# Sikkerhetsstyringssystem for høytrafikkerte tunneler i drift


Prosjektoppgave skrevet av:
Corinne Chiodini, Solvor Sandal, Ole Jørgen Lind
og Tore Breisnes

EVU Sikkerhetsstyring Region øst
07.12.2007

# 1 Introduksjon

## *1.1 Målsetting*

Tunneler er en krevende del av vegnettet, både for trafikanten og vegholdere.

Ulykkesfrekvensen er lavere i tunneler enn på vegnettet utenfor. Men tunnelene utsetter trafikanter for en høyere risiko enn veg i dagen, fordi konsekvenser av trafikale hendelser, slik som motorstopp, ulykker, branner, er større i et lukket rom. For å kompensere den risiko, byr spesielt høytrafikkerte tunneler på flere muligheter til å begrense utvikling av hendelser, ved høy beredskap og avanserte tekniske systemer. Slike tiltak er kjent fra øvrige transportsystemer, som flygeledelse i lufttrafikken og togledelse i jernbanetrafikken.

Disse tekniske systemene gjør tunneler sårbare på grunn av deres kompleksitet og krav til pålitelighet. Daglig detekteres og registreres det en mengde hendelser i trafikkrommet, samt tekniske feil, som er av større eller mindre viktighet for sikkerheten til trafikantene.

Denne oppgaven analyserer hvordan etaten sikrer at svikt/feil og hendelser blir ivaretatt og behandlet (reaktivt). Deretter stiller vi spørsmål om hva og hvordan vi lærer av disse hendelsene, og om systemet kan forbedres for en bedre effektivitet og en bedre sikkerhet (proaktivt).

## *1.2 Metode*

Vi begynner med å beskrive systemet som vi vil analysere. Deretter setter vi fokus på oversvømmelsen i Oslofjordtunnelen der mange forskjellige feil (tekniske, menneskelige og organisatoriske) har ført til alvorlige konsekvenser. Vi analyserer feilene og tiltakene. I lyset av dette eksemplet, forsøker vi å analysere dagens sikkerhetsstyringssystem, og kommer med forslag til forbedringer.

Analysen av oversvømmelsen foretar vi ved bruk av STEP-metoden for å synliggjøre sikkerhetsproblemene som har forårsaket hendelsen. Hendelsen fremstår som en typisk systemulykke, og vi analyserer den ved hjelp av noen av de fem teoriene om systemulykker. [Rosness 2004]

Analysen av sikkerhetsstyringssystemet foretar vi ved bruk av Tinmannsviks modell [Tinmannsvik 2005] og sammenlikner relevante elementer med ledende prinsipper i de forskjellige teoriene om systemulykker eller ”organisational accidents”.

Her følger en oppsummering av de fem teoriene [Rosness 2004]:

1. *Energi og barriereperspektivet*. Ulykker kan bli forstått og hindret ved å fokusere på farlig energi og væremåter, som gjør at slik energi kan bli skilt fra sårbare mål (Gibson 1961; Haddon, 1970; 1980). Dette perspektivet er tatt med på grunn av dets påvirkning på praktisk sikkerhetsstyring.

2. Perrows teori om ”*Normal accidents*”, som forklarer store ulykker ut fra et misforhold mellom egenskapene for teknologien som skal kontrolleres og strukturen til organisasjonen som er ansvarlig for å kontrollere teknologien (1984). Denne teorien har framprovosert en nyttig diskusjon, hovedsakelig fordi den konkluderer med at noen

teknologier skulle vært forlatt i sin nåværende form, fordi de ikke kan bli tilfredsstillende kontrollert av noen tenkelig organisasjon.

3. Teorien om *høypålitelighetsorganisasjoner* (HRO) ble utviklet delvis som et motsvar til utfordringen som ble fremsatt av Normal accidents teorien (Rochin et al., 1987, La Porte og Consilini, 1991). HRO-teorien er basert på grundige studier av organisasjoner som har vist en fremtredende kapasitet til å håndtere ganske komplekse teknologier uten å få alvorlige ulykker. Viktige sider ved denne forskningen er *organisatorisk redundans* og en kapasitet i organisasjonen til omstilling for å tilpasse seg toppbelastning og kriser.

4. Informasjonsbehandlingsperspektivet har Turners teori om ”*Man-made disasters”* som utgangspunkt (Turner, 1978; Turner og Pigeon, 1997). I dette perspektivet er en ulykke sett på som et sammenbrudd i strømmen og forståelsen av informasjon som er knyttet til fysiske hendelser.

5. *Beslutningstakingsperspektivet* fokuserer på håndtering av motstridende mål. Her introduseres Rasmussens (1997) modell om aktiviteter som nærmer seg grensen for akseptabel utførelse, og også forestillingen om distribuert beslutningstaking.

# 2 Definisjon av sikkerhetsstyringssystemet

## *2.1 Systemets funksjon*

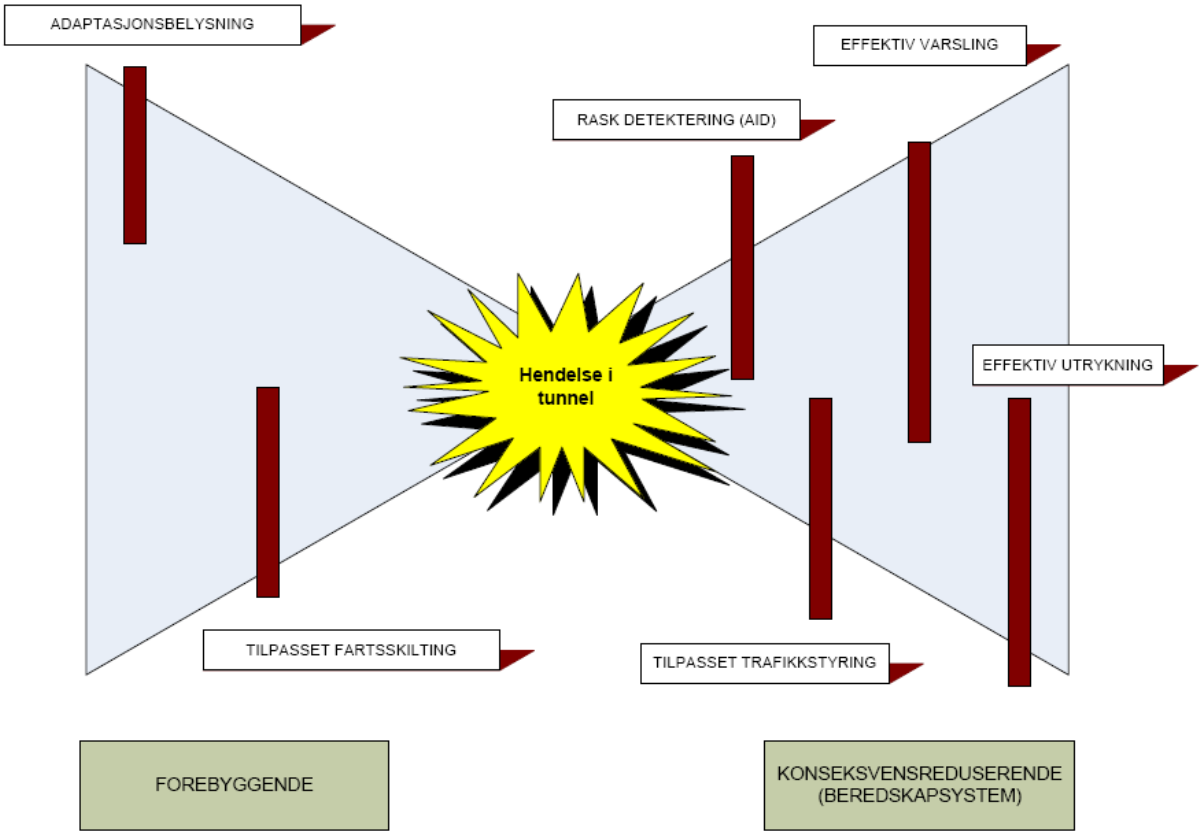
Som *sikkerhetssystem* velger vi organisasjonen rundt høytrafikkerte tunneler i Osloområdet. Vi betrakter kun eksisterende tunneler i drift og deres beredskapssystem, både ved trafikale hendelser og driftsfeil.

Systemet omfatter
- Tunnelene
- Vegtrafikksentralen (VTS) i Oslo, som overvåker tunnelene
- Driftsorganisasjonen, dvs. Statens vegvesen (SVV) og driftsentreprenører som opprettholder funksjonen til tunnelene
- Redningsetater, dvs. brannvesen, politi og ambulanse

**Funksjonen** av dette system er å ”produsere” sikkerhet ved å

- Hindre at hendelser forekommer (”forebyggende”) ved å oppfylle alle krav i dagens normaler [Hb021 2006]. Dette skal gi oss et sikkerhetsnivå i tråd med etatens akseptkriterier for sikkerhet (for eksempel belysning, ventilasjon, oppmerking, skilting).
  *Den forebyggende funksjonen i drift og vedlikehold er å opprettholde sikkerhetsnivået ved hjelp av systematisk forebyggende vedlikehold, inspeksjoner (funksjonskontrakter) og eventuelle reparasjoner/utskiftninger.*

- Hindre at hendelser utvikler seg til noe verre. Dette gjelder alle konsekvensreduserende tiltak, deriblant beredskapssystemet.
  *Funksjonen av systemet når en hendelse oppstår er å muliggjøre behandling av hendelsen, ivareta trafikkavviklingen for å unngå sekundære ulykker og muliggjøre retur til normal situasjon så fort som mulig.*




**Figur 1 Bowtie-figur for hendelser i vegtunneler, med eksempler på forebyggende og konsekvensreduserende barrierer**

## Barrierer

- Forebyggende barrierer
  *Belysning, fartskontroll, rumlefelt…*
- Konsekvensreduserende barrierer
  *Detektering, varsling, trafikkstyring, utrykning,…*

Konsekvensreduserende barrierer er hovedsakelig basert på beredskapssystemet, fordi standard på tunnelutrustningen påvirker direkte beredskapsytelsen gjennom responstiden.

Det beste eksemplet på dette er *detektering av hendelser*, som er det aller første skrittet i beredskapsarbeidet:

- Detektering av en hendelse (kjøretøystopp, gjenstand i vegbanen eller fortgjenger i tunnel) skjer i løpet av *noen sekunder* når tunnelen er utstyrt med AID (videoovervåknning med automatisk hendelsesdetektering)
- Når tunnelen er utstyrt kun med videokameraer, blir en hendelse detektert stort sett hvis det kommer varsling fra tunnelen, det vil si at noen tar en nødtelefon eller åpner brannskap. Da vil et bilde fra kamera ved den nødstasjonen som er i bruk, poppe opp for VTS-operatørene, slik at de får et bilde av situasjonen mens de kommuniserer med vedkommende. Beredskapsarbeidet vil antageligvis ikke starte før etter *noen minutter*, siden trafikanter må forlate kjøretøyet og ta i bruk utstyr de ikke er vant å betjene.

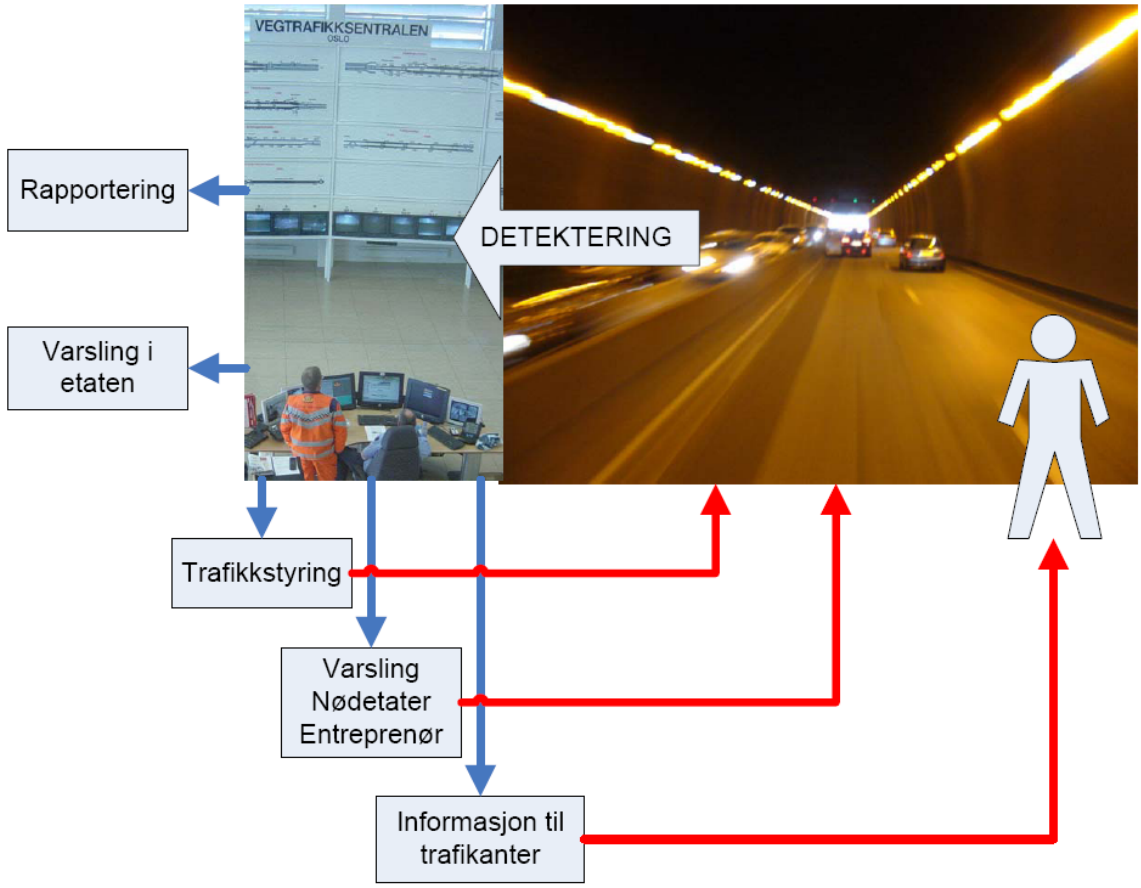
- Når tunnelen ikke er utstyrt med videoovervåkning, er VTS-operatørene fullstendig avhengige av varsling fra trafikanter i tunneler. Kvalitet på kommunikasjonen ved varsling er viktig for at det settes i gang relevante tiltak.

Et annet eksempel på hvordan tunnelutrustning påvirker beredskapen, og dermed sikkerhetsnivået, er *trafikkavviklingsfunksjoner*. Trafikkavvikling er viktig for å unngå sekundære ulykker, det vil si ulykker som oppstår som følge av en annen ulykke (for eksempel påkjøring av et stanset kjøretøy, av fotgjengere, eller påkjøringer bakfra på grunn av kø).

- Kjørefeltssignaler tillater stenging av et kjørefelt. Det er den raskeste stengingsformen, siden den kan settes i gang i løpet av noen sekunder og forstyrrer trafikken minimalt.
- Fjernstyrte bommer tillater stenging av et tunnelløp på kort tid. Stenging ved fjernstyrte bommer er den mest effektive stengingsformen, fordi det er en fysisk hindring kombinert med rødt vekselblink.
- Når det er installert manuelle bommer, brukes de kun av nødetater ved utrykning. Så lenge disse ikke har kommet til stedet, er tunnelen stengt ved at det blinker rødt ved tunnelinngangen. Våre erfaringer tilsier at dette er en lite pålitelig stengingsform.

Jo mer avanserte stengingssystemene er, desto mer krevende er de.
Drift- og vedlikehold påvirker direkte påliteligheten til disse systemene.

Oppgaven vil fokusere på konsekvensreduserende tiltak, det vil si sikkerhetsutrustning og beredskapssystemet, fordi det er avgjørende for sikkerhetsnivå i tunneler i drift. Sikkerhetsutrustning bestemmes av tunnelstandard. Den er fastsatt av regelverket gjennom plan- og byggefasen, men er avhengig av et velfungerende drifts- og vedlikeholdssystem for at sikkerhetsnivået skal bli opprettholdt.




**Figur 2 Beredskapssystemet for høytrafikkerte tunneler**

Beredskapssystemet er avhengig av et velfungerende sikkerhetssystem, både teknisk og organisatorisk, med tilfredsstillende pålitelighet. For at barrierene skal fungere, er et operativt og effektivt drift- og vedlikeholdssystem vesentlig. "Vi må ta hensyn til at barrierer kan forvitre og trenger å bli overvåket og vedlikeholdt" [Rosness 2004].

Beredskapssystemet for trafikale hendelser og teknisk svikt i høytrafikkerte tunneler i Stor-Oslo innbefatter, i grove trekk (se Figur 2).

- **Detektering av hendelser**
  I høytrafikkerte tunneler skjer detektering av *hendelser* i trafikkrommet ved videoovervåkning med automatisk hendelsesdetektering (AID), varsling fra trafikanter via nødtelefoner eller mobiltelefon, alarm ved bruk av brannslokkingsapparater.
- **Detektering av driftsfeil/-stans**
  Detektering av *driftsfeil/-stans* skjer ved alarmer/feilmeldinger til VTS.
- **Varsling**
  I henhold til prosedyrer, varsler VTS-operatørene etter behov nødetater, vaktbil, entreprenør.
- **Trafikkstyring**
  VTS iversetter trafikkavviklingstiltak (stenging av kjørefelt, tunnelløp, etablering av omkjøring)
- **Igangsettelse av andre tiltak**
  I henhold til prosedyrer: styring av ventilasjon ved brann, fullt lys i inngangssoner

- **Informasjon til trafikanter** (innsnakk på bilradio til trafikanter i tunnelen, vegmeldingstjeneste)
- **Rapportering ved logg**
  Alle hendelser, hendelser i trafikkrommet registreres i forskjellige systemer

Disse elementene er barrierefunksjoner i beredskapssystemet vårt.

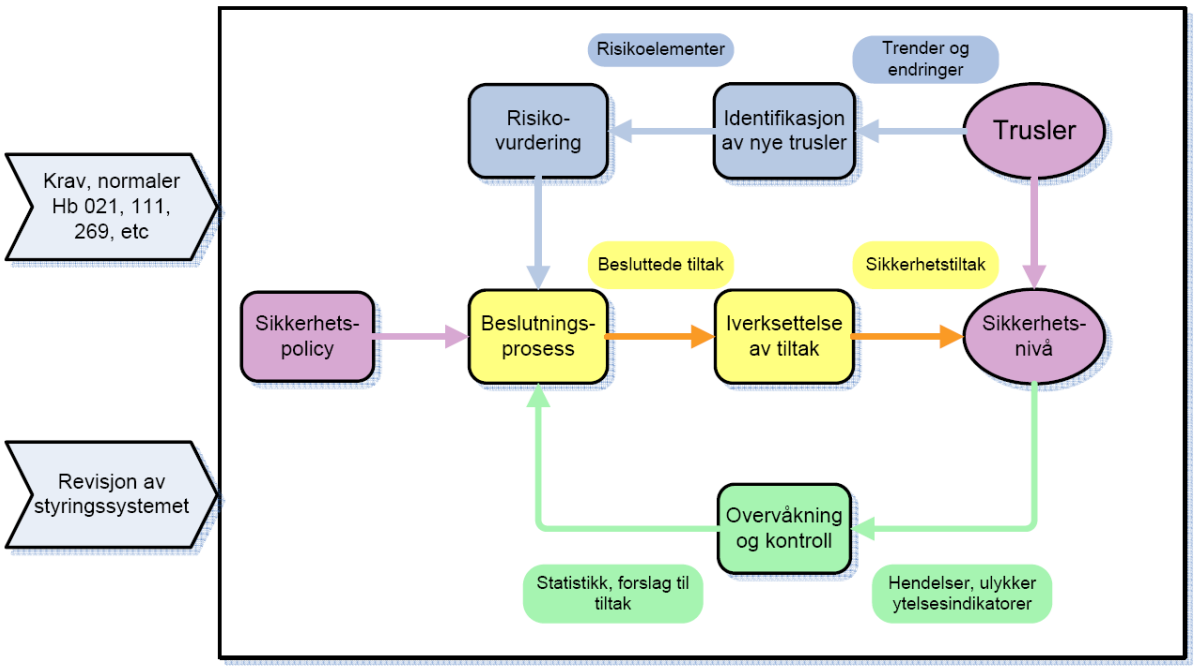
Vi har valgt å begrense oppgaven til det Statens vegvesen har ansvar for. Vi vil for eksempel ikke drøfte mulighetene for innsats fra nødetatene (politi, brannvesenet, ambulanse), selv om deres utrykningstid og tilgjengelige ressurser er et viktig aspekt for utgang, utvei, utfall, beredskapsarbeidet.

## *2.2 Sikkerhetsstyringssystemet*

Vi beskriver vårt sikkerhetsstyringssystem i lys av Tinmannsviks modellen [Tinmannsvik 2005].

Figur 3 viser en modell for sikkerhetsstyring. Den gir en oversikt over hvilke elementer og aktiviteter som må være tilstede for at en virksomhet skal kunne oppnå og opprettholde et ønsket sikkerhetsnivå. Pilene gir indikasjoner om sammenhenger, bl.a. hvordan resultatene fra en aktivitet kan være input til en annen aktivitet. I tillegg er det nødvendig å klarlegge hvem som har ansvar for de forskjellige aktivitetene, og dette er vist i side 9.

De ytre rammebetingelsene framgår av håndbok 021 Vegtunneler, håndbok 269 Sikkerhetsforvaltning av vegtunneler og håndbok 111 Standard for drift og vedlikehold. Gjennom disse kravene er det fastlagt et visst sikkerhetsnivå for bygging og drift av vegtunnelen. Revisjoner av styringssystemet er kvalitetssikring av systemet for å se at forutsatte tiltak følges opp.




**Figur 3 Tinmannsviks modell for sikkerhetsstyringssystemer [Tinmannsvik 2005].**

Sikkerhetspolicy i Statens vegvesen er knyttet til nullvisjonen, det vil si at hendelser i vegtrafikken ikke skal føre til drepte eller varig skadde. Dette innebærer fokus på de

alvorligste personskadeulykkene. I 2006-09 er målet i Region øst å redusere antall drepte og hardt skadde med 60. For drift av tunneler bør det utarbeides mer operative mål.

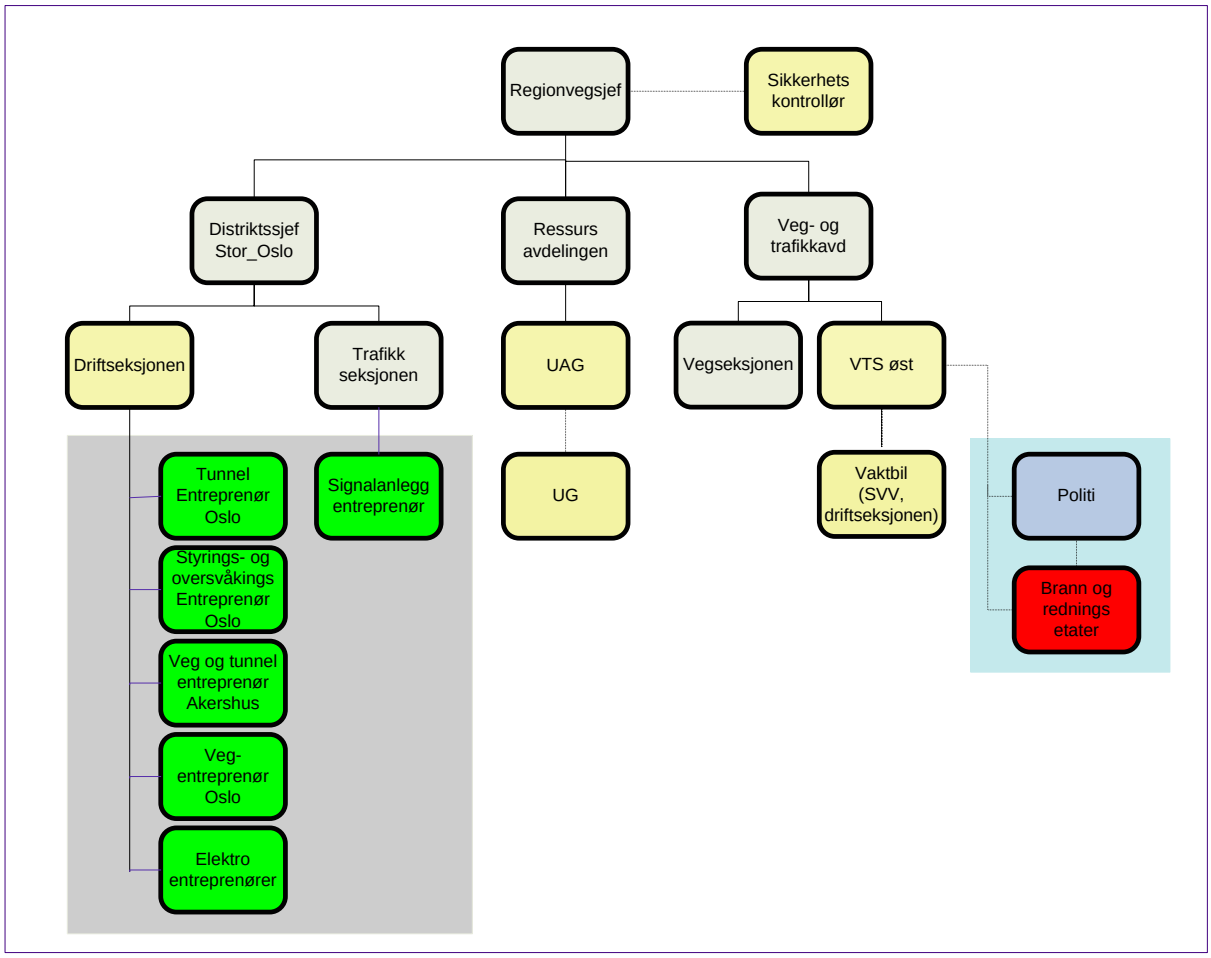
Sikkerhetsstyringssystemet omfatter:

- *en reaktiv del*: Når hendelser kommer i kontakt med sikkerhetsnivå, settes det i gang behandling, rapportering/analyse, beslutning med prioritering, eventuelt tiltak for endring av sikkerhetsnivået.
- *en proaktiv del*: Hvordan lærer organisasjonen av hendelser for å forebygge liknende situasjoner, andre trusler, utvikling av systemet.

Identifikasjon av trusler gjelder nye eller endrede forhold som kan påvirke sikkerhetsnivået knyttet til teknologi, økonomi, miljømessige eller driftsmessige forhold.

Beslutningsprosess innebærer en vurdering av behovet for iverksettelse av tiltak i forhold til målsetting for sikkerhet og akseptkriterier for risiko.

**Ansvarsforhold**
Organisasjonskartet i Figur 4 viser den delen av organisasjonen i Region øst som er sentral når det gjelder styringssystemet for tunneler i drift i Stor-Oslo. Nederst vises de eksterne utførende organisasjoner.




**Figur 4 Organisasjonskart for drift av veger i region øst**

Regionvegsjefen har det overordnede ansvar for all virksomhet i regionen. 13 enheter rapporterer til henne, herunder 7 distriktssjefer, leder av Prosjekt øst (store prosjekt), 4 ledere av styringsenheter på regionnivå og leder av ressursavdelingen.
Distriktssjefen har ansvar for framkommelighet og trafikksikkerhet i sitt distrikt, og ivaretar eieransvaret til vegnettet og tunnelene på vegne av regionvegsjefen.

Stor-Oslo distrikt har eieransvaret alle tunnelene i Oslo, Follo, Asker og Bærum. I distriktet ivaretas vegforvaltning, drift og vedlikehold av hhv. trafikk- og driftsseksjonen. Gruppa for trafikkstyring og elektro, en del av driftseksjonen, har et regionalt ansvar for sitt fagområde. Dette innebærer bl.a. at de er byggeledere på elektrokontrakter i flere distrikt. Dette arbeidet er basert på myndighet fra distriktssjefen.

Nedenfor følger en oversikt over de forskjellige aktørenes ansvarsområder for tunneler.

| ***Enhet*** | ***Ansvar og oppgaver for trafikkstyring, drift og vedlikehold*** |
|---|---|
| Vtr, vegseksjonen | Samordningsansvar for drift- og vedlikeholdsoppgaver. Fordeling av drifts- og vedlikeholdsmidler i regionen. |
| Sikkerhetskontrollør | Regionalt ansvar. Gir anbefalinger til Vegdirektoratet ved godkjenning av planer og ferdige tunneler. Har oppfølging av øvelser og hendelser. Kontrollerer opplæringen av innsatspersonell. |
| Elektroansvarlig | Regionalt ansvar. Kontrollerer at elektroforskriftene blir fulgt. |
| VTS | Overvåker og styrer trafikken i tunnelene. Formidler info til publikum. Varsler redningsetater og internt etter varslingsplanen. |
| Trafikkseksjonen (distrikt) | Ansvar for trafikkregulerende tiltak, f. eks skilting, stengningstillatelser, arbeidsvarsling og signalanlegg. |
| Driftseksjonen (*bygg, veg*) | Ansvar for drift- og vedlikehold av vegnettet inkludert det strukturelle i tunneler, det vil si rømningsveier, sluker, vann- og frostsikring m.m. |
| Driftseksjonen (*elektro*) | Ansvar for drift- og vedlikehold av elektroteknisk utstyr, overvåking og styring. Utvikling av overvåkings- og styringssystemer på VTS, samt kommunikasjonsnettet. Har også et regionalt ansvar bl.a. for utvikling av policy og retningslinjer for bruk av elektrisk utstyr. |
| Vaktbil (Driftseksjonen, elektro) | Byggherrens ”beredskap” i Oslo. Prioriterer trafikksikkerhet. Bistår ved trafikale hendelser. Ved behov tilkaller entreprenør. Har byggherreoppgaver, dvs. oppfølging av entreprenørene vha. stikkprøver (sjekk av sperringer, vedlikehold). Har faste inspeksjonsruter på vegnettet, (sjekk av pumpesumper, tekniske rom). |
| Brannvernleder (Driftseksjonen) | Kontaktperson for branntilsyn. Skal ivareta beredskapsplaner og arrangere beredskapsøvelser. |
| Entreprenører | Utfører drift- og vedlikeholdsoppgaver for distriktet. Har beredskap 24t i døgnet |
| Redningsetater | Bistår ved hendelser. Politiet har bemanning på VTS. |

# 3 Eksempel: Oversvømmelsen i Oslofjordtunnelen

I august 2003 skjedde det en oversvømmelse i Oslofjordtunnelen, som vakte stor oppmerksomhet i media og hadde store økonomiske konsekvenser. Den var forårsaket av en rekke hendelser og feil, som man ikke hadde klart å fange opp før det ble "for sent". Det hadde i de nærmeste årene før hendelsen vært flere tilløp til oversvømmelser i ulike tunneler. Disse situasjonene ble avverget så tidlig at det ikke oppsto skader, men spørsmålet er om man hadde lært noe av hendelsene?

Derfor ønsker vi å bruke dette eksemplet som et utgangspunkt for å analysere sikkerhetssystemet som vi har beskrevet.

## *3.1 Beskrivelse av et system som skulle være "mer enn godt nok"*

**Beskrivelse av pumpestasjonen:**
Oslofjordtunnelen har et lavbrekk som ligger ca 140 m under havnivå. Innlekkasjen er ca 1500 l/min og det er viktig at pumpestasjonen til enhver tid er i stand til å pumpe ut vannet som kommer inn.

- Pumpestasjon består av tre parallelle, likeverdige pumper som rullerer basert på driftstid. Ved ekstremt stort tilsig der en pumpe ikke klarer å ta unna vannet, vil suksessivt andre og tredje pumpe startes.
- Hver pumpe har stor nok kapasitet nok til å pumpe ut vannet.
- Anlegget fjernovervåkes fra VTS, 24t i døgnet og også av driftsentreprenør på dagtid. Ved forhøyet vannivå (over høyeste startnivå) skal det elektroniske styresystemet sende "høy alarm" til VTS.
- Ved svikt i det elektroniske styresystemet eller nivåmåleren, skal en flottør gi "kritisk høy" alarm uavhengig av pumpestyresystemet, men via det overordnede styresystemet i tunnelen.
- Det er også montert en flottør som vil stanse pumpene ved unormalt lav vannstand. Dette kunne oppstå ved feil i pumpestyresystemet eller nivåmåleren.

Anlegget ble bygget etter "best praksis". Som ekstra sikkerhetstiltak, ble det kjøpt inn en reservepumpe spesielt til dette anlegget, slik at det skulle alltid være 3 pumper i drift.

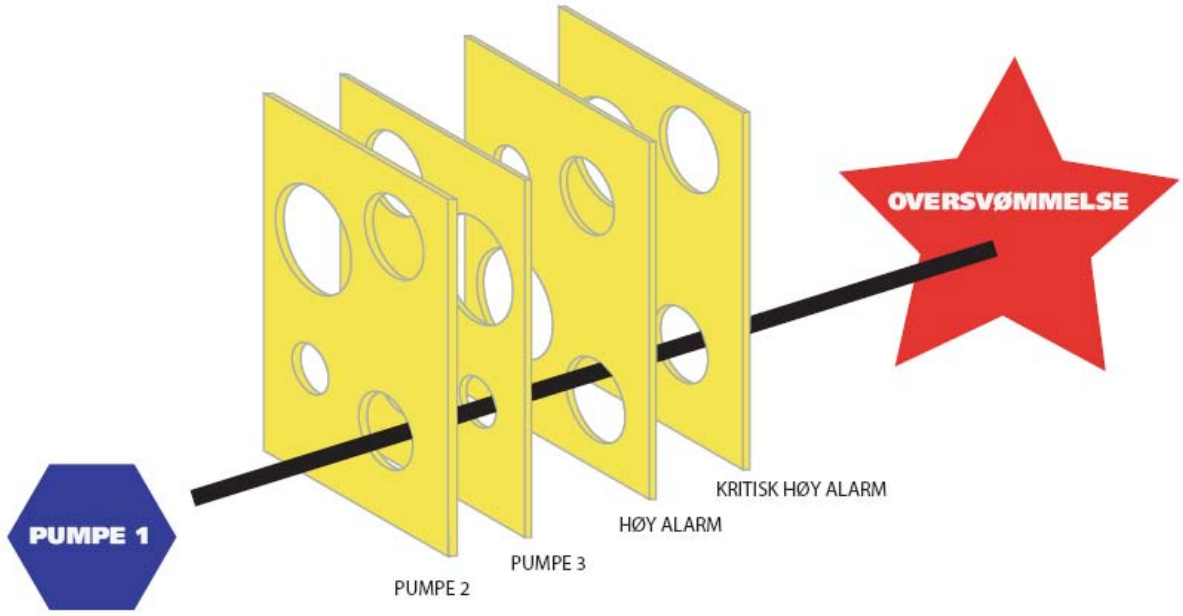
**Energi- og barrieremodell:**
I sitt avsnitt om "sterke sider og begrensninger av energi- og barrieremodellen", påpeker Rosness at i noen tilfeller er energiaspektet trivielt. I vårt tilfelle, er faren i systemet at vannet som strømmer inn i tunnelen kan forårsake oversvømmelse. Det kan føre til både trafikkfarlige situasjoner og store og kostbare ødeleggelser. Under bygging reduseres risikoen ved at det settes krav til maks tillatt innlekkasje. Faren for oversvømmelse kunne vært redusert ytterligere ved å redusere innlekkasjen med enda bedre tetting av tunnelen. Dette skapte en målkonflikt idet ytterligere tetting hadde medført store kostnader.

Etter at tunnelen er bygget er det lite som kan gjøres for å redusere innlekkasje. Det må settes barrierer for å hindre at den uønskede hendelsen oppstår. Barrierefunksjonen [Rosness 2004 (Haddon, Kjellen 2000)] mot oversvømmelse er at det pumpes vann ut av tunnelen.

I prosjekteringen av Oslofjordtunnelen ble det planlagt fire operasjonelle barrierer:

- Normalsituasjonen er at en pumpe står for utpumping av vannet.
- Barriere 1 er at andre pumpe starter ved svikt i første.
- Barriere 2 er at tredje pumpe starter ved svikt i begge de to foregående
- Barriere 3 er ”høy alarm” (ved nivå over startnivå for tredje pumpe) som ville sette i gang tiltak fra driftsentreprenør
- Barriere 4 er ”kritisk høy alarm” (som går utenom systemet for pumpestyring) som ville sette i gang tiltak fra driftsentreprenør

Beredskapsapparatet virket ikke som en egen barriere i dette systemet, fordi det ikke var utformet (designet) for å ivareta sikkerhetsbehovene. For eksempel skulle det foretas inspeksjoner av pumpesumpen kun annenhver uke, mens stopp av pumpene ville lede til oversvømmelsen i løpet av 2-3 døgn.




**Figur 5 Reasons modell [Reason 1997] for oversvømmelsen i Oslofjordtunnelen, med de fire barrierene som forsvant**

## *3.2 Analyse av hendelsen*

Hendelsen ble gransket i et samarbeid mellom Veritas og Statens vegvesen, og det er laget en egen rapport som beskriver hendelsesforløpet i detalj [Veritas 2003].
Vi har utformet STEP-diagram som viser de viktigste hendelsene som utløste oversvømmelsen.

STEP-diagrammet viser sikkerhetsproblem/årsaker som førte til at de 4 barrierene ble borte:

1. Ufullstendig testing ved overtagelse av anlegg.
2. Ingen prosedyre for uttesting etter utskifting.
3. Servicemann setter inn måler med feil måleområde.
   Ingen prosedyre for å finne riktig 0-punkt.
4. Endret måleområde => endrede forutsetninger.
   Ingen prosedyre for test etter utskifting.
5. Pumpen starter ikke siden den ikke er innkoblet etter service.
6. ”Lav” flottør stopper pumpe mens det elektroniske systemet samtidig gir startkommando. Konflikt mellom to system som begge styrer.

7. Kortvarige stoppimpulser gir tilsvarende kortvarige stanser.
8. Kontrollamper på tavlefront og VTS lyser grønt selv om det ikke pumpes vann.
9. Driftsentreprenør gir VTS beskjed om å overse alarm.
10. Driftsentreprenør forlater anlegget uten å forsikre seg om at vannstanden går ned.

Hendelsen var et sammentreff av så mange omstendigheter at det ville være svært vanskelig på forhånd å forutse at et slikt scenario. Man trodde man hadde laget et system som var elastisk/motstandsdyktig nok [Rosness 2004(Foster 1993)] til at enhver hendelse eller feilhandling skulle blitt ivaretatt av systemet eller detektert i overvåkningssystemet, slik at det kunne iverksette tiltak i beredskapssystemet.

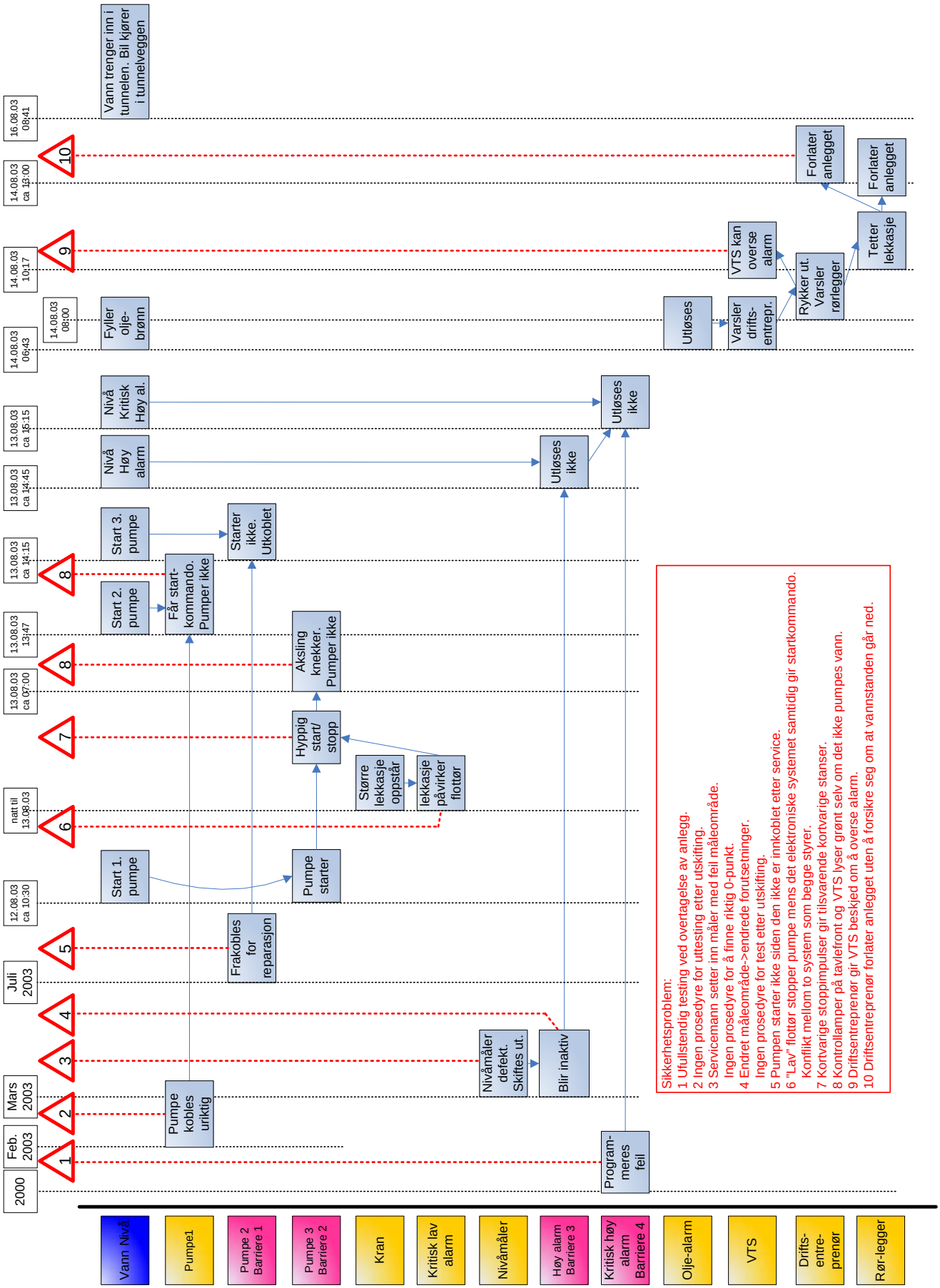
Det tekniske systemet viste seg under hendelsen å fungere *slik det var laget og programmert til å fungere*, og det var menneskelige aktiviteter som gjorde at systemet ikke oppførte slik det var tiltenkt.

Påliteligheten og effektiviteten av barrierene er i dette systemet i utgangspunktet gode, men sårbarheten viste seg å være stor. Systemet ble bygget med full tiltro til barrierene som ble etablert. Det var for eksempel ikke etablert visuelle inspeksjoner med en hyppighet som kunne avdekket hendelsen i tide når hendelsen først var i gang. Det var etablert regelmessige testrutiner, men disse var ikke tilpasset *barrierefunksjonen*, kun test av *barriereelementene*.

Overvåkningssystemet som ble bygget viste seg også å overvåke kun barriereelementer og ikke barrierefunksjonen. En annen svakhet i barrierene i systemet er at flere av elementene er avhengig av at styresystemet fungerer. For eksempel, ved en svikt i nivåmåleren vil tre av barrierene kunne bli satt ut av funksjon.

I hovedsak kan sikkerhetsproblemene og manglene som påpekes i rapporten [Veritas 2003] relateres til:

- **Menneskelige aspekt**
  - Programmeringsfeil, skyldes mangelfull spesifikasjon.
  - Driftsentreprenør og underentreprenører hadde ikke nok kunnskap om anlegget og forsto ikke feilsignalene. Dermed eskalerte hendelsen og ble til en ulykke. Manglende opplæring.
- **Teknisk aspekt**
  - Pumpestyresystemet var levert av tredjepart og var dårlig integrert i det overordnede systemet i tunnelen. Derfor var signalgangen til VTS begrenset til et fåtalls alarmer. Signalene eller indikatorene til VTS var til dels også direkte upålitelige. For eksempel var tilbakemelding på om pumpen virket kun et signal om at kontaktor var aktivert. Det var ingen tilbakemelding på at det ble pumpet vann.
- **Organisatorisk aspekt**
  - Dette systemet ble levert i ”bygg”-entreprisen som ble styrt av personell uten kompetanse på pumpestyring.
  - Kunnskap ble borte når produksjonsavdelingen ble skilt ut (Mesta) ved omorganiseringen i 2003.
  - Driftsentreprenøren (Mesta) hadde ansvar for forskjellige underentreprenører
  - Vegvesenet, som har ansvar for sikkerheten, ble etter omorganiseringen fjernere fra systemet idet en hadde kontrakt med en driftsentreprenør. Under hendelsen var ikke vegvesenet tilstede før oversvømmelsen var et faktum




**Figur 6 Step-diagram over oversvømmelsen i Oslofjordtunnelen.**

Veritas' granskning av hendelsen avdekker mangler på mange stadier.
Granskningen avdekket såkalte "direkte årsaker" til hendelsen:

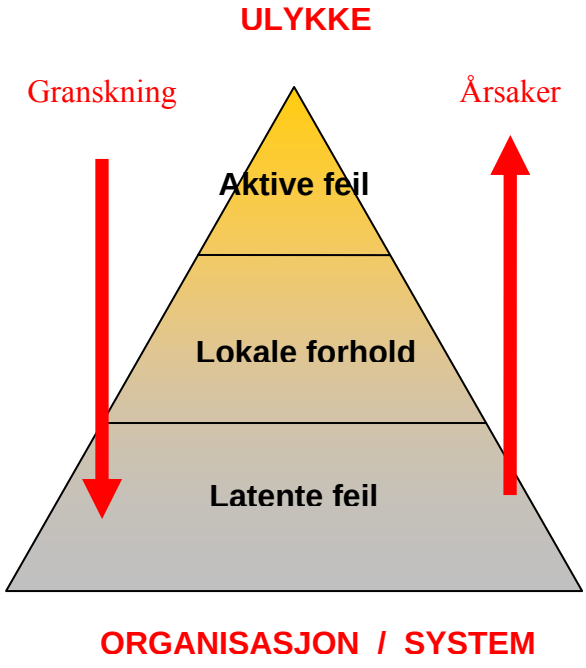
- Svikt i pumpesystemet
- Feil i systemet for overføring av alarmer.

Granskningen pekte videre på mange mangler ved det organisatoriske i rapporten kalt "indirekte årsaker" til hendelsen:

- Spesifikasjon og design av anlegget fra byggherres side
- Oppfølging fra byggherre i byggefasen
- Overlevering fra prosjekt til drift
- Dokumentasjon
- Drift og vedlikehold / Opplæring
- Operasjonsprosedyre

**Hendelsen sett i lys av Reasons teori:**
Reason skiller mellom to typer feil: *aktive feil* (individuelle feilhandlinger) og *latente feil* (usynlige feilproduserende forhold) [Reason 1997].

- *Aktive feil* er de synlige feilene som leder mest direkte til feilhandlinger og eventuelt ulykker. De er for eksempel manglende kunnskap eller dårlige holdninger.
- Aktive feil er et produkt av, eller er nær knyttet til *lokale forhold.* Disse er f.eks. utforming, vedlikehold, opplæring, dokumentasjon, etc.
- Latente feil skaper forutsetninger til (noen) lokale forhold og til feilhandlingene. De er f.eks. lover, regler for design, sikkerhetskultur.




**Figur 7 Reasons trekant**

Konklusjonen i rapporten er at det meste som gikk galt i Oslofjordtunnelen skyldtes *latente feil,* deriblant manglende kunnskap som relateres til nederste nivå i Reasons trekant. Dette forårsaket de aktive feilene underveis. Feilene har dels vært der hele tiden eller har oppstått

underveis som følge av manglende kunnskap og prosedyrer. Hendelsen må derfor sees på som en *systemulykke* der små feil førte til en stor hendelse.

Beskrivelsen av hendelsesforløpet viser at det var forskjellige aktiviteter (*aktive feil*) utført av forskjellige aktører i forkant av hendelsen som hadde ført til at barrierene forvitret i systemet uten at noen oppdaget det.

**Hendelsen sett i lys av Turner: "Man-made accidents"**
Turners teori "Man-made accidents" forklarer ulykker som en feil i informasjonsflyten, som følge av mangel på informasjon og på misforståelser [Rosness 2004 (Turner 1978)]. Han beskriver at i de fleste ulykker er det som regel indikasjoner (faresignaler) på at noe er galt på et tidlig stadium, men at dette ikke oppfattes.

I vårt tilfelle hadde vi hatt flere tilløp til oversvømmelser, uten at det ble gjort noen analyse for å avdekke eventuelle svakheter i systemet. I Oslofjordtunnelen ble en pumpe satt inn i et halvt år før oversvømmelsen uten at denne ble testet tilstrekkelig. Resultatet ble at pumpen "gikk" (lyste grønt), men det ble ikke pumpet vann. Loggen fra systemet viser i ettertid at hver gang denne pumpen ble "startet", gikk det kun kort tid før neste pumpe 2 startet. Det er en klar indikasjon at den første pumpen ikke pumpet vann, men det *fantes verken tekniske system eller kunnskap* blant de som overvåket prosessen til å *forstå dette faresignalet*.

Driftsentreprenøren og underleverandører ble sendt ned i tunnelen på grunn av alarmer, men misoppfattet situasjonen og *overså faresignaler*, dels på grunn av mangel på kompetanse og opplæring, dels på grunn av kompleksitet i situasjonen.

Selve alarmene var dårlig tilpasset som indikatorer, fordi de ikke ga VTS den riktige informasjonen til å forstå situasjonen. Det man trenger å vite, er ikke om pumpen går (barriereelementet fungerer) men om den pumper nok vann (barrierefunksjon er i orden).

**Perrow, normalulykker**
Sett i lys av Perrows teori om normalulykker [Rosness 2004] ser vi pumpestasjonen som et relativt komplekst og middels tett koblet system. Det er ikke en tidskritisk prosess, men manglende indikatorer til å detektere avvik gjør at en pumpesvikt ubønnhørlig vil føre til oversvømmelse.

Den høye kompleksiteten i anlegget tilsier både sentralisert og desentralisert styring, noe som i dette tilfelle var på plass (VTS og entreprenør). Systemet var imidlertid så komplekst at aktørene som var involvert, ikke forsto dem fullt ut (Nancy Leveson - Systemperspektiv).

**High Reliability-teori**
Om pumping i Oslofjordtunnelen skulle betraktes som en HRO, ville tiltakene fokusere på opprettelse av et robust og motstandsdyktig sikkerhetsstyringssystem [Rosness 2004] hovedsakelig ved hjelp av organisatorisk redundans.

I 4.2.1 Loop A: Operativ drift stilles det spørsmål om det er organisatorisk redundans både på VTS og hos driftsentreprenører, i vår daglige drift av tunneler.

Når det gjelder oversvømmelsen, ville den organisatoriske redundansen lokalt hos entreprenøren vært tilstrekkelig om kompetansen og opplæring hadde vært tilpasset kompleksitet på anlegget.

### *3.3 Tiltakene etter oversvømmelsen*

Etter hendelsen ble det satt i gang arbeid med å bygge ny pumpestyring.
Det opprinnelige styresystemet ga svært begrenset informasjon til VTS, kun enkle feilmeldinger og alarmer. Utfra erkjennelsen av at en ikke har fantasi nok til å forutse alle scenarier som kan oppstå, ble den nye pumpestyringen bygget med fokus på at menneskelig feilhandling ikke skal kunne få fatale følger.

Det ble iverksatt *tekniske og operasjonelle tiltak* i anlegget [Veritas 2003], som skal detektere de menneskelige feilhandlingene eller konsekvensen av disse. Dette oppnås bl.a. ved diagnostisering av hver enkelt pumpe og trendkurver som viser vannivå, trykk og effekt på pumper. Det er etablert flere alarmer for å varsle uregelmessigheter som kan være tegn på feil i systemet. Systemet er bygget "failsafe", slik at utfall av systemet eller kommunikasjon vil gi alarm.

Dette er ifølge [Rosness 2001] tiltak som er basert på ren *instrumentell* eller *operasjonell redundans*. Spørsmålet er om at mangel på *organisatorisk* redundans hos driftsentreprenør gjør systemet for lite robust. For eksempel, hvis en medarbeider med lite kompetanse (sommerhjelp) skulle være innblandet i oppretting av en teknisk feil, ville et system med lite organisatorisk redundans klare å sikre at medarbeideren vil forstå alvoret i de signalene han vil oppfatte?

Tiltakene er i hovedsak *reaktive*, men omfanget av hendelsen gjorde at det også ble iverksatt proaktive tiltak. I Oslofjord ble det blant annet installert full videoovervåkning av tunnelen for å bedre sikkerheten for trafikantene.

Som forsøk på *proaktive* tiltak etter hendelsen, ble det iverksatt undersøkelser av de øvrige pumpestasjonene for å avdekke om de hadde tilsvarende svakheter, og det ble utført endringer i en del av stasjonene. Vegdirektoratet iverksatte også daglige inspeksjoner av alle undersjøiske pumpestasjoner, inntil alle pumpeanlegg var kontrollert og testet opp mot svakhetene som ble avdekket under hendelsen.

Videoovervåkning er et godt eksempel på et *reaktivt* tiltak som kunne vært *proaktivt*, men ble avvist gjennom beslutningsprosessen. Installering av videoovervåkning hadde blitt foreslått ved flere anledninger før oversvømmelsen, av både brannvesenet og vegkontoret. Dette (proaktive) forslaget til tiltak ble avvist av Vegdirektoratet fordi tunnelen ville få en sikkerhetsstandard som var vurdert som for høy i forhold til dens tunnelklasse.

På organisatorisk plan er det, etter denne og andre hendelser i vegvesenet, satt større fokus på og krav til oppfølging i byggefasen og uttesting ved overlevering til "drift". Likeledes er det satt svært høye krav til dokumentasjon og operasjonsprosedyrer. Etter at EU-direktivet om sikkerhet i vegtunneler kom, er det utarbeidet en egen håndbok med krav til dokumentasjon (Hb 269).

Det har imidlertid ikke ført til endrede rapporteringsrutiner eller rutiner for analyse av uønskede hendelser.

### *3.4 Bruker vi lærdommen av denne hendelse?*

Det at det ble en stor hendelse i Oslofjordtunnelen gjorde at hele organisasjonen inkludert øverste ledelse ble involvert og det ble iverksatt tiltak for å unngå nye tilsvarende hendelser.

Ved tidligere tilløp til tilsvarende hendelser ble dette ikke systematisk rapportert oppover i systemet. Hendelsene ble registrert og rapportert i systemet, men tiltakene besto kun i avviksbehandling for å normalisere situasjonen. Siden disse tilløpene "bare" var uønskede hendelser uten personskade var det ingen som hadde som oppgave å analysere hendelsene for å avsløre eventuelle latente feil.

Skal man referere til modellen i 2.2 [Tinmannsvik 2005], kan vi bygge en teori om at

- den *proaktive* delen antageligvis ikke er i bruk
- den *reaktive* delen består av 2 atskilte systemer: et operativt ett og et langsiktig ett.

I lys av dette eksemplet stilles flere spørsmål:

- Blir registreringen av tekniske feil og hendelser brukt til noe?
- Hvordan registrerer vi feil i behandlingen i den operative driften?
- Hvordan lærer vi at den operative driften?
- Hvordan fungerer vårt system i den proaktive delen?
- Hva baserer beslutningsprosessen seg på?

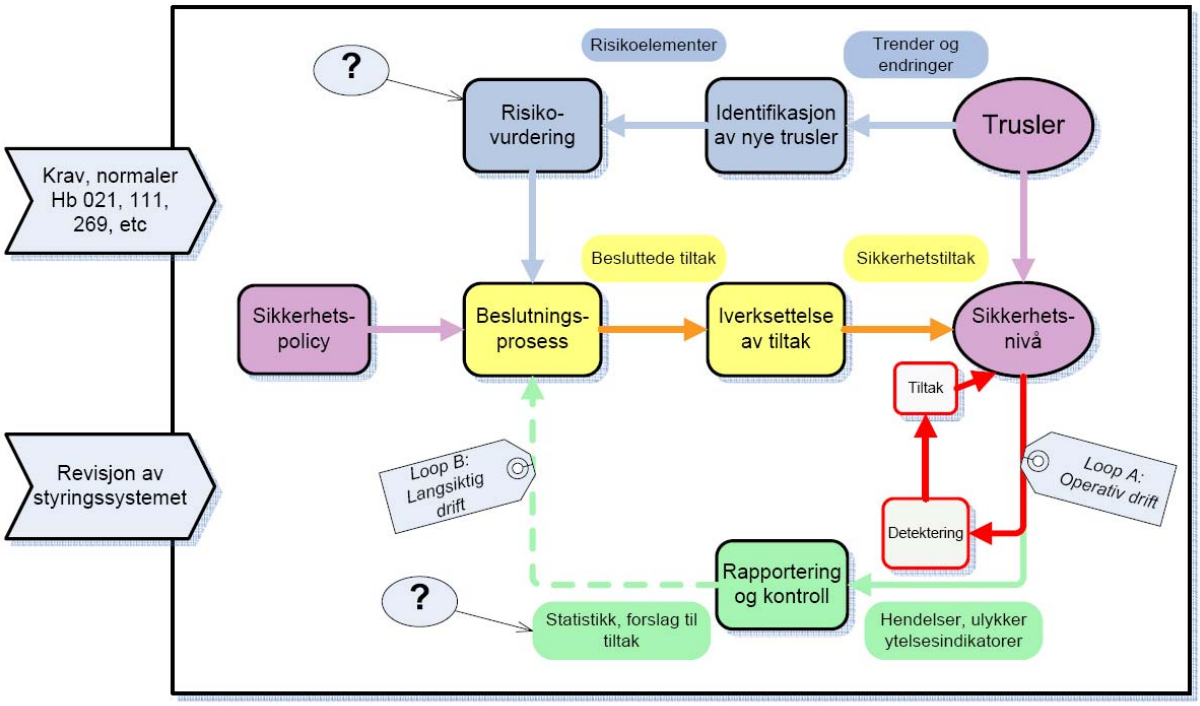
# 4 Analyse av systemet

Her vil vi drøfte vår hypotese

- Organisasjonen fungerer bra i den daglige avvikshåndteringen, men er ikke optimalt designet for å takle systemulykker
- Tilbakemeldinger fra hendelser og svikt kommer ikke systematisk videre inn i sikkerhetsstyringssystemet
- Organisasjonen lærer kun av katastrofale hendelser
- Risikovurderinger fullføres ikke systematisk for tunneler (eller tunnelsystemet, vegnettet) i drift

I Tinmannsviks-modellen [Tinmannsvik 2005] vil det illustreres med

- en loop for "*operativ drift*" eller "loop A", som består av detektering og fortløpende igangsettelse av tiltak. Hendelsen eller feilen registreres, samt deres behandling. *Er det operative systemet robust og motstandsdyktig?*
- en loop for "*langsiktig drift*" eller "loop B", som skulle bære videre i systemet lærdommen fra hendelser og avvik. *Fullfører loopen sin rolle systematisk, eller kun ved katastrofale hendelser?*
- en proaktiv loop med risikovurdering. *Fungerer den?*

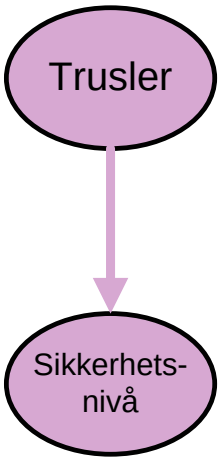



**Figur 8 Vår teoretiske Tinmannsvik-modell, revidert i lys av våre konklusjoner etter oversvømmelsen i Oslofjordtunnelen.**

## *4.1 Trusler og sikkerhetsnivå*

**Trusler**: Hendelser av betydning for trafikantenes sikkerhet.

- *trafikale hendelser* (motorstopp, gjenstand i vegbanen, ulykker, brann, velt, …)
- *interne hendelser* (oversvømmelser, ras, tekniske feil)




**Sikkerhetsnivå**: Evnen tunnelene og beredskapssystemet har til å identifisere trusler, behandle og komme tilbake til normalen.

- Sikkerhetsnivået er fastsatt av regelverket (og sikkerhetspolicy når det finnes).
- Drift og vedlikehold skal opprettholde sikkerhetsnivået, gjennom funksjonskontrakter og beredskap for teknisk feil.

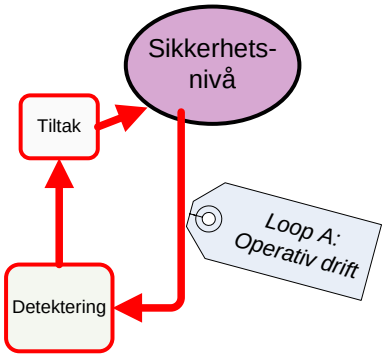
**Trusselvurdering.**

- Trafikkutviklingen er større enn planlagt, og køer i tunnelene er et økende problem.
- Tungtransporten øker mer enn den generelle trafikkutviklingen.
- Omfanget av farlig gods øker. Hvordan er restriksjonene på farlig gods i tunnelene. Er det sikrere å ha slike transporter i tunnelene enn utenfor med tanke på skadepotensial ved eksplosjoner og forurensing.
- Terrorsituasjonen kan medføre sabotasjeaksjoner i tunnelene
- Bortfall av strøm kan medføre at overvåking og styring av tunnelene blir borte. Tunnelene må tømmes. Hva med trafikkavviklingen deretter?

## 4.2 Den reaktive delen

*Denne delen handler om å løse problemer som oppstår, enten de er trafikale hendelser eller teknisk svikt.*

### 4.2.1 Loop A: Operativ drift




*Loop A gjelder fortløpende behandling av hendelser og feil.*

Den operative driften fungerer som avvikshåndtering. Den fungerer stort sett effektivt og godt. Vi har gode beredskapsordninger, kommunikasjonskanaler, vaktoperatører med lang erfaring, velfungerende styrings- og overvåkingssystemer.

Likevel stiller oversvømmelsen i Oslofjordtunnelen, som typisk systemulykke, spørsmål om hvor *sårbar* vår operative drift er.

Ifølge [Rosness 2004], skal man analysere hvordan systemulykker er knyttet til organisasjonens egenskaper i normal drift[1].

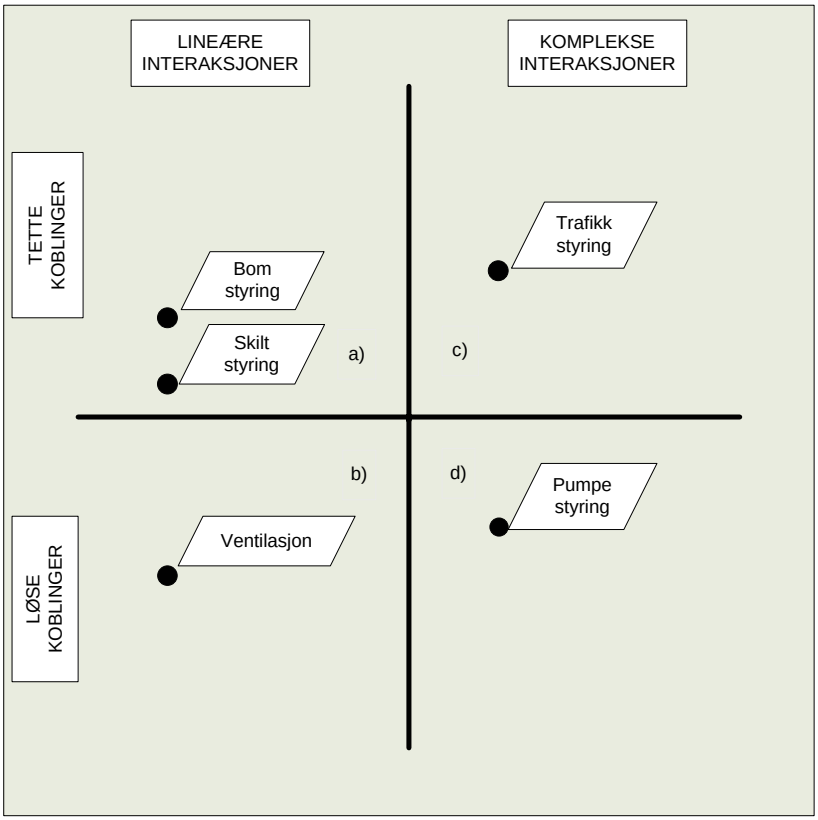
**Sentralisert eller desentralisert styring**

Ifølge "Normal accident"-teorien [Rosness 2004 (Perrow 1984)], forklares slike ulykker med en "*misforhold mellom teknologien som skal kontrolleres og strukturen til organisasjonen som er ansvarlig for kontrollen.*" Systemet kan klassifiseres i mer eller mindre tette koblinger, og lineære/komplekse interaksjoner.

Sikkerhetssystemet for tunneler har forskjellig grad av kompleksitet/koblingstetthet.
Vi kan klassifisere våre fysiske barriereelementer (tunnelutrustning) slik:

a) Bom- og skiltstyring er enkle systemer (en kommando). De må fungere umiddelbart for å opprettholde sin funksjon: så lenge bommen ikke senkes, er ikke tunnelen stengt og barrierefunksjonen "stenging" er ute.
b) Ventilasjon er et enkelt system (en kommando). Hvis en vifte er ute av drift, kan de andre viftene ivareta et akseptabelt nivå, dermed er ikke barrieren ute (løs kopling)
c) Avansert trafikkstyring er både kompliserte systemer (flere kommandoer og tilbakemeldinger, programmering) og enkle feil kan lede til raske store konsekvenser.
d) Pumpestyring er komplisert system men teknisk redundans (med flere pumper) skal sikre at barrierefunksjonen blir ivaretatt.

[1] "How organizational accidents are related to the properties for the organization during normal operations"




**Figur 9 Kompleksitet og koblinger i vårt tekniske sikkerhetssystem - Perrow "Normal accidents"**

Eksemplene a) og b) krever ifølge Perrow en sentralisert styring. Det er det vi har med VTS. For kompliserte og tette systemer, anbefaler Perrow at det brukes både sentralisert og desentralisert styring (som c)). Dette kan ivaretas i vårt system i en kombinasjon av sentralisert styring fra VTS og en lokal styring fra driftsentreprenører.
*En viktig utfordring er grensenittet mellom disse to styringene.*

High Reliability- organisasjoner (HRO) beviser i praksis at den utfordringen kan løses ved hjelp av systematisk redundans[2] [Rosness 2004 (Rochin 1987)].

**Teknisk redundans**
Styringssystemene er redundante gjennom duplisering. Det er tokrets-systemer som forsikrer at hvis en del av systemet svikter, tar den andre over, for å ivareta funksjonen som sviktet.

| | ***Dagens situasjon*** | ***Merknad*** |
|---|---|---|
| *Tunnel* | I tunnelene er de viktigste systemene teknisk redundante, det vil si at kommunikasjon og til en viss grad styresystem. Dette sikrer detektering av tekniske feil og overføring av alarmer. | *Teknisk redundant* |
| *VTS* | På VTS, vegtrafikksentralen øst, er styringssystemene teknisk redundante, dvs. at det finnes to servere. Skjer det noe med selve bygget, så begge svikter, har vi ikke noe reservesystem. | *Teknisk redundant, men på samme sted* |

[2]"HRO can handle complex technologies by organisational redundancy"

| | | |
|---|---|---|
| *Vaktbil* | Når teknikken svikter har vi en beredskap som skal tre i kraft ved at vaktbilen, driftsentreprenør og/eller politiet rykker ut for å sikre skadested hvis f. eks en bom ikke vil gå ned. Dette tar selvfølgelig lengre tid, og vi kan risikere å få sekundære hendelser. | *Organisatorisk redundans ved teknisk svikt. Begrenset beredskap.* |

**Organisatorisk redundans**
Organisatorisk redundans er definert som "samhandlingsmønstre som setter en organisasjon i stand til å utføre oppgaver mer pålitelig enn enkeltperson" [Rosness 2001].

| | ***Dagens situasjon*** | ***Merknad*** |
|---|---|---|
| *VTS* | VTS har en minimums bemanning på to vaktoperatører. Med dagens store og avanserte anlegg utfører to operatører de mest omfattende trafikkstyringene, så de kan dobbeltsjekke og rådføre seg med hverandre. For å avvikle trafikken toveis i et løp kreves det to vaktoperatører. Kun en sperring kan utføres på en gang, i normal situasjon. Til tider kan det være opptil 11 sperringer på en kveld. | *VTS er organisatorisk redundant, men med store begrensninger.* |
| *VTS* | Alle operatørene har tilgang til styrings- og varslingssystemene. De får inn varsler om feil og alarmer fra tunnelutrustning i alarmloggen, og varsel i styringsbilde. Til en hver tid er det mange "stående" alarmer i loggen (for eksempel åpning/lukking av en dør), og en viktig alarm kan fort forsvinne i mengden.<br>VTS har en egen tavle i styringsrommet hvor kritiske feil for trafikkregulering er notert. Denne blir løpende oppdatert av operatørene. | *Operasjonell og organisatorisk redundans men "drukning" av alarmer.* |
| *Drift* | Avvik behandles i tur og orden under ansvar av elektrogruppen. På grunn av lav bemanning og mangel på faglig ledelse, kan ikke mannskap drive med noe annet enn "brannslokking". | *Lavt bemanningsnivå fører til tap av organisatorisk redundans [Rosness 2001]* |

At riktig kompetanse finnes på riktig sted i organisasjonen er en forutsetning for den kulturelle organisatoriske redundansen. Det skal tildeles mye ressurser til "utvikling og vedlikehold av individuell og kollektiv kompetanse" [Rosness 2004].

| | ***Dagens situasjon*** | ***Problem*** |
|---|---|---|
| *VTS* | Alle VTS-operatørene skal ha simulatortrening med faggruppeleder en gang i året for å trene på sjeldne faresituasjoner. Andre oppgaver tar stadig mer tid hos faggruppelederen, og det begrenser tid til slik trening. | *Tilfredsstillende opplæringsopplegg, men begrenset mannskap.* |
| *Entrepr.* | Eksemplet i kapittel 3 viste at entreprenøren ikke hadde nok kunnskap om anlegget til å tolke faresignalene. Det finnes ikke tilfredsstillende bevis på at de har dette i dag. Det mangler systematisk opplæring eller kontroll av kompetanse fra SVV side. | *Krav om kompetanse og opplæring hos entreprenør, men mangel på oppfølging.* |

| | | |
|---|---|---|
| *Drift* | Det stilles spørsmål ved om det foreligger tilstrekkelig dokumentasjon. | *Dokumentasjon er kanskje ikke tilpasset sikkerhetsbehovene.* |

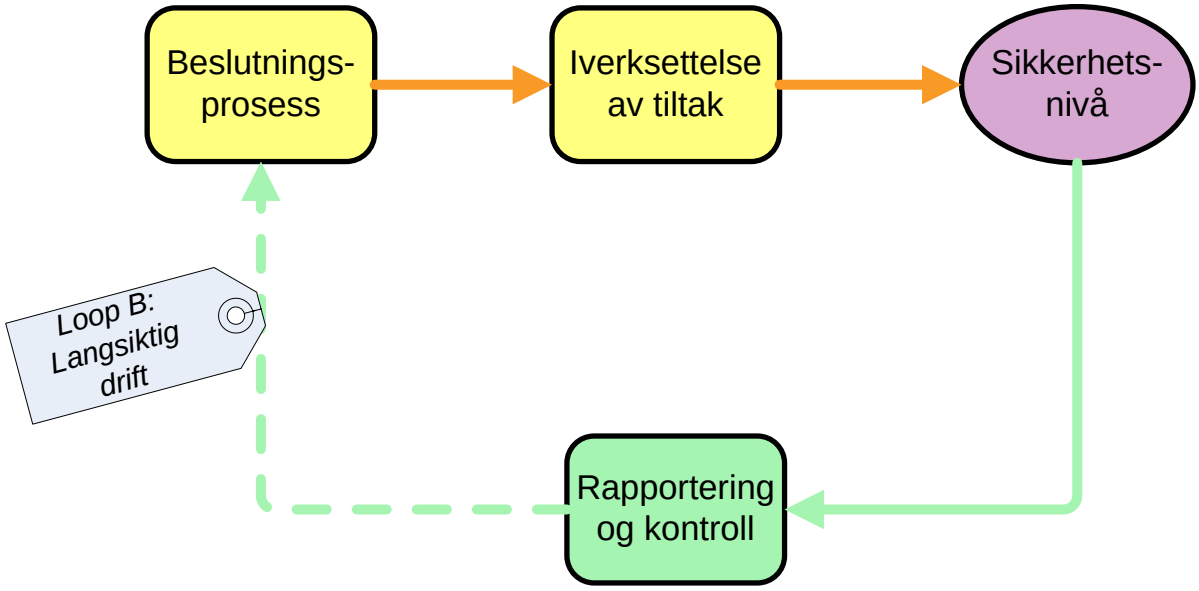
Dessuten er det viktig med såkalt ”mindfulness” [Rosness 2004], som kapasiteten til å improvisere ved detektering og behandling av uforutsatte hendelser.

Weick og Sutcliffe (2001) definerer de 5 elementene av ”mindfulness”
- Fokus på feil
- Motstand mot overforenkling
- Forståelse av hva som faktisk skjer
- Evnen til å tåle feil
- Underbestemte systemer (problemets karakter avgjør hvor det skal løses)

Disse er kulturelt betinget, og fungerer bra på VTS på grunn av den eierfølelsen som operatørene har for vegnettet. Man kan stille spørsmål om den eierfølelsen kan gjenskapes hos eksterne entreprenører gjennom funksjonskontrakter.

### *4.2.2 Loop B: Langsiktig drift*

*Loop B gjelder en mer overordnet, langsiktig behandling av hendelser og feil*




Som beskrevet i kapittel 3, er vår hypotese at loop B ikke fungerer med mindre hendelsen får store konsekvenser eller media oppmerksomhet. Først vil vi beskrive hvilke data som er rapportert, og deretter hvilken bruk organisasjonen har av disse.

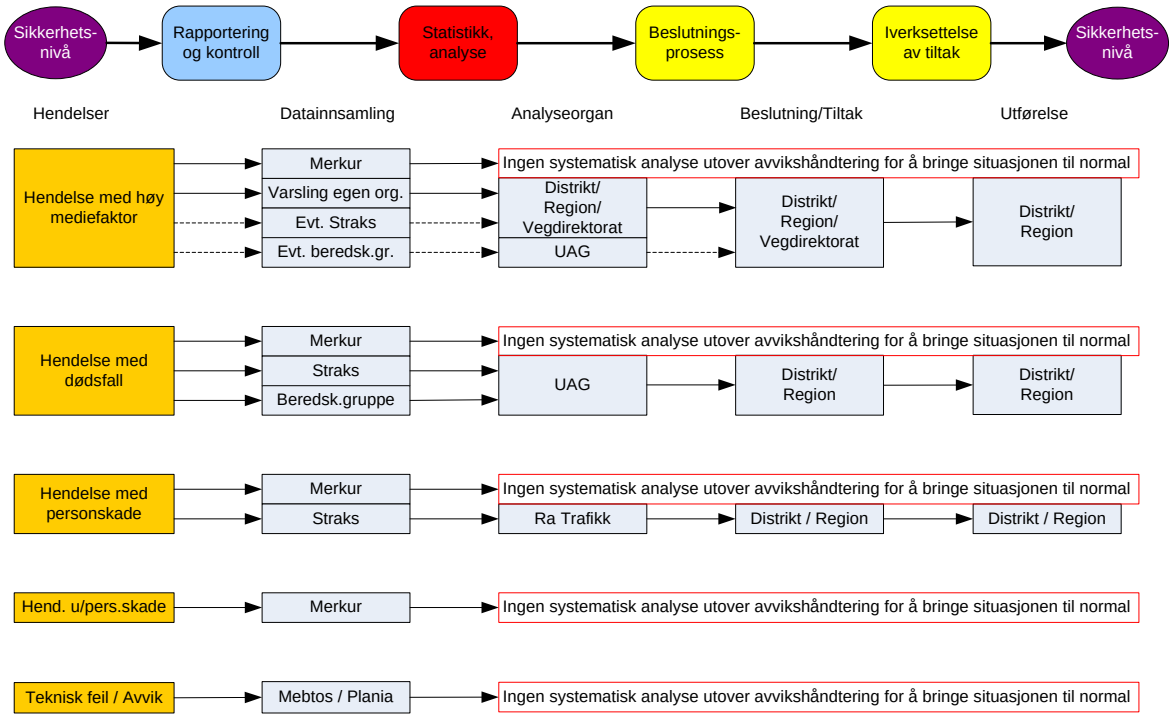
**Rapporteringssystemene**

| | |
|---|---|
| Alle hendelser (trafikale, tekniske) | **Merkur** er et loggførings og videreformidlingssystem hvor hendelser på vegnettet inkl arbeidsvarslingsvedtak blir loggført av VTS. Enkelte byggeledere for drift- og vedlikeholdskontraktene har tilgang til dette programmet, slik at de selv kan gå inn å få en oversikt over de hendelsene som har skjedd for sitt ansvarsområde. I rapporten blir bl.a meldingstype, |

| | |
|---|---|
| | dato, klokkeslett, vegtype, område, sted, hendelsesforløp og tiltak loggført. |
| Tekniske feil | I **Mebtos** blir feil som skjer med objekter/systemer som er tilknyttet Oslos tekniske styresystem automatisk loggført. Drift og vedlikeholdspersonalet bruker denne basen til å få oversikt over feil, og til å følge opp saker. De legger fortløpende rapporter direkte inn i programmet. |
| Tekniske feil (drift-og vedlikeholds-oppfølging) | **Plania**: Tekniske feil blir lagt inn av entreprenør. Rapporter blir lagt direkte under hver sak. Alle arbeidsordrer for løpende drift- og vedlikeholdsoppgaver blir lagt inn av drift. Entreprenøren legger inn en kort rapport under hver utførte arbeidsordre. Dokumenter og objekt oversikter tilhørende tunnelene kan bli lagt inn i Planias databasen, men dette er et meget omfattende arbeid og dermed lite utnyttet. |
| Personskade-ulykker | **STRAKS**, er systemet der personskadeulykker registreres. Statens vegvesen registrerer ulykkene på grunnlag av politirapporter, etter kvalitetssikring av data, derav innhenting av manglende opplysninger. |
| Dødsulykker | Rapportering av dødsulykker skjer ved at en medarbeider fra SVV drar til åstedet ved varsling fra politiet via VTS. Data samles inn av ulykkesgruppa og analyseres av ulykkesanalysegruppen (UAG), som legger frem en årlig rapport for regionen og Vegdirektoratet. |

**Er rapporteringen god nok?**

- Dødsulykker får egen granskning og rapportering oppover i systemet.
- Ulykker med personskade er statistisk behandlet, og brukes aktivt av Trafikkseksjonen for trafikksikkerhetstiltak.
- Trafikale hendelser og tekniske svikt registreres i Merkur, men programmet er ikke en database og egner seg dermed ikke til en statistisk behandling av hendelser og tekniske svikt.
- Tekniske svikt registreres i Mebtos/Plania men brukes kun for kortsiktig avvikshåndtering (loop A)




**Figur 10 Oversikt over rapportflyt ved hendelser i tunnel**

Trafikale hendelser blir behandlet etter gjeldende prosedyrer, men det utføres ingen ytterligere studie eller beslutningsprosess. Det stilles spørsmål på kvalitet på de registrerte dataene. Ifølge Vegdirektoratet [Vegdirektoratet 2004], er det "usikkert om operatørene selv forstår meningen med det de registrerer". Meningen er selvfølgelig uklar når data ikke etterbehandles.

Tekniske feil blir rettet (loop A), men blir ikke rapportert oppover i systemet på en systematisk måte.

Dessuten mangler det et systematisk opplegg for kommunikasjonsflyt ved avvik i behandlingen av hendelser/feil. Noen avvik er spesielt viktige, fordi de kan forårsake at en barriere forsvinner.

Det framgår av tabellen at det lages lite statistikk og oppfølgingsdata av dagens rapportering, og det som lages benyttes i liten grad i driften.

Vegdirektoratet har laget en statistikk fra Merkur for hendelser i tunneler for 2001-03 som viser:

- Type hendelser: Teknisk feil på kjøretøy 40 %, bensinmangel 15 %
- Bistand ved hendelsen: Redningsselskap og vaktbil 27 %, politi 15 %

Med bakgrunn i denne analysen og Straksregisteret kan vi sette opp følgende tabell:

| Tunnel | Hendelser 2001-03 | Stengninger antall | Stengningstid min. | Personskade-ulykker pr. år | Drepte eller alvorlig skadde 1996-2005 |
|---|---|---|---|---|---|
| Festning | 859 | 45 | 33 | 9 | 5 |
| Ekeberg | 298 | 14 | 22 | 5 | 2 |
| Nordby | 188 | 126 | 24 | 1 | 0 |

Dette er bare en illustrasjon over hvilke data som kan avledes av rapporteringen. Det er ikke mulighet for feltstenging i Nordbytunnelen, slik at den må stenges når det skjer et uhell, mens i de andre tunnelene blir trafikken ledet over til et felt.

Ulykkesoversikten viser at det skjer få alvorlige ulykker i tunnelene, og påkjørsel bakfra utgjør den største ulykkesandelen.

Her listes viktige feil som *ikke systematisk* rapporteres oppover i organisasjonen:

- beredskapsplanen er ikke tilpasset/oppdatert
- tekniske feil hindrer for eksempel stenging eller skilting
- kommunikasjonsvikt VTS/vaktbil/entreprenør/drift
- trafikanter respekterer ikke sperring
- viktige alarmer som ble oversett i mengden
- avvik ved oppfølging av feiloppretting
- nestenulykker for vaktbilen og entreprenørene

"The accumulation of more data *per se* does not prevent accidents" [Rosness 2004]. Rapporteringen uten ytterligere behandling kan dermed ikke vurderes som god nok.

- mangel på analyseorgan

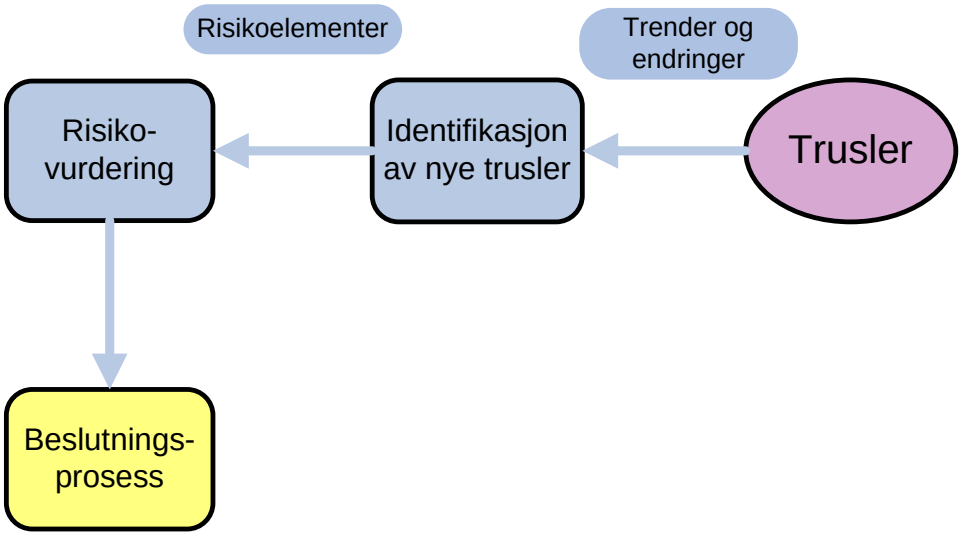
- mangel på indikatorer

Det bør vurderes i hvilken grad antall hendelser, stengningstid og personskadeulykker kan brukes som ytelsesindikatorer. I en sikkerhetsorganisasjon er det viktig å sette fokus på feil, dvs. uønskede hendelser. På denne måten vil rapporteringen bli bedre og VTS kan få en klarere forståelse av hvordan antall hendelser og ulykker utvikler seg.

### *4.3 Den proaktive delen*

*Den gjelder en forebyggende forbedring av systemet, det vil si behandling av hendelser og feil som enda ikke har oppstått.*

Hvordan jobber man med å identifisere nye trusler og vurdere risiko på disse? Er det noe system rundt dette? Hvor er ansvaret?




Det utarbeides en del risikoanalyser i forbindelse med planlegging/prosjektering av nye tunneler. Men vi kan ikke se at det finnes et systematisk opplegg knyttet til tunneler i drift.

Ved katastrofale hendelser, eller med stor media oppmerksomhet, kan det settes i gang omfattende kontrolltiltak som gjelder alle tunneler i Norge. I dag brukes mye ressurser på ras etter hendelsene i Hanekleiv og Oslofjord. Tidligere har det bl.a. vært: Pumper i undersjøiske tunneler etter Oslofjord, og brann i tunneler etter at vi hadde en bussbrann. Slike tiltak synes å være forebyggende, men er likevel ganske reaktive, siden de kreves der og da og gjelder kun en begrenset del av virksomheten.

Til tross for begrensede ressurser både økonomisk og menneskelig, bør flere forhold bli mer i fokus, for eksempel
Vann og frostsikring.

- Hva skjer hvis vi får en kald vinter igjen? Har vi bra nok beredskap for dette?
- Tåler utstyret vi har is, og det å bli slått på for å få ned istapper?

Andre aktuelle trusler

- naturfarer (jordskjelv, oversvømmelse)
- sårbarheten til VTS

- ventilasjonskapasitet i de eldste tunnelene
- lengre strømstans i hovedstaden og nødstrøm-forsyning
- effekt av fremtidig utbygging (Oslopakke 3)

Vi ser et behov for å utrede sikkerheten på et mer overordnet nivå.
Hvilke kanaler skal man bruke for å nå frem? Nå sendes behovet til nærmeste leder.

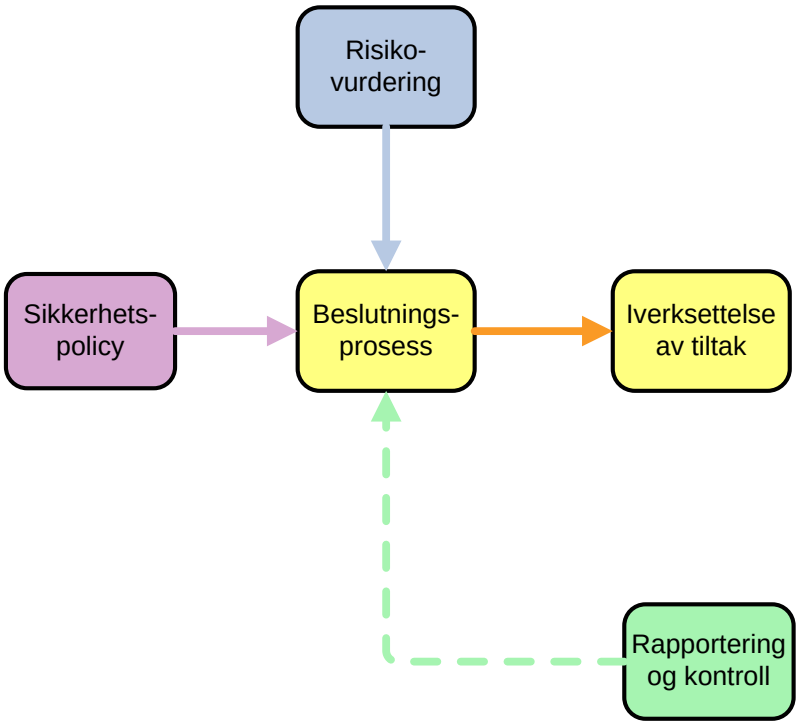
Risikovurderinger bør utføres systematisk ved
- endringer i eksisterende anlegg
- systematiske oppgraderinger (ved beregnet levetids slutt)

**Kunnskapsoverføring**
Driftseksjonen er tatt med i samarbeidsgrupper for nye prosjekter**.** Prosjektet får da glede av den praktiske erfaringen drift har, og kan da tidlig luke ut det de har erfart at fungerer dårlig.

VTS, representert ved faggruppeleder for styring og overvåking eventuelt med en erfaren vaktoperatør, deltar i arbeidet med beredskapsplaner for nye prosjekter. Dette gjøres i samarbeid med nødetatene og prosjektet. De er også aktivt med i risikoanalyser av nye tunneler, og er tidlig med inn i prosjektene. Når et nytt prosjekt er risikoanalysert sendes dette videre til Vegdirektoratet og sikkerhetskontrolløren for tunneler. Sikkerhetskontrolløren sender sin anbefaling til Vegdirektoratet.

### *4.4 Beslutningsprosessen*

*Her snakker vi om beslutningsprosess på et større nivå, når det bør planlegges utbedringer, eller ved ny utbygging, for eksempel skifte styringssystemet på VTS, velge et AID-system, etc.*



Beslutninger tas på flere organisasjonsnivå, avhengig av type oppgave og finansiering. Det er viktig at alle beslutninger treffes på et best mulig grunnlag basert på faktiske opplysninger og erfaringer.

Beslutninger omfatter i hovedsak følgende tiltak:

- *Feilretting og vedlikehold*. Funksjons- eller fagkontrakter finansieres av post 23 gjennom distriktets tildeling fra regionkontoret. Mindre tiltak eller reparasjoner treffes normalt av byggeleder med utgangspunkt i inspeksjoner og feilmeldinger (rapportering og kontroll). Større vedlikeholdstiltak besluttes av seksjonsleder.

- *Oppgradering og fornyelse av utstyr*. I prinsippet skal alle investeringstiltak under post 30 tas inn i det 4-årige handlingsprogrammet til NTP. For stamveger er det regionen som fremmer forslag til Vegdirektoratet etter innspill fra distriktene. For øvrige riksveger er det fylkesvise rammer fra Vegdirektoratet, og regionen bestemmer etter innspill fra distriktene og i forståelse med fylkeskommunen.. Vegdirektoratet etablerte i 2005 et eget program under post 30 for sikkerhet i tunneler for 2006-15, basert på en beregning av behov for utskifting av utstyr. Region øst fikk tilsagn om 15 mill. kroner i 2009.

- *Trafikksikkerhetstiltak* omfatter flere typer tiltak:
    - Strakstiltak etter trafikksikkerhetsrevisjoner utføres på ulykkesutsatte strekninger med høy skadegradstetthet og finansieres med 50 % fra hhv. post 23 og 30 (del av NTP).
    - Øvrige trafikksikkerhetstiltak som etablering av ATK, oppsetting av veglys og ombygging av vegkryss, finansieres av post 30 (del av NTP).
    - Forvaltningsmessige vedtak som regulering av fartsgrense. Slike vedtak fattes av distriktssjef etter uttalelse fra kommune og politi.

**Prioriteringer for beslutningsprosessen**

*Trafikkseksjonen* tar beslutninger knyttet til trafikksikkerhet og trafikkavvikling i Stor-Oslo. De baserer seg på registrerte data og analyser av disse (ulykkesrapporter, TS-inspeksjoner, m.m.). Men det taes i bruk kun data fra Straks-registret, det vil si personskadeulykker. Andre hendelser registrert i Merkur kunne påvise behov for trafikksikkerhetstiltak i noen tunneler (for eksempel systematiske påkjøringer av veggelementer i Vassumtunnelen).

*Driftsseksjonen*

Distriktsledelsen får sine innspill fra ulike seksjoner, og behovene som meldes inn må som regel konkurrere om en altfor liten pott. Dette gir målkonflikter (grovt sagt: ”asfalt eller sikkerhet?”). Måten det meldes inn behov for nye tiltak er ofte idédugnad. Innmelding av behov er prisgitt enkeltmedarbeideres kunnskap og erfaring og er en reaktiv måte å vurdere på.

Det benyttes ikke systematisk analyse for å finne og prioritere de tiltakene som ville gi best effekt. Det utføres heller ikke analyser for å finne eventuelle nye trusler.

Derfor blir beslutningsprosessen på drift som oftest en ren reaktiv prosess.

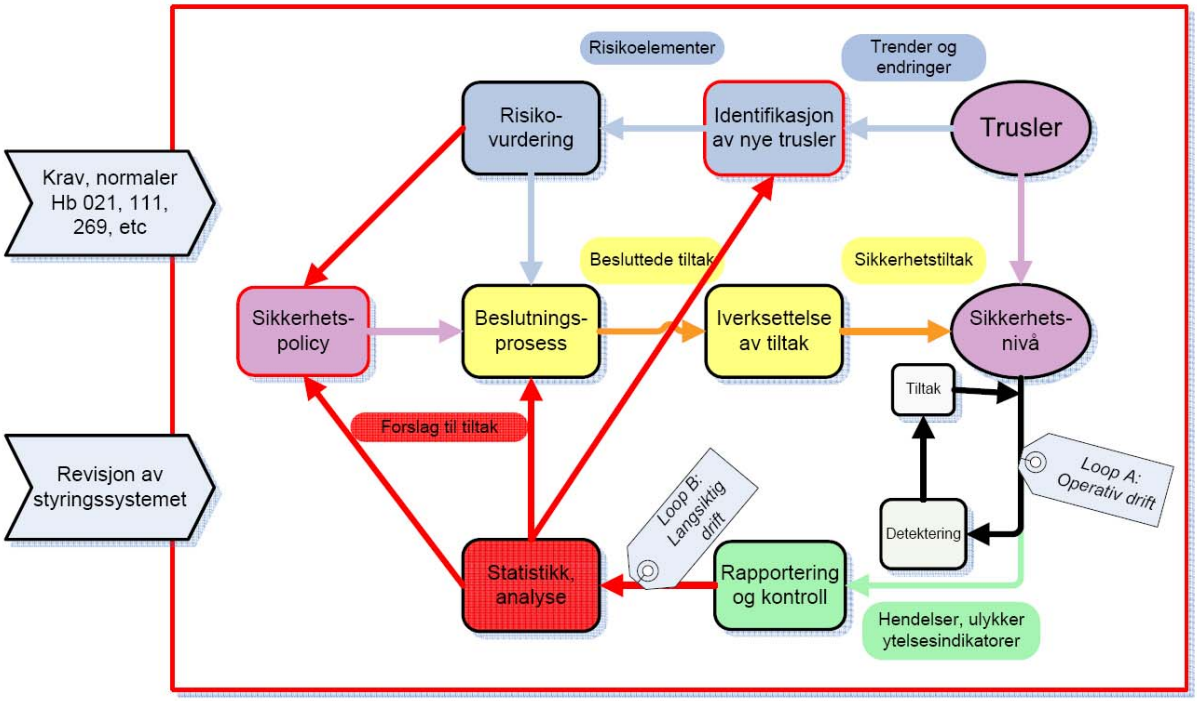
**Sikkerhetspolicy**

Eksisterende sikkerhetspolicy i vår organisasjon er basert på trafikksikkerhet og null-visjonen. Vi mangler sikkerhetspolicy spesifikt knyttet til tunneler, sikkerhetsstyringssystemet og oppfølging av drift og vedlikehold av tunneler.

# 5 Forslag til forbedringer

I lys av vår analyse, bør vi forandre sikkerhetsstyringssystemet slik at loopene fungerer tilfredsstillende, det vil si at de betjener beslutningsprosessen.

- Loop A kan trenge litt mer mannskap og redundans
- Loop B bør tilføyes analyseorganer
- Den proaktive delen trenger datarapporter fra loop B
- Utarbeidelse av sikkerhetspolicy må trekkes inn i systemet og beslutningsprosessen




**Figur 11 Tinmannsviks modellen, revidert med tanker om forbedringer.**

## *5.1 Forbedringer i Loop A*

Fungerer ganske bra, men når det går skeis, gjør det det skikkelig (normalulykker [Rosness 2004]).

**Tekniske (se 4.2.1)**

- Løse problemet med drukning i alarmer. Dette bør/må gjøres både nye og for eksisterende tunneler (sikkerhetspolicy).
- Forsikre oss at vi får tilbakemelding fra *barrierefunksjoner* og ikke bare *barriereelementer* i både nye og for eksisterende tunneler (for eksempel i tillegg til at vi får tilbakemelding om at pumpen går, skal vi få melding om at vannet faktisk synker)

**Organisatoriske (se 4.2.1)**

**VTS**

- Øke bemanningen på VTS for bedre organisatorisk redundans ved flere hendelser

**Drift**
- □ Bedre ledelse av elektrogruppa

**VTS/Drift**
- □ Systematisere kommunikasjon mellom drift og VTS med konkrete tiltak, for eksempel møter, informasjonssystem med tilbakemeldingssløyfer
- □ Innføre teknisk beredskapsplan (hva som skal gjøres hvis for eksempel strømmen går)

**Drift/entreprenør**
- □ Fokusere på mer styring fra Statens vegvesen som byggherre (skal vi styre mer (flere stikkprøver), skal vi bli bedre bestillere)
- □ Øke bemanningen hos drift for å bedre styringen av entreprenørene
- □ Systematisere oppfølging av opplæring og kompetansekrav i funksjonskontraktene
- □ Lage operasjonsprosedyrer eller "bruksanvisning" (for eksempel i oljeutskilleren skal det verken forekomme olje og/eller vann).
- □ Sørge for (kreve) organisatorisk redundans hos entreprenører

### *5.2 Forbedringer Loop B (se 4.2.2)*

- □ Vegloggen skal erstatte Merkur og Evita i 2008. Nye muligheter må utnyttes for å skaffe bedre rapportering og statistikk.
- □ Opprette relevante analyseorganer som vil se etter trender i hendelsene som rapporteres, og eventuelt analysere deres årsaker.
  - Ressurs til statistikk/analyse av hendelser i tunnel (Merkur)
  - Drift Stor-Oslo til statistikk/analyse av tekniske svikt (Mebtos/Plania)

Disse rapporter bør brukes for beslutningsprosessen og sendes til sikkerhetskontrolløren for forbedringer av sikkerhetspolicy.

- □ Bruke indikatorer for å vurdere pålitelighet av sikkerhetssystemet, for eksempel antall alarmer, uforutsatte stenginger, lengde på stenginger.

### *5.3 Forbedringer proaktiv del (se 4.3)*

- □ Risikovurderinger skal utføres systematisk ved utvikling av vegnettet og fornyelse av utstyr/oppgraderinger
- □ Risikovurderinger i den daglige driften bør utføres som et prosjekt, eller etter hvert som nye trusler (nye eller gjentagende problemer) dukker opp. Vurderinger kan utføres på gruppemøter med relevant kompetanse, eller eventuelt som tema i tverrfaglige fora. I alle tilfeller er struktur, målretting, oppfølging viktige.
- □ Data som er nødvendige for risikovurderingene kommer fra analyseorganene (loop B)

### *5.4 Forbedringer beslutningsprosess (se 4.4)*

Beslutningsprosess skal innebære en vurdering av behovet for iverksettelse av tiltak i forhold til målsetting for sikkerhet og akseptkriterier for risiko modellen [Tinmannsvik 2005].

Beslutningsprosessen på driftsseksjonen består av prioritering av vedlikeholdsoppgaver, utskiftninger, investeringer, og oppfølging av funksjonskontrakter. For å forbedre den prosessen bør man samkjøre proaktive og reaktive tankeganger, eventuelt ved hjelp av sikkerhetspolicy.

- □ Systematisere bruk av data, ved å bestille og innhente analyserapporter om de registrerte hendelsene og driftsfeil.
- □ Bruke risikovurdering, og melde behov for andre/ytterligere vurderinger
- □ Bruke sikkerhetspolicy

En viktig forutsetning for å kunne behandle den ovennevnte informasjonen er å etablere bedre ledelse av elektrogruppa.

### *5.5 Om sikkerhetspolicy (se 4.4)*

Sikkerhetspolicy bør svare på forskjellige behov:

- hjelpemiddel for revisjonssystemet, i form av premisser og prinsipper for sikkerhetsstyringssystemet, akseptkriterier (feil og beredskap, funksjonskontrakter)
- hjelpemiddel for revisjonssystemet, med indikatorer for måling av beredskapsytelsen og drift- og vedlikeholdsoppgaver
- supplering av normaler og retningslinjer, med rapportering av ”beste praksis”

Sikkerhetspolicy kan være i form av notater eller regionale retningslinjer som supplerer Vegdirektoratets håndbøker. For eksempel ”Hvordan planlegge og bygge et trygt pumpesystem”. Sikkerhetspolicy bør utarbeides på regions nivå (Utbyggingsavdeling eller Veg- og Trafikkavdelingen, gjerne i samarbeid) på grunnlag av erfaringsdata og de ovennevnte risikovurderingene. Sikkerhetskontrolløren skal bistå dette arbeidet.

# 6 Referanseliste


Reason (1997): Kap 1-3 fra "Managing the risks of organizational accidents" (1997)

Rosness (2001): "Slank og Sårbar. Om verdien av organisatorisk redundans" (april 2001)

Rosness (2004): Med forfattere: Guttormsen, Steiro, Tinmannsvik, Herrera. "Organisational Accidents and Resilient Organisations: Five Perspectives" (januar 2004)

Tinmannsvik(2005): Notat SINTEF "En modell for sikkerhetsstyring" (mai 2005)

Veritas (2003): Teknisk Rapport Veritas 2003-1517

Vegdirektoratet (2004): Rapporten "Hendelser i vegtunneler, Analyse av registreringer i MERKUR utført av de fem Vegtrafikksentralene" (juni 2004)

Veileder for sikkerhetsstyring.. Høringsutgave (2006)

Regelverket for planlegging og drift av vegtunneler:
Hb 021Vegtunneler (2006)
Hb 111 Standard for drift og vedlikehold av riksveger (2003)
Hb 269 Sikkerhetsforvaltning av vegtunneler (2006)