forbedring, og sette i verk nødvendige forbedringstiltak. Tiltakene skal følges opp og effekten evalueres.* Det henvises videre til Rammeforskriftens § 15 (/24/): *En god helse-, miljø- og sikkerhetskultur som omfatter alle faser og aktivitetsområder skal fremmes gjennom kontinuerlig arbeid for å redusere risiko og forbedre helse, miljø og sikkerhet.*

I St. Meld. 29 (2010-2011) /31/ vises det også til arbeidet med kontinuerlig forbedring i petroleumsindustrien, herunder å etablere barrierer mot storulykkesrisiko (kapittel 20.2.2). Ptil sitt barrierenotat (/1/) peker dessuten på at *kravet til risikoreduksjon (kontinuerlig forbedring)* må inkluderes som en del av konteksten.

Gitt det generelt høye sikkerhetsnivået i norsk petroleumsindustri, er det viktig å jobbe strukturert og systematisk for å oppnå en ytterligere forbedring. Gjennom eksemplet i kapittel 4 ser vi både potensial og flere muligheter for at denne systematikken kan forbedres.

Potensialet for forbedring av barriereytelsen ut fra et vedlikeholdsperspektiv er åpenbar ut fra (1) at mange barriereelementer (eksempelvis ESV og BDV) jf. RNNP /6/ har en for stor andel feil (antall feil per test), (2) at situasjonen kan være enda verre enn det RNNP viser dersom man også tar hensyn til feil i normal drift, og (3) at en betydelig andel av feilene direkte eller indirekte kan tilskrives manglende eller mangelfullt (ikke utført eller for dårlig utført) vedlikehold.

Mulighetene til forbedring er blant annet knyttet til følgende:

- Vi har i forbindelse med driftsgjennomganger observert at gjentakende feil er forholdsvis vanlig. Dette vitner om mangelfull årsaksanalyse og tilhørende mangel på systematikk i arbeidet.
- I forhold til feilklassifisering gjøres det en del feil. Mangel på kvalitetssikring, kunnskap og opplæring er vanlige årsaker. Dette kan medføre:
  - At utstyr får feil prioritet og dermed ikke den "riktige" oppfølgingen
  - At samme type utstyr og samme type feil får ulik oppfølging på ulike innretninger (og risikobildet dermed utvikler seg forskjellig)
  - At en får et feilaktig inntrykk av totalt antall kritiske feil (jf. testrapporten)
- Rapportering av "diverse utstyr" (av type solenoider, I/O kort, barrierer, endebrytere, koplingsbokser, kabler, etc.) som kan være kritisk for at sikkerhetsfunksjonen skal fungere, er ofte mangelfull, og slikt utstyr får dermed ikke en systematisk oppfølging.

Vi har tidligere påpekt behovet for å fjerne årsaker til utstyrsfeil i stedet for å korrigere symptomer, ved kartlegging av vedlikeholdsstatus opp mot tilstanden slik den er beskrevet i Stortingsmelding nr. 7 (2001-2002) /33/. I statuskartleggingen fra 2004 (/11/ og oppsummert i /13/) står det følgende: *Dette krever svært gode data (og kompetanse), bl.a. på feilmekanismer som vibrasjon, korrosjon, osv. Feilmekanismer er imidlertid ikke obligatorisk å rapportere.*

I følge sf § 19 (om innsamling, bearbeiding og bruk av data) skal den ansvarlige: *sikre at data som har betydning for helse, miljø og sikkerhet, blir samlet inn, bearbeidet og brukt til å a) overvåke og kontrollere tekniske, operasjonelle og organisatoriske forhold, b) utarbeide måleparametere, indikatorer og statistikk, c) utføre og følge opp analyser i ulike faser av virksomheten, d) bygge opp generiske databaser, og e) sette i verk korrigerende og forebyggende tiltak, deriblant forbedring av systemer og utstyr. Det skal settes krav til dataenes kvalitet og validitet ut fra det aktuelle bruksbehovet.*

Regelverket setter med andre ord ikke eksplisitte krav til rapportering av feilmekanismer, selv om en indirekte kan tolke kravene som at analyse av rot-årsaker vil være en naturlig del av det å identifisere tiltak for å forbedre systemer og utstyr. Dagens praksis varierer nok betydelig mellom operatører og innretninger; Rapportering av feilmekanismer foregår på kodenivå i vedlikeholdssystemer og delvis i fritekstfelte. I hvilken grad dette datamaterialet er gjenstand for videre analyse og vurderinger er varierende og i liten grad formalisert hos operatørene.

Øvrige mer generelle observasjoner knyttet til mangel på systematikk i vedlikeholdsarbeidet er:

- Det er ofte ikke noen åpenbar eller entydig kobling mellom SIL klassifisering og den kritikalitetsvurderingen av utstyr som skjer knyttet til vedlikeholdssystemet (jf. kapittel 3.1.2). Det foreligger informasjon (fra arbeidet med å sette SIL krav til barrierene) som i mange tilfeller ikke benyttes på en systematisk måte og som kunne høynet kvaliteten på kritikalitetsvurdering av sikkerhetskritisk utstyr.
- Diverse funn fra RNNP /6/ viser at det er stor variasjon mellom selskap og mellom innretninger når det gjelder ytelsen på sentrale barriereelementer. Dette tyder på at det ikke er noe systematisk forbedringsarbeid gjennom eksempelvis erfaringsoverføring mellom innretninger i samme selskap eller på tvers av selskap.

## 5.2 Viktigheten av tverrfaglig involvering

*Å komme sammen er begynnelsen. Å holde sammen er framgang. Å arbeide sammen er suksess [Henry Ford]*

Styringsforskriften § 14 første ledd /22/ stiller krav til bemanning og kompetanse: *Den ansvarlige skal sikre tilstrekkelig bemanning og kompetanse i alle faser av virksomheten, jf. rammeforskriften § 12.*

I veiledning til styringsforskriften § 14 /32/ står det videre: *Kompetanse som nevnt i første ledd, omfatter både individuell kompetanse og gruppekompetanse, deriblant fagkompetanse, systemkunnskap og helse-, miljø- og sikkerhetskompetanse, se også aktivitetsforskriften § 20<sup>13</sup> og teknisk og operasjonell forskrift § 51<sup>14</sup>.*

Kravet til gruppekompetanse kan også ses på som behov for tverrfaglig kompetanse gjennom tverrfaglig involvering.

<sup>13</sup> Skal nok være § 21.

<sup>14</sup> Skal nok være § 50.

Viktigheten av tverrfaglig involvering og multidisiplint samarbeid er generelt noe som er enklere å påpeke enn å gjøre noe med. I praksis dreier dette imidlertid seg ofte om å legge til rette for samarbeid på tvers der dette er nødvendig, samt følge opp at dette blir gjort i tilstrekkelig grad. Dette kan være utfordrende ved at disipliner som eksempelvis vedlikehold og teknisk sikkerhet vanligvis er organisasjonsmessig og lokasjonsmessig adskilt.

Vi vil i dette kapitlet nøye oss med å diskutere og eksemplifisere noen områder hvor vi ser et forbedringspotensial med tanke på tverrfaglig samarbeid knyttet til vedlikehold og barrierestyring.

Som diskutert tidligere i rapporten (kapittel 3.1.2 og kapittel 5.1) har vi hos selskapene sett en manglende sammenheng mellom SIL nivå og kritikalitetsklassifisering for utstyr. Dette tyder på at det er mangelfull kommunikasjon mellom vedlikeholdsmiljøet og de disipliner som fastsetter ytelseskrav til barrierer i form av SIL (instrument og teknisk sikkerhet). Resultatet kan være komponenter som inngår i et HIPPS system (SIL 3) i vedlikeholdssystemet "behandles likt" med komponenter som inngår i et PSD system (SIL 2 eller SIL 1). Det er derfor viktig med bedre kommunikasjon og samarbeid mellom disse miljøene.

Videre har vi påpekt behovet for tverrfaglig samarbeid i forbindelse med optimalisering av testintervall, jf. kapittel 3.3.1: Behovet for mer effektive barrierer vurderes av barriereansvarlige (for eksempel teknisk sikkerhetsmiljø), mens mulighetene (eksempelvis endring av testintervall) kan bedømmes av blant annet vedlikeholdspersonell, ut i fra at data for verifikasjon av ytelsen til barrierene kommer fra vedlikeholdsinformasjonsystemer. Det er derfor viktig med tett samarbeid mellom disse fagmiljøene, også i forbindelse med optimalisering av testintervall.

Vi har tidligere påpekt behov for tettere samarbeid mellom vedlikehold og teknisk sikkerhet ved kartlegging av vedlikeholdsstatus opp mot tilstanden slik den er beskrevet i Stortingsmelding nr. 7 (2001-2002) /33/. I statuskartleggingen fra 2004 (/11/ og oppsummert i /13/) står det følgende: *I de siste årene har operatørselskapene lagt ned en betydelig innsats i forhold til det å stille krav til barrierer (sikkerhetskritiske systemer) og oppfølging av disse kravene. Dette er blitt initiert av myndighetenes økte fokus på kontroll med barrierer, og forsterket gjennom konkrete prosjekt som risikonivå på norsk sokkel (RNNS) hvor selskapene må melde inn resultater fra testing av viktige barrierer. Parallelt med RNNS har selskapene utviklet systemer for gjennomgang av alle sikkerhetssystemene på sine installasjoner, betegnet som TTS- eller TST-gjennomganger (som står for hhv. Teknisk Tilstand Sikkerhet og Teknisk Sikkerhetstilstand). Både når det gjelder RNNS og TTS/TST er vedlikehold sentralt, men det kan se ut som om arbeidet med dette i enkelte selskap ikke har inkludert vedlikeholdsfunksjonen i tilstrekkelig grad, fordi "eierskapet" ligger i andre organisatoriske enheter som "teknisk sikkerhet" eller tilsvarende. Det er derfor fortsatt en utfordring for næringen å anvende vedlikeholdskompetanse i et helse-, miljø- og sikkerhets-perspektiv i tilstrekkelig grad. Fagmiljøene innen vedlikehold burde i større grad involveres i sikkerhetsarbeid slik som RNNS og TTS/TST.*

Også ved driftsgjennomganger er det viktig med tverrfaglig involvering for å oppnå en felles forståelse av problemområder og behov for forbedringer. Gjennomgangene utføres typisk som en samhandling mellom fagansvarlig instrument/automasjon, teknisk sikkerhet og fagansvarlig vedlikeholdsstyring (jf. kapittel 4.4.1).

Det vil i tillegg til teknisk sikkerhet være andre fagmiljø som det er potensial for tettere samarbeid med, eksempelvis risikoanalysemiljøet. Dette har vi påpekt i kapittel 3.2.3: Risikoanalyser som utføres som en del av beslutningsunderlaget for barrierestyring må planlegges og utføres slik at de er detaljerte nok og formålstjenlige, inklusive at de skal kunne formidles til ulike brukergrupper – inklusive vedlikeholdspersonell. Vedlikeholdspersonell må ha kjennskap til både hvilken risiko de utsettes for og hvordan de påvirker risikoen gjennom de vedlikeholdsaktiviteter de utfører, herunder oppfølging av forutsetninger relatert til vedlikehold som inngår i risikoanalysene.

Ved gjennomgang av forutsetningene relatert til vedlikehold vil det også kunne gis nyttig tilbakemelding til risikoanalytikerne i forhold til om forutsetningene er realistiske, eventuelt om det er andre forhold som burde vært inkludert. Dette inkluderer forhold rundt modellering av barrierer, blant annet hvorvidt testintervall inngår som parameter og hvilke parameterverdier som er benyttet.

### 5.3 Behandling av eventuelle avvik knyttet til vedlikehold av barrierer (enkeltvis og samlet)

*Den som vet når nok er nok, vil alltid ha nok [Lao Tzu]<sup>15</sup>*

Styringsforskriften § 22 første ledd /22/ stiller krav til avviksbehandling: *Den ansvarlige skal registrere og følge opp avvik fra krav i helse-, miljø- og sikkerhetslovgivningen, deriblant avvik fra interne krav som er av betydning for å oppfylle krav i helse-, miljø- og sikkerhetslovgivningen. Det skal tas stilling til avvikenes betydning for helse, miljø og sikkerhet enkeltvis og i forhold til andre avvik.*

I veiledning til styringsforskriften § 22 /32/ står det videre: *Oppfølging av avvik som nevnt i første ledd, kan ivaretas blant annet i de etablerte systemene for vedlikeholdsadministrasjon, arbeidstillatelser, fare- og ulykkesoppfølging og i systemet for avviksbehandling.*

Når det gjelder avvik knyttet til vedlikehold av barrierer så er dette særlig knyttet til manglende overholdelse av tidsfrister for gjennomføring av vedlikeholdsaktiviteter. Dette er det stilt krav til i aktivitetsforskriften § 48 /21/ om planlegging og prioritering, andre ledd: *Det skal foreligge kriterier for setting av prioritet med tilhørende tidsfrister for utføring av de enkelte vedlikeholdsaktivitetene. Kriteriene skal ta hensyn til klassifiseringen som nevnt i § 46.*

I veiledning til aktivitetsforskriften § 48 /34/ står det videre: *For å oppfylle kravet til tidsfrister som nevnt i andre ledd, bør fristene regnes fra det tidspunktet en identifiserer en feilmodus som er under utvikling eller er inntrådt.*

Aktivitetsforskriften § 48 og kriterier/metoder for setting av prioritet ble diskutert i kapittel 3.1.1 som en del av konteksten til barrierestyling, og vi vil gå litt videre på denne diskusjonen her (og tar utgangspunkt i den metoden som ble beskrevet i kapittel 3.1.1). Dersom tidsfristene (som avhenger av prioriteten; eksempelvis 5, 30, 180 eller 365 dager) overskrides så blir dette registrert som utestående vedlikehold. Noen vil betrakte dette som avvik (fra interne krav), mens andre har kriterier for hvor stor overskridelsen skal være før det registreres som et avvik, med tilhørende/påfølgende krav til avviksbehandling.

Uansett om man betrakter det som formelle avvik eller ikke, så har man i denne sammenheng to typer "avvik": (1) mengde utestående vedlikehold (HMS-kritisk og totalt), og (2) antall avvik (eventuelt målt i antall avvik ganger varigheten av avviket).

La oss anta at mengden utestående vedlikehold og/eller antall avvik øker jevnt og trutt: Når vil man si at "nok er nok"?

Det er et godt spørsmål, men dessverre er vår erfaring at det er svært vanskelig å få et svar på når nok er nok!

---

<sup>15</sup> Og den som ikke vet når nok er nok, vil aldri få nok ... (avvik) ...

Vår erfaring er også at man har relativt god kontroll på det som har *høy prioritet* (uten at man nødvendigvis har noen grenser for mengde eller antall her heller), men at man ikke nødvendigvis har god kontroll på alt utstyr som er *sikkerhetskritisk*, fordi dette kan være gitt lav prioritet, jf. diskusjon av kriterier/metode i kapittel 3.1.1.

Et annet nærliggende spørsmål (og utfordring for mange innretninger jf. RNNP /6/) er hvordan man forholder seg til totalvolumet av utestående vedlikehold og etterslep (uavhengig av om dette defineres som avvik eller ikke). Hvor stort kan dette få lov til å bli?

Heller ikke her er det lett å få svar, selv om enkelte innretninger har så stort totalvolum av utestående vedlikehold og etterslep at det ikke er mulig å snu en negativ trend uten betydelig ressurstilgang ved for eksempel innleie av flotell for å få stor nok kapasitet (antall sengeplasser).

Grunnen til dette er at for de fleste innretninger så er de viktigste rammebetingelsene (1) driftsmodellen som angir grunnbemanning, (2) tillatt antall personer om bord (POB) og (3) eventuelle operasjonelle begrensninger. Den eneste rammebetingelsen man ofte kan påvirke i stor nok grad er nummer 2, og da ved å leie inn flotell. Selv en revisjonsstans er i mange tilfeller ikke tilstrekkelig dersom man ikke øker sengekapasiteten med flotell.

Den siste utfordringen vi vil peke på her er knyttet til kontroll med (og risikomessig betydning av) sikkerhetskritisk utstyr som inngår i totalvolumet av utestående vedlikehold (uavhengig av prioritet – siden feil på sikkerhetskritisk utstyr også kan ligge som uprioriterte arbeidsordrer, jf. kapittel 3.1.1). Har operatørene en systematisk måte å følge opp utviklingen i degradering for det totale volumet av sikkerhetskritisk utstyr som har en begynnende eller degraderende feil, mens det "ligger i påvente av vedlikehold" – som kan være opptil 365 dager?

Vår erfaring er at det både kan være utfordringer for utstyret enkeltvis (eksempelvis at et utstyr som allerede er rapportert med degraderende feil "oppgraderes" til kritisk feil fortløpende) og for en samlet vurdering av risikomessig betydning definert med en øvre grense (når "nok er nok").

Det er i diskusjonen over fokusert på avvik i forhold til utestående vedlikehold. Det er også verdt å nevne at mange innretninger opererer med en rekke temporære og mer permanente avvik knyttet til design og operasjon av sikkerhetssystemer. Dette kan gå på brannskiller som er svekket i forbindelse med pågående modifikasjoner, det kan være brann og gassdetektorer som er koblet ut i et helt område i forbindelse med pågående vedlikehold eller det kan være permanente avvik slik som et instrument installert oppstrøms stigerørs ESV, brannvannskapasitet som kun dekker deler av innretningen, eller et HIPPS system (som erstatning for en fullstrøms PSV). En utfordring er at analyser ofte viser at slike enkeltavvik er akseptable, men har en kontroll med helheten?

--- ● ---



## 6 Oppsummering

Vedlikeholdets plass i barrierestyringen kan oppfattes både enkelt og vanskelig. Enkelt sagt skal vedlikeholdet bidra til å opprettholde og gjenopprette de tekniske barrierenes funksjon, samt verifisere ytelsen til barrierene. Når det er sagt er det ikke like rett frem hvordan dette skal gjøres i praksis. Heller ikke barrierestyringen i seg selv er rett frem.

I denne rapporten diskuterer vi vedlikeholdets plass i barrierestyringen både på prinsipielt grunnlag, trinn for trinn i barrierestytingsprosessen, gjennom konkrete eksempler, samt i forhold til utvalgte sentrale tema.

### *Vedlikeholdets plass i barrierestyringen – prinsipielle sammenhenger*

Barrierestyring inngår som en del av annen styring, bl.a. risikostyring (på selskapsnivå). Barrierestyring er ikke en separat aktivitet, men er en integrert del av bl.a. risikostyringen. Vedlikeholdet er i kraft av sitt formål (å opprettholde ytelsen til blant annet barriereelementene) en viktig del av barrierestyringen.

De prinsipielle sammenhengene har tatt for seg:

- Prinsippene for risiko-/barrierestyring
- Styringssløyfa for styring av rammeverket
- Rammeverket for barrierestytingsprosessen
- Selve barrierestytingsprosessen (for alle faser)
- Oppfølging i driftsfasen, inklusive måling og verifikasjon av barrieretelse
- Vedlikeholdsstyringssløyfa og koplingen mellom vedlikeholdsstyring og barrierestyring

De prinsipielle sammenhengene med hensyn til vedlikeholdets plass i barrierestyringen viser koplingen mellom de ulike elementene i vedlikeholdsstyringssløyfa og henholdsvis rammeverket for barrierestytingsprosessen og selve barrierestytingsprosessen (med nærmere spesifisering av oppfølging i driftsfasen, inklusive måling og verifikasjon av barrieretelse). Sammenhengene baserer seg blant annet på vår fortolkning av ISO 31000, som er beskrevet og forklart i vedlegg B.

### *Vedlikeholdets rolle i barrierestytingsprosessen – trinn for trinn*

Vedlikeholdets rolle er drøftet for hvert av trinnene i barrierestytingsprosessen. Hoveddelene av prosessen er:

1. Kontekst
2. Risikovurderinger
3. Risikohåndtering
4. Kommunikasjon og konsultasjon
5. Overvåking og gjennomgåelse

Drøftingen har blitt understøttet med data fra RNNP, der dette har vært mulig og hensiktsmessig. Drøftingen har tatt utgangspunkt i barrierenotatet og dets behandling av vedlikehold og vedlikeholdsstyring, som er gjengitt i vedlegg C.

### *Konkrete eksempler på vedlikeholdets betydning for god barrierestyring*

Når vi har gitt konkrete eksempler på vedlikeholdets betydning for god barrierestyring har vi tatt utgangspunkt i føringer og antakelser fra design og sett på videre oppfølging i driftsfasen, spesielt gjennom driftsgjennomganger av feil i sentrale barriereelementer. Dette inkluderer beskrivelse av fremgangsmåte og omfang, feilklassifisering, diskusjon rundt feil oppdaget ved test versus feil oppdaget i normal drift, samt gjennomgang av generelle nytteverdier av driftsgjennomganger.

Avslutningsvis har vi presentert og diskutert resultatene av driftsgjennomgangene, og en hovedkonklusjon er at en betydelig andel av feilene (på utvalgte barriereelementer) kan direkte eller indirekte tilskrives manglende eller mangelfullt (ikke utført eller for dårlig utført) vedlikehold. Det er derfor et stort potensiale for å redusere antall sikkerhetskritiske feil ved å fokusere på et bedre vedlikehold.

Dessuten har vi vist et eksempel som viser hvor "ømfintlig" og avhengig en barriere kan være for et korrekt tilpasset vedlikehold, dersom kravet til ytelse skal opprettholdes i driftsfasen i samsvar med krav stilt under design.

### Utvalgte tema

Vi har tatt for oss følgende utvalgte sentrale tema knyttet til vedlikeholdets plass i barrierestyringen:

- Viktigheten av strukturert tilnærming og kontinuerlig forbedring
- Viktigheten av tverrfaglig involvering
- Behandling av eventuelle avvik knyttet til vedlikehold av barrierer (enkeltvis og samlet)

Her peker vi blant annet på utfordringer med gjentakende feil og behovet for å fjerne årsaker til utstyrsfeil i stedet for å korrigere symptomer. Videre har vi påpekt behovet for tverrfaglig samarbeid i forbindelse med kritikalitetsklassifisering, optimalisering av testintervall, ved driftsgjennomganger av notifikasjoner, samt ved kommunikasjon rundt risikoanalyser (blant annet forutsetninger knyttet til barrierer som krever oppfølging i drift av vedlikeholdspersonell).

Når det gjelder håndtering av avvik stiller vi spørsmålet når "nok er nok". Hvor mye utestående vedlikehold og etterslep skal man få lov å ha? Hvor mange avvik? Hvor stort totalvolum av vedlikehold som ikke er utført? Svaret er at det er svært vanskelig å få et svar på når nok er nok. Spørsmålet blir da om man oppnår god nok kontroll uten å sette tydelige og målbare grenser.

## Referanser

- /1/ Petroleumstilsynet, Prinsipper for barrierestyring i petroleumsvirksomheten, 29.01.2013
- /2/ ISO 31000:2009, Risk management – Principles and guidelines
- /3/ Petroleumstilsynet, 2010. Risikonivå i petroleumsvirksomheten. Hovedrapport, utviklingstrekk 2009, norsk sokkel
- /4/ Petroleumstilsynet, 2011. Risikonivå i petroleumsvirksomheten. Hovedrapport, utviklingstrekk 2010, norsk sokkel
- /5/ Petroleumstilsynet, 2012. Risikonivå i petroleumsvirksomheten. Hovedrapport, utviklingstrekk 2011, norsk sokkel
- /6/ Petroleumstilsynet, 2013. Risikonivå i petroleumsvirksomheten. Hovedrapport, utviklingstrekk 2012, norsk sokkel
- /7/ Øien, K., Schjølberg, P., Meland, O., Leto, S., Spilde, H., 2010. The importance of maintenance to prevent major accidents. Euromaintenance International Conference (Euromaintenance 2010), May 12-14, Verona, Italy
- /8/ Hauge, S., Øien, K., 2012. Deepwater Horizon; Lessons learned for the Norwegian Petroleum Industry. 5th International Conference on Safety & Environment in Process Industry, 3-6 June 2012, Milan, Italy
- /9/ Tinmannsvik, R.K., Albrechtsen, E., Bråtveit, M., Carlsen, I.M., Fylling, L., Hauge, S., Haugen, S., Hynne, H., Lundteigen, M.A., Moen, B.E., Okstad, E., Onshus, T., Sandvik, P., Øien, K., 2011. Deepwater Horizonulykken: Årsaker, lærepunkter og forbedringstiltak for norsk sokkel. SINTEF A19148 (ISBN 978-82-14-05088-2)
- /10/ Tinmannsvik, R.K., Albrechtsen, E., Bråtveit, M., Carlsen, I.M., Fylling, L., Hauge, S., Haugen, S., Hynne, H., Lundteigen, M.A., Moen, B.E., Okstad, E., Onshus, T., Sandvik, P., Øien, K., 2011. Deepwater Horizonulykken: Vedleggsrapport. SINTEF A19148 (ISBN 978-82-14-05088-2)
- /11/ Øien, K., Schjølberg, P., 2005. Gjennomgang av operatørenes vedlikeholdsstyring; Samlerapport. SINTEF-rapport F04429. (Fortrolig)
- /12/ Øien, K., Schjølberg, P., 2007. Vedlikehold som virkemiddel for å forebygge storulykker; Vedlikeholdsstatus og utfordringer i den forbindelse. SINTEF-rapport A2535
- /13/ Øien, K., Schjølberg, P., 2008. Vedlikehold som virkemiddel for å forebygge storulykker; Vedlikeholdsstatus og utfordringer i den forbindelse. SINTEF-rapport A8222
- /14/ Meland, O., Schjølberg, P., Øien, K., 2008. Vedlikehold for aldrende innretninger – en utredning. SINTEF-rapport A11701
- /15/ Øien, K., Schjølberg, P., 2009. Kartlegging av konsekvensene for vedlikeholdsstyring ved aldring og levetidsforlengelse. SINTEF-rapport A12843
- /16/ Tinmannsvik, R. K., Øien, K., 2010. Kartlegging av læring og oppfølging av uønskede hendelser hos vedlikeholdsentreprenørene – særlig med tanke på forebygging av storulykker. SINTEF-rapport A16717
- /17/ Øien K, 2012. RNNP-vedlikeholdsindikatorer: Erfaringer knyttet til kvaliteten av innrapporterte vedlikeholdsdata. SINTEF-rapport A23398
- /18/ Petroleumstilsynet, 2013. Forslag til definisjoner av barriereelementer
- /19/ NS-EN 13306:2010 Vedlikehold - Vedlikeholdsterminologi
- /20/ OD, 1998. Basisstudie vedlikeholdsstyring. Metode for egenvurdering av vedlikeholdsstyring. Revisjon 0, 1.5.1998
- /21/ Petroleumstilsynet, Forskrift om utføring av aktiviteter i petroleumsvirksomheten (aktivitetsforskriften 29.4.2010), [www.ptil.no](http://www.ptil.no)
- /22/ Petroleumstilsynet, Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften 29.4.2010), [www.ptil.no](http://www.ptil.no)

- /23/ NORSOK Standard Z-008, Risk based maintenance and consequence classification, Edition 3, June 2011
- /24/ Petroleumstilsynet, Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg (rammeforskriften 12.2.2010), [www.ptil.no](http://www.ptil.no)
- /25/ NORSOK Z-013, Risk and emergency preparedness assessment, ver. 03, October 2010
- /26/ Petroleumstilsynet, Forskrift om utforming og utrusting av innretninger med mer i petroleumsvirksomheten (innretningsforskriften 29.4.2010), [www.ptil.no](http://www.ptil.no)
- /27/ IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7. International Electrotechnical Commission, Geneva
- /28/ IEC 61511 (2003). Functional Safety: Safety Instrumented systems for the Process Industry Sector, Part 1-3. International Electrotechnical Commission, Geneva
- /29/ OLF 070, Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, Rev. 02, 29.10.2004
- /30/ PDS prosjektet, <http://www.sintef.no/pds>
- /31/ Arbeidsdepartementet (AD), Melding til Stortinget nr. 29 (2010-2011) Felles ansvar for eit godt og anstendig arbeidsliv; Arbeidsforhold, arbeidsmiljø og sikkerheit
- /32/ Petroleumstilsynet, Veiledning til forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (veiledning til styringsforskriften 29.4.2010), [www.ptil.no](http://www.ptil.no)
- /33/ Arbeids- og administrasjonsdepartementet (AAD), Stortingsmelding nr. 7 (2001-2002) Om helse, miljø og sikkerhet i petroleumsvirksomheten
- /34/ Petroleumstilsynet, Veiledning til forskrift om utføring av aktiviteter i petroleumsvirksomheten (veiledning til aktivitetsforskriften 29.4.2010), [www.ptil.no](http://www.ptil.no)
- /35/ Øie, S., 2013. Defining and operationalizing the barrier concept; The human contribution, ESRA-seminar, 30 April 2013
- /36/ ISO 14224:2006 Petroleum, petrochemical and natural gas industries -- Collection and exchange of reliability and maintenance data for equipment

## Vedlegg A: Begreper og fortolkninger

### A.1 Generelt om definisjoner

Det å definere noe har både fordeler og ulemper. Hovedformålet er at man skal ha lik forståelse av et begrep for å unngå at man snakker forbi hverandre. Ulempen er at definisjoner ofte er veldig "eksakt" og avgrenset, og dermed gir en lite utfyllende forklaring/forståelse av et begrep. Dessuten er det ikke noen fasit på hva som er den "riktige" definisjonen. I hovedsak velges definisjoner fra anerkjente internasjonale standarder.

Det er den som omtaler begrepene som gjennom definisjoner "forklarer" hvordan de ulike begrepene skal forstås. Man kan være enig eller uenig i definisjonene, og man kan foretrekke en bestemt definisjon framfor en annen, men det er som sagt ingen fasit på hva som er den riktige definisjonen.

I noen tilfeller kan det være "berikende" og øke forståelsen dersom man angir flere alternative definisjoner. Samtidig er omforente definisjoner viktige for å oppnå en felles forståelse av begreper som i utgangspunktet kan oppfattes ulikt.

Definisjoner er utfordrende. De tenderer å skape en form for konsensus, men blant annet ulike faglige ståsted medfører ulik tolkning, noe som igjen medfører at dersom en ønsker å begrense tolkningsrommet må definisjonen være svært avgrenset og "smal". En mulighet er derfor å gi eksempler på hvordan en definisjon skal fortolkes og/eller utdype definisjonen i form av merknader/noter.

Barrierebegrepet er et eksempel på at ulike definisjoner og ulike tilstøtende begreper kan virke forvirrende. Det er derfor behov for å operasjonalisere begrepene.

### A.2 Operasjonalisering av begreper

Det er behov for å operasjonalisere begreper slik som barrierer, barrierestyring, vedlikehold og vedlikeholdsstyring. Operasjonalisering (jf. Wikipedia<sup>16</sup>) er prosessen med å definere et ullent ("fuzzy") begrep slik at begrepet er tydelig skillbart eller målbart samt å forstå det i form av empiriske observasjoner. I en videre betydning refererer det til prosessen med å spesifisere omfanget av et begrep – beskrive hva som inngår og hva som ikke inngår i begrepet.

Barrierer og barrierestyring vil mange (eksempelvis /35/) hevde er ulne ("fuzzy") begreper som ennå ikke fullt ut er entydig operasjonalisert i industrien – noe som i seg selv gjør det utfordrende å knytte andre begreper og områder slik som vedlikeholdsstyring opp mot dette.

Dette peker for så vidt videre mot behovet for å ha definisjoner som er rimelig avgrensbare og som blir entydig oppfattet i industrien. Eller for å si det på en annen måte: dersom forståelsen av hva som er en barriere varierer, vil også forståelsen av vedlikeholdets plass i barrierestyringen variere.

---

<sup>16</sup> Wikipedia:

- Operationalization is the process of defining a fuzzy concept so as to make the concept clearly distinguishable or measurable and to understand it in terms of empirical observations.
- In a wider sense it refers to the process of specifying the extension of a concept — describing what is and is not a part of that concept.

### A.3 Barrierestyring og vedlikehold

Barrierestyring: Koordinerte aktiviteter for å etablere og opprettholde barrierer slik at de til enhver tid opprettholder sin funksjon. (/1/)

Vedlikehold: Kombinasjon av alle tekniske, administrative og ledelsesmessige aktiviteter i levetiden til en enhet, som har til hensikt å opprettholde eller gjenopprette den til en tilstand som gjør den i stand til å utføre den krevde funksjonen. (Basert på /19/)

Vedlikehold handler både om å opprettholde (gjennom forebyggende vedlikehold) og gjenopprette (gjennom korrigerende vedlikehold) funksjonsevnen til en enhet – eksempelvis en barriere. Ved å benytte "opprettholde" i definisjonen til barrierestyling kan det gis et inntrykk av at det ikke er behov for gjenoppretting etter svikt, noe som også indikeres av at funksjonen skal opprettholdes "til enhver tid".

Dersom man i stedet velger å bruke "vedlikeholde" i definisjonen av barrierestyling, samt sløyfe "til enhver tid" (noe som aldri kreves av noen funksjon), så fremgår det tydelig at barrierer kan svikte og at de da må gjenopprettes. Dessuten får vedlikehold en tydelig og sentral plass i barrierestylingen. En alternativ definisjon kan være:

Barrierestyling (alternativ definisjon):

Koordinerte aktiviteter for å etablere og vedlikeholde barrierer slik at de ivaretar sin krevde funksjon.

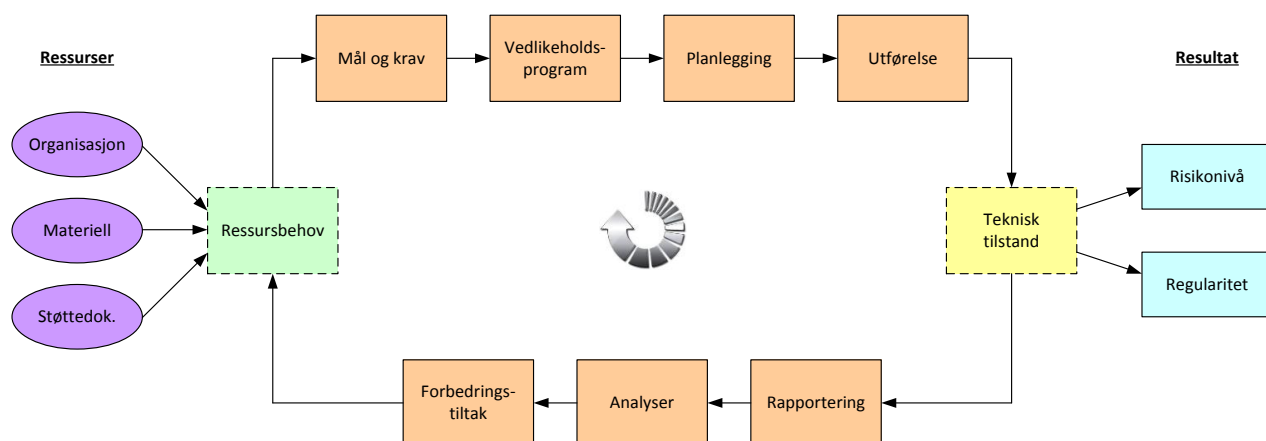
Vedlikehold som fagdisiplin retter seg mot teknisk utstyr (for eksempel tekniske barriereelement), jf. henvisning til "en enhet" i definisjonen av vedlikehold. Det vil imidlertid også være viktig å holde vedlike ikke-tekniske forhold (for eksempel organisatoriske barriereelement) gjennom eksempelvis trening og øvelser, men denne type "vedlikehold" er ikke en del av fagdisiplinen vedlikehold. Når vi i dette dokumentet bruker begrepet vedlikehold er det i en teknisk betydning, som angitt i definisjonen ovenfor. Det vil som oftest naturlig fremgå av sammenhengen hvilken form for vedlikehold det er snakk om, men dersom dette er uklart og det gjelder vedlikehold i en ikke-teknisk betydning så angis dette eksplisitt.

### A.4 Vedlikeholdsstyring

Vedlikeholdsstyring er et begrep som er omfattende og som kan være enklere å forstå gjennom en figur som viser ei typisk vedlikeholdsstyringssløyfe. Figur A1 som er angitt her er vedlikeholdsstyringssløyfa som ble definert i basisstudien (/20/), og som er velkjent i petroleumsvirksomheten i Norge.

Ressursene i form av vedlikeholdspersonell/vedlikeholdsorganisasjon, materiell og støtte-dokumentasjon styres slik at det ønskede resultat oppnås i form av teknisk tilstand, risikonivå og regularitet. Dette innebærer at innretningene eller deler av disse er i stand til å utføre sine tiltenkte funksjoner, jf. aktivitetsforskriften § 42 om vedlikehold /22/.

Styringen skjer ved at det etableres mål og krav, utvikles vedlikeholdsprogram (jf. aktivitetsforskriften § 44 om vedlikeholdsprogram og § 43 om klassifisering), og at vedlikeholdet planlegges og utføres i henhold til programmet (jf. aktivitetsforskriften § 45 om planlegging og prioritering). Derneft tilbakerapporteres resultatene, de analyseres og eventuelle forbedringstiltak iverksettes (jf. aktivitetsforskriften § 46 om vedlikeholdseffektivitet). Sløyfa er dermed lukket.



**Figur A1** Vedlikeholdsstyringssløyfa (/20/)

Selve vedlikeholdet er mer rettet mot aktivitetene som bidrar til ivaretagelsen av krevd funksjon gjennom opprettholdelse eller gjenoppretting. Dette er ikke utelukkende knyttet til den fysiske utførelsen av vedlikeholdet, men også administrative og ledelsesmessige aktiviteter knyttet til utførelsen.

## A.5 Barrierefunksjon

**Barrierefunksjon:** Oppgaven eller rollen til en barriere. Eksempler på barrierefunksjoner er: forhindre lekkasje, forhindre antenning, redusere brannbelastning, sikre forsvarlig evakuering, forhindre hørselsskade. (/1/)

Eksempler bør prinsipielt ikke inngå direkte i definisjonen. Det kan inngå i en merknad eller forklaring til definisjonen.

**Barrierefunksjon (alternativ definisjon):**

Oppgaven eller rollen til en barriere.

Merknad: Eksempler på barrierefunksjoner er: forhindre lekkasje, forhindre antenning, redusere brannbelastning, sikre forsvarlig evakuering, forhindre hørselsskade.

## A.6 Barrieredefinisjonen

**Barriere:** Tekniske, operasjonelle og organisatoriske elementer som enkeltvis eller til sammen skal redusere muligheten for at konkrete feil, fare- og ulykkessituasjoner inntreffer, eller som begrenser eller forhindrer skader/ulemper. (/1/)

**Barriere (alternativ definisjon):**

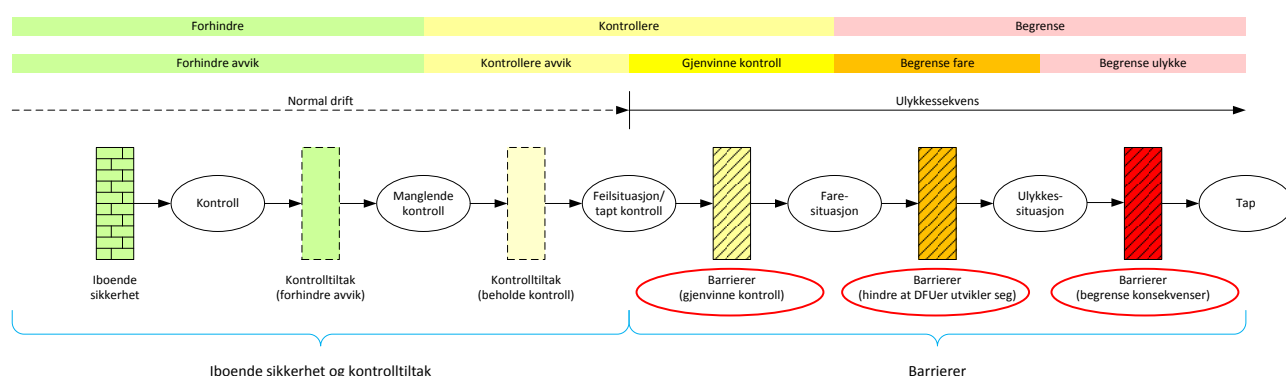
Planlagte tiltak for å gjenvinne kontroll, hindre at definerte fare- og ulykkessituasjoner utvikler seg, eller begrense konsekvenser.

Merknad: Barrierer kommer i tillegg til iboende sikkerhet og kontrolltiltak som skal hindre feil og tap av kontroll.

Noen av argumentene for den alternative definisjonen sammenliknet med den som er benyttet i barriere-notatet er etter vår mening:

- At tiltakene kan være tekniske, operasjonelle eller organisatoriske er en utdyping som ikke behøver å inngå i selve definisjonen. Kan eventuelt inngå som merknad eller forklaring.
- Barrierer er planlagte tiltak, noe som bør inngå som del av definisjonen.
- Barrierer skal stoppe eller begrense en situasjon, ikke stoppe noe "før det har startet". For å unngå tap av kontroll har vi kontrolltiltak. Barrierer skal hindre en videre utvikling. (Helst vil vi unngå å komme i en situasjon hvor det er behov for barrierer.)

Barriere definisjonen er illustrert i figur A2.



**Figur A2** Barrierer versus iboende sikkerhet og kontrolltiltak

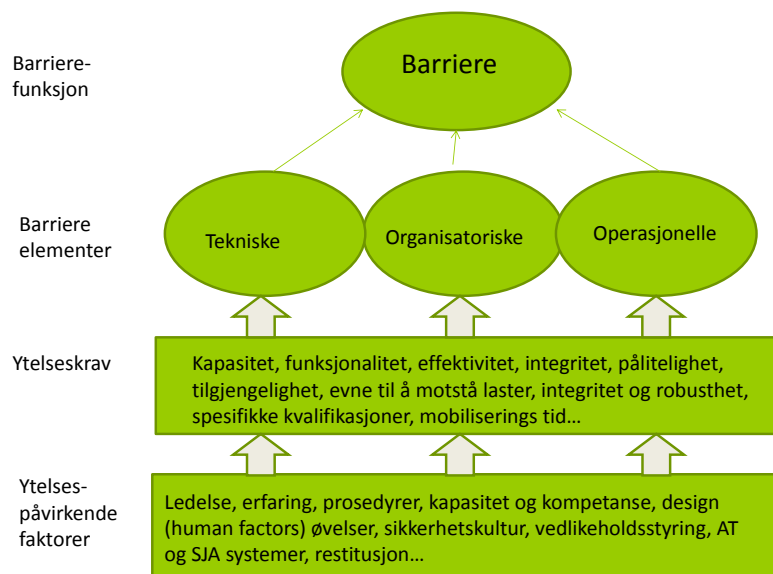
## A.7 Sammenhenger

Figur A3 skal illustrere forholdet mellom barrieren som skal ivareta en funksjon, barriereelementene, ytelseskrav og ytelsespåvirkende faktorer. Figur og beskrivelse baserer seg på en presentasjon fra Ptil (2013).

Eksempler på tekniske barriereelementer: Gassdetektorer, brannmotstand, nødavstengningsventiler, brannvann, BOP, divertere, evakueringsmidler...

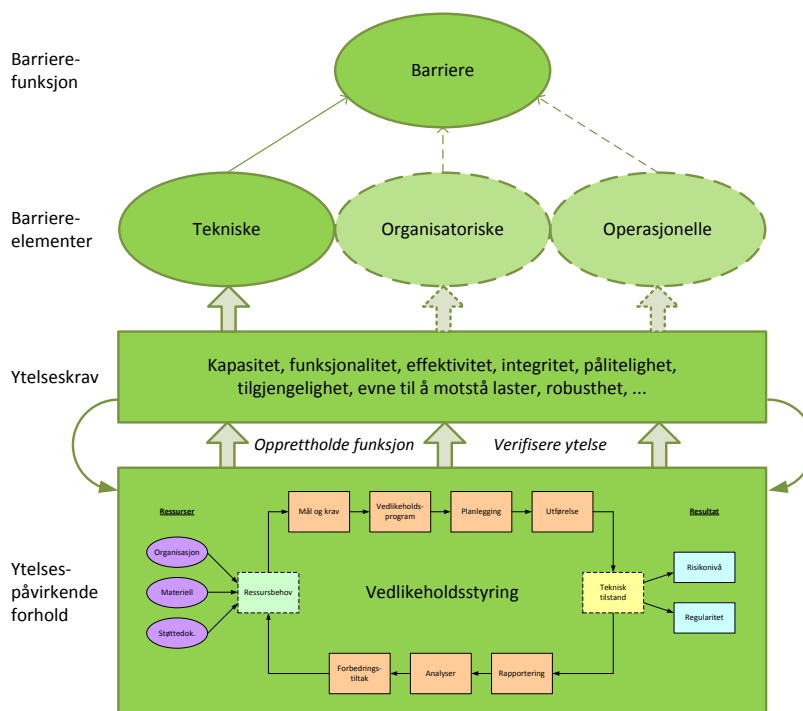
Eksempler på organisatoriske barriereelementer: Kontrollromsoperatør, mudlogger og borer, alarmreaksjonslag, beredskapsledelse, livbåtfører - altså personell med tilhørende roller som skal ivaretas for å realisere en barrierefunksjon.

Eksempler på operasjonelle barriereelementer: Utløse deluge og sette i verk trykkavlastning (hvis det ikke er gjort automatisk), overvåke innstrømming av formasjonsvæske fra brønnen, trykke på knappen for å stenge BOP'en, beslutte og iverksette evakuering, med andre ord de handlinger som personellet utfører for å realisere en barrierefunksjon.



**Figur A3** Sammenheng mellom definisjoner – i henhold til Ptil

Dersom vi tilpasser figuren og sammenhengen til vedlikehold/vedlikeholdsstyring kan dette illustreres som vist i figur A4.



**Figur A4** Sammenheng mellom definisjoner – tilpasset vedlikeholdsstyring

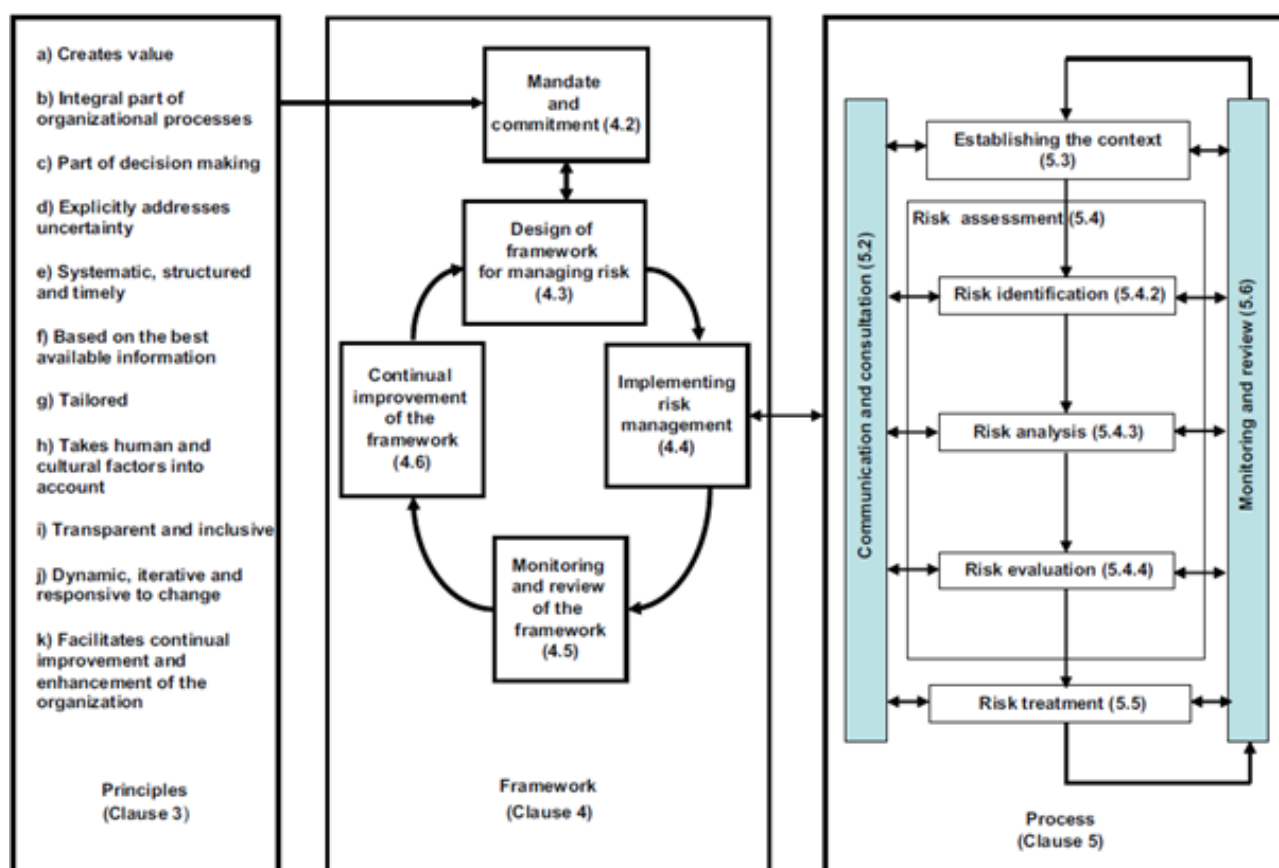
Vedlikeholdet skal bidra til å opprettholde barrierefunksjon og verifisere ytelsen til barrierene. Dette gjelder de tekniske barriereelementene (for vedlikehold som disiplin, jf. kapittel A3). Ytelseskravene påvirker også (stiller krav til) vedlikeholdsstyringen, som vist på figuren.



## Vedlegg B: ISO 31000

ISO 31000 /2/ har vært et sentralt grunnlagsdokument ved utarbeidelsen av Ptils barrierenotat /1/. ISO 31000 er en generell standard for risikostyring som består av 3 hovedelementer: Prinsipper for risikostyring (kapittel 3), rammeverk for risikostyring (kapittel 4) og risikostyringsprosessen (kapittel 5).

ISO 31000 skiller mellom prinsipper for risikostyring (venstre del av figur B1), rammeverk for risikostyring (midtre del) og "selve" risikostyringsprosessen (høyre del).



**Figur B1** Sammenheng mellom risikostyrings-prinsipper, -rammeverk og -prosess (/2/)

Prinsippene gir input til "mandat og forpliktelse" som igjen er styrende for rammeverket, eller mer presist "styringssløyfa for rammeverket" siden dette er utformet som en styringssløyfe (se midtre del av figuren). Rammeverket definerer rammebetingelsene for risikostyringsprosessen.

ISO 31000 inneholder kun 3 figurer som vist i figur B2. Figur 1 angir som nevnt sammenhengen mellom de 3 hovedelementene "prinsipper", "rammeverk" og "prosess". Figur 2 er en utdyping av "rammeverket", mens figur 3 kun er en gjengivelse av "prosessen".

Fig. 1

Utdyping av  
rammeverk

Gjengivelse  
av prosess

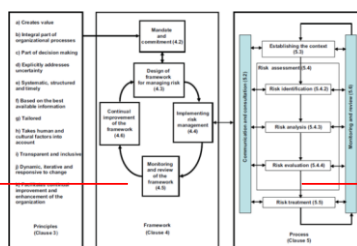
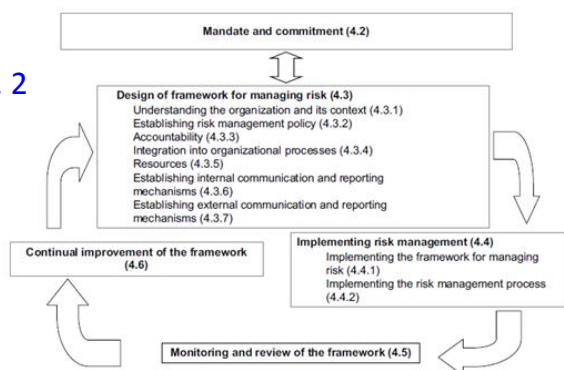
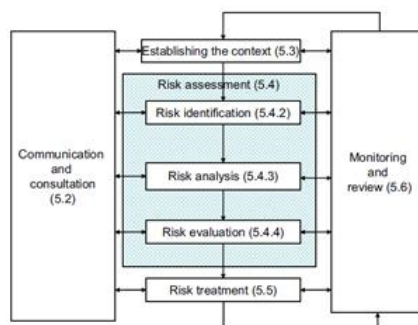


Fig. 2



Sammenheng mellom komponentene i rammeverket

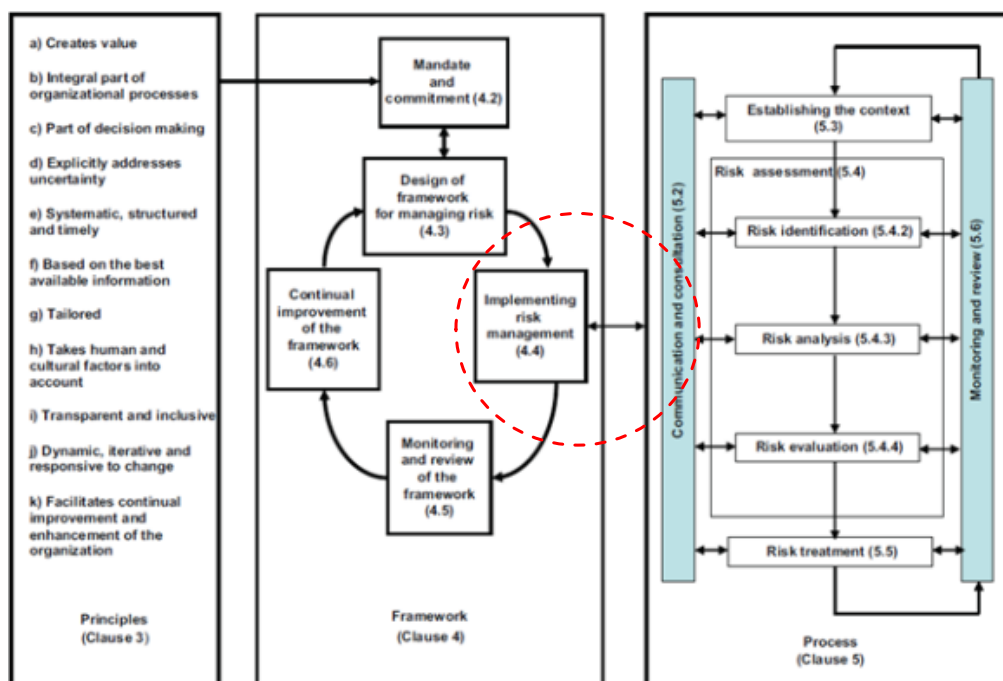
Fig. 3



Risikostyringsprosess

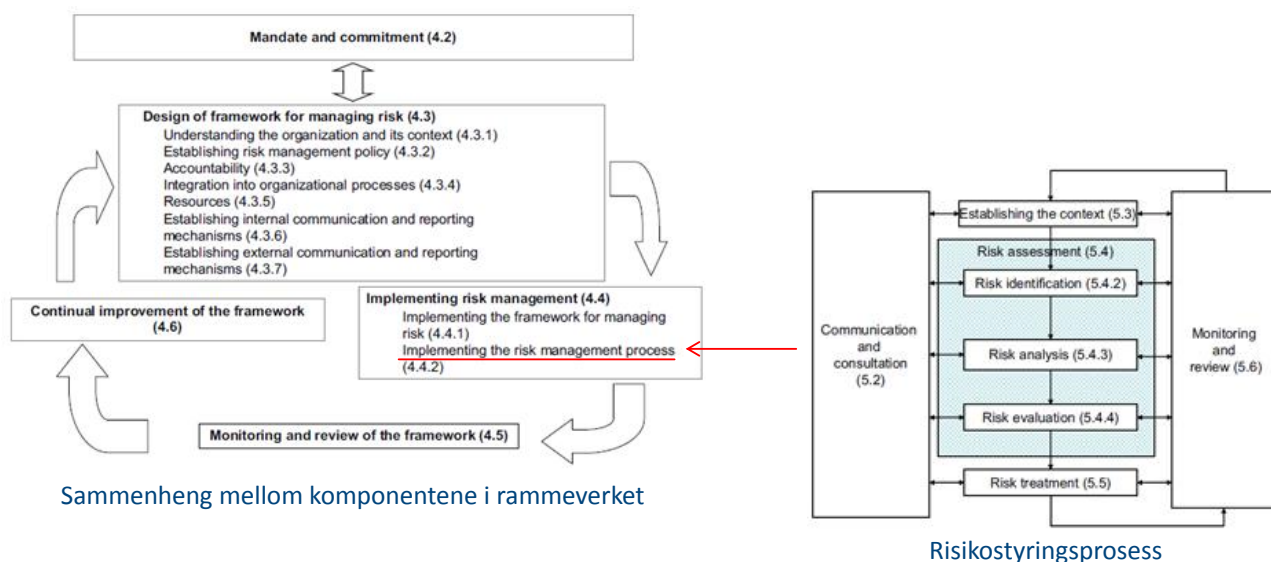
**Figur B2** Illustrasjoner benyttet i ISO 31000 /2/ – helhet, rammeverk og prosess (basert på /2/)

Av figur B3 (ISO 31000 figur 1) fremgår det tydelig at koplingen mellom "rammeverket" og "prosessen" går mellom implementeringsfasen av rammeverket (ikke hele "rammeverkssløyfa") og prosessen. De øvrige fasene i rammeverkssløyfa gjelder kun for "rammeverket" og ikke for "prosessen".



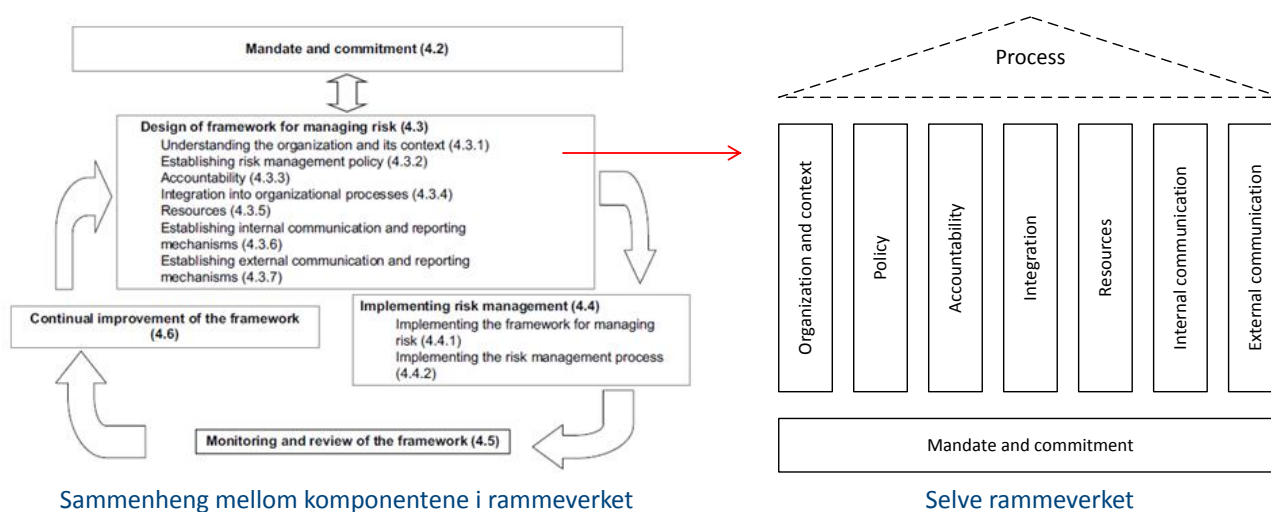
**Figur B3** Prosessen knyttet til implementeringsfasen av "rammeverkssløyfa" (basert på /2/)

Dette går enda tydeligere frem av figur B4 (ISO 31000 figur 2) som tydelig angir at implementeringsfasen (implementeringsboksen) består av 2 deler: Implementering av rammeverket for risikostyring og implementering av risikostyringsprosessen, mens de øvrige boksene kun omhandler "rammeverket".



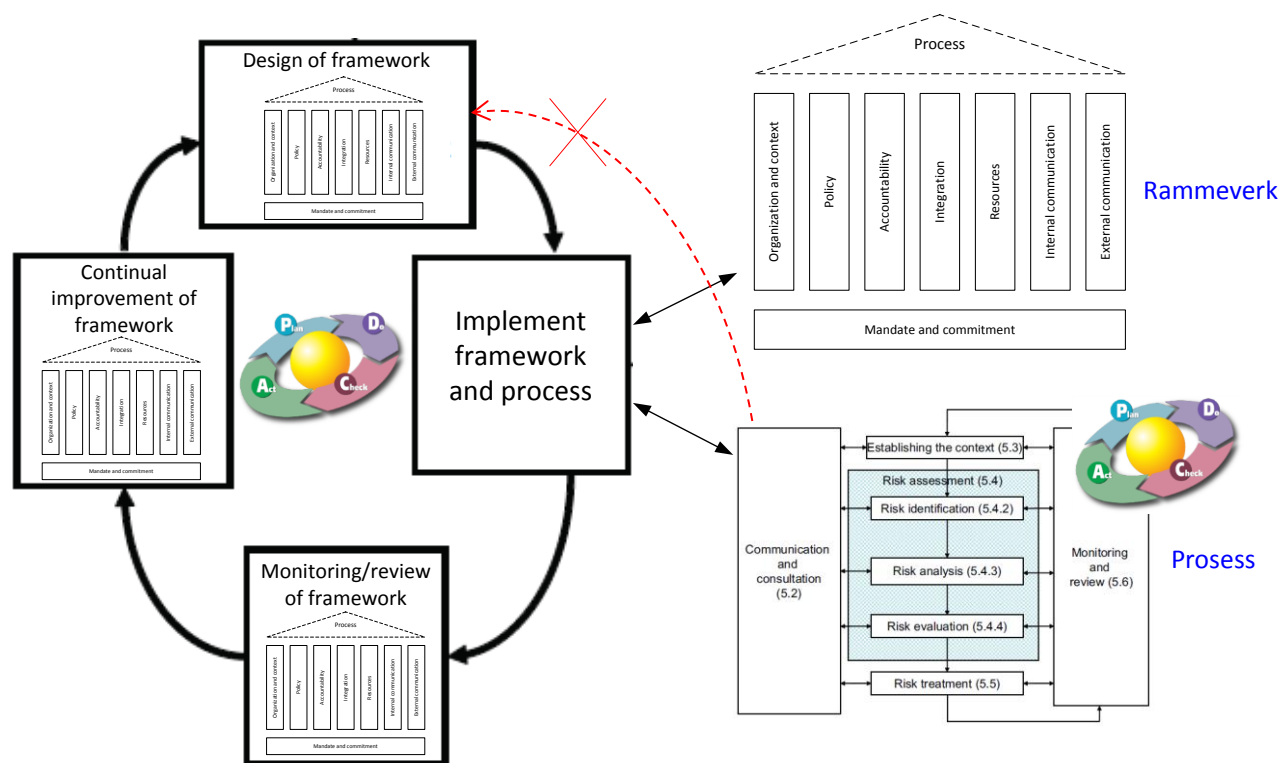
**Figur B4** Prosessen er *kun* knyttet til implementeringsfasen av rammeverkssløyfa (basert på /2/)

Hva "rammeverket" består av er angitt i boksen for design/etablering av rammeverket. Rammeverket kan illustreres som fundamentet og pilarene for risikostyringsprosessen, jf. figur B5. Dette må være på plass for at risikostyringsprosessen skal kunne integreres med organisasjonens overordnede styring, strategi og planlegging, ledelse, osv.



**Figur B5** Selve rammeverket – fundamentet for prosessen (basert på /2/)

Dersom vi nå benytter illustrasjonen av "rammeverket", så inngår denne i alle fasene/boksene i styringsløyfa for rammeverket (se figur B6) – også i den øverste boksen, mens risikostyringsprosessen kun inngår i den høyre boksen og har sin egen styringssløyfe(-r). "Styringssløyfa for rammeverket" og "risikostyringssløyfa" er altså 2 separate styringssløyfer/kontrollsløyfer.



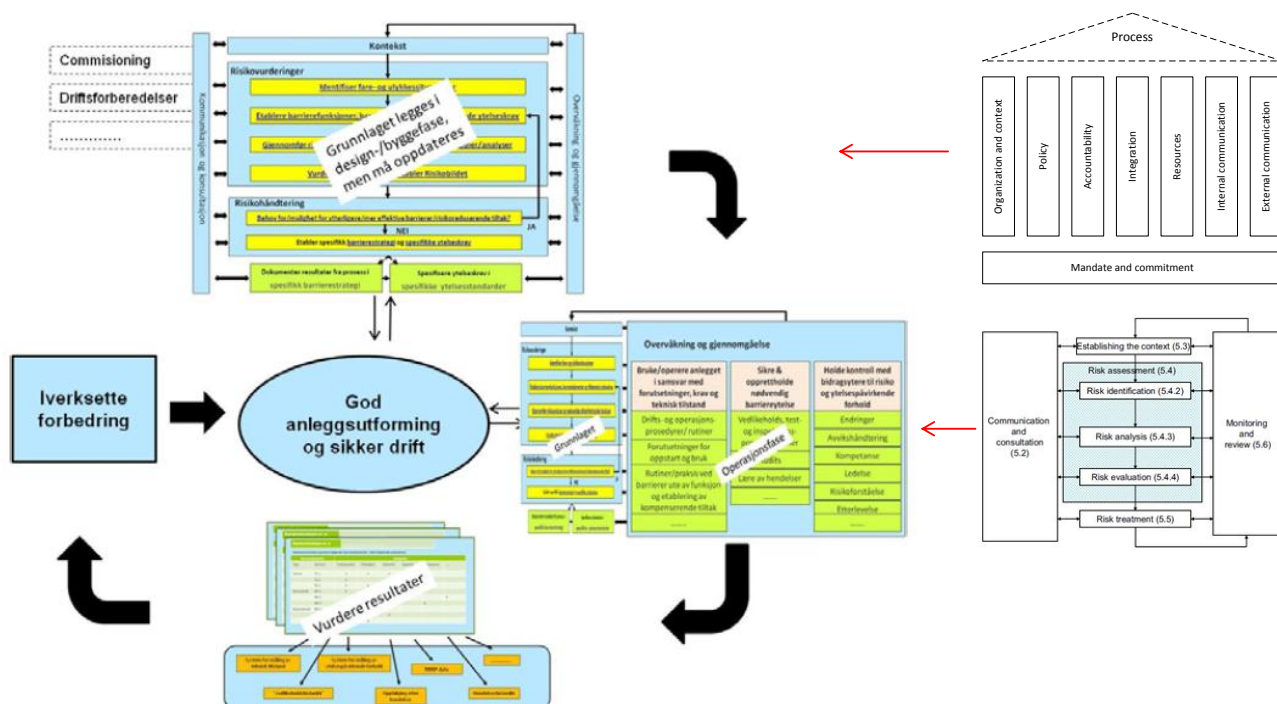
**Figur B6** To separate styringssløyfer; rammeverkssløyfa og risikostyringssløyfa (basert på /2/)

"Risikostyringssløyfa" er ikke en del av rammeverket og skal etter vår mening ikke inngå i den øverste boksen i "styringssløyfa for rammeverket" – slik det er gjort i barrierenotatet /1/.

Figuren som er hentet fra barrierenotatet /1/ (se figur B7) viser at barrierestyringsprosessen er tatt inn i designfasen (øverste boks) i styringssløyfa/kontrollsløyfa som i ISO 31000 er "forbeholdt" styringssløyfa/kontrollsløyfa for rammeverket. "Prosessen" (for risikostyring) er i henhold til ISO 31000 kun knyttet til etableringsfasen (høyre boks).

En alternativ fortolkning er at man i barrierenotatet /1/ mener det er tilstrekkelig med én kontrollsløyfe (og at man velger ikke å behandle "rammeverket" i en egen kontrollsløyfe).

Dette er imidlertid etter vår oppfatning ikke helt korrekt og det er også forvirrende i forhold til en ISO 31000 tilnærming. Dessuten burde en slik "forenklet" fortolkning (med bruk av kun én kontrollsløyfe) vært forklart og begrunnet i barrierenotatet. Enten bør man forholde seg til ISO 31000 og benytte to styringssløyfer, eller forenkle og kun benytte barrierestyringssløyfa, men da både forklare dette samt unngå å fremstille dette "identisk" med styringssløyfa for rammeverket. Figuren for barrierestyringsprosessen (i forbindelse med planlegging) er ei styringssløyfe i seg selv, eller riktigere flere styringssløyfer.



**Figur B7** Modell for barrierestyring – ikke i tråd med ISO 31000 (basert på /1/ og /2/)

Vi mener det kan være hensiktsmessig å holde fast på de to kontrollsløyfene ("kontrollsløyfa for rammeverket" og "kontrollsløyfa for barrierestyring") slik dette er gjort for risikostyring i ISO 31000, fordi styring av rammeverket (inklusive rammebetingelser som nødvendige ressurser) for barrierestyringen er fundamentet for å opprettholde god barrierestyring.

Dette er også en fordel ved at vi benytter ISO 31000 /2/ som et grunnlagsdokument som vi henter informasjon fra ut over det som er inkludert i barrierenotatet /1/.

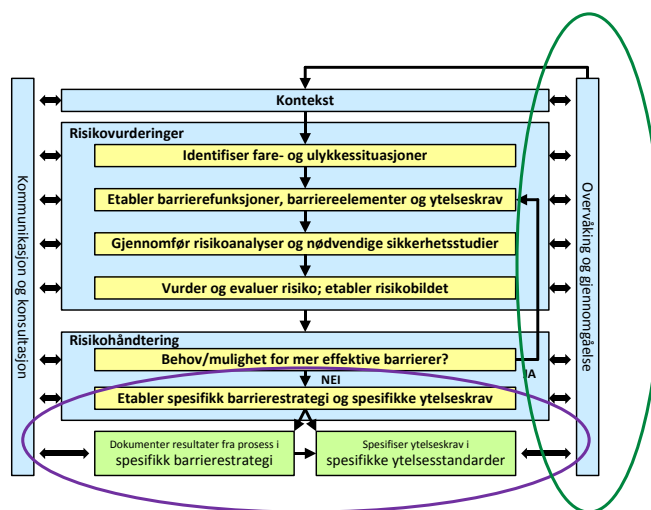


## Vedlegg C: Barrierenotatets behandling av vedlikehold/vedlikeholdsstyring

Barrierenotatet /1/ henviser til vedlikehold i følgende avsnitt (jf. innholdsfortegnelsen):

- Etablere spesifikk barrierestrategi og spesifikke ytelsesstandarder
- Overvåking og gjennomgåelse
- Hva er å betrakte som barriereelementer?
- Måling og verifisering av ytelse
- Vedlikeholdsstyring

De eneste trinnene i barrierestyingsprosessen hvor barrierenotatet omtaler vedlikehold er i siste trinn av "risikohåndteringen" og i "overvåking og gjennomgåelse", jf. figur C1.



**Figur C1** Omtale av vedlikehold i barrierenotatet

### Etablere spesifikk barrierestrategi og spesifikke ytelsesstandarder

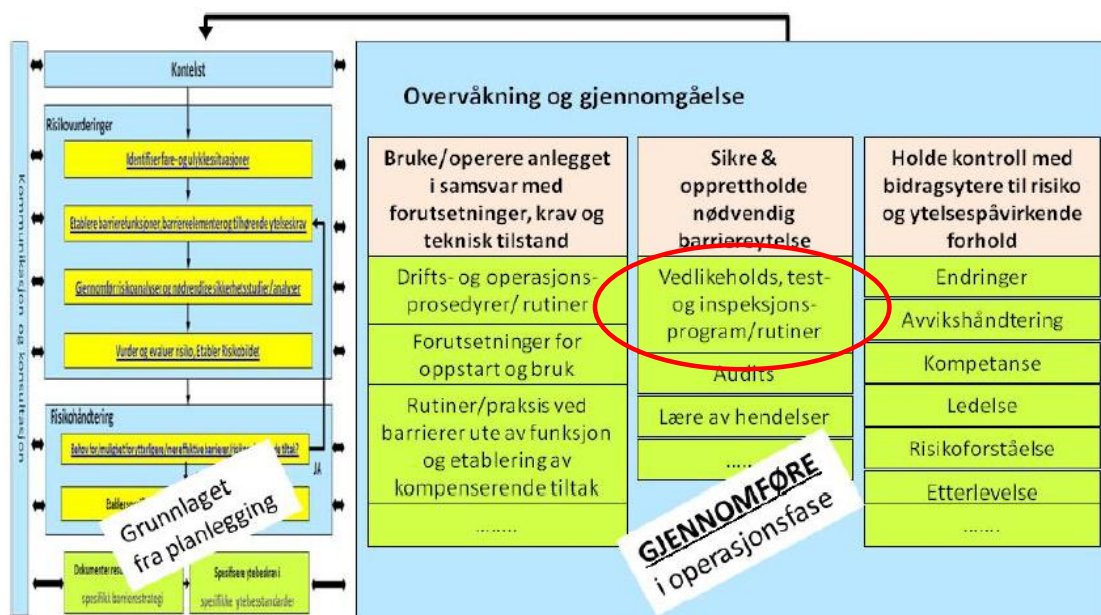
Spesifikke barrierestrategier og tilhørende ytelsesstandarder kan eksempelvis benyttes til:

- Identifisere og klassifisere systemer/utstyr med hensyn til konsekvenser av potensielle funksjonsfeil
- Planlegge og/eller utføre vedlikehold for å sikre ytelse til barrierefunksjoner og barriereelementer i alle faser av levetiden
- Osv.

### Overvåking og gjennomgåelse

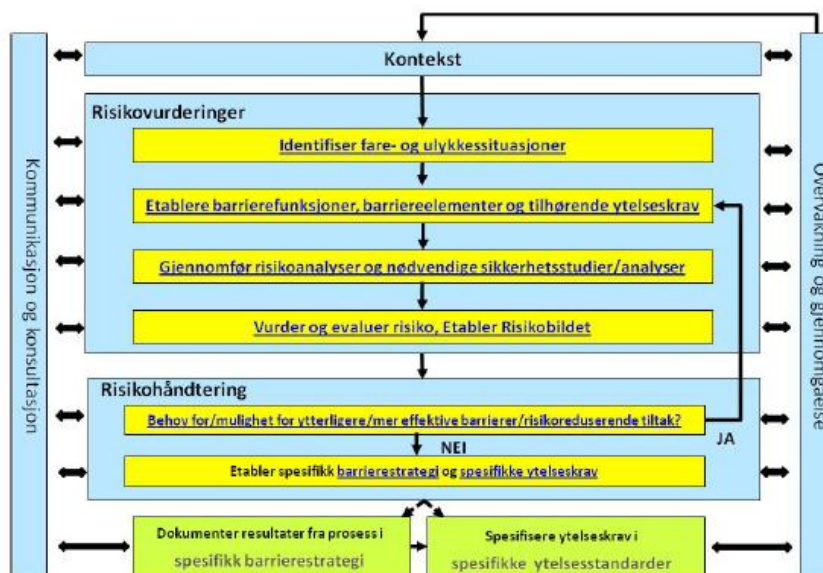
Figur C2 (figur 15 i barrierenotatet /1/) detaljerer boksen "overvåking og gjennomgåelse", og inkluderer noen av de forholdene som må følges opp for å sikre en god barrierestyling etter at strategi og ytelseskrav er etablert. Et av disse som eksplisitt nevner vedlikehold er "vedlikeholds, test- og inspeksjonsprogram/rutiner" (angitt med rød ellipse i figur C2).

Det vil være en rekke antakelser og forutsetning som legges til grunn når en gjennomfører prosessen illustrert i figur C3 (figur 6 i barrierenotatet /1/). Dette kan blant annet være forutsetninger om hvordan en innretning skal opereres eller antakelser som berører utførelse av test- og vedlikehold av utstyr.



Figur 15 Eksempler på sentrale elementer for å sikre god overvåkning og oppfølging

Figur C2 Inkludering av vedlikehold i overvåking og gjennomgåelse (basert på /1/)



Figur 6 Barrierestyringsprosess i forbindelse med planlegging

Figur C3 Vedlikehold inkludert (implisitt) som forutsetning/antakelse i barrierestyringsprosessen (/1/)

### Hva er å betrakte som barriereelementer?

Eksempelvis må det etableres et vedlikeholds- test- og inspeksjonsprogram som sikrer og verifiserer at de ulike ytelseskravene er ivaretatt. Betyr det at vedlikehold skal betraktes som en barrierefunksjon og/eller et barriereelement? Vedlikehold er en nødvendig forutsetning for at ytelsen til en barriere skal kunne opprettholdes over tid, men vedlikehold i seg selv er i denne sammenheng ikke å betrakte som en barrierefunksjon eller et barriereelement. Kvaliteten på vedlikeholdet, herunder planer og evnen til å opprettholde ytelsen for de ulike barrierene, vil derimot være *et sentralt ytelsespåvirkende forhold*.

### Måling og verifisering av ytelse

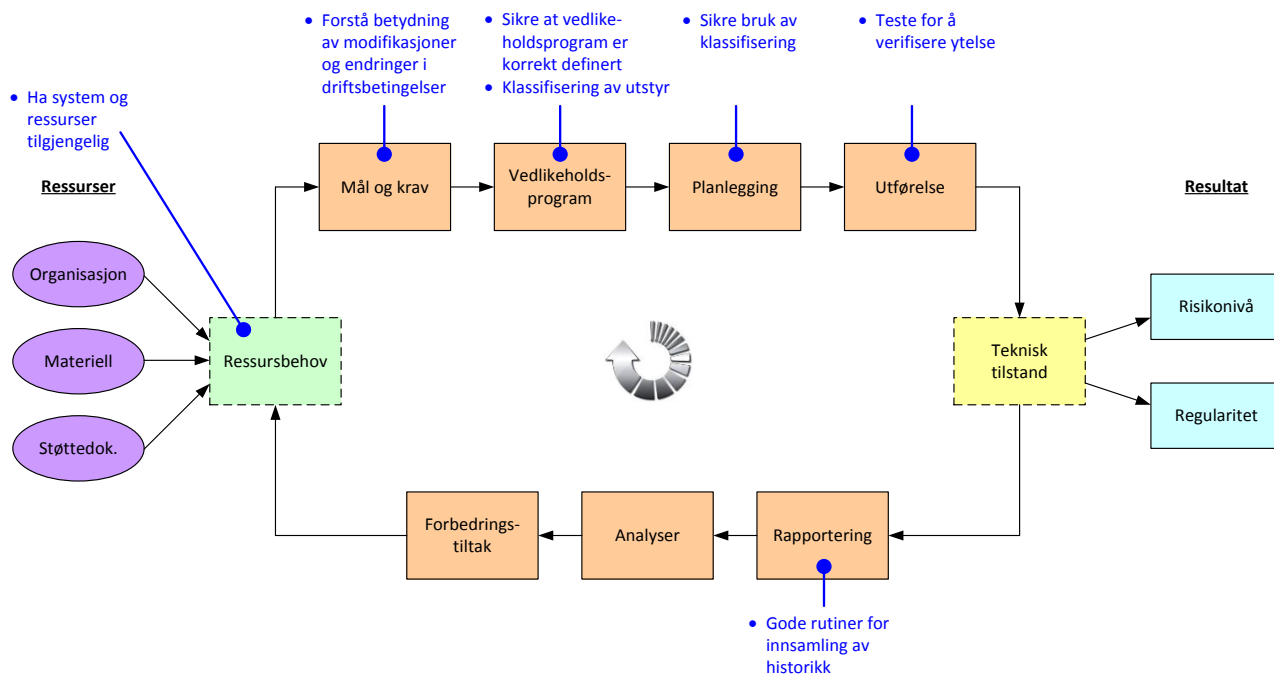
Regelverket stiller krav til at det skal være kjent hvilke barrierer som er ute av funksjon eller svekket. Det betinger at den ansvarlig etablerer systemer og prosesser som verifiserer at etablerte barrierefunksjoner og tilhørende barriereelementer har de tiltenkte egenskapene. For enkelte egenskaper, og da spesielt egenskaper til tekniske barriereelementer, vil test- og vedlikeholdsaktiviteter i mange tilfeller være en tjenlig løsning for å verifisere tilstand og samsvar med etablerte ytelseskrav. For en rekke andre egenskaper vil det derimot være behov for andre systemer og prosesser for å verifisere ytelse.

### Vedlikeholdsstyring

I forhold til vedlikeholdsstyring er det spesielt viktig å /1/:

- sikre at vedlikeholdsprogram er korrekt definert slik at programmet bidrar til opprettholdelse av nødvendig og helhetlig barriereytelse i alle faser av levetiden. Forebyggende vedlikehold som kan hindre degradering eller reduksjon av ytelse til barriereelementer er like viktig enten årsaker skyldes slitasje eller aldringsforhold.
- benytte informasjon fra barrierestrategi og ytelsesstandarder til klassifisering av utstyr og systemer mht. kritikalitet.
- sikre bruk av klassifiseringen, eksempelvis som del av beslutningsgrunnlaget ved prioritering av både korrektive jobber og for å angi krav til testing og vedlikehold av barriereelementer (enten dette kalles sikkerhetskritisk utstyr- eller sikkerhetskritiske elementer).
- teste barriereelementer slik at en verifiserer ytelsen ift tiltenkt bruk og rolle. Eksempelvis bør en teste ventiler under reelle driftsbetingelser, herunder:
  - At delugeventiler åpner etter at brannpumper har startet og trykksatt systemet oppstrøms ventilen.
  - At Ving ventil kan stenge ved den gjennomstrømning som kan inntreffe ved lekkasje/brudd i nedstrøms strømningsrør.
- ha gode rutiner mht. innsamling av historikk på utstyret, og bruke dette grunnlaget til ytelsesvurderinger og for å forbedre vedlikeholdet.
- ha system og ressurser tilgjengelig slik at man greier å ta unna planlagt og korrektivt vedlikehold
- forstå hva modifikasjoner eller endringer i driftsbetingelser/prosessbetingelser (som eksempelvis vanninnhold, trykk, temperatur) betyr i forhold til vedlikeholdsbehov, slik at vedlikeholdet kan tilpasses.

De fleste, men ikke alle, elementene i vedlikeholdsstyringssløyfa er inkludert i barrierenotatet. Analyser og forbedringstiltak er eksempelvis ikke kommentert, jf. figur C4.



**Figur C4** Elementer fra vedlikeholdssløyfa som er omtalt i barrierenotatet



Teknologi for et bedre samfunn

[www.sintef.no](http://www.sintef.no)