World Class Maintenance

TÜVRheinland®
safetec

Ragnar Aarø, Sjefrådgiver, Safetec

6.3 – Analysemetoder

Modul 6 – Vedlikeholdsoptimalisering

World Class Maintenance

Innhold

1. (Hva er risiko? Hvorfor trenger vi risikoanalyseverktøy?)
2. Risikovurdering / ROS-analyse
3. Sikker-jobb-analyse (SJA)
4. Hazard and Operability Review (HAZOP) / Hazard Identification (HAZID)
5. Feilmode og feileffektanalyse (FMEA)
6. (Feiltreanalyse – som vi dekket i forrige innlegg)
7. Rotårsaksanalyse

To innlegg som må sees i sammenheng

6.2 RAMS

- Hva er RAMS (Reliability – Avialability, Maintenability – Safety)
- Hvordan beregne pålitelighet=
- Mål for pålitelighet
- Systemklassifisering, komponent-, system- og strukturpålitelighet
- Bruk av systemanalyser – strukturfunksjon

6.3 ANALYSEMETODER

- Analytiske metoder: FTA, HAZOP, Hendelsestre
- Klassiske feilmetoder (eks badekarkurven)
- Betydningen av MTTR, MTTF, MTBF
- RBD – serie og parallellsystemer
- Rotårsaksanalyser

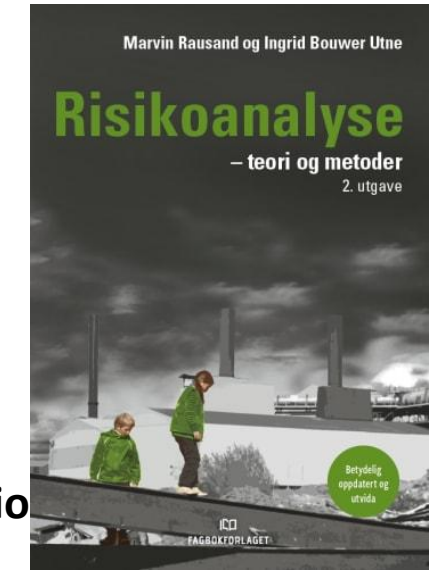
TÜVRheinland® safetec

Ønskemål for innlegget

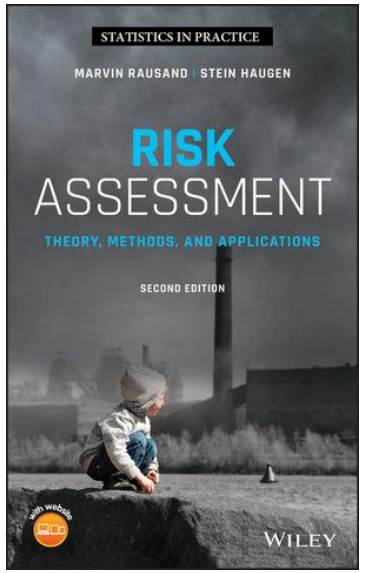
- Et riktig vedlikehold vil være med på å sikre en akseptabel teknisk tilstand. Selve arbeidet med både forebyggende og korrigerende vedlikehold kan medføre sikkerhetsutfordringer både når arbeidet utføres, og i driftssituasjonen etterpå hvis arbeidet ikke er utført riktig. Bruk og anvendelse av analytiske verktøy er viktig i vurdering av tekniske systemer, både i konstruksjons- og driftsfasen, og i planlegging og gjennomføring av arbeidsoperasjoner.
- Målet er å gi en oversikt over og litt innblikk i analytiske verktøy som benyttes innenfor fagområdet risiko, sikkerhet og pålitelighet.

- Risikovurdering (også gjerne kalt «ROS-analyse» og «grovanalyse»)
- Sikker-jobb-analyse (SJA)
- Hazard and Operability Review (HAZOP) / Hazard Identification (HAZID)
- Feilmode og feileffektanalyse (FMEA)
- Feiltreanalyse *(dvs. den har dere allerede hørt litt om, forrige innlegg)*
- Rotårsaksanalyse

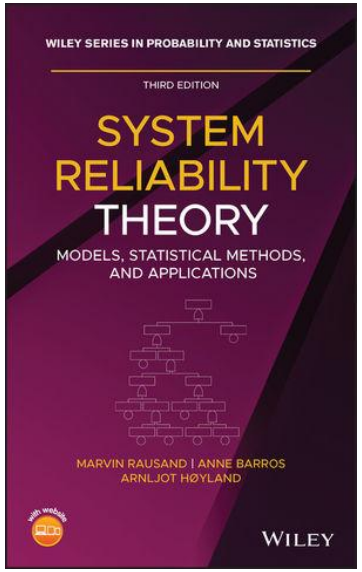
Anbefalt støttelitteratur



- **Risikoanalyse – teori og metoder**
  - https://www.ntnu.edu/ross/books/risikoanalyse
- Alternativt (og mer omfattende):
  - **Risk Assessment: Theory, Methods, and Applicatio**
    - https://www.wiley.com/en-gb/Risk+Assessment%3A+Theory%2C+Methods%2C+and+Applications%2C+2nd+Edition-p-9781119377221



  - **System Reliability Theory: Models, Statistical Methods, and Applications**
    - https://www.wiley.com/en-gb/System+Reliability+Theory%3A+Models%2C+Statistical+Methods%2C+and+Applications%2C+3rd+Edition-p-9781119373957



- Generell og god **referanseside for fagområdet** (blir nok ikke holdt så godt oppdatert lenger, men har stor verdi fortsatt):
  - https://www.ntnu.edu/ross/

World Class Maintenance

TÜVRheinland®
safetec

Hva er risiko?

Hvorfor trenger vi risikoanalyseverktøy?

Risikovurderinger – hva handler dette om

- Forstå hva som kan gå galt og hvordan vi best kan unngå og/eller begrense omfanget

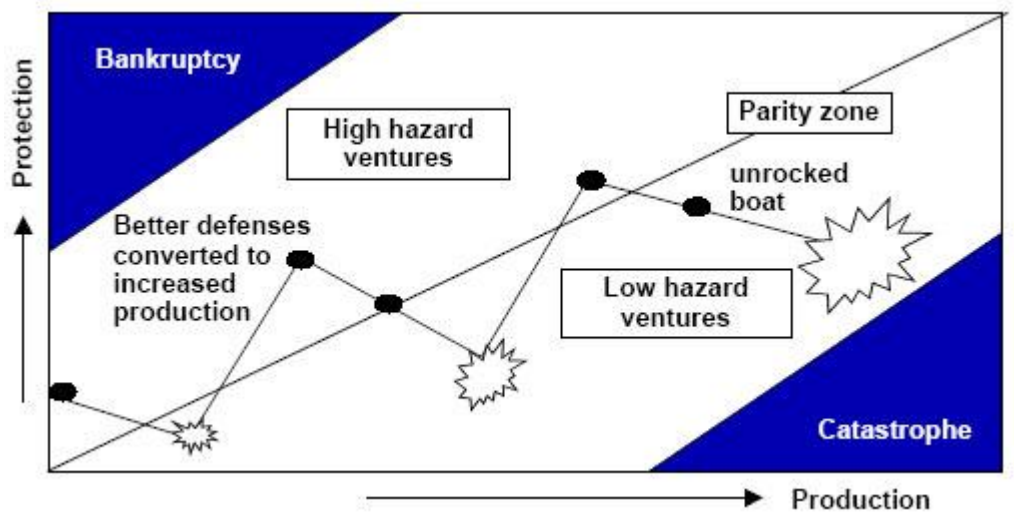
Etterpåkloklskap – på forhånd eller etterpå?

Påstand 1

- Det vil sjelden (aldri?) være verken mulig eller ønskelig å eliminere all risiko

- Målet må være å :
  - tilstrebe at risikoen holdes så lav som praktisk mulig, og
  - være bevisst restrisikoen og forberedt på å håndtere den

Balansen mellom produksjon og sikkerhet



J. Reason

- Nullvisjon – mulig i praksis ?
- Hvor sikkert er sikkert nok ?
  - Akseptkriterier
  - Restrisiko

Påstand 2

- ***"Maintenance can seriously damage your system"*** (James Reason)

- Hvorfor?
  - Det har vært en rekke storulykker hvor vedlikehold enten har vært en direkte utløsende eller medvirkende årsak
  - Bidrar vesentlig mer til risiko enn aktiviteter under normal drift og i nødsituasjoner
  - Reinstallering av komponenter etter vedlikehold er mest kritisk
  - Den mest vanlige feilen er å hoppe over nødvendige steg i vedlikeholdsprosessen – enten bevisst eller ubevisst

Risikobegrepet

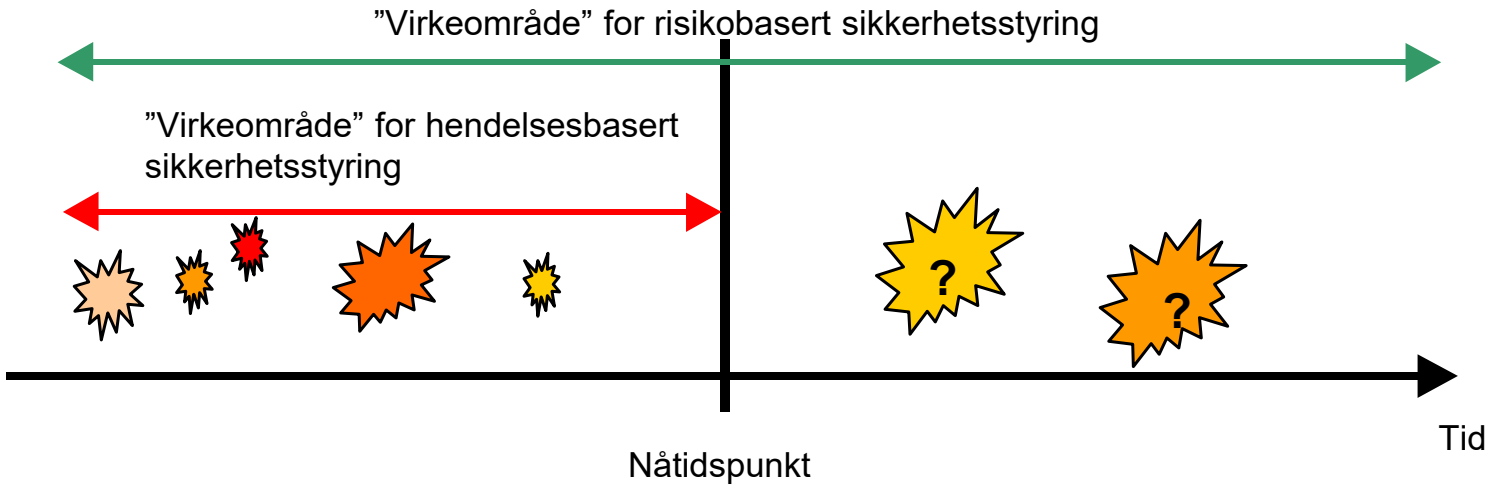
- **Risiko** er et uttrykk for den fare uønskede hendelser representerer for mennesker, miljø eller materielle verdier. Risikoen uttrykkes ved **sannsynligheten for og konsekvensene av de uønskede hendelsene**. (Norsk Standard, NS 5814:2006).

- I 2021-versjonen av standarden er definisjonen endret til «**usikkerhet knyttet til om en uønsket hendelse vil inntreffe og hvilke konsekvenser den kan få. Usikkerhet kan uttrykkes gjennom sannsynlighet.**

- **Risiko = frekvens/sannsynlighet x konsekvens** er oftest en ok forenkling
  - Frekvens/sannsynlighet: Hvor ofte vurderer en at hendelsen skjer/kan skje
  - Konsekvens: Hvor alvorlig er følgen (konsekvensen) av hendelsen, gitt at hendelsen skjer

- (Det finnes flere varianter/definisjoner, men for de fleste praktiske formål er denne definisjonen ok.)

Hendelsesbasert vs risikobasert risikostyring



Uønsket hendelse

- Hendelse som kan medføre tap av verdier
  - Utilsiktet eller tilsiktet
  - Kan også omfatte uønskede tilstander

- Verdier kan være så mangt, for eksempel liv og helse, miljø, omdømme, økonomiske verdier, materielle verdier mm.

Årsak

- Hver uønsket hendelse kan ha flere årsaker
- Disse må behandles separat fordi sannsynligheten for hver hendelse/årsak kan være svært ulik

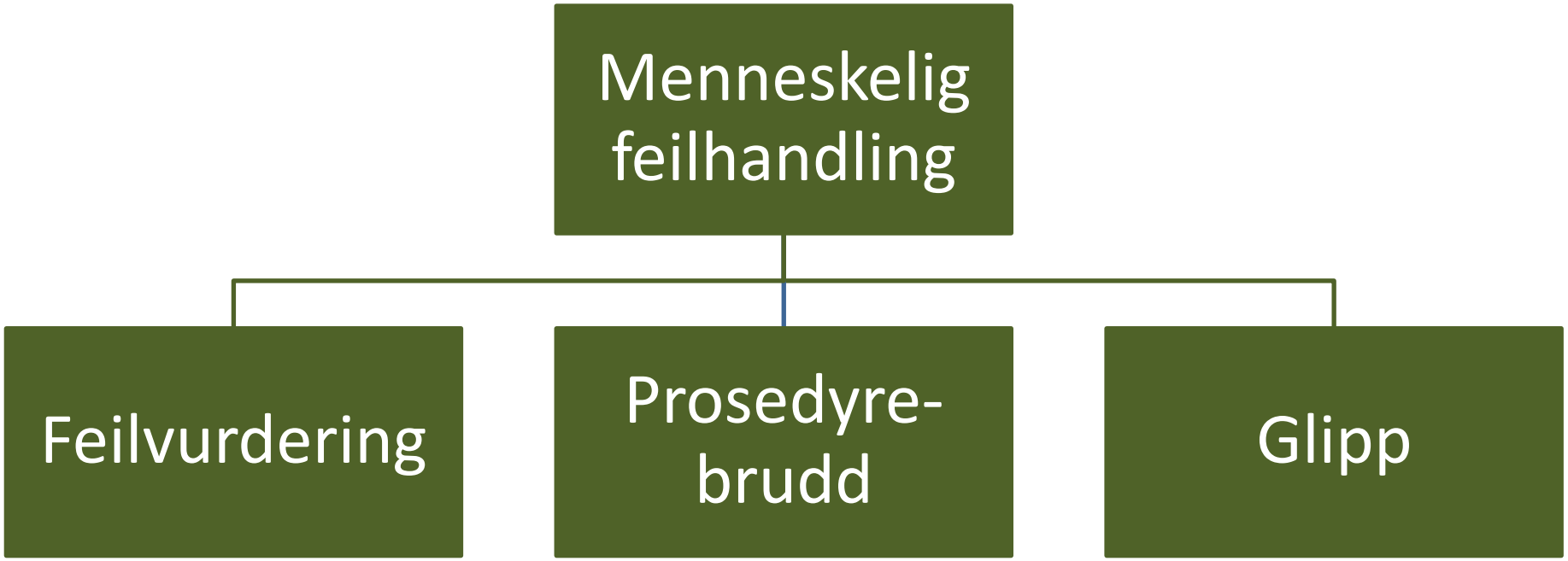
- Skiller gjerne mellom
  - Teknisk svikt
  - Menneskelig feilhandling, latent effekt
  - Menneskelig feilhandling, umiddelbar effekt
  - Designfeil
  - Ytre påvirkning

Latente feil introdusert gjennom vedlikehold

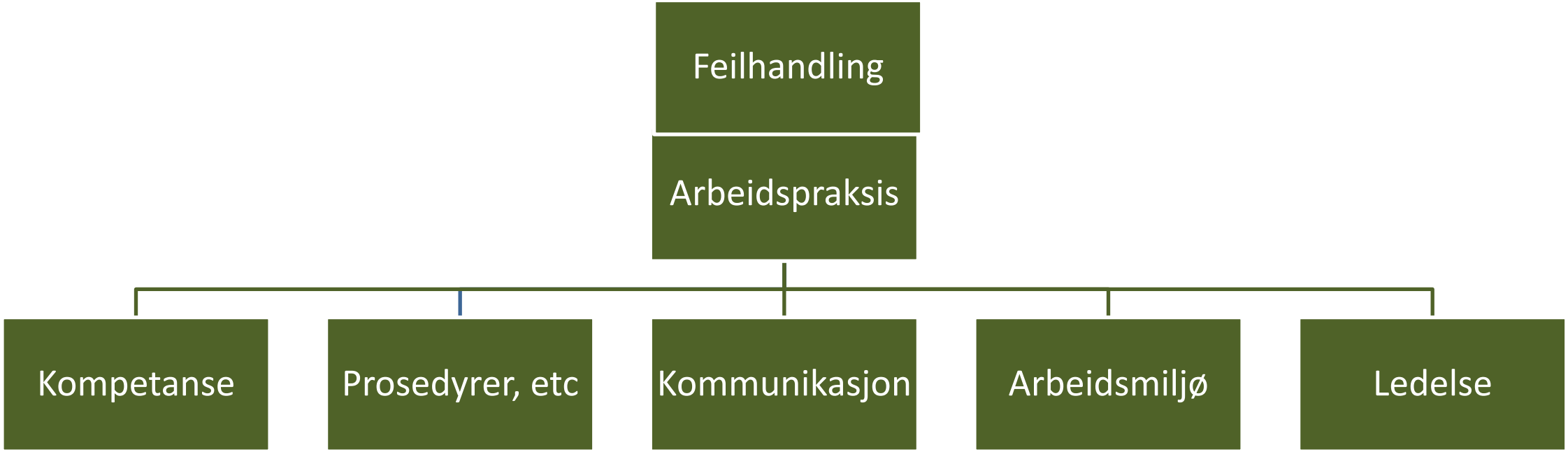
- Eksempel: Rengjøring av tank i hydrokarbonførende system
- Mulige latente feil:
  - Feil isolering/blinding
  - Ventil i feil posisjon etter vedlikehold
  - Feil valg av flenspakning
  - Feil tiltrekking av flens

- Alle disse forholdene kan føre til gasslekkasje når systemet kjøres opp etter vedlikehold

Typer menneskelige feil

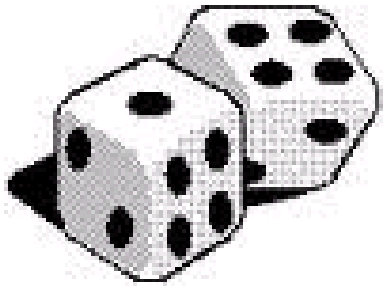


Bakenforliggende årsaker



Sannsynlighet

- I hvilken grad det er trolig at en uønsket hendelse vil kunne inntreffe



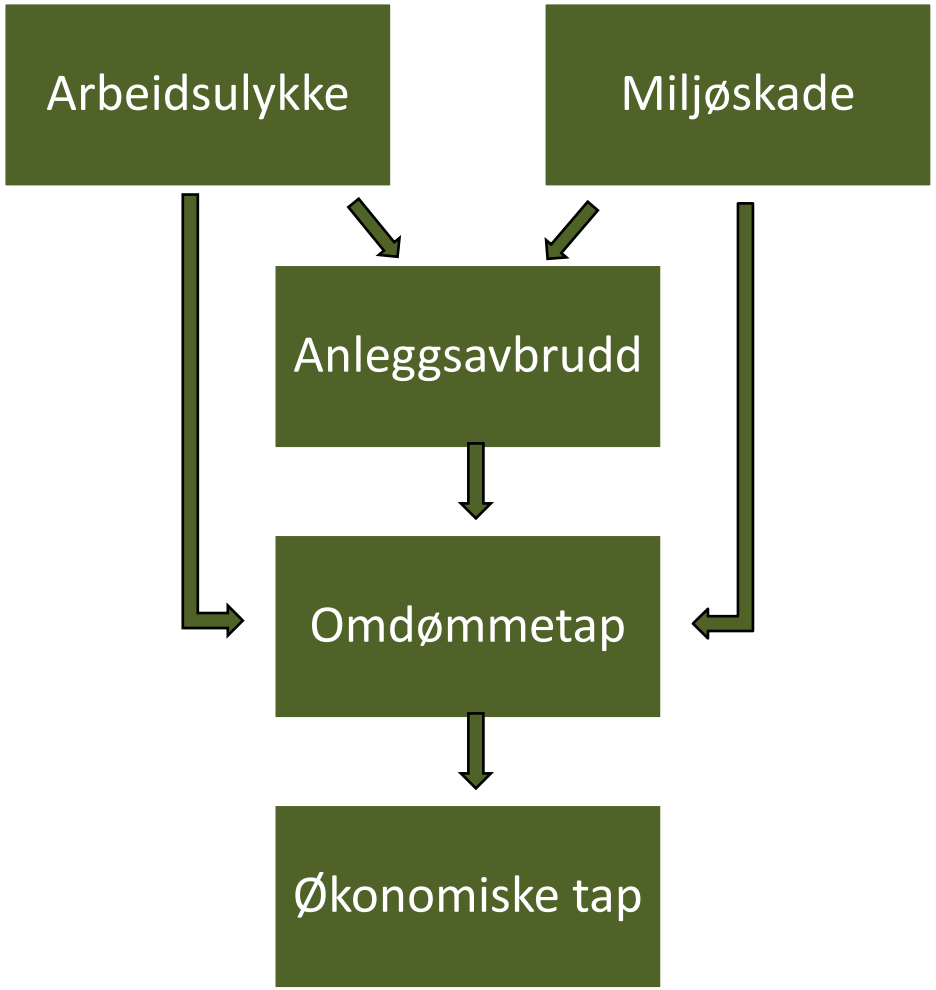
- Kvantitativt:
  - Alltid et tall mellom 0 og 1 (uttrykkes ofte som %)
  - Kan også bruke frekvens

- Kvalitativt:
  - Vurdering basert på flere kilder (erfaring, kjennskap til virksomheten, osv)

Konsekvenser

- Mulig(e) følge(r) av en uønsket hendelse
  - Mennesker
  - Miljø
  - Materiell
  - Andre økonomiske tap (driftsavbrudd, omsetningstap, etc)
  - Omdømme

Konsekvenskjeder



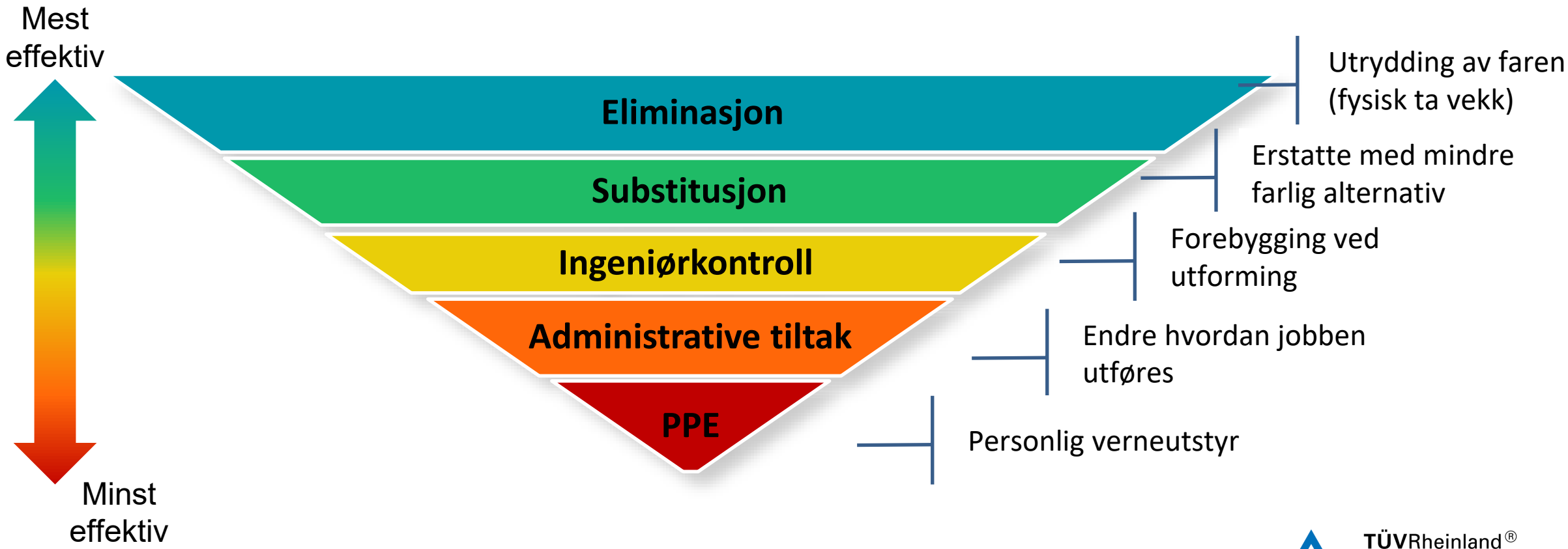
Barrierer / tiltak

- Forebygging, f. eks
  - Tekniske barrierer
  - Organisatoriske barrierer
  - Lover og regler

- Skadebegrensning, f. eks
  - Beredskapsplaner
  - Forsikring

Forebyggingstrappa for forebygging av skader og sykdommer

Tiltak – hvor effektive er de? Hvilke tiltak er «best»?

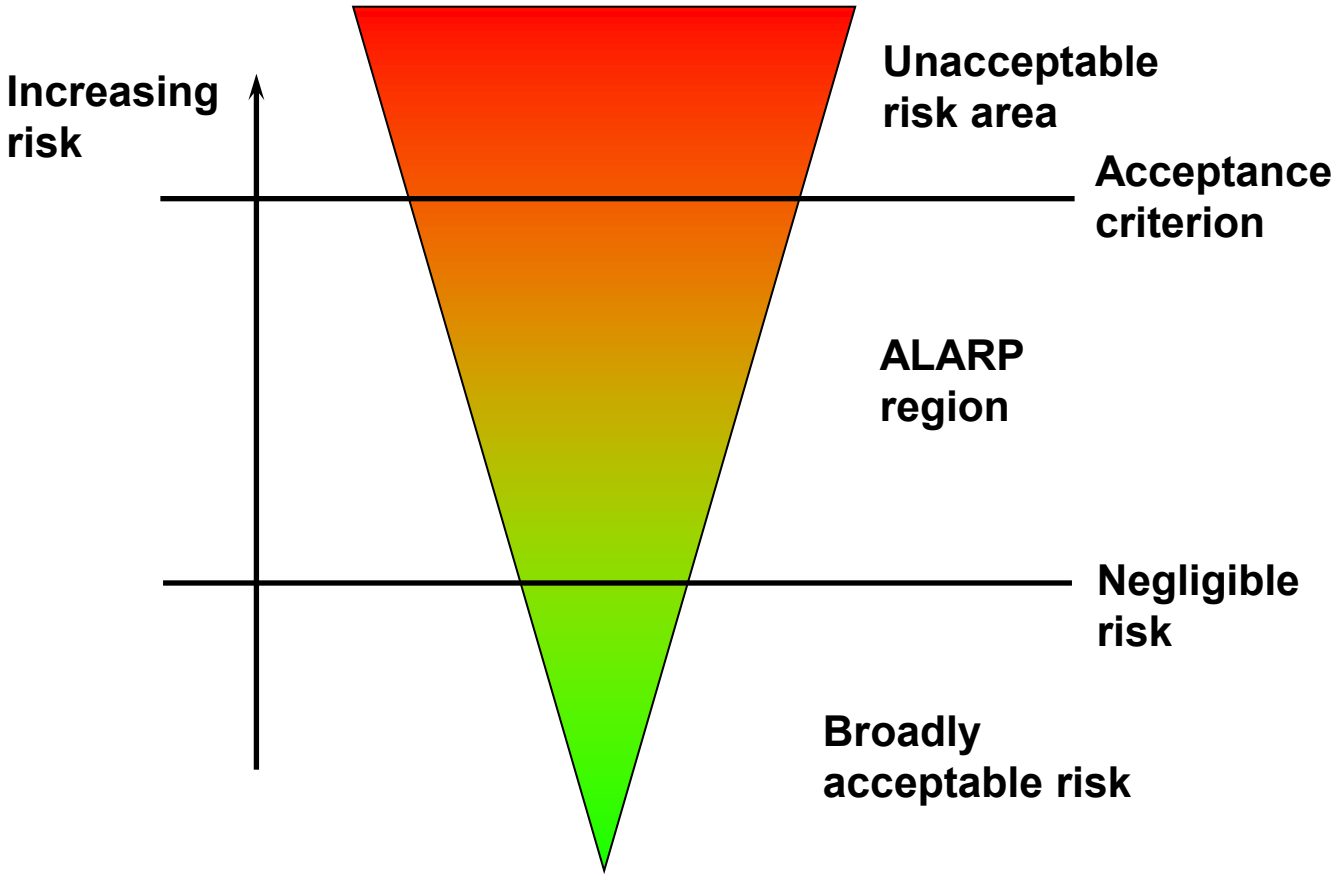


Kilde: Arbeidstilsynet

Akseptkriterier

- Kriterier basert på forskrifter, standarder, erfaring og/eller teoretisk kunnskap som legges til grunn for beslutninger om akseptabel risiko.
- Akseptkriterier kan uttrykkes med ord (kvalitative) eller være tallfestet (kvantitative).

ALARP-prinsippet



ALARP = «As low as reasonably practicable»

«Så lav som praktisk rimelig»

Restrisiko

- Den resterende delen av risiko som verken sikkerhets- eller beredskapstiltak kan ta hånd om eller som er ukjent
- Restrisiko skal ideelt sett være analysert og akseptert

World Class Maintenance

TÜVRheinland®
safetec

Risikovurdering

ROS-analyse

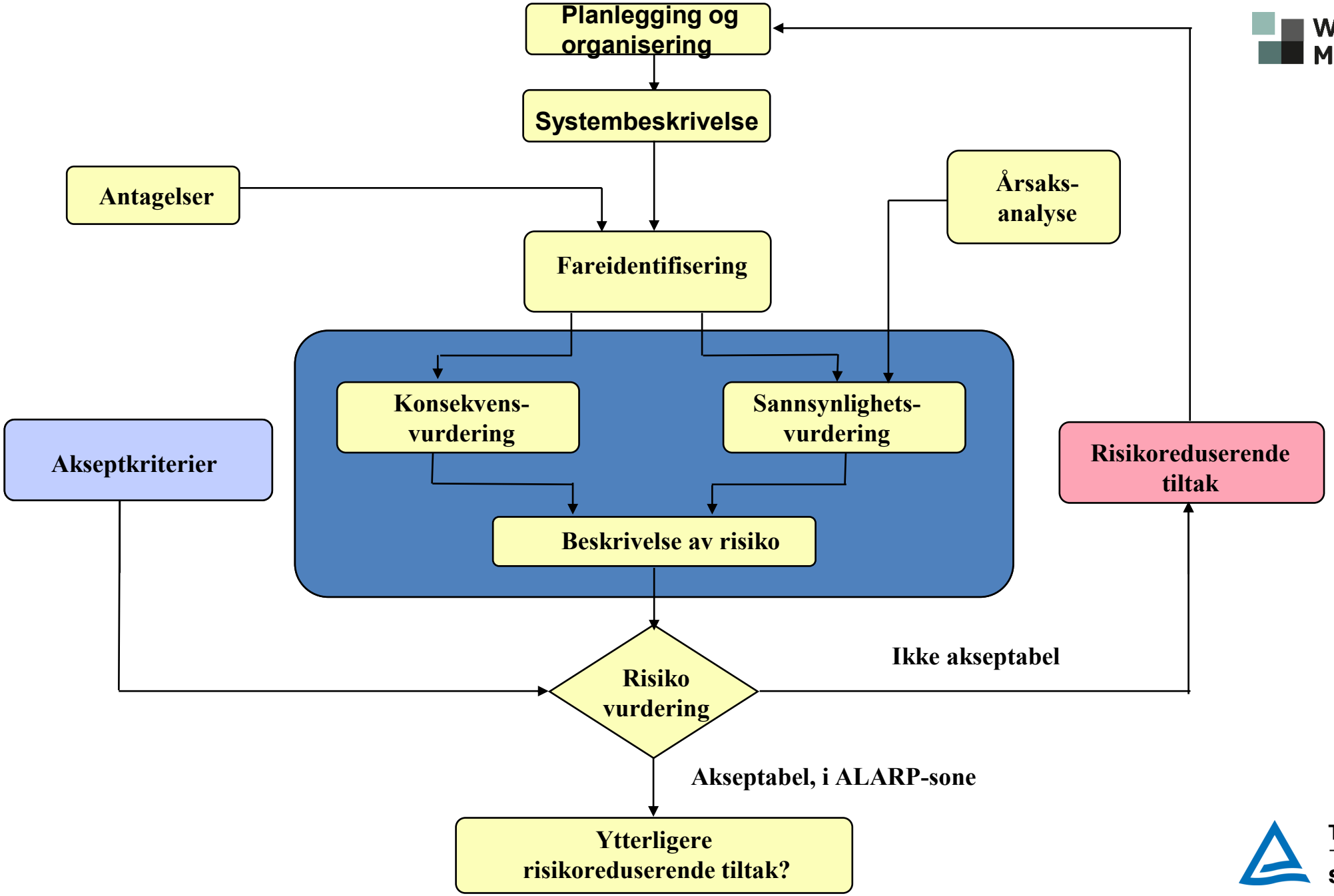
Hva er risikovurdering?

- Systematisk framgangsmåte for å beskrive og/eller beregne risiko
- Risikoanalysen utføres ved kartlegging av uønskede hendelser, og årsaker til og konsekvenser av disse

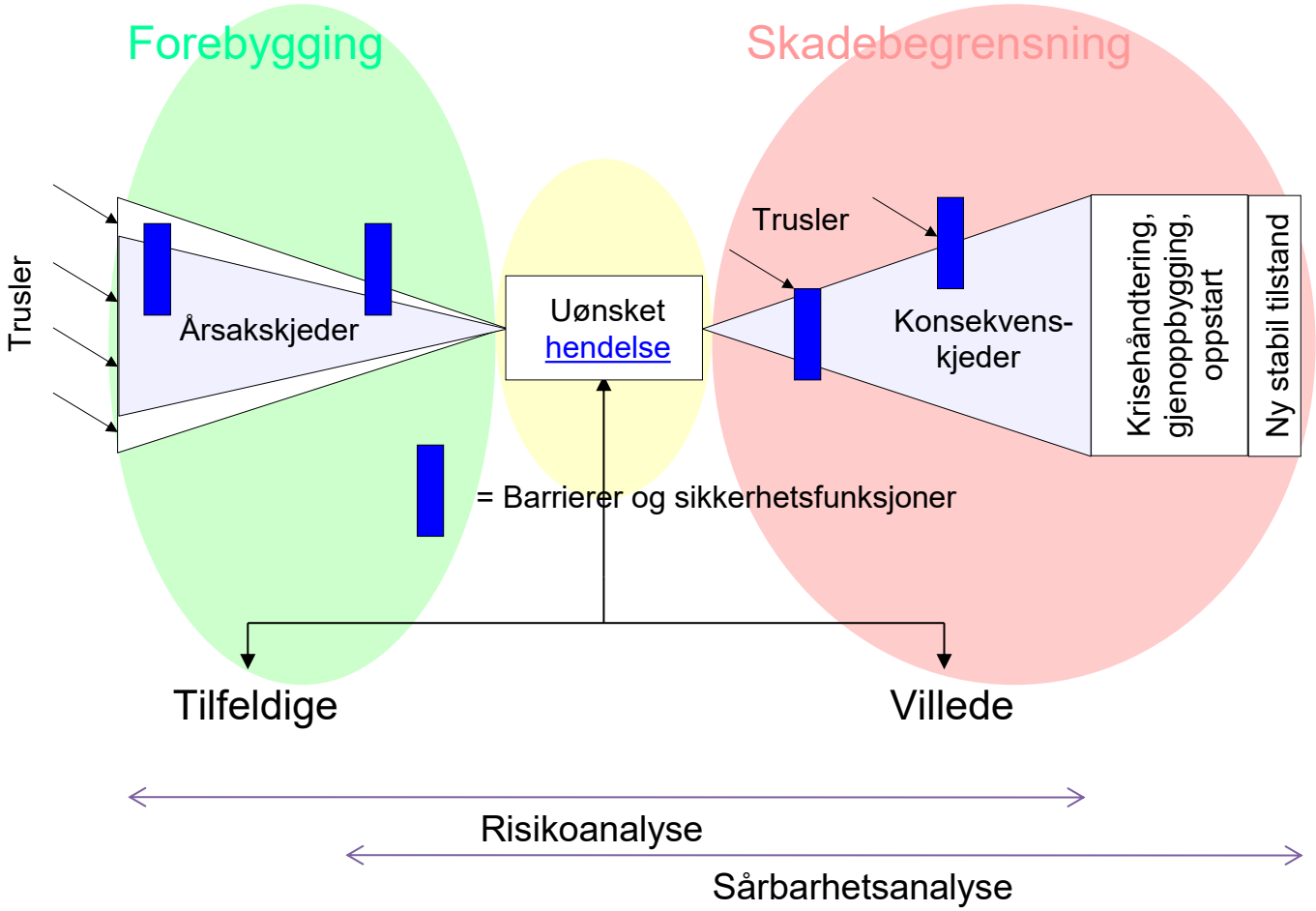
Hvorfor gjøre risikovurderinger?

- Av egeninteresse:
  - Får kartlagt uønskede hendelser
  - Grunnlag for å etablere så vel forebyggende som skadebegrensende tiltak
  - Økt bevisstgjøring og risikoforståelse
  - Dokumentert beskrivelse av risiko
  - Grunnlag for målrettet og effektiv ressursinnsats
  - Systematisk arbeid med sikkerhet

- God forretning!
  - Unngå uforutsette avbrudd
  - Unngå avhengighet av andre
  - Unngå dårlig PR
  - Trygt arbeidsmiljø er et viktig konkurransefortrinn

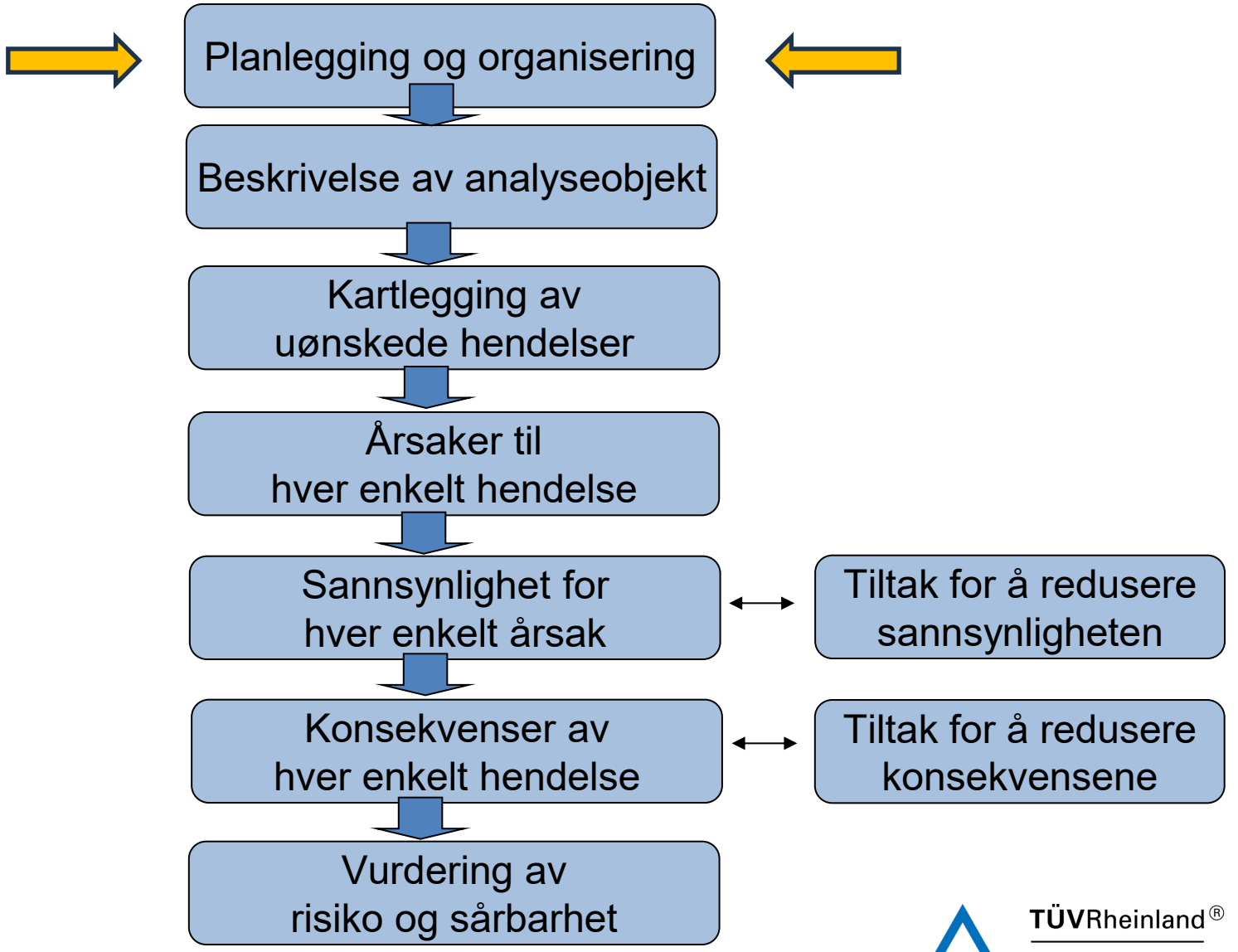

Planlegging og organisering
Systembeskrivelse
Antagelser
Årsaks-analyse
Fareidentifisering
Konsekvens-vurdering
Sannsynlighets-vurdering
Akseptkriterier
Risikoreduserende tiltak
Beskrivelse av risiko
Risiko vurdering
Ikke akseptabel
Akseptabel, i ALARP-sone
Ytterligere risikoreduserende tiltak?

Risiko- og sårbarhetsanalyse – Metodisk prinsipp



Fra NTNU, ROSS (2000)

Fremgangsmåte



Planlegging organisering

- Rammebetingelser og forutsetninger

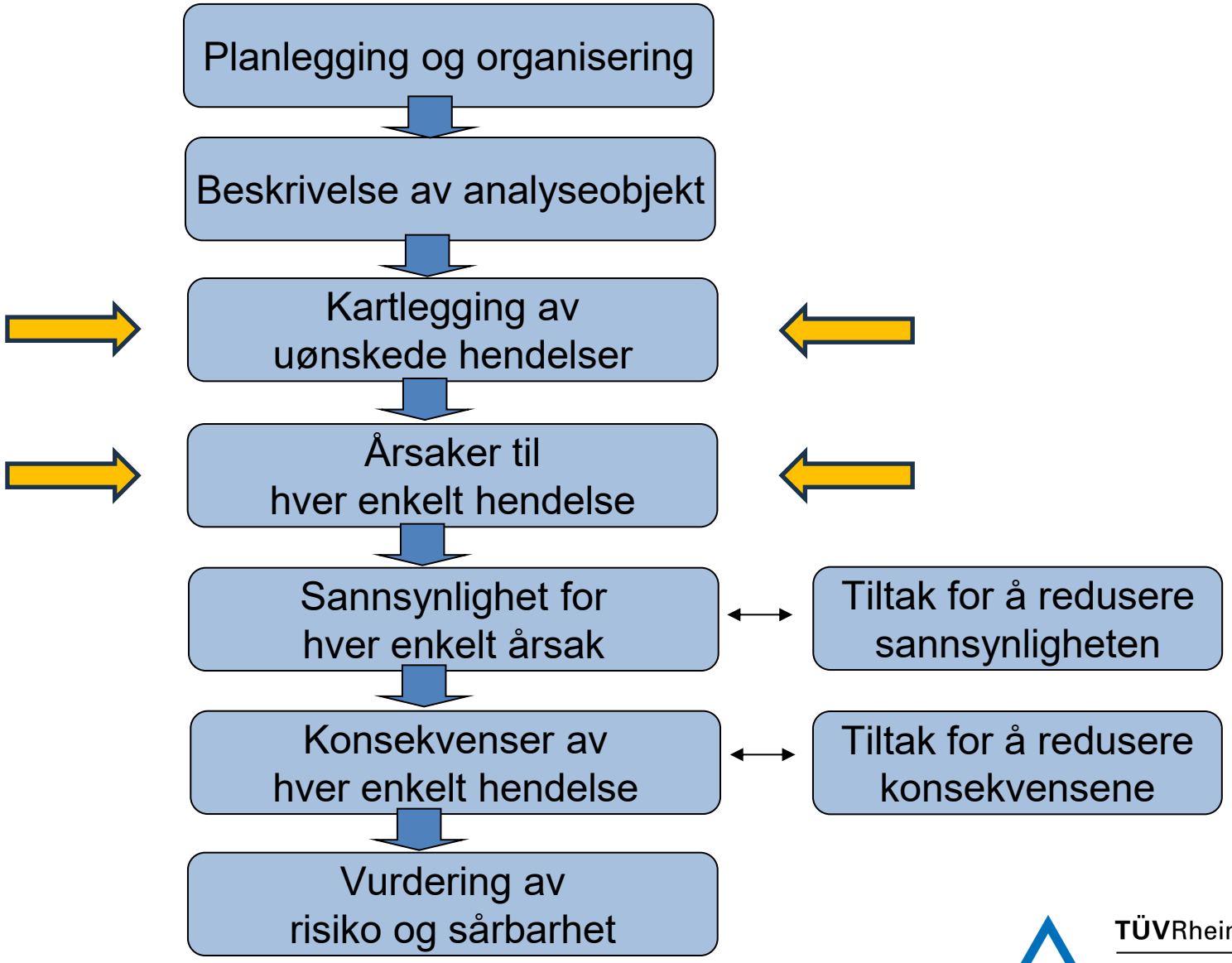
- Kriterier for vurdering av
  - Sannsynlighet
  - Konsekvens

- Etablere akseptkriterier

Akseptkriterier – eksempel på risikomatrise

Konsekvens (kategori) **Frekvens/sannsynlighet**	Neglisjerbar skade	Liten skade	Alvorlig skade	1-2 dødsfall	>2 dødsfall
>1/måned					
1/mnd – 1/år					
1/år – 1/10 år					
1/10 år – 1/100 år					
< 1/100 år					

Fremgangsmåte



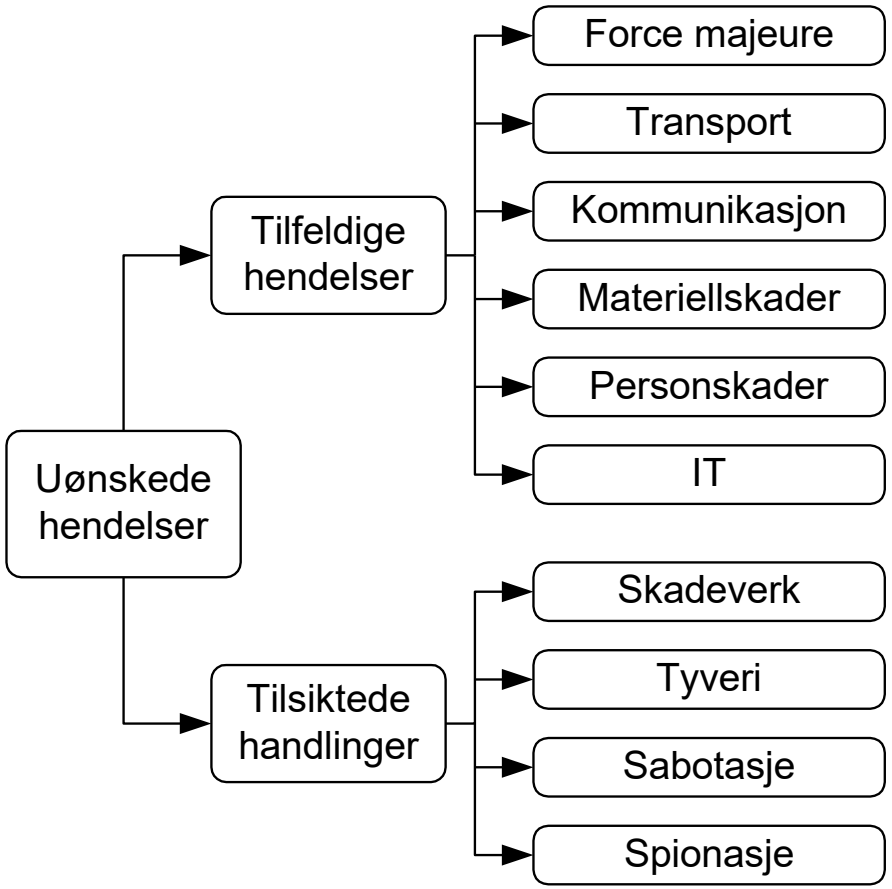
Kartlegging av uønskede hendelser og mulige årsaker

- Med utgangspunkt i ditt kjennskap til din organisasjon og dine ansvarsområder :
- Hva kan gå galt?
- Hvordan kan det gå galt?

Identifikasjon av uønskede hendelser

- Rapporterte nestenulykker
- Tilsynsrapporter
- Ulykkesstatistikk
- Ekspertuttalelser
- Driftsdata
- Eksisterende beredskapsplaner
- Dokumentasjon av anlegg
- Fantasi …

Uønskede hendelser – eksempler på kategorier



Force majeure	Snøras, jordras, flom, oversvømmelse, storm, skogbrann
Transport	Trafikkulykker, svikt i transportnett, drivstoffmangel
Kommunikasjon	Brudd i telekommunikasjon, lokalt samband, e-post systemer
Materiellskader	Brann, eksplosjon, slitasjeskader
Personskader	Fall, klem, trafikkulykker, brann, belastning
IT	Virusangrep, feil på server/klienter, programvarefeil, systemhavari
Skadeverk	Datavirus, påført strømbrudd, hærverk, brannstifting
Tyveri	Tyveri av utstyr og inventar, ran, innbrudd
Sabotasje	Tap av personell og materiell, informasjonsendring, bombeattentat
Spionasje	Innbrudd, hacking, avlytting

Mulig sortering av hendelser

- Listen over hendelser fra idédugnaden sorteres og filtreres
- De forskjellige hendelsene vurderes opp mot hvilke enheter som skal analyseres.

Hendelse / Enhet	trafikkulykker	brann	klemskade	datavirus	tyveri av utstyr	drivstoffmangel				
sentral dataserver				X						
kantine		X								
firmabiler	X				X	X				
adm. bygg		X								
laboratorium		X	X	X	X	X				
lager		X	X		X	X				

Hva med årsaken(e)?

Eksplosjonen på Texas City-raffineriet

The Texas City Refinery explosion occurred on March 23, 2005, when a hydrocarbon vapor cloud was ignited and violently exploded at the ISOM isomerization process unit at BP's Texas City refinery in Texas City, Texas, killing 15 workers, injuring more than 180 others and severely damaging the refinery. The Texas City Refinery was the second-largest oil refinery in the state, and the third-largest in the United States with an input capacity of 437,000 barrels (69,500 m3) per day as of January 1, 2000.[1] BP acquired the Texas county refinery as part of its merger with Amoco in 1999.[2][3]

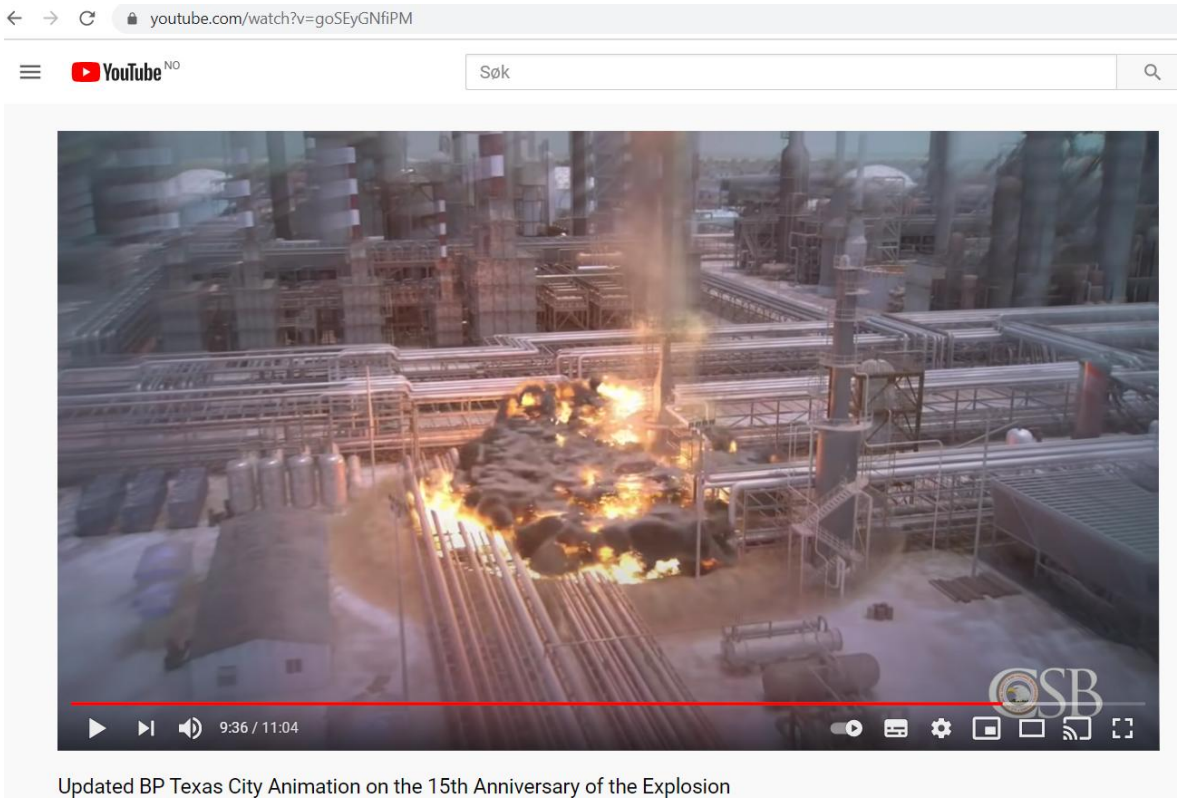
BP's own accident investigation report[4] stated that the **direct cause** of the accident was

"[...]heavier–than-air hydrocarbon vapors combusting after coming into contact with an ignition source, probably a running vehicle engine. The hydrocarbons originated from liquid overflow from the F-20 blowdown stack following the operation of the raffinate splitter overpressure protection system caused by overfilling and overheating of the tower contents."

Both the BP and the U.S. Chemical Safety and Hazard Investigation Board reports[5] identified numerous technical and organisational failings at the refinery and within corporate BP.

In 2011 BP announced that it was selling the refinery as part of its ongoing divestment plan to pay for ongoing compensation claims and remedial activities following the Deepwater Horizon disaster in 2010. The sale of the refinery was successfully completed at the start of 2013 to Marathon Petroleum Corporation for US$2.5 billion.[6]

Eksplosjonen på Texas City-raffineriet

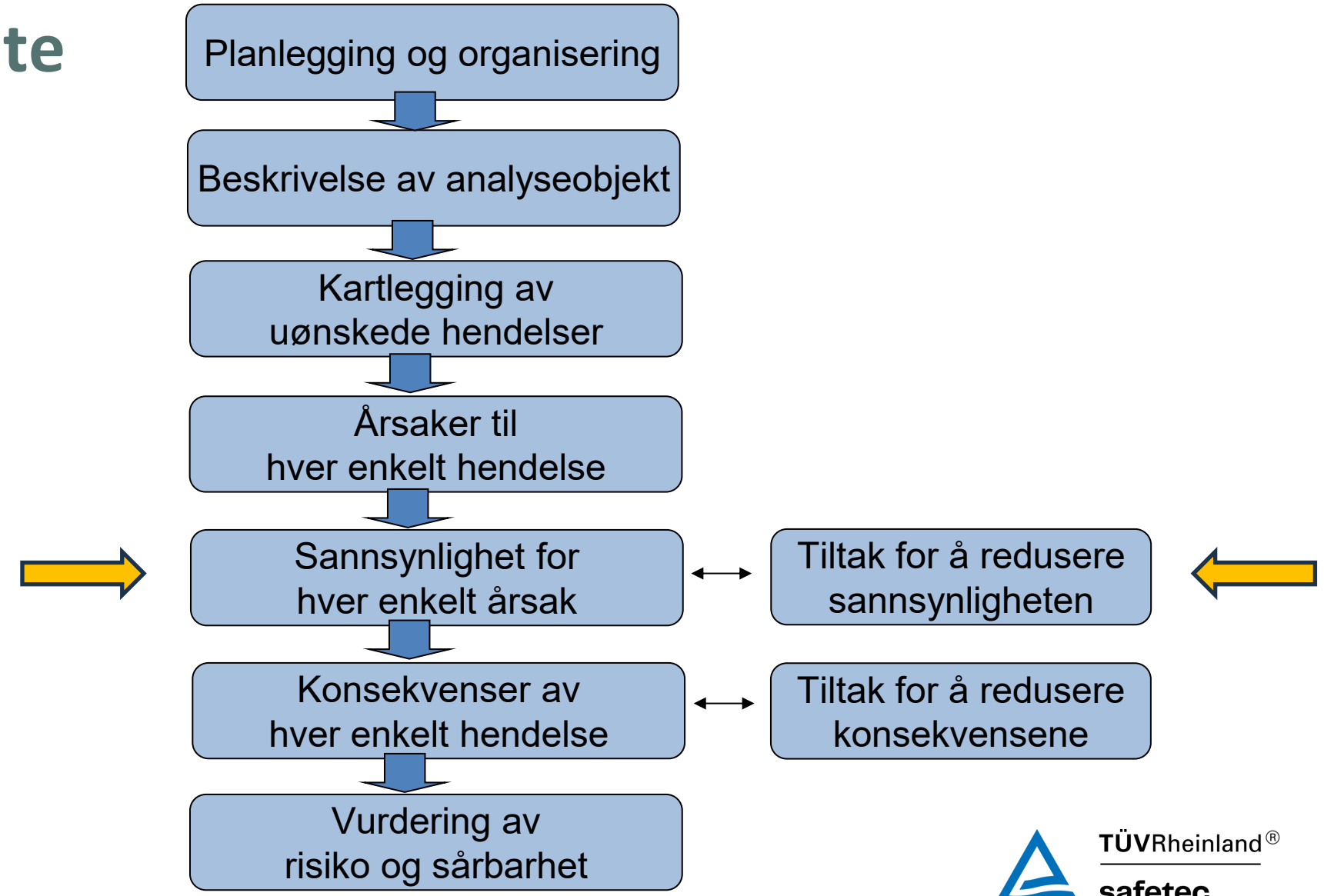


https://www.youtube.com/watch?v=goSEyGNfiPM

Eksempler på årsaker til prosesslekkasje

- Teknisk svikt
- Menneskelig feilhandling, latent effekt
- Menneskelig feilhandling, umiddelbar effekt
- Feil i prosesstyringssystemet
- Designfeil
- Ytre påvirkning

Fremgangsmåte



Vurdering av sannsynlighet

Kategori	Forklaring
Svært lite sannsynlig	Mindre enn en hendelse hvert år
Lite sannsynlig	Mindre enn en hendelse hvert halvår
Sannsynlig	Mellom en hendelse hver måned og en hendelse hvert halvår
Meget sannsynlig	Mellom en hendelse hver uke og en hendelse hver måned
Svært sannsynlig	Mer enn en hendelse hver uke

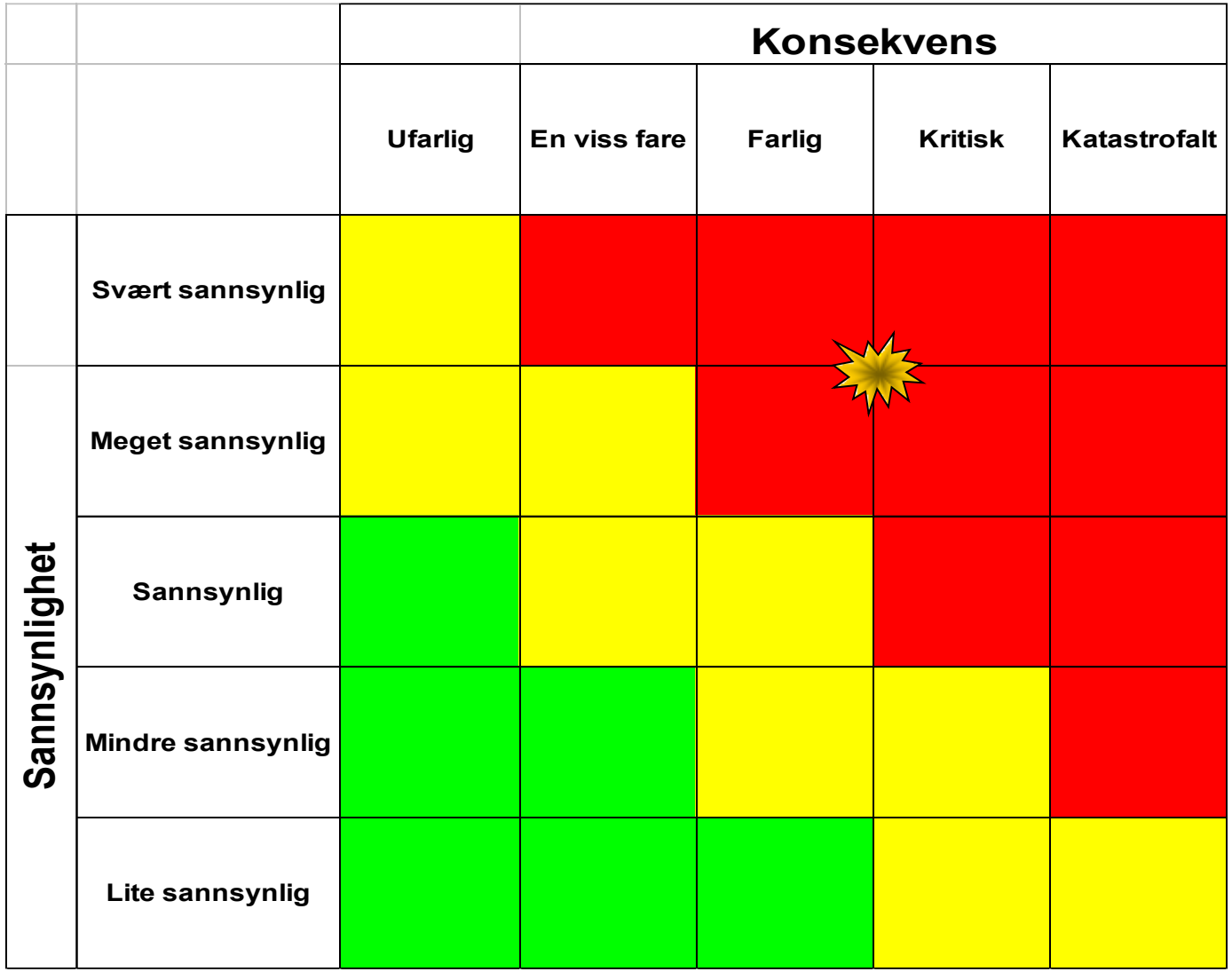
Fremgangsmåte

Vurdering av konsekvens

	Mennesker, liv og helse	Drift/ tjenesteprod.	Miljø	Økonomi
Ufarlig	Ingen personskader	Produksjon midlertidig ut av drift, uten behov for reserveprod.	Ingen miljøskader	Skader opp til kr…
En viss fare	Få og små personskader	Produksjon midlertidig ut av drift, behov for reserveprod.	Mindre miljøskader	Skader opp til kr…
Farlig	Få, men alovorlige personskader	Driftsstans i flere døgn	Alvorlige skader på miljøet	Skader opp til kr…
Kritisk	Opp til … døde Opp til … alvorlig skadde Opp til … evakuerte	Prod ute av drift i lengre tid. Avh prod.linjer rammes midlertidig	Omfattende skader på miljøet	Skader opp til kr…
Katastrofalt	Over … døde Over … alvorlig skadde Over … evakuerte	Hoved- og avhengige prod.linjer settes permanent ut av drift	Svært alvorlige og langvarige skader på miljøet	Skader på over kr…

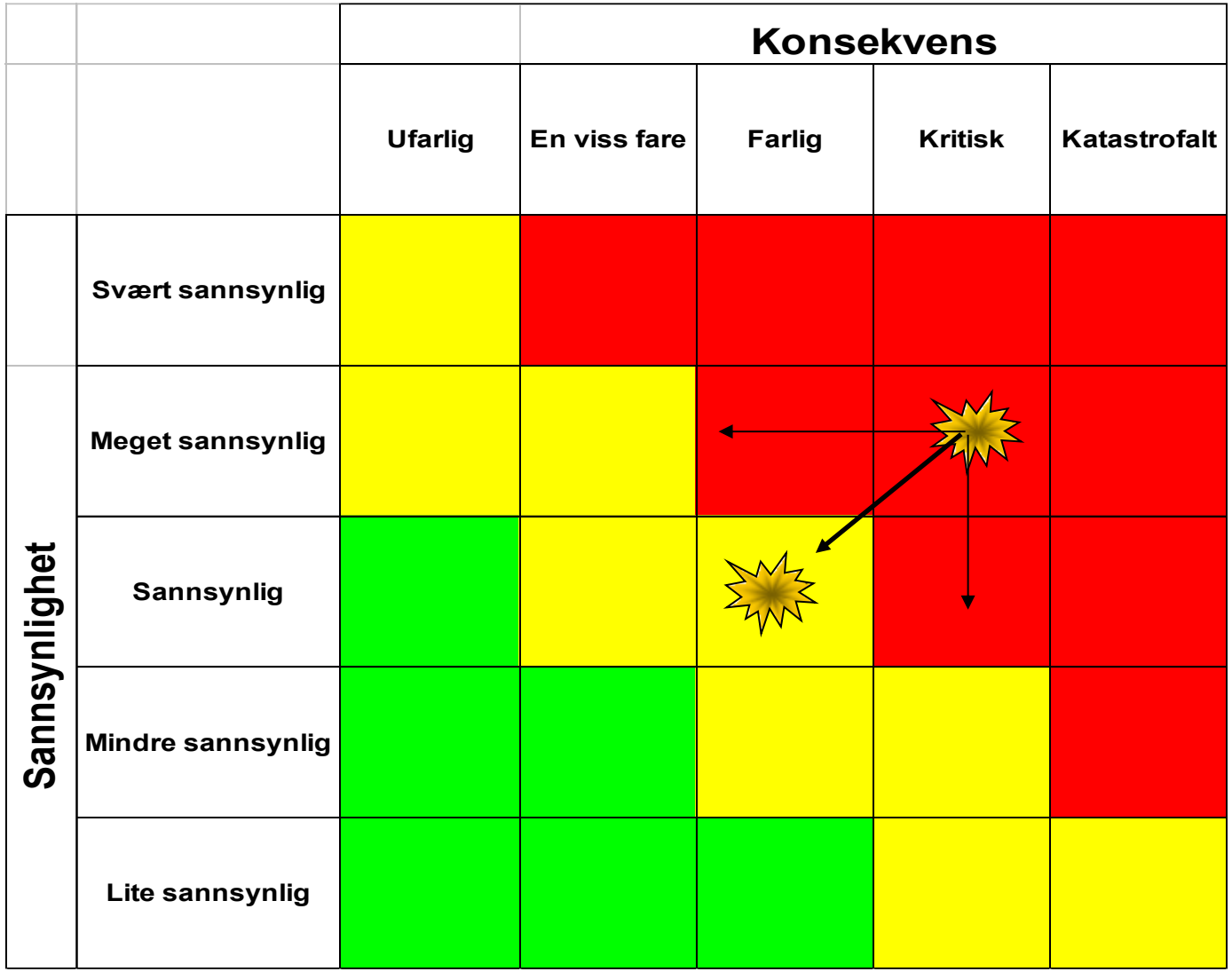
Fremgangsmåte

Vurdering av risiko



Fremgangsmåte

Implementering av tiltak



Rapportering og skjemabruk

- Skjema er nødvendig og nyttige hjelpemiddel
- På papir eller digitale varianter

- To eksempler:

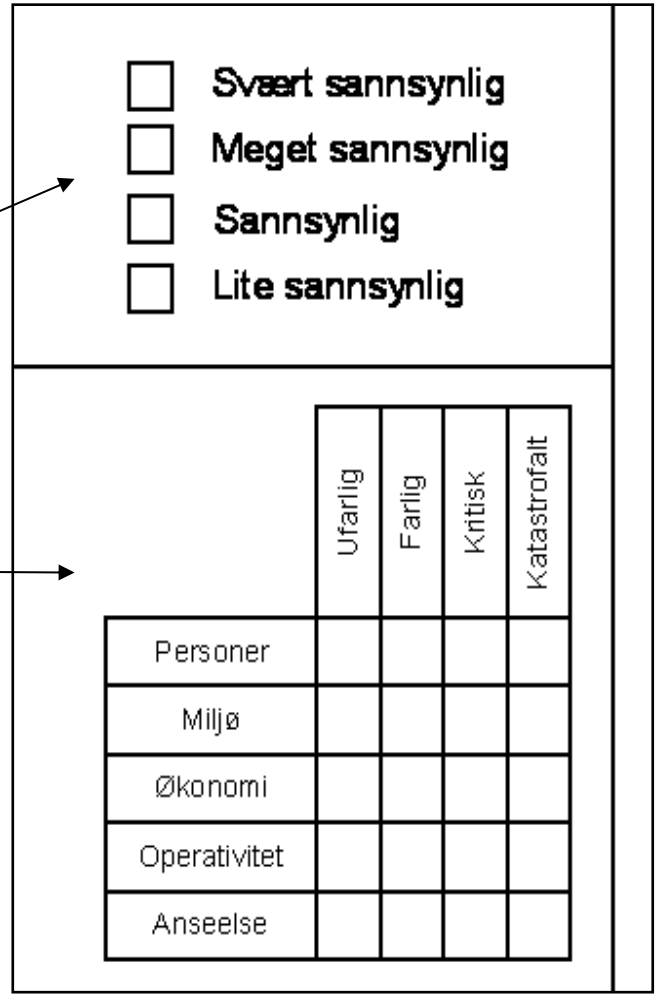
Skjema 1

Id	Objekt/funksjon	Hendelse	Årsak	Frekvens	Konsekvens	Kommentar

Skjema 2

Grovanalyseskjema		Skjema nummer:
Analyseobjekt:	Dato:	Utført av:
Hendelse (nr, navn): Beskrivelse:		
Beskrivelse av årsaker og sannsynlighet: ☐ Svært sannsynlig ☐ Meget sannsynlig ☐ Sannsynlig ☐ Lite sannsynlig Eksisterende forebyggende tiltak:		
Beskrivelse av konsekvens: Eksisterende skadebøtende titak:		
Forslag til nye tiltak (forebyggende og/eller skadebøtende):		
Kommentar:		

	Ufarlig	Farlig	Kritisk	Katastrofalt
Personer				
Miljø				
Økonomi				
Operativitet				
Anseelse				



Styrker og svakheter ved metoden

+

- Enkel metode å bruke
- Involverer de som selv ”eier risikoen”
- Kan raskt gi en oversikt over risikobildet
- Anvendelig til svært mange formål
- Kan tas i bruk i tidlige prosjektfaser – gir større påvirkning på risikobildet

÷

- Vanskelig å estimere sannsynligheten for en hendelse
- Vanskelig å representere hendelser med svært varierende konsekvenser
- Vanskelig å dokumentere effekt av tiltak og dermed prioritering av tiltak

Forutsetninger for en god risikoanalyse

- Opplæring i ROS-metodikk
- Forankring, engasjement, prioritering og styring
- Tverrfaglig samarbeid internt og eksternt
- Oppfølging av funnene og mottiltakene i ROS-analysen

World Class Maintenance

TÜVRheinland®
safetec

Sikker-jobb-analyse (SJA)

Hva er sikker jobbanalyse?

- Enkel risikoanalyse der man trinnvis vurderer alle farer knyttet til en bestemt arbeidsoperasjon eller en jobbsekvens

- Utføres i forkant av en konkret arbeidsoppgave slik at tiltak kan iverksettes for å fjerne eller kontrollere de farene som avdekkes

Hensikt

- Avdekke mulige farekilder
- Gjøre ledere og operatører mer oppmerksomme og bevisste om farer
- Gi innspill til sikker gjennomføring
- Opplæring gjennom praksis
- Bedre kommunikasjonen mellom involverte aktører

- Dokumentasjon
  - Planlegging av liknende arbeidsoppgaver
  - Granskning av uønskede hendelser

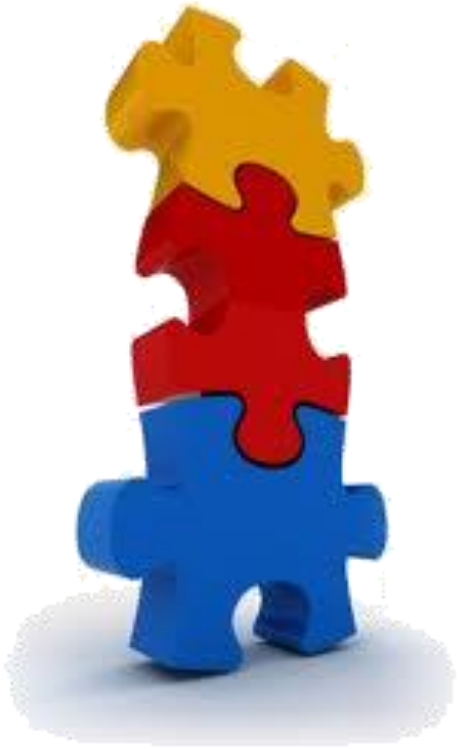
Anvendelse

- Når arbeidsoppgaver og/eller farer knyttet til en av arbeidsoppgavene ikke er tilstrekkelig kjente eller kontrollerte, for eksempel når
  - Lignende oppgaver har ført til hendelser
  - Lang tid mellom hver gjennomføring
  - Nytt utstyr skal tas i bruk
  - Nytt personell skal utføre arbeidsoppgaven
- Når farer/risiko forbundet med en arbeidsoppgave ikke er tilstrekkelig belyst gjennom prosedyrer, for eksempel for å utarbeide jobbinstruks
- Bør utføres så tett opp til jobben som mulig, men også i forbindelse med planlegging av jobben

Metodebeskrivelse

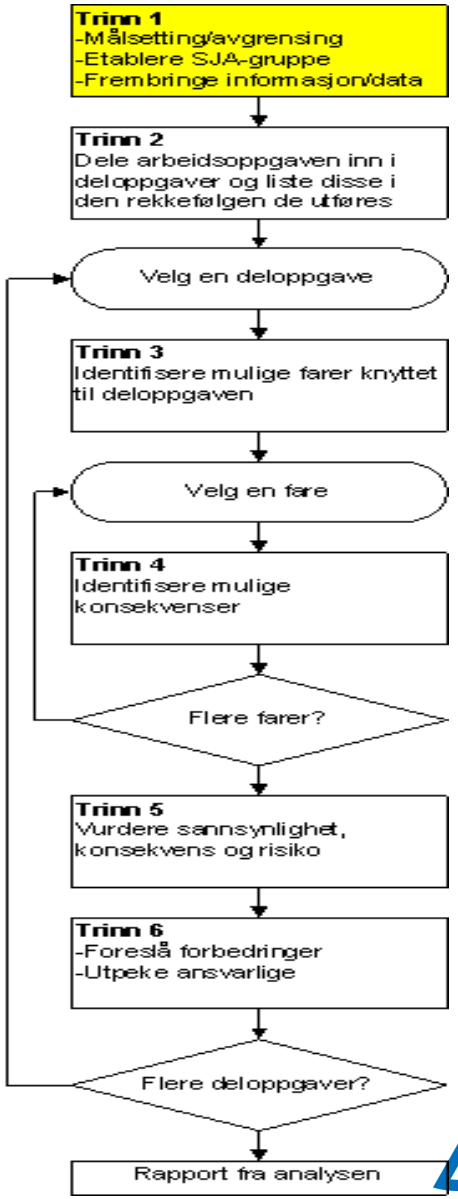
En sikker jobbanalyse (SJA) utføres normalt i 6 trinn:

1. Oppstart
2. Nedbrytning av arbeidsoppgaven i deloppgaver
3. Identifikasjon av mulige farer knyttet til hver deloppgave
4. Identifisering av konsekvenser knyttet til hver fare
5. Vurdering av risiko
6. Forslag til tiltak



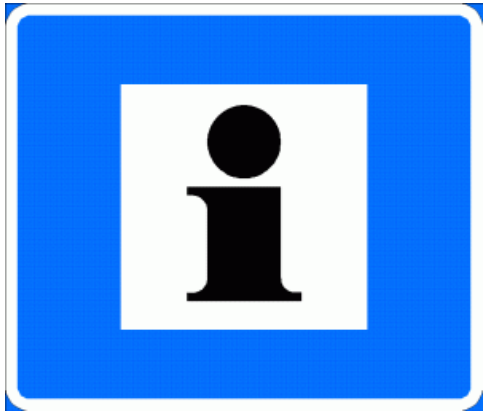
Trinn 1: Oppstart

- Ta utgangspunkt i planen for arbeidsoperasjonen, for eksempel løfteoperasjon
- Etablere SJA-gruppa
- Fremskaffe nødvendig informasjon
  - Plan, prosedyrer, manualer, tegninger
  - Tidligere erfaringer
  - SJA-skjema
  - Sjekkliste



Sjekkliste

- Dokumentasjon og erfaringsdata
- Kompetanse
- Kommunikasjon og koordingering
- Barrierer
- Utstyr
- Området
- Arbeidsstedet
- Anne



SJA-gruppa

- En SJA-gruppe kan bestå av:
  - SJA-leder (arbeidsleder)
  - Linjeleder (ansv for arbeidsoppgaven)
  - HMS-person
  - Utførende personell
  - Person med kunnskap til SJA-metoden
  - Sekretær
  - ”Djevelens advokat”

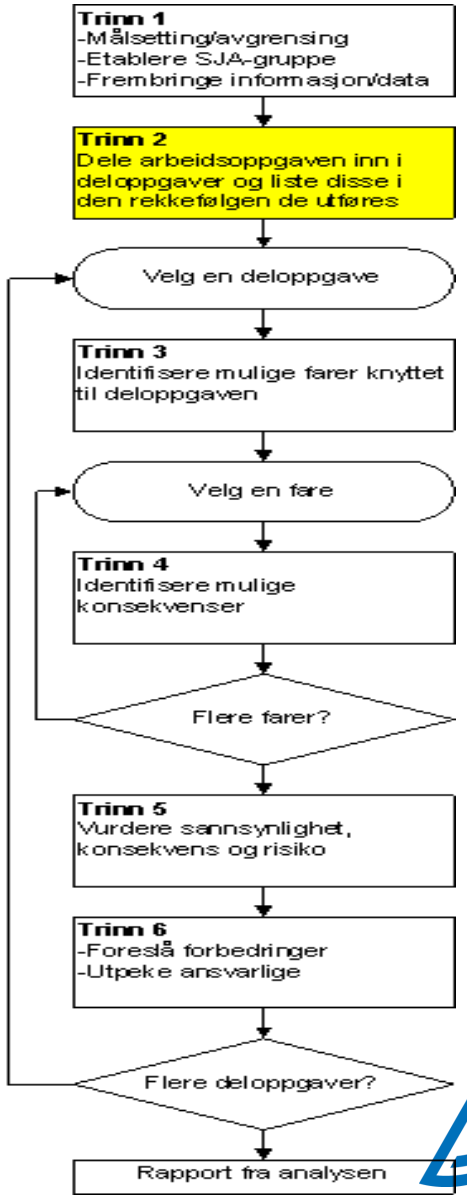
- Helst alle som er involvert i arbeidsoperasjonen

Trinn 2: Nedbrytning i deloppgaver

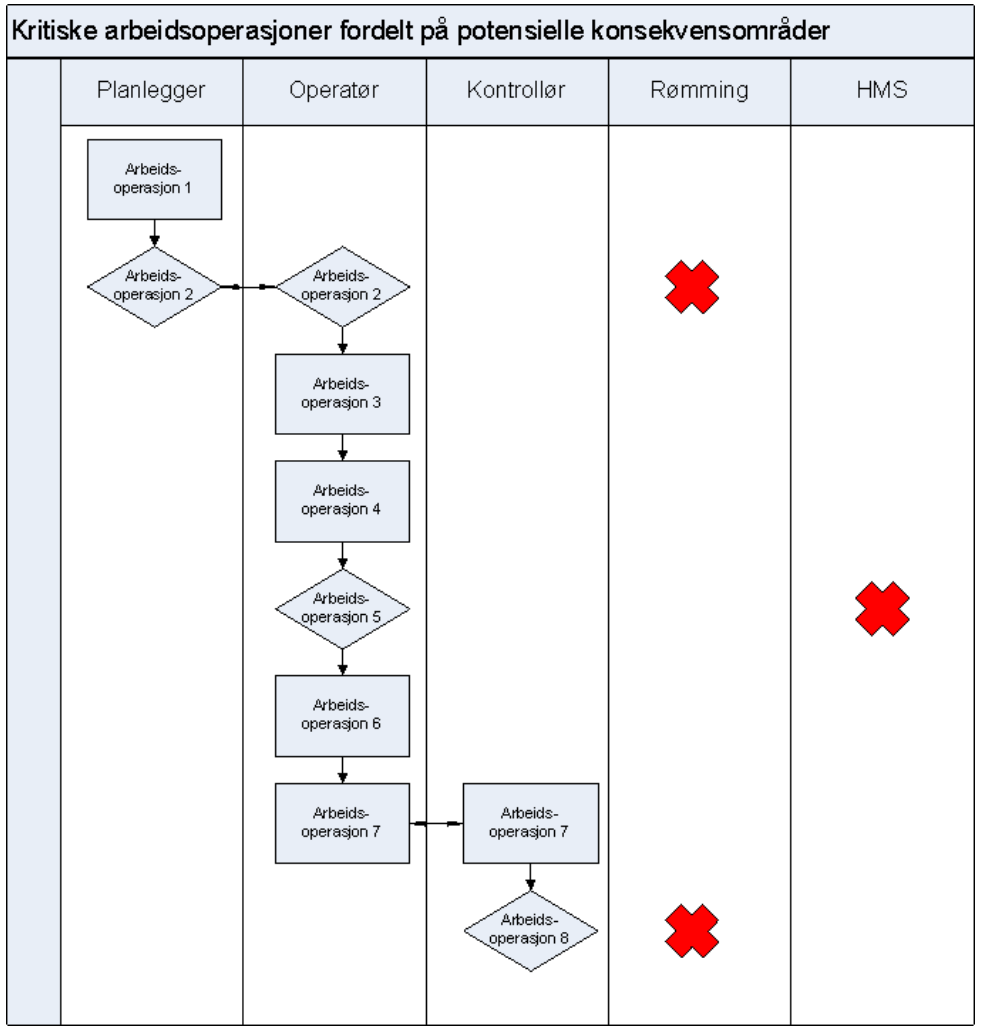
- Hva skal gjøres og i hvilken rekkefølge?

- En arbeidsoppgave består vanligvis av en sekvens av deloppgaver
- Eksempel: nedsetting av last

- Ta hensyn til forhold utenfor ”den ideelle arbeidsgangen”
  - Faktisk arbeidspraksis
  - Mulige avvik som kan oppstå
  - Eventuelle støtteoperasjoner



Kritiske arbeidsoperasjoner

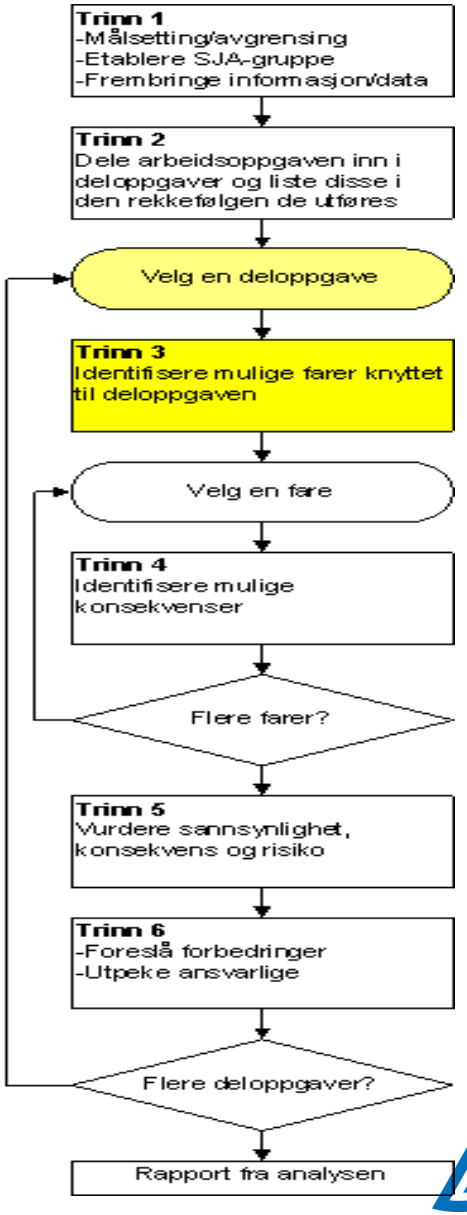


Trinn 3: Identifikasjon av mulige farer knyttet til hver deloppgave

- Hva kan kan gå galt – og hvordan? (hendelse + årsak)

- Så konkret og nært praksis som mulig.
- Eksempel: personell klem på grunn av sving i lasten

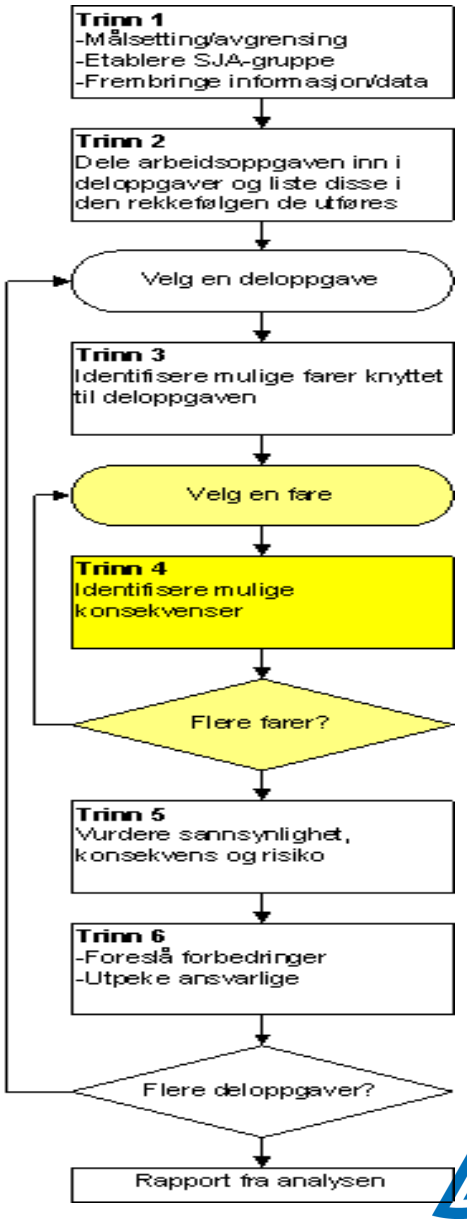
- Faretyper
  - Farekilder (mekaniske, kjemiske, etc)
  - Farlige måter å utføre arbeidet på
  - Menneskelige feilhandlinger
- Fareidentifikasjon forgår per deloppgave



Trinn 4: Identifisering av konsekvenser knyttet til hver fare

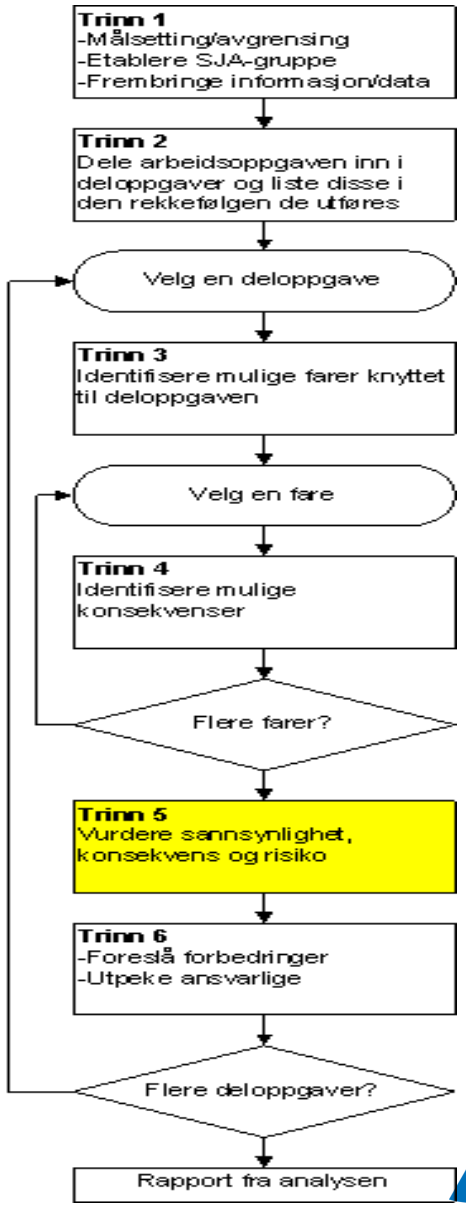
- Hvilke konsekvenser kan forekomme?
  - Personskader?
  - Miljøskader?
  - Økonomi?

- Eksempel: Personskade



Trinn 5: Vurdering av risiko

- Hvor kritisk er faren?
- Enkel vurdering av hver enkelt fare
  - Sannsynlighet (høy, middels, lav)
  - Konsekvens (høy, middels, lav)
- Risiko = sannsynlighet x konsekvens
- Grunnlag for prioritering av tiltak

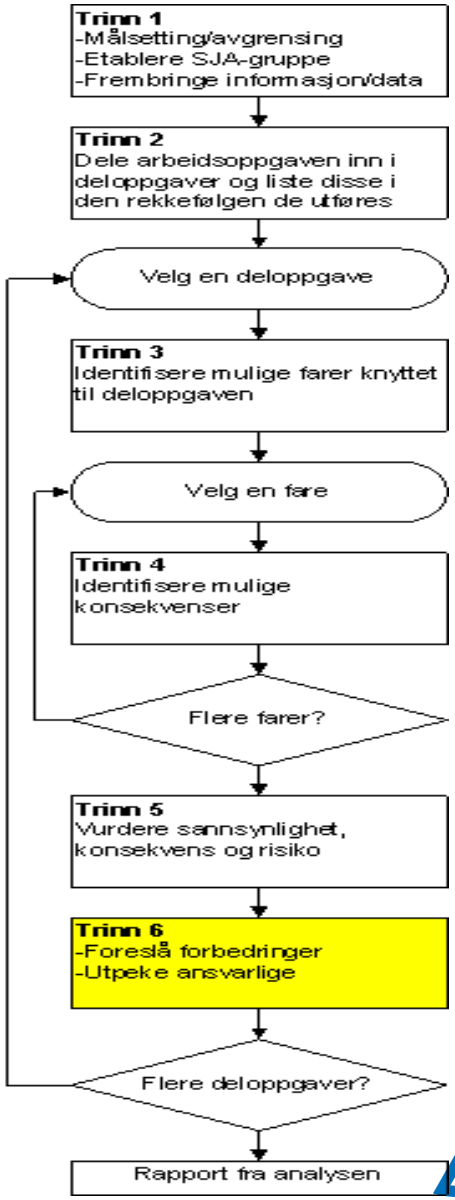


Trinn 6: Forslag til tiltak

- Hva kan gjøres for å redusere risikoen?

- Eksempler:
  - Forebygging: kontinuerlig kommunikasjon
  - Skadebegrensning: bruk av riktig sikkerhetsutstyr

- Tiltak for å redusere risikoen – tenk barrierer!
  - Personlig verneutstyr
  - Annet utstyr/hjelpemidler
  - Arbeidsrutiner/-metoder
  - Forbedre arbeidsinstrukser
  - Forberede avviks/-beredskapssituasjoner
  - Mer omfattende tiltak som kompetanseheving, etc



I praksis

- Sett av nok tid til SJA
- Inviter eventuelt personer med spesialkunnskap
- Deltakerne bør kjenne jobben på forhånd
- Bruk mest tid på de mest kritiske (farligste) trinnene i jobben

Styrker og svakheter

+

- Enkel metode å bruke – krever lite forkunnskap
- Involverer de som selv ”eier risikoen”
- Nærhet til der risikoen ”eksisterer”
- Problemer løses med en gang – tiltak
- Underlag for å utarbeide og forbedre prosedyrer

÷

- Svært enkel metode, ikke veldefinert systematikk
- Ikke egnet for komplekse operasjoner med mange interaksjoner

World Class Maintenance

TÜVRheinland®
safetec

HAZOP: Hazard and operability study

HAZID: Hazard identification

Hva er HAZOP ?

- HAZOP = HAZard and OPerability Study

- Formell, systematisk og kritisk granskning av de enkelte delene av et prosessanlegg
  - Baseres normalt på P&IDs (“Piping and Instrument Diagram” ev. “prosess- og instrumentdiagram)
  - Prosessen gjennomgås seksjonsvis ved hjelp av prosessparametre og ledeord (guidewords)
- Benyttes primært i forbindelse med design og modifikasjoner

Hensikt

- Identifisere og vurdere mulige avvik som kan føre til driftsavbrudd eller representere fare for personell eller utstyr
  - Årsaker
  - Effekt/ konsekvens
  - Eksisterende barrierer
  - Mulige nye barrierer (tiltak)
  - Ansvarlige for oppfølging av tiltak

- Problemorientert (ikke løsningsorientert)

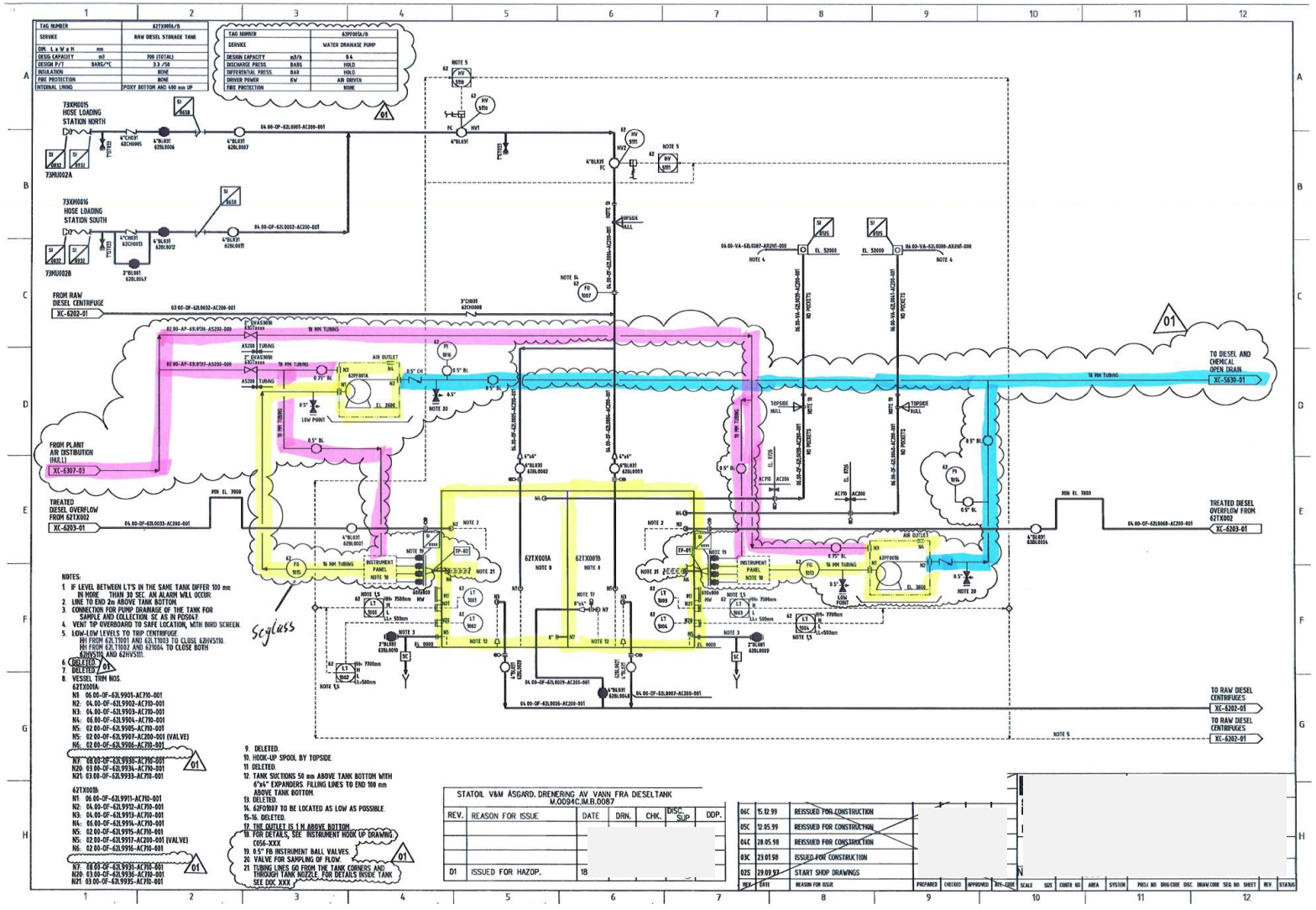
Typer av HAZOP

- Prosess HAZOP
  - Den opprinnelige HAZOP-teknikken, utvikliet for å vurdere prosessystemer/ -fabrikker
- Prosedyre HAZOP (HAZID)
  - Gjennomgang av prosedyrer eller kompliserte arbeidsoperasjoner
- Human HAZOP
  - Fokusert på menneskelige feil (human errors)
- Software HAZOP
  - Identifisering av mulige feil i utviklingen av software

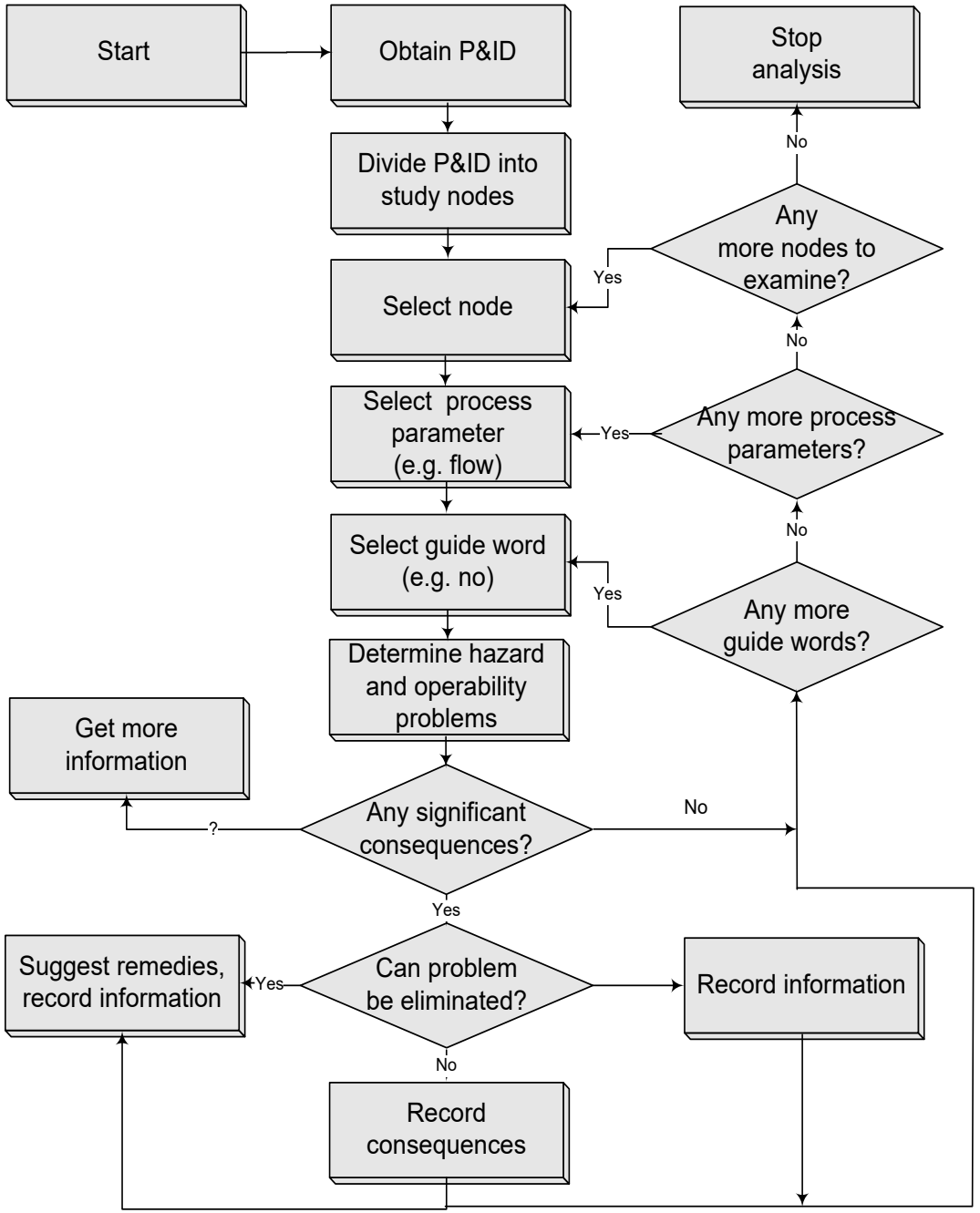
Prosess HAZOP

- Anvendes primært ifm design eller modifikasjon av prosessanlegg
- Gangen i analysen
  - Utgangspunkt i store enheter, feks tanker, kompressorer el
    - Noder for hver enhet: logisk del av systemet, feks en bestemt rørstrøm
      - Prosessparameter for hver node, feks flyt, trykk, temperatur, etv
        - Ledeord for hver prosessparameter, feks mer, mindre, ingen, etc
- Gjennomgang of P&IDs og/eller flytdiagram

Nodeinndeling på P&ID



Prosess HAZOP – Framgangsmåte



HAZOP – parametre og ledeord

Parameter:

- Strømning
- Trykk
- Temperatur
- Nivå
- Sammensetning
- ……

Ledeord:

- Ingen
- Mindre
- Mer / høy
- Retning / helning
- Grensesnitt
- Reverse
- Forskjellig fra / ulik
- ……

Prosessparametre og ledeord

Prosess-parametre	Ledeord						
	Mer	**Mindre**	**Ingen**	**Motsatt**	**Del av**	**I tillegg til**	**Annet enn**
Flyt/ strøm	For sterk/ rask	For svak/ sakte	Ingen	Feil retning	Komponent mangler	Forurens-ning	Lekkasje
Trykk	For høyt	For lavt	Ikke trykk		Del-trykk		
Temperatur	For høy	For lav					
Nivå	For høyt	For lavt	Ikke nivåmåling				Lekkasje/ flyter over

Prosedyre HAZOP

- Metodemessig svært lik en prosess HAZOP
- Anvendes for å avdekke mulige avvik i kompliserte arbeidsoperasjoner, både menneskelige feil og teknisk svikt

- Arbeidsoperasjonen brytes ned i enkeltoppgaver og analyseres hver for seg

Prosedyre HAZOP – ledeord

Ledeord	Forklaring
Tidlig	Før – i forhold til fastsatt klokketid
Sent	Etter – i forhold til fastsatt klokketid
Før	Før – i forhold til en annen oppgave
Etter	Etter – i forhold til en annen oppgave
Feil sted	Handlingen gjøres på feil sted
Utelatt	Handlingen utelates
Feil	Feil handling utføres
For sterk	Handlingen utføres med for stor kraft
For svak	Handlingen utføres med for liten kraft

Parametrene som benyttes i en prosess HAZOP har ingen naturlig parallell i prosedyre HAZOP

HAZID

- Benyttes ifm planlegging av potensielt risikofyllte operasjoner, feks en modifikasjonsjobb

- Basert på ledeord tilpasset den aktuelle jobben

HAZID – ledeord eksempler

Parameter	Ledeord
Oppstart	Uklart, mangler, feil. Hva sier prosedyren for dette / Hva skjer? Fjernstyring? Operasjonstemperaturer
Kommunikasjon	Rekkevidde, Frekvens, Støy, Synlighet
Lekkasje	Lekkasje av hva (Giftig stoffer, Flytende, Fast, Flyktig) Typiske lekkasjekilder Typiske lekkasjevolum
Brann/eksplosjon	Brennbart materiale, trykkbeholdere, tennkilder, slukkemidler, kontrollsystem, deteksjon/varsling, kontrollsystem.
Sikkerhet	Sikker Jobb Analyse, rømningsveier, varmt arbeid, barrierer, beredskap, fallende eller svingende last, trening/kompetanse/erfaring Annet
Arbeidsmiljø	Støy, arbeid i høyden, varme overflater, klemfare, lys, tilgang, støv, kjemikalier, annet

Suksessfaktorer

- Den “rette” sammensetningen av HAZOP-teamet
- Erfaren HAZOP-leder
  - Kjent med arbeidet/ prosessen som skal analyseres
  - Autoritet til å kontrollere diskusjonen
  - Ferdigheter som “katalysator”

- Erfarne og deltagende team-medlemmer

- Planlegging og forberedelse

Planlegging og forberedelse

- Planlegge gjennomføringen
  - Detaljnivå
  - Tidsramme
  - Rekkefølge av prosessen (noder)
- Sette sammen HAZOP-teamet
- Forberede nødvendig dokumentasjon
- Send møteinnkalling, inkludert:
  - Tid og sted
  - Deltagerliste
  - Dokumentasjon

Nødvendig dokumentasjon

- Oversiktstegninger
- Prosess- og instrumentdiagram (P&ID)
- Prosessdata
- Driftsprosedyrer
- Data om farlige stoffer etc

HAZOP-teamet

- **HAZOP-leder**
  - Uavhengig (uten ansvar for selve operasjonen)
  - Ansvarlig for å forberede HAZOPen (sammen med eieren av operasjonen/ systemet)
  - Lede HAZOP-møtet:
    - Sette i gang diskusjon omkring guide-words
    - Følge opp fremdrift etter agenda/ timeplan
    - Ferdigstille vurderingen
  - Ansvarlig for endelig rapport
- **HAZOP-sekretær**
  - Forberede HAZOP work-sheets
  - Ta notater fra HAZOP-møtet
  - Forberede utkast til rapport
- **Representanter fra alle parter og fagområder** som er involvert i operasjonen
  - Gi innspill basert på deres rolle/ ansvar i gjennomføringen av operasjonen
- HAZOP-teamet **bør bestå av 6-10 personer** for best mulig effektivitet

Hvordan være en god HAZOP-deltager

- Vær aktiv! Alle bidrag er viktige
- Vær poengtert! Unngå endeløse diskusjoner om detaljer
- Vær kritisk på en positiv måte – ikke negativ, men konstruktiv
- Vær ansvarlig! Del din kunnskap

HAZOP-møtet

- Agenda:
  - 1. Introduksjon og presentasjon av deltagerne
  - 2. Samlet presentasjon av operasjonen som er gjenstand for HAZOP
  - 3. Beskrivelse av HAZOP-metoden
  - 4. Presentasjon av første logiske del av operasjonen
  - 5. Analyse av første del av operasjonen ved bruk av guide-words
  - 6. Gjenta punkt 4 og 5 for alle deler av operasjonen
  - 7. Grov sammenfatning av funn

- Hver sesjon i HAZOP-møtet bør ikke strekke seg over for lang tid

HAZOP-notater

- Notater fra HAZOP-møtet gjøres av HAZOP-sekretæren ved bruk av work-sheets:
  - 1. Papirkopier av work-sheets, eller
  - 2. Bruk av PC og prosjektor

- Worksheets kan variere veldig med scope på studie. Normalt er følgende kolonner inkludert:
  - 1. Ref. nr. (Step no.)
  - 2. Guide-word
  - 3. Avvik (Deviation)
  - 4. Potensiell årsak/ kilde (Cause/source)
  - 5. Potensielle konsekvenser (Consequences)
  - 6. Aksjon/ anbefaling (Action/recommendation)
  - 7. Oppfølgingsansvarlig (Follow-up)

HAZOP-rapportering

- Det er ingen “korrekte svar”
  - Avhengig av deltagernes erfaringer
  - Avhengig av prioritering
- Foreløpige funn/konklusjoner presenteres på slutten av møtet
- Kladd av work-sheets blir distribuert til alle deltagerne for gjennomgang og kommentarer
- HAZOP-rapporten blir sendt ut når alle kommentarer til work-sheet er lagt inn

HAZOP work-sheet

Node:	Reference doc:
Operation:	Date:

Item	Deviation (Guidew. + Process param)	Source/cause	Consequence	Action/Recomm.	Follow-up

Feller og svakheter ved HAZOP

- For stort fokus på løsninger
- Endeløse diskusjoner om detaljer
- Noen få personer dominerer diskusjonen
- `Dette er min design/prosedyre'
- Forsvar av design/prosedyre
- HAZOP er ikke en revisjon
- "No problem"
- "Wasted time"

World Class Maintenance

TÜVRheinland®
safetec

FMEA - Feilmode og feileffektanalyse

(FMECA - Feilmode, feileffekt og kritikalitetsanalyse)

Bakgrunn

- En av de eldste formelle risiko/pålitelighets -analytiske metodene (ca 1950)
- Mange bransjer stiller krav om FMECA
- Hensikten med FMECA er å avdekke svakheter i et system for å kunne foreta konstruktive endringer
- Brukes ofte som innledende metode i større analyser
- Enkel metode som krever liten formell kunnskap

F M E A

System:
Referanse/tegn.nr:

Utført av:
Dato:
Side: av

Komponent	Funksjon/operasjonell tilstand	Feilmode	Effekt på andre enheter i systemet	Effekt på system	Kommentar

FMEA vs. FMECA

- Feilmode og feileffektanalyse
- Failure Mode and Effects Analysis

En framgangsmåte der hver potensielle feilmode analyseres for å:

- vurdere hvilke konsekvenser eller effekter de har på systemet
- foreslå tiltak for å eliminere eller kompensere for uakseptable effekter

- Feilmode, feileffekt og kritikalitetsanalyse
- Failure Mode, Effects and Criticality Analysis

- En utvidelse av en FMEA analyse til også å omfatte vurdering av feilmodenes feileffektgradering (alvorlighetsgrad) og feilfrekvens (sannsynlighet)

Formål og hensikt med FMEA

1. Forbedre sikkerheten ved å avdekke feilmoder som gir farlige situasjoner
2. Vurdere effekten av kritiske og/eller ikke-detekterbare feil på systemets primæroppgaver
3. Påvirke utformingen for å redusere effekten av feil i sluttproduktet
4. Støtte verifikasjonsarbeidet
5. Sikre at feildeteksjon/feilisolering som bygges inn møter sluttkravene
6. Hjelpe utviklerne til å utforme et system med høy sannsynlighet for operasjonell suksess
7. Framskaffe informasjon for å kunne utforme et effektivt vedlikehold

Fra SAE ARP5580

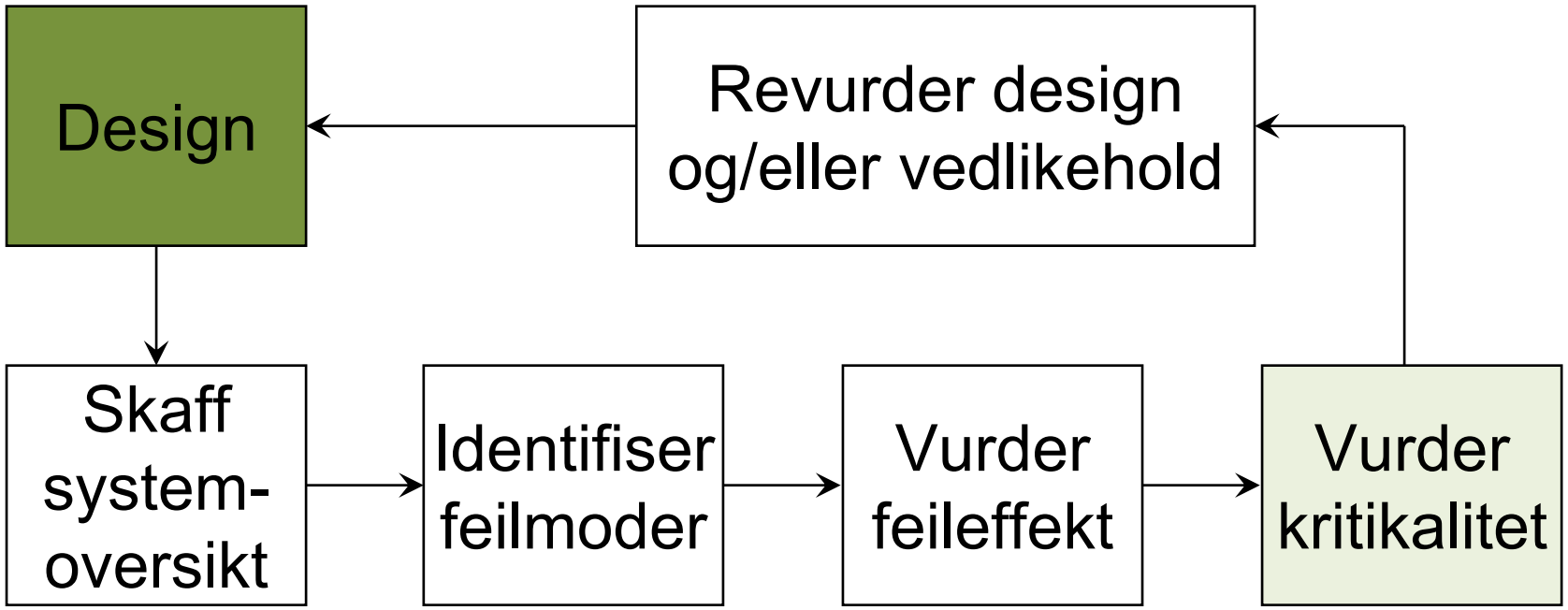
Bakgrunn og historikk

- En av de første systematiske metoden for å analysere feil i tekniske systemer
- Effekt av komponentfeil har ”alltid” vært vurdert, men formelle teknikker ikke utviklet før sent på 1950-tallet/tidlig på 1960-tallet
- Bakgrunn for utviklingen: Romfartsindustrien
- Sent på 1960-tallet: Profesjonelle organisasjoner gir ut de første prosedyrer/standarder
- 1980-tallet: FMEA standard del av designprosess
- Spesielt mye brukt innenfor:
  - Rom- og luftfartsindustri
  - Bilindustri
  - Militærindustri
  - Offshore industri

FMEA framgangsmåte

- Skaff oversikt over systemet og avgrens analysen
  - Del eventuelt systemet inn i delsystemer som analyseres separat
  - Finn funksjonen til alle komponentene
  - Etabler funksjons- og pålitelighetsblokkdiagram
  - Dokumenter driftsbetingelsene og hensikten med systemet
- For hver komponent: Identifiser alle potensielle feilmoder
- Vurder og beskriv årsakene til feilmodene
- Vurder og beskriv effekten av feilmodene, herunder
  - Vurder hvordan feil kan/vil bli detektert
  - Vurder om det kan være feil med felles årsak (”common mode”)
- Vurder og beskriv alvorligheten av de ulike feileffektene
- Foreslå passende oppfølging eller korrigerende tiltak

FMEA flytskjema



Fra M. Rausand

Skjema med sentrale begrep

F M E A

System:
Delsystem:
Referanse/tegn.nr:

Utført av:
Dato:
Side: av

Komponent			Beskrivelse av feil		Effekt av feil		Kommentar
ID	Funksjon	Operasjonell tilstand	Feilmode	Feilårsak og feilmekanisme	På andre enheter i systemet	På system	

Funksjon
(Function)

Operasjonell tilstand
(Operational mode)

Feilmode
(Failure mode)

Feilårsak og feilmekanisme
(Failure cause and mechanism)

Feileffekt
- ”lokalt”
- system
(Failure effect)

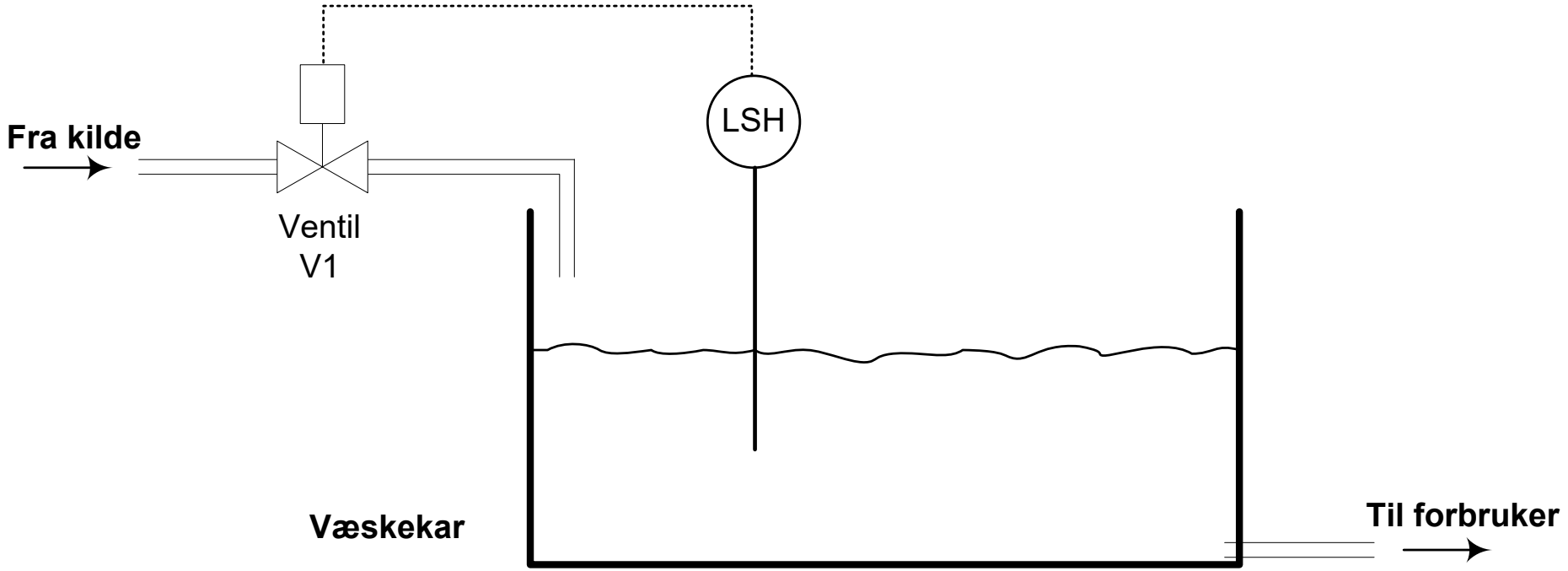
World Class Maintenance

TÜVRheinland®
safetec

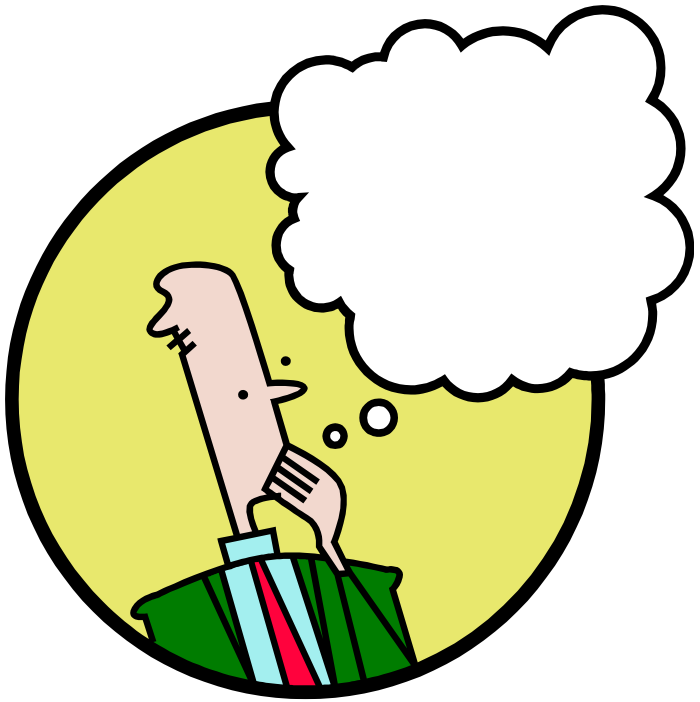
FMEA «tavleøving»

- Om vi rekker det -

Tavleoppgave



FMEA - Grunnleggende spørsmål



- På hvilke tenkelige måter kan enheten feile?
- Hvilke mekanismer vil kunne forårsake disse feilmodene?
- Hva kan effektene bli hvis feilen inntreffer?
- Er feilen i sikker eller farlig retning?
- Hvordan blir feilen oppdaget?
- Hvilke iboende egenskaper finnes i designet for å kompensere for feilen?

Fra M. Rausand

World Class Maintenance

TÜVRheinland®
safetec

FMECA

FMEA med kritikalitetsvurdering

- Husk - FMECA:
  En utvidelse av en FMEA analyse til også å omfatte vurdering av feilmodenes feileffektgradering og feilfrekvens
- Med denne utvidelsen kan feilmodenes relative betydning vurderes og rangeres
- Akseptgrenser (kan) innarbeides
- To (minst!) forskjellige framgangsmåter er vanlig for å visualisere kritikalitet:
  - Kritikalitets- eller risikomatrise
  - Beregning av ”Risk Priority Number” (RPN)

FMECA med kritikalitetsmatrise

- ”Ny” kolonne for feilfrekvens, f.eks.:
  - 1-Svært usannsynlig *(1 gang per 1000 år eller sjeldnere)*
  - 2-Usannsynlig *(1 gang per 100 år)*
  - 3-Lite sannsynlig *(1 gang per 10 år)*
  - 4-Sannsynlig *(1 gang per år)*
  - 5-Skjer ofte *(1 gang per måned eller oftere)*

- ”Ny” kolonne for feileffektgradering, f.eks.:
  - 1-Liten *(… ikke degraderes utover akseptable grenser…)*
  - 2-Stor *(… utover akseptable grenser, men som kan ivaretas …)*
  - 3-Kritisk *(… som degraderer systemet utover akseptable grenser..)*
  - 4-Katastrofal *(… hindrer systemet i å utføre sin hovedfunksjon)*

Eksempel på FMECA skjema

System: Performed by:

Ref. drawing no.: Date: Page: of

Description of unit			Description of failure			Effect of failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. no	Function	Opera-tional mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				

Oppsummering i matrise [1)]

Feilfrekvens	Feileffektgradering 1	2	3	4
5				
4				
3		(ant. feilmoder)		
2		(ev. ref.)		
1				

Ukritisk
Noe kritisk
Kritisk

[1)] *Både "kritikalitets-matrise" og "risiko-matrise" er vanlige benevnelser.*

World Class Maintenance

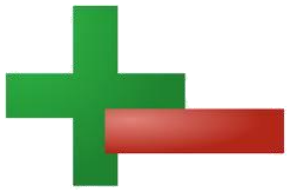
TÜVRheinland®
safetec

FMEA / FMECA

Fordeler og begrensninger

Fordeler

- Enkel metode som kan læres raskt
- Systematisk - sikrer komplett gjennomgang av systemet
- Effektiv for systemer som mest sannsynlig vil svikte pga. feil i enkelt-komponenter
- Kan benyttes som prioriteringsverktøy når forbedringer skal innføres
- Velegnet for problemløsning i grupper



- Begrensninger

- Vil lett omfatte kun tekniske feil
- Gir ingen kvantitativ beregningsmodell
- Fokus på effekter av en og en feil - Feilkombinasjoner avdekkes dårlig eller ikke
- ”Interface”-feil er ofte vanskelige å få med
- Kan lett bli svært arbeidskrevende med stor mengde dokumentasjon
- I stor grad avhengig av analytikeren (evnen til å se årsakssammenhenger)

World Class Maintenance

TÜVRheinland®
safetec

Feiltreanalyse

→ *SE FORRIGE INNLEGG ☺*

World Class Maintenance

TÜVRheinland®
safetec

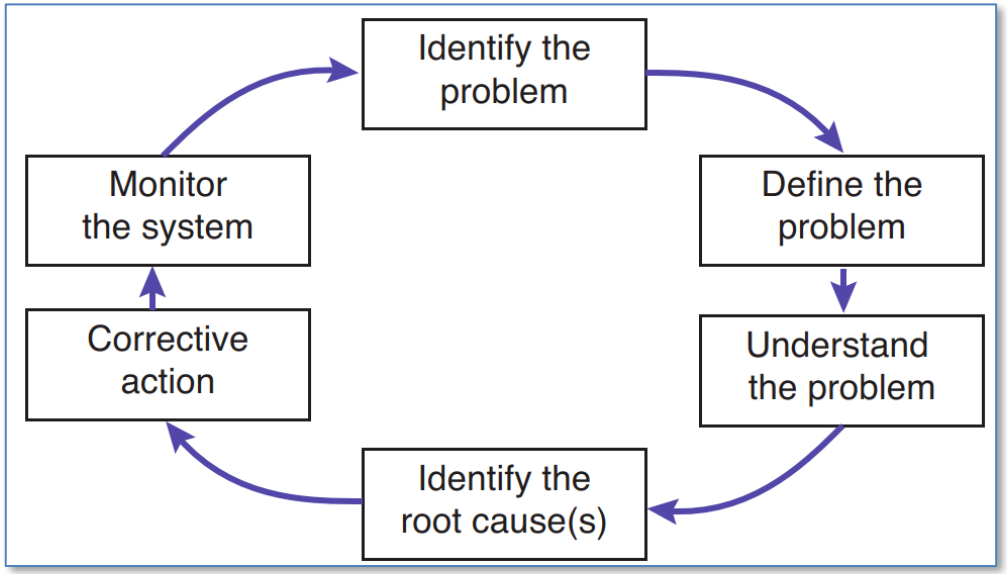
Rotårsaksanalyse

RCA (root cause analysis)

Har basert en del av presentasjonen på *«Veiledning i rotårsaksanalyse»* fra Direktoratet for økonomistyring, versjon 2 oppdatert 11.12.2015 (peker til denne), ref. til denne som «DFØ, 2015».

Hva er rotårsaksanalyse ("root cause analysis"/RCA)

- **Formål**
  - Identifisere de underliggende årsakene («rotårsakene») til et problem eller en hendelse
  - Finne ut hva som egentlig forårsaket problemet, slik at man kan iverksette tiltak for å forhindre at det skjer igjen
- **Formell framgangsmåte**, som typisk inneholder **følgende trinn**:
  1. Identifisér og avgrens problemet
  2. Definér (beskriv)
  3. Forstå problemet
  4. Identifisér og analysér rotårsaker
  5. Foreslå og implementer nødvendige korrektive tiltak
  6. Overvåk; evaluere effekten
- Flere forskjellige teknikker er vanlig, f.eks. **5 Whys** og **fiskebeinsdiagram** (**Ishikawa-diagram**)
- Egner seg best som en **gruppeøvelse**; involver de som har best kunnskap om problemet. Også viktig: **Ikke let etter skyldige**



Kilde: «System Reliability Theory» (Rausand og Høyland)

1 – Identifisér og avgrens problemet

- **Hva?**
  - Hva skjedde?
  - Kommentar: Ofte vil det kun være symptomer
- **Når?**
  - Når skjedde det?
- **Hvor?**
  - Hvor skjedde det?
- **Hvor alvorlig?**
  - Hvor alvorlig er (hvor stor betydning har) problemet?

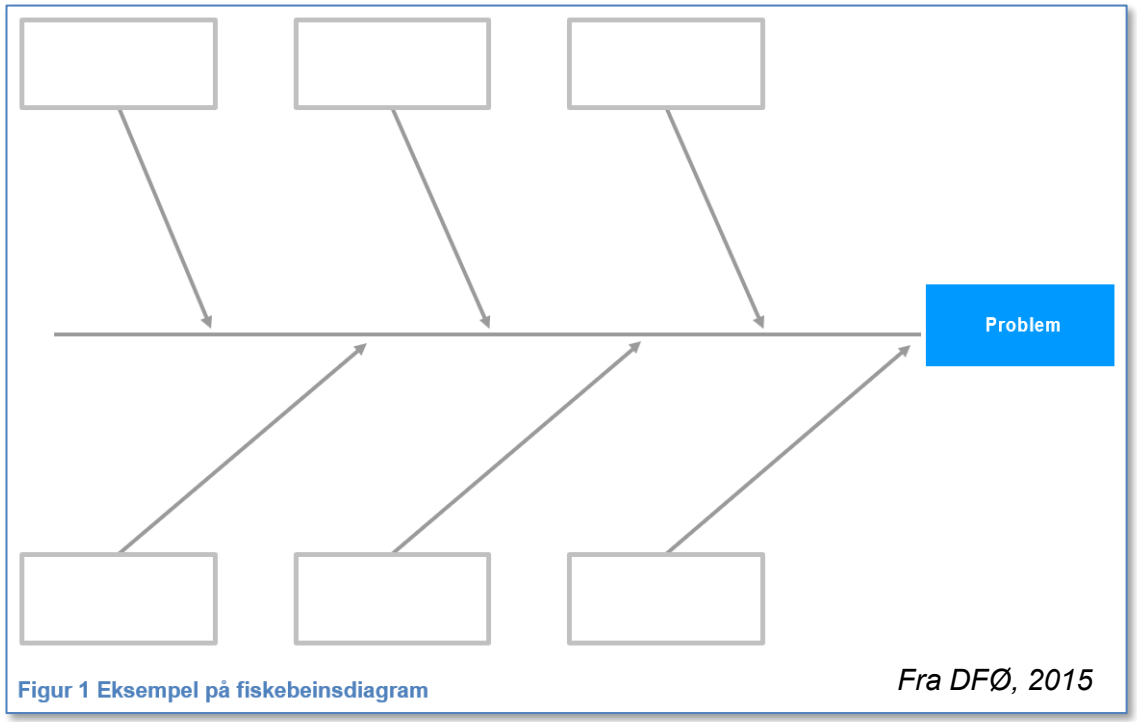
2/3 – Definér (beskriv) og forstå problemet

- **Definere problemet**
  - Beskriv problemet klart og tydelig
  - Samle inn data og informasjon om hva som skjedde, når det skjedde, og hvilke konsekvenser det hadde
- **Samle informasjon**
  - Innhent all relevant informasjon og data som kan hjelpe til med å forstå problemet bedre
  - Kan inkludere intervjuer, dokumenter, logger, og observasjoner

Kilde: DFØ, 2015

4 – Identifisér og analysér rotårsaker (1/3)

- Definer hovedkategorier/større årsaker (f.eks. etter faktorer som «målinger», «mennesker», «teknologi», «miljø», «material» og «metode»)
- Bruk brainstorming/eksisterende data til å generere underliggende/mindre årsaker under hovedkategoriene/større årsaker
- Bruk gjerne *fiskebeinsdiagram* (*Ishikawadiagram*) (se også neste slide)
- Spør arbeidsgruppen: Hvorfor skjer dette?
  - Gjenta dette spørsmålet for neste detaljnivå for å bore ned til de mest grunnleggende årsakene
  - Benytt gjerne metoden *5 Whys; «Fem hvorfor»* (se senere slide)
- Bli enige om hvilke årsaker som er de viktigste bakenforliggende årsakene, "rotårsakene"



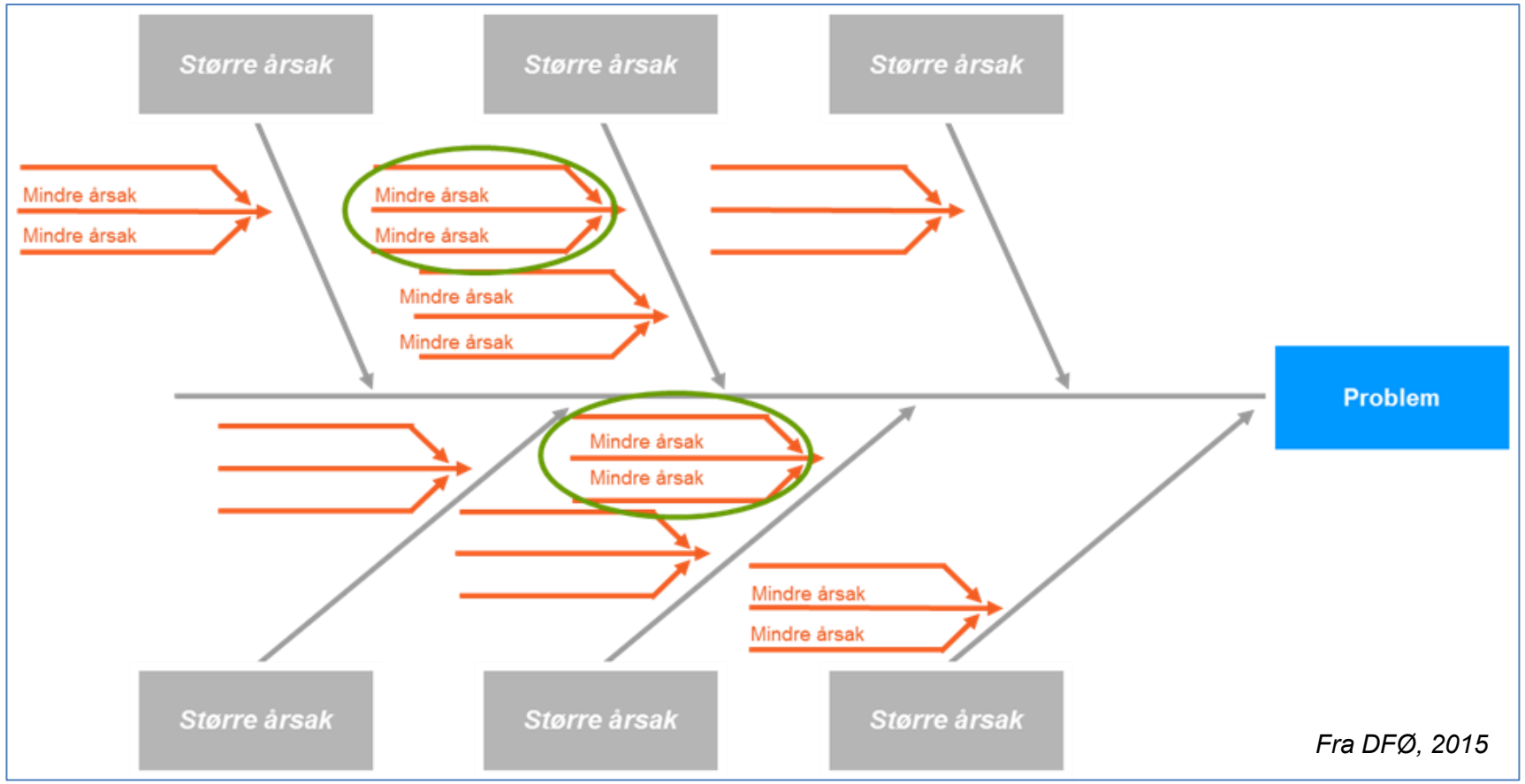
Figur 1 Eksempel på fiskebeinsdiagram

Fra DFØ, 2015

Kilde: DFØ, 2015

4 –Identifisér og analysér rotårsaker (2/3)

Eksempel på fiskebeinsdiagram (Ishikawadiagram) med prioriterte rotårsaker illustrert ved grønn sirkel



Fra DFØ, 2015

4 –Identifisér og analysér rotårsaker (3/3)

5 Whys – «Fem hvorfor»

- Still spørsmålet «Hvorfor?» gjentatte (vanligvis fem) ganger etter hverandre
- Hensikten er å gå dypere inn i problemet for å avdekke den underliggende årsaken
- Kan brukes i kombinasjon med fiskebeinsdiagram – da gjerne for å gå dypere inn i (bak) hovedkategoriene/de større årsakene først identifisert
- Kan også brukes direkte, uten først å ha etablert hovedkategoriene/de større årsakene

- Eksempel på «direkte» bruk (*fra Copilot*), med problemet «Maskinen stopper ofte opp»:
  1. **Hvorfor** stopper maskinen opp? Fordi den overopphetes.
  2. **Hvorfor** overopphetes maskinen? Fordi kjølesystemet ikke fungerer som det skal.
  3. **Hvorfor** fungerer ikke kjølesystemet som det skal? Fordi det er en blokkering i kjølerørene.
  4. **Hvorfor** er det en blokkering i kjølerørene? Fordi vedlikeholdsrutinene ikke har blitt fulgt.
  5. **Hvorfor** har ikke vedlikeholdsrutinene blitt fulgt? Fordi det mangler opplæring og ressurser for vedlikeholdspersonalet.

5 – Foreslå og implementer nødvendige korrektive tiltak

- Identifisere og utvikle tiltak og løsninger som kan eliminere eller redusere disse årsakene
- Kan inkludere endringer i prosesser, opplæring, eller teknologiske løsninger
- Løsningene bør formuleres som tiltak
  med ansvarlig person og frist
- Tiltakene kan dokumenteres i en enkel tiltaksliste (se eksempel) eller i en mer omfattende tiltaksrapport
- Prioritér tiltak: Når mulige tiltak er er beskrevet bør det gjennomføres en kost-nytte vurdering – f.eks. i en 2x2-matrise:
  - Verdi for virksomheten: Høy vs. lav
  - Realiserbarhet: Høy vs. lav
- Person med myndighet og ansvar prioriterer og beslutter tiltak

NR	Årsak problem	Tiltak	Prioritering	Ansvar	Frist

Figur 4 Eksempel mal tiltaksliste

Fra DFØ, 2015

6 – Overvåk; evaluere effekten

- Overvåk og evaluer effekten av de tiltakene som er iverksatt for å sikre at problemet er løst og ikke oppstår igjen
- Juster tiltakene om nødvendig

- Eksempel på problem, tiltak og overvåking (måling) av effekt *(generert av Copilot)*:
  - Problem: I løpet av de siste tre månedene har antallet defekte produkter økt med 30 %
  - Tiltak:
    - Implementere et nytt vedlikeholdsprogram
    - Gi opplæring til produksjonspersonell om viktigheten av vedlikehold
    - Allokere ressurser til regelmessig vedlikehold av maskiner
  - Overvåking:
    - Overvåk antallet defekte produkter over de neste månedene for å se om tiltakene har hatt ønsket effekt

World Class Maintenance

TÜVRheinland®

safetec

Sjefrådgiver

Ragnar Aarø

+47 934 83 940

Ragnar.Aaro@safetec.no