TTK2 – Pålitelighetsanalyse av sikkerhetsfunksjoner

Seminar 1 – Praktisk, introduksjon til case og sentrale begrep

Versjon:
05.08.2026

2026

Faglærer: Mary Ann Lundteigen

https://www.itk.ntnu.no/emner/fordypning/TTK2

Om bruk av innhold fra slidene

© 2026 Mary Ann Lundteigen.

This presentation is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. Under these terms, you are free to share and adapt the material for non-commercial purposes, provided you give appropriate credit to the original author.

Please note: Images, figures, and other materials cited or reproduced from external sources are not covered by this license and remain the intellectual property of their respective rights holders.

The content is updated regularly to improve precision and ensure relevance, which is reflected in the revision number. Please reach out to mary.a.lundteigen@ntnu.no if you have comments or suggestions for improvement.

La de gjerne inspirere, men husk å referere meg om du bruker noe fra presentasjonen direkte

Agenda

Praktisk:

- Om emnet og oversikt innhold/seminarplan
- Deling av informasjon i TTK2
- Muntlig eksamen – hvordan det er tenkt organisert

Teori seminar 1:

- Begreper og intro relevant for miniprosjektet
- Miniprosjekt (anvendt på case)
- Miniprosjektets oppgave 1 (tilknyttet teori seminar 1)

Hva handler dette temaet om?

Pålitelighetsanalyse av **sikkerhetsfunksjoner**

- **Pålitelighet** handler om **sannsynligheten** for at for at sikkerhetsfunksjonen virker eller ikke, eventuelt hvor ofte (**frekvensen**).

- **Sikkerhet** er fravær av uakseptabel risiko for skade på personer, miljø og kritiske verdier
- **Sikkerhetsfunksjoner** implementert i egne sikkerhetssystemer som har i oppgave å **håndtere farlige hendelser uavhengig** av de normale styringsfunksjonene.

Betydning

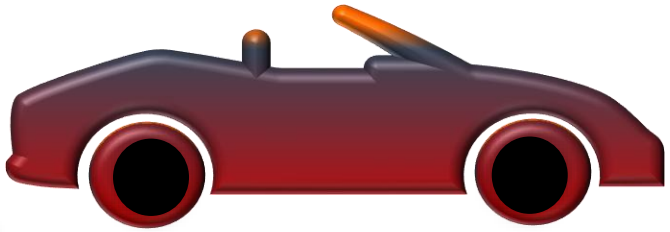
- Uttrykker hvor **mye vi kan stole** på sikkerhetsfunksjonen.
- Implisitt betydning for hvilken **risiko** man blir utsatt for.

Implikasjoner

- Ekstra krav til hvordan sikkerhetsfunksjoner skal designes og driftes.
- Å demonstrere at kravene er oppfylt inkluderer blant annet **pålitelighetsanalyser**.

Pålitelighet *generelt* vs pålitelighet *for sikkerhet*

Pålitelighet alltid knyttet til enkeltvise funksjoner.

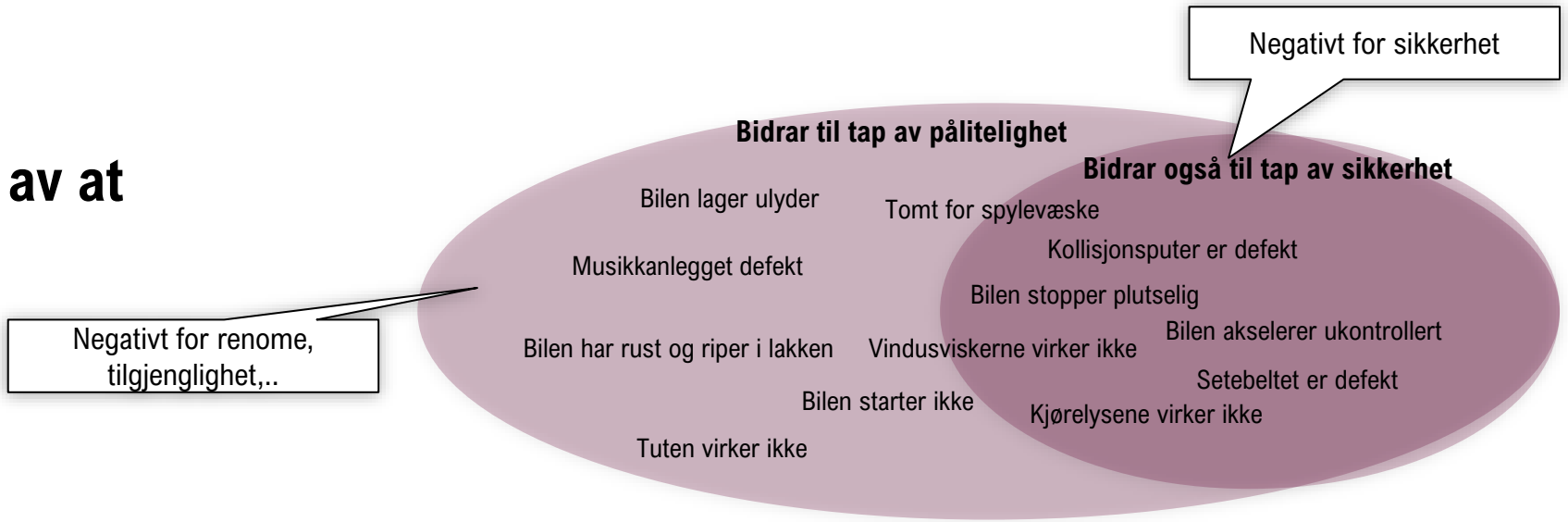


Eksempler:

- Transportere fører og eventuelt passasjerer som skal fra A til B
- Ha lydanlegg som imponerer
- Være enkelt å skru og fix'e på selv for den motorinteresserte
- **Løse ut airbag v/ detektert kollisjon eller utforkjøring**
- **Utløse nødbremsassistanse for å hindre tap av kontroll med bilen**
- Styre lysstyrke i mørket
- …

Eksempler på Sikkerhetsfunksjoner

Pålitelighet påvirkes negativt av at funksjoner feiler.



Hva er en sikkerhetsfunksjon (SIF) og et sikkerhetssystem (SIS)?

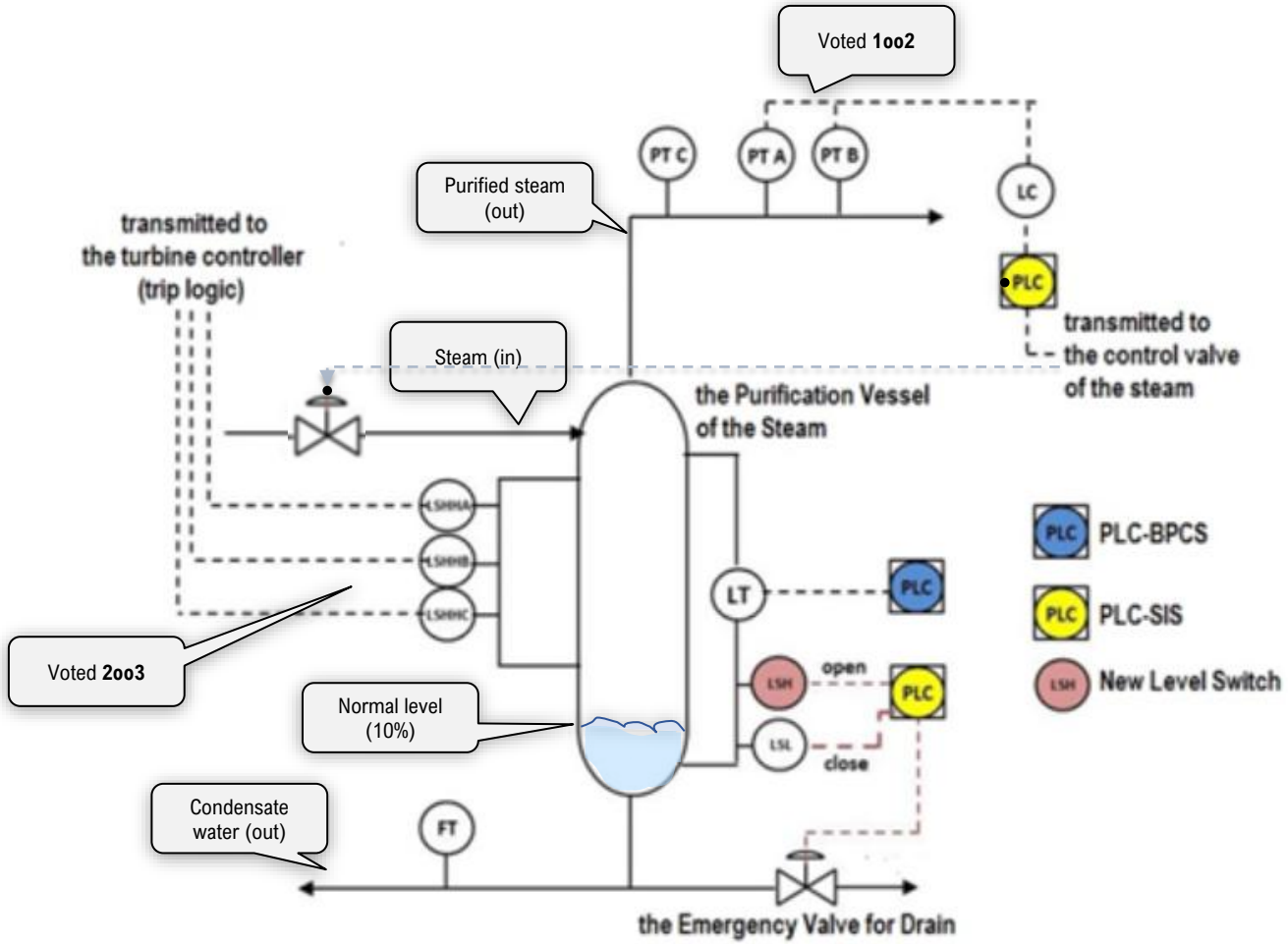


Figure 5. Development of the system of instrumentation and process control for the steam purification system

System:

- Producing purified steam to turbines that produce electricity in an old nuclear plant
- An old system that was subject to re-design to improve safety, adding new SIFs

- PLC: Programmable logic controller («logic solver»)
- LC: Level controller
- PT: Pressure transmitters
- LT: Level transmitter
- LSH: Level switch high (Eks: 20%)
- LSL: Level switch low (Eks: 5%)
- BPCS: Basic process control system (reguleringssystem/regulator)
- FT: Flow transmitter

Kilde. https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.100504

Standarder for funksjonell sikkerhet

Kravene som gjelder for design og drift av SIFer er forankret i standarder for **funksjonell sikkerhet**

IEC 61508: Generic and an umbrella/cross-sector standard

Funksjonell sikkerhet: Sikkerheten (i form av redusert risiko for ulykker) som oppnås når SIFer gir en del av bidraget (fritt oversatt av definisjon I IEC 61508)

Medical	Process	Machinery	Nuclear	Automotive	Railway	Escalators	Avionics	Ships and marine technology
								
IEC 62304	IEC 61511	IEC 62061 (ISO 13849)	IEC 61513	ISO 26262	EN 50126 EN 50128 EN 50129	ISO 22201	**Airborne:** DO-178B (USA) ED 12b (Europe) **Air traffic management:** ESARR 3 SAF.ET1.ST03.100 0.REP-01-00	ISO 17894 (compatible with DNV-GL RP D201)

Hva er en sikkerhetsfunksjon (SIF) og et sikkerhetssystem (SIS)?

SIF1: Stop turbines upon too high condensate level (damage turbine/electricity Production)

SIF4: Force steam inlet so that pressure drop and loss of electricity production is avoided.

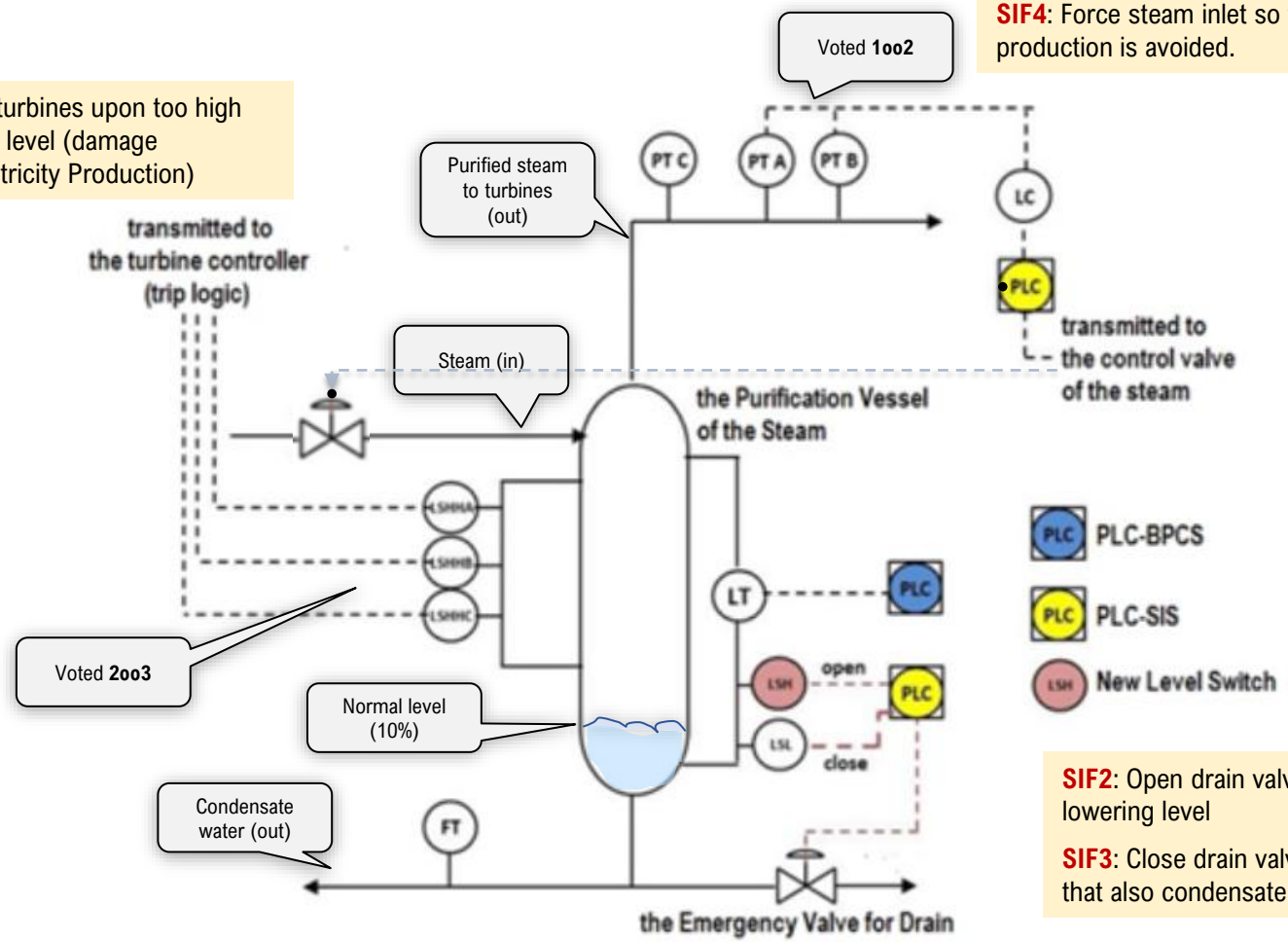


Figure 5. Development of the system of instrumentation and process control for the steam purification system

- Safety instrumented function (SIF):
  - Includes sensor(s), logic solver, and final (usually actuated) devices
  - Identifies equipment involved in solving specific safety tasks
- Safety instrumented system (SIS)
  - Containing the SIFs
- SIS/SIF vs process control

SIF2: Open drain valve to assist lowering level

SIF3: Close drain valve to ensure no hot steam into water system (assume that also condensate outlet has a valve that is closed)

Kilde. https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.100504

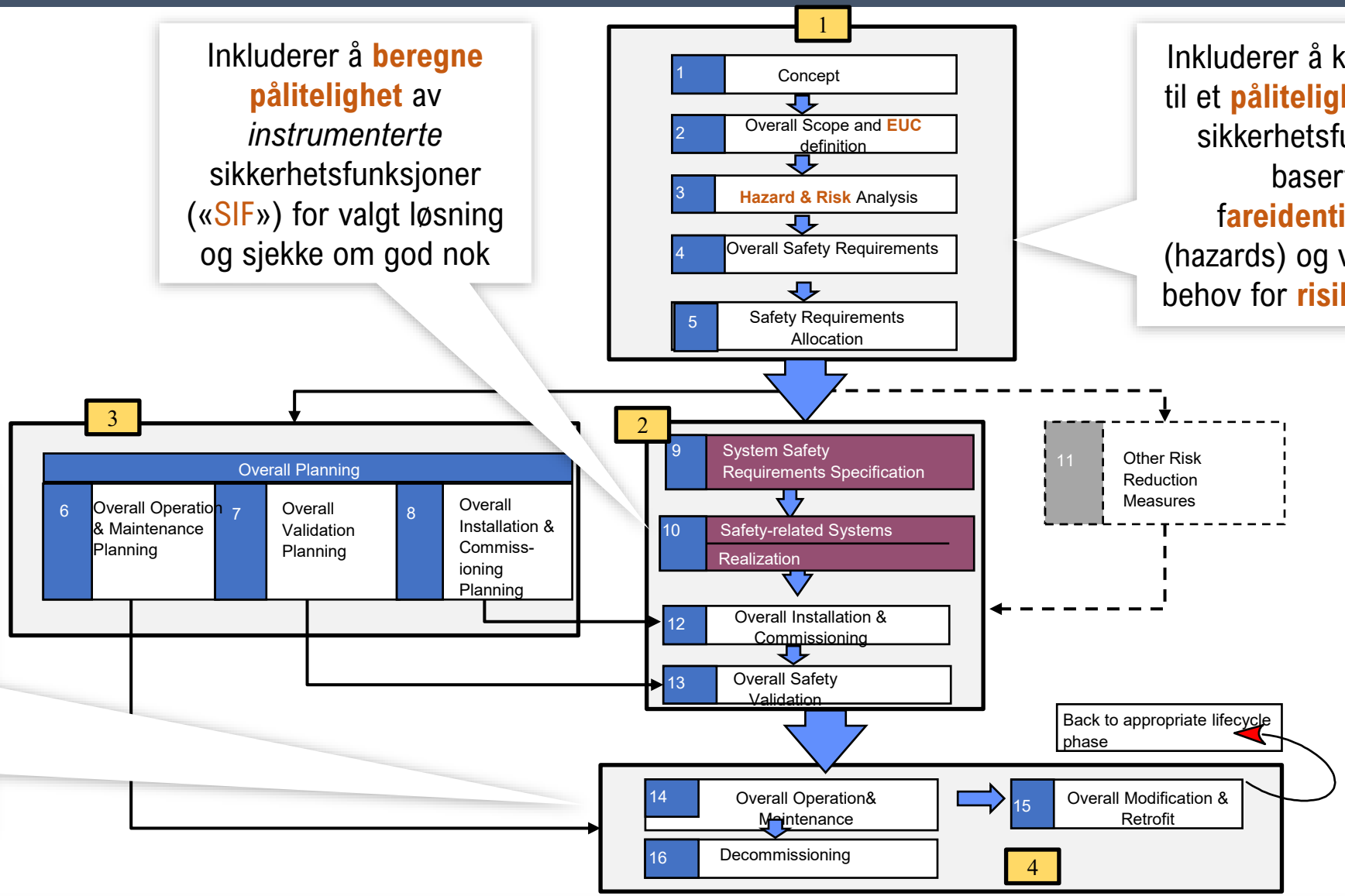
Hvilken rolle har pålitelighetsanalyser?

Figur: Adoptert fra IEC 61508

Inkluderer å **beregne pålitelighet** av *instrumenterte* sikkerhetsfunksjoner («SIF») for valgt løsning og sjekke om god nok

Inkluderer å komme frem til et **pålitelighetskrav** for sikkerhetsfunksjoner basert på **fareidentifisering** (hazards) og vurdering av behov for **risikoreduksjon**

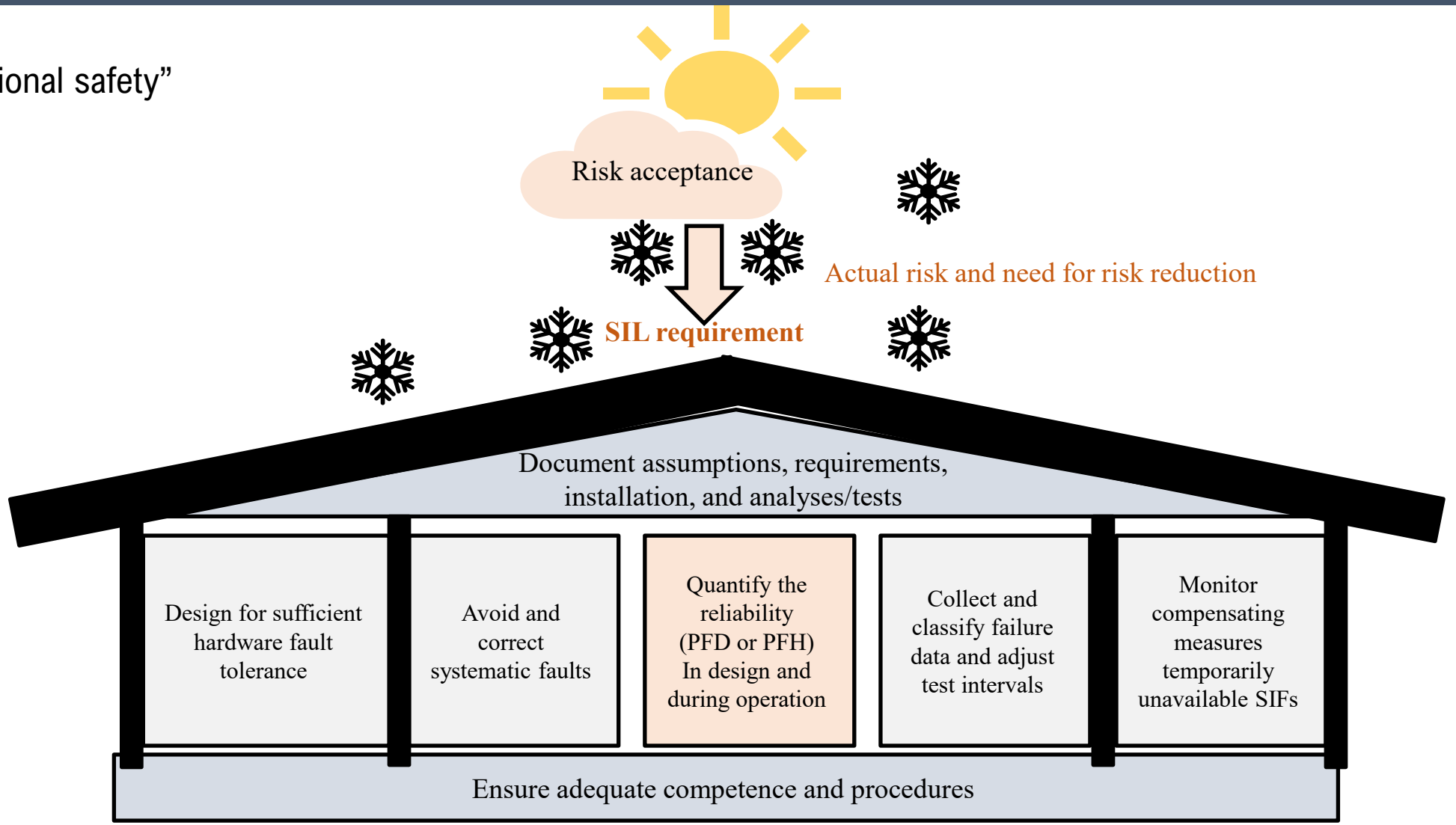
Inkluderer å beregne på nytt – med jevne mellomrom - **påliteligheten** av SIFer i drift og gjøre kompenserende tiltak om nødvendig



TTK2

Hva vi dekker I TTK 2 innenfor funksjonell sikkerhet

"House of functional safety"



Pålitelighetsanalyse – er det flere måter å gjøre det på da?

Ja, det er det. **Ulike metoder** – **ulike egenskaper** – gir normal samme/nesten samme resultat ved samme antagelser og forenklinger. Men enkelte metoder gir **mer fleksibilitet** til å ta med flere faktorer der dette har betydning.

Målet med dette emnet er å bli kjent med ***noen*** av de som brukes.

Er det nyttig da?

Ja, det kan det bli.

- Har selv erfart at **kybernetikere** gir **viktige innspill** til de som har ansvar for å gjøre pålitelighetsanalyse – som er helt avhengig av å forstå hvordan systemet virker
- Kjenner mange med **kybernetikkbakgrunn som aktivt jobber med pålitelighetsanalyse** i sin daglige jobb

Seminarplan

Seminar 1: Introduksjon og teori for oppgave 1

Seminar 2: Teori for oppgave 2

Seminar 3: Teori for oppgave 3

Seminar 4: Teori for oppgave 4

Seminar 5: Jobbe med miniprosjekt (1-4)

Seminar 6: Jobbe med miniprosjekt (1-4)

Seminar 7 (6): Refleksjon (oppgave 5) og forberedelse muntlig eksamen

Miniprosjekt

Oppgave 1: Forankring og konsept

Oppgave 2: Pålitelighets-nettverk

Oppgave 3: Feiltreanalyse

Oppgave 4: Markovanalyse

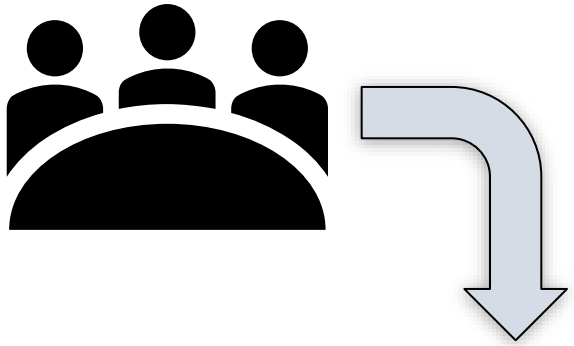
Oppgave 5: Refleksjon

Løsning på oppgavene dokumenteres i en presentasjon.
Denne gjøres tilgjengelig på eksamen.

TTK 4555 Muntlig eksamen
(Dato blir publisert på ordinær måte)

- Tema for utspørring på muntlig eksamen er individuell og det trekkes blant spørsmålene i oppgavene i miniprosjektet.
- Fokus på forstå tematikken og begrepene, kjennetegn ved metodene, hvordan dere gikk fremfor løsning av oppgaver.

Hvor dere finner materiale for TTK2



https://www.itk.ntnu.no/emner/fordypning/TTK2

Om miniprosjektet

Miniprosjekt i TTK2 – Pålitelighetsanalyse av sikkerhetskritiske funksjoner

Forfattet av: Mary Ann Lundteigen

Revisjon: 07.08.2026 (Dokumentet oppdateres jevnlig og sjekk alltid om du har siste versjon)

Dokumentet er utviklet for bruk i et fordypningsemne på teknisk kybernetikk, NTNU.

© 2026 Mary Ann Lundteigen.

This document is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. Under these terms, you are free to share and adapt the material for non-commercial purposes, provided you give appropriate credit to the original author.

Please note: Images, figures, and other materials cited or reproduced from external sources are not covered by this license and remain the intellectual property of their respective rights holders.

The content is updated regularly to improve precision and ensure relevance, which is reflected in the revision number. Please reach out to mary.a.lundteigen@ntnu.no if you have comments or suggestions for improvement.

Oversikt over miniprosjektet

Oppgaver for seminar 1

4 Oppgave 1 (seminar 1) – Bestemme krav til sikkerhetsfunksjoner

I oppgave 1 er formålet å gjennomføre en risikoanalyse og komme frem til et pålitelighetskrav til sikkerhetsfunksjonen SIF1.

a) Foreslå en naturlig avgrensning av EUC for hendelsen «overtrykking av separator», og gi eksempler på utfordringer eller problemstillinger man må ta hensyn til for å gjøre denne avgrensningen.

b) Bruk en sjekkliste til å identifisere mulige årsaker til overtrykking og identifiser hvilke som PSD-systemet og PSV-ventilen kan stanse.

c) Lag et hendelsestre som identifiserer mulige utfall av hendelsene, der rollen til ESD og F&G systemet vises

d) Overfør informasjonen fra forrige deloppgave til et bowtie-diagram og angi hvor sikkerhetsfunksjoner implementert via PSD, ESD og F&G, samt trykkavlastningsventilen PSV, vil plassere seg.

e) Regn ut pålitelighetskravet, uttrykt som PFD, for PSD SIF-en dersom vi antar en demand-rate for PSD SIF på 1/10 år, et akseptkriterium på 1/100 000 år og at PSV-ventilen har en feilsannsynlighet på 1%. Illustrer grafisk og vis utregning.

f) Regn også ut demand-ratene for PSV-ventilen, ESD-systemet og F&G-systemet, dersom vi for dette eksempelet legger til at funksjonene i ESD- og F&G-systemene er designet for å oppfylle SIL 2-krav. Tegn opp et barrierediagram med alle demand-ratene.

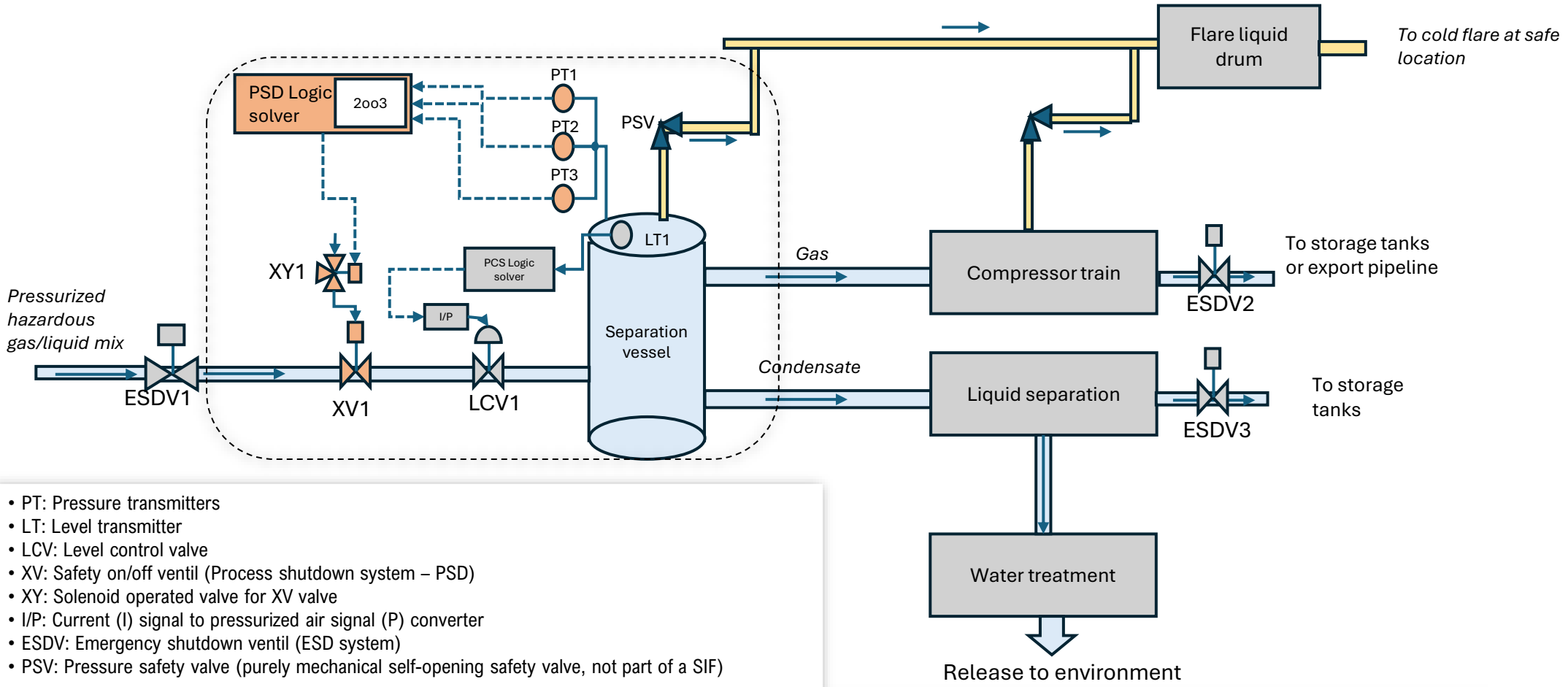
g) Anta at man ønsker å introdusere en ny sensorteknologi for overtrykksdeteksjon i PSD SIF som bruker KI (AI).

   i. I hvilken grad påvirker dette usikkerheten forbundet med risikoreduksjonen for PSD SIF-en isolert sett, og hvilken konsekvens kan dette ha for risikoreduksjonen totalt sett?
   ii. Hvordan vil ALARP-prinsippet kunne påvirke hvordan man håndterer dette? (ikke utregninger, her er det ment å resonnere litt frem og tilbake)

TEORI SEMINAR 1

- Case miniprosjekt
- Begreper

Case for miniprosjektet: En prosess med storulykkespotensiale



- PT: Pressure transmitters
- LT: Level transmitter
- LCV: Level control valve
- XV: Safety on/off ventil (Process shutdown system – PSD)
- XY: Solenoid operated valve for XV valve
- I/P: Current (I) signal to pressurized air signal (P) converter
- ESDV: Emergency shutdown ventil (ESD system)
- PSV: Pressure safety valve (purely mechanical self-opening safety valve, not part of a SIF)

TTK2

Pålitelighet og feil

Pålitelighet: (eng: Reliability)

- Evnen en funksjon har til å utføre en tiltenkt oppgave innenfor angitt tid og angitte omstendigheter.

Tilgjengelighet: (eng: Availability)

- Andel av tid en funksjon er tilgjengelig, tatt høyde for også nedetid

Svikt: (eng: Failure)

- Hendelsen der en angitt funksjon opphører å fungere

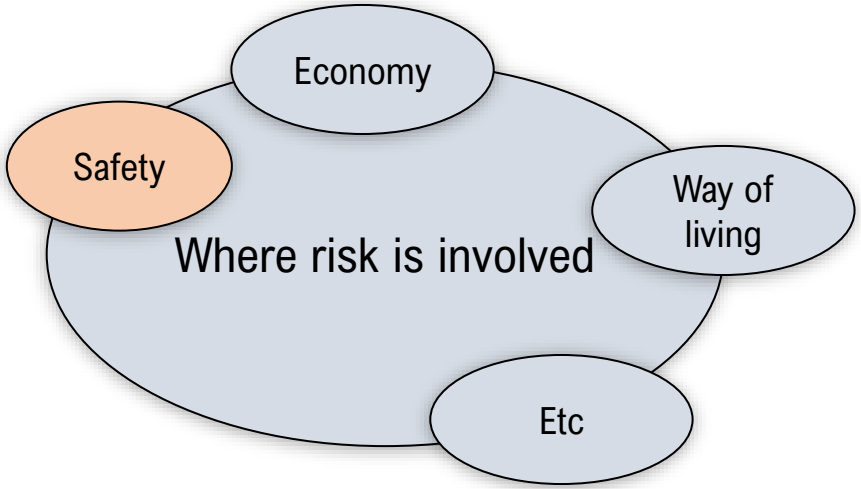
Feil: (eng: Fault)

- Tilstanden der funksjonen har opphørt å fungere

Sikkerhet vs risiko

Sikkerhet (eng: safety):

- Å være beskyttet fra å bli utsatt for uakseptabel risiko («freedom from unacceptable risk») av ikke-villede handlinger og tilfeldige hendelser.
- Knyttet til risiko for skade på personer, miljø eller samfunnskritiske verdier.
- **Safety skilles klart** fra **security** på engelsk, da security har med skade påført av villede handlinger
- På norsk har vi bare ett begrep (sikkerhet) og betydningen må forstås utfra kontekst.



Risiko:
En måte å uttrykke eller avdekke utsatthet for noe uønsket, som skade.

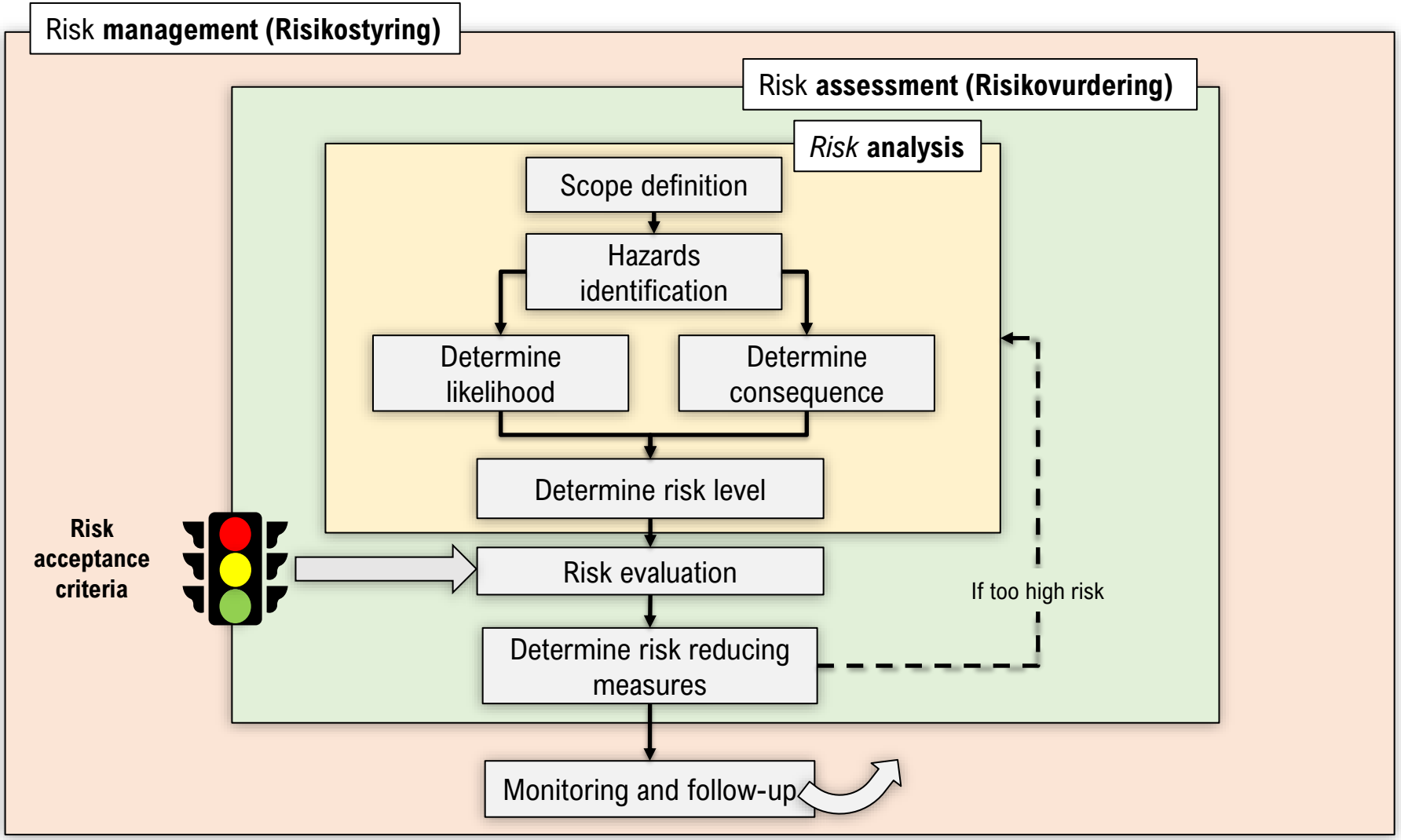
Tradisjonelt definert via å besvare tre spørsmål:

- Hva kan gå galt?
- Hvor sannsynlig er det (hvor ofte kan det skje)?
- Hva er konsekvensene?

Ri = Pi (eller F) x Ci
i: Scenario (hva kan gå galt)
Pi (alternativt Fi): Sannsynlighet eller frevens for i
Ci: Et bestemt utfall eller aggregert for et utfallsrom

Det er viktig å vurdere hvor god innsikt/mulighet til å besvare spørsmålene, det vil si grad av usikkerhet. Dette er reflektert i ny definisjon av risiko.

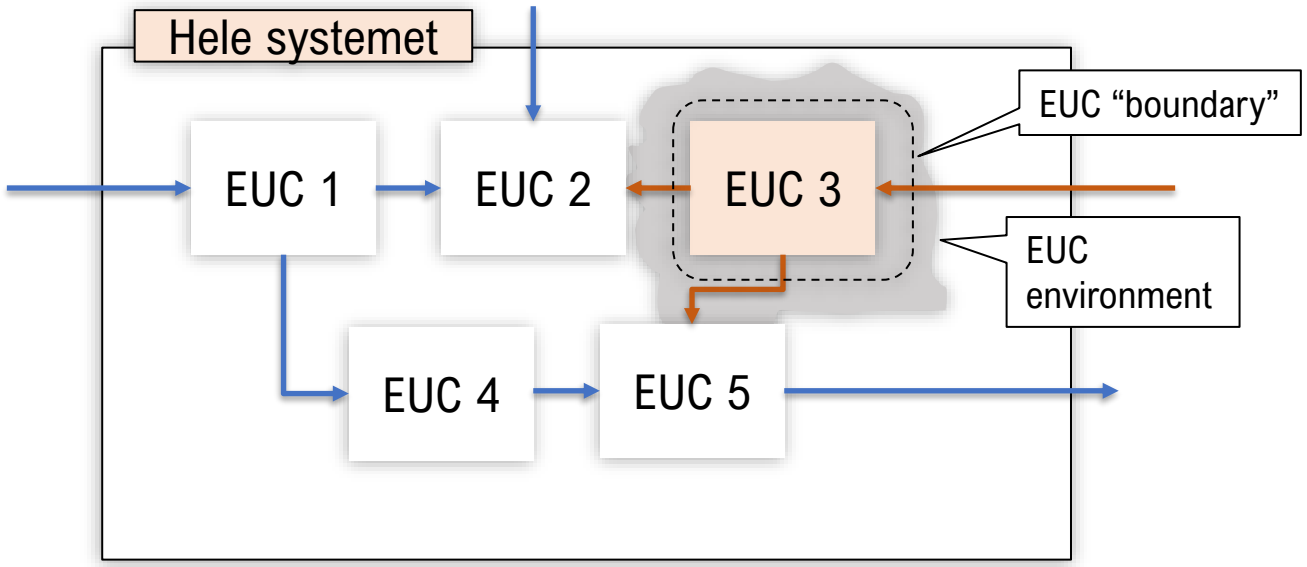
Risikoanalyse og mer til



En risikoanalyse starter med å definere EUC

Equipment under control (EUC):

- Et generelt begrep brukt for **et avgrenset system** som blir gjenstand for en risikoanalyse
- Inkluderer et avgrenset område, en maskin, et utstyr, et prosessavsnitt Brukes for å avgrense risikoanalysen og gjøre «modularisert»



Ikke for stort (omfang), men heller ikke for lite…

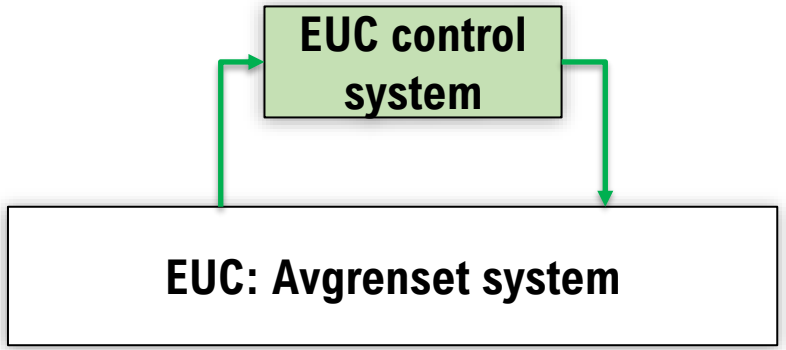
EUC control system

- EUC control system:

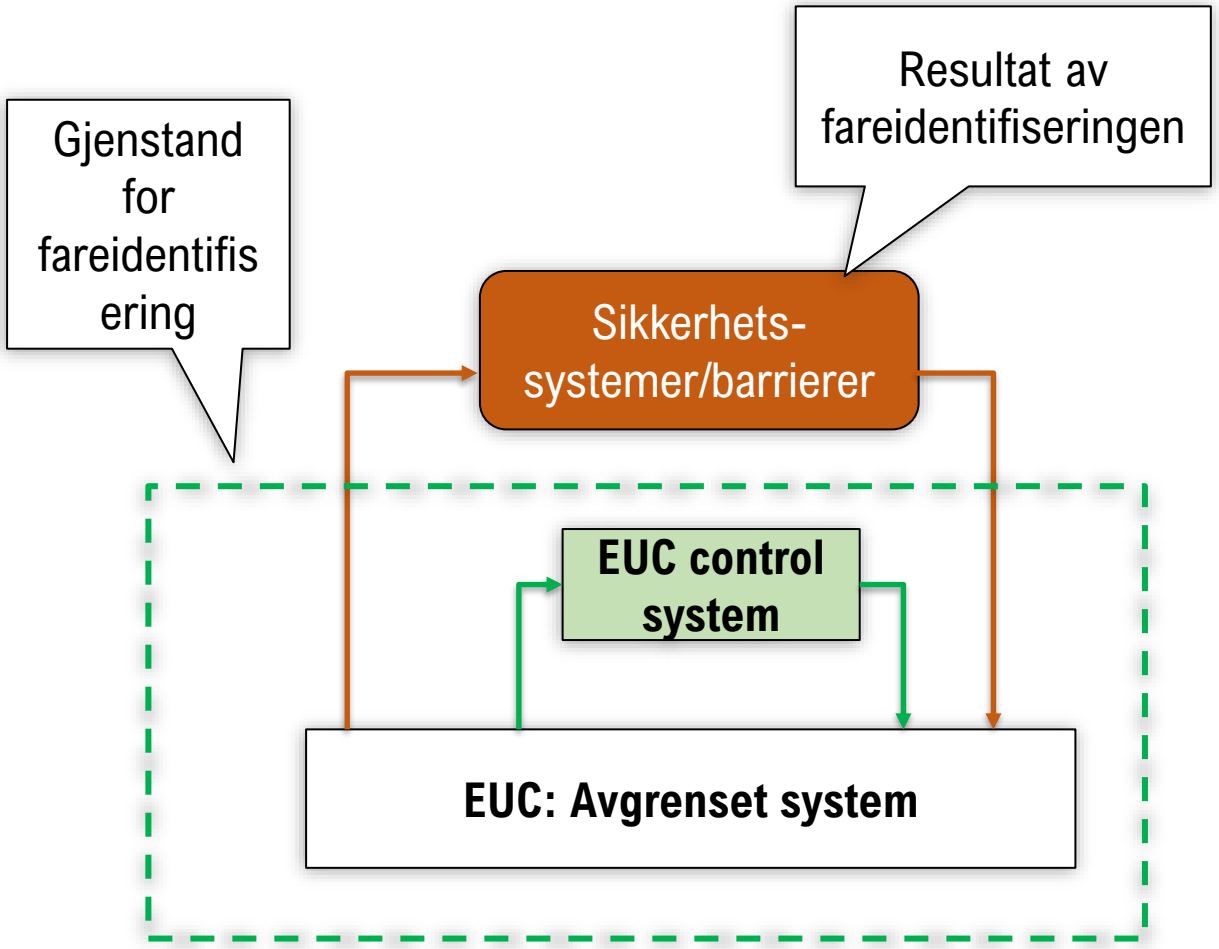
  Utstyr og programmerte funksjoner som inngår i å håndtere hendelser under normal drift (Eksempel: Prosessreguleringssystem)

- Regnes IKKE som en del av, men kommer i tillegg til, **EUC**, til tross for at mye utstyr er plassert innenfor EUC

- Kan være opphav til farer og hendelser som risikovurderes



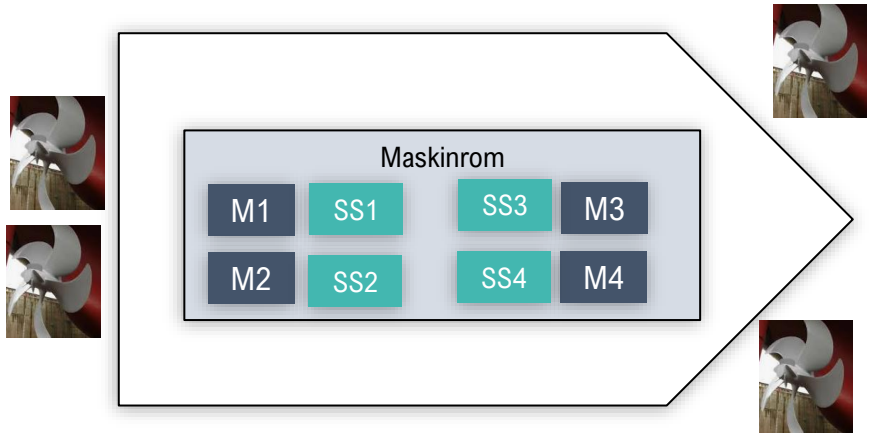
Hva som kommer i tillegg til EUC



- Fareidentifisering tar utgangspunkt i farer og hendelser innenfor EUC, også de som trigges av feil i EUC control system
- Sikkerhetssystemer (eller sikkerhetsbarrierer) avdekkes *som følge av* fareidentifisieringen og kommer også i tillegg (og er ikke en del av EUC) selv om utstyr er installert innenfor.
- Dersom et EUC control system også utfører sikkerhetsfunksjoner holdes disse utenfor fareidentifisieringen.

Eksempel: Valg av EUC avhenger litt av formålet

Inspirert av Viking Sky (nesten) ulykken



Hva er et bra valgt EUC dersom en skulle vurdere:

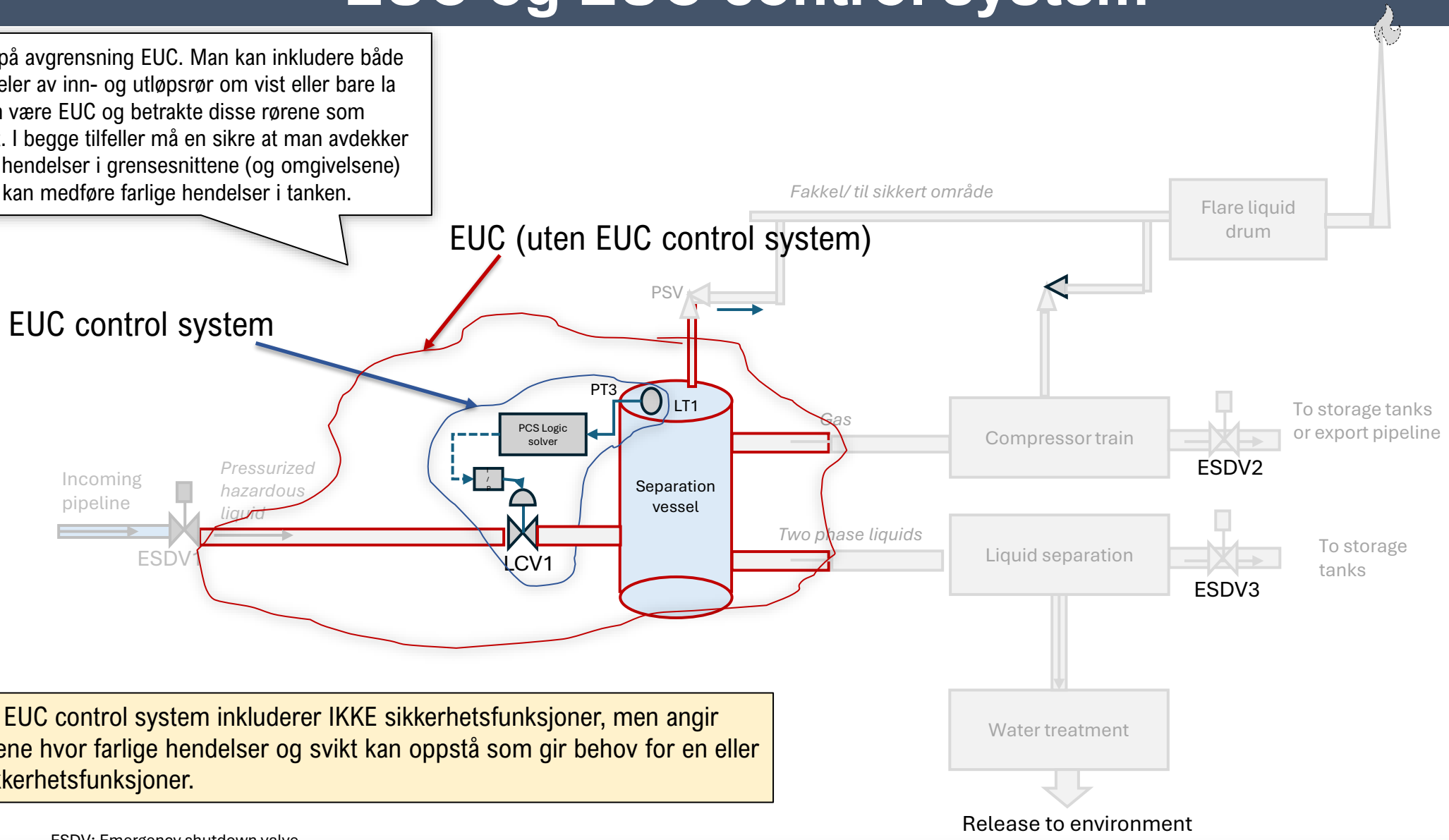
- Maskinbeskyttelse av individuelle motorer
- Mulighet til å opprettholde motorkraft på skip
- Brann i maskinrom

Ulike fokus for analysen vil kunne bidra til ulike valg om EUC

M: Motor, SS: Smøresystem

EUC og EUC control system

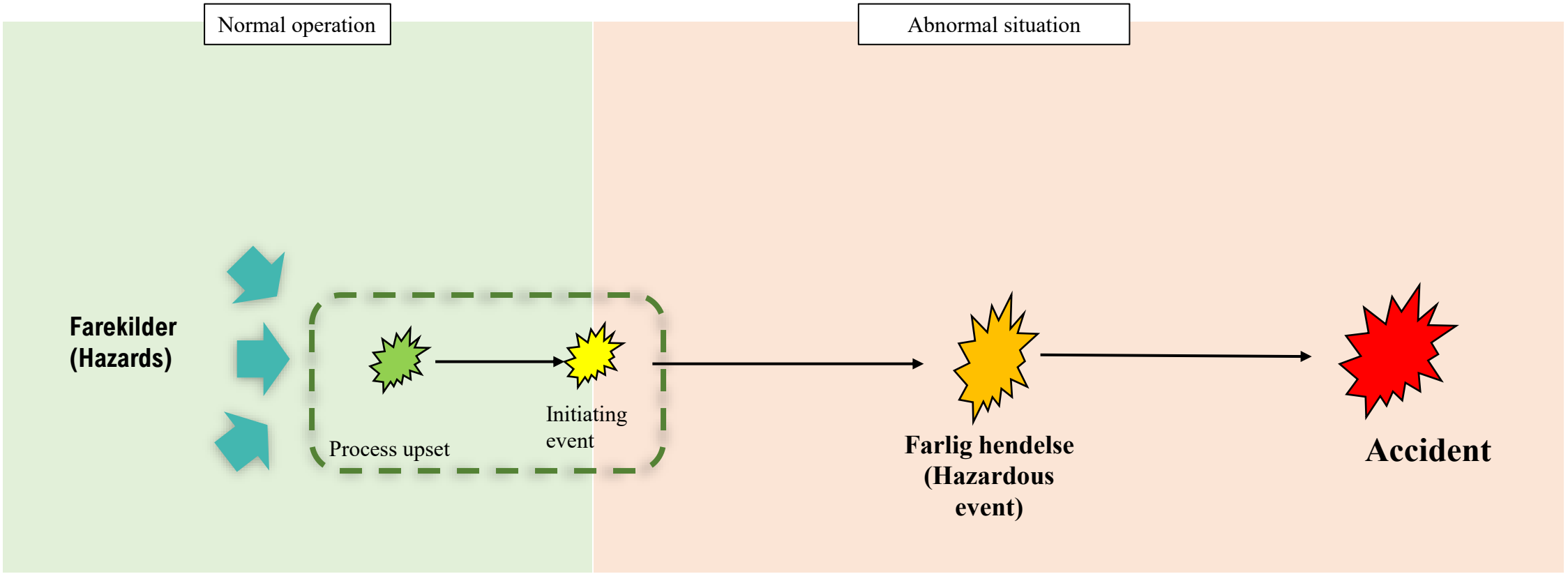
Eksempel på avgrensning EUC. Man kan inkludere både tank og deler av inn- og utløpsrør om vist eller bare la tanken være EUC og betrakte disse rørene som grensesnitt. I begge tilfeller må en sikre at man avdekker årsaker til hendelser i grensesnittene (og omgivelsene) som kan medføre farlige hendelser i tanken.



EUC og EUC control system inkluderer IKKE sikkerhetsfunksjoner, men angir systemene hvor farlige hendelser og svikt kan oppstå som gir behov for en eller flere sikkerhetsfunksjoner.

ESDV: Emergency shutdown valve

Hva skaper en ulykke i forbindelse med et EUC?



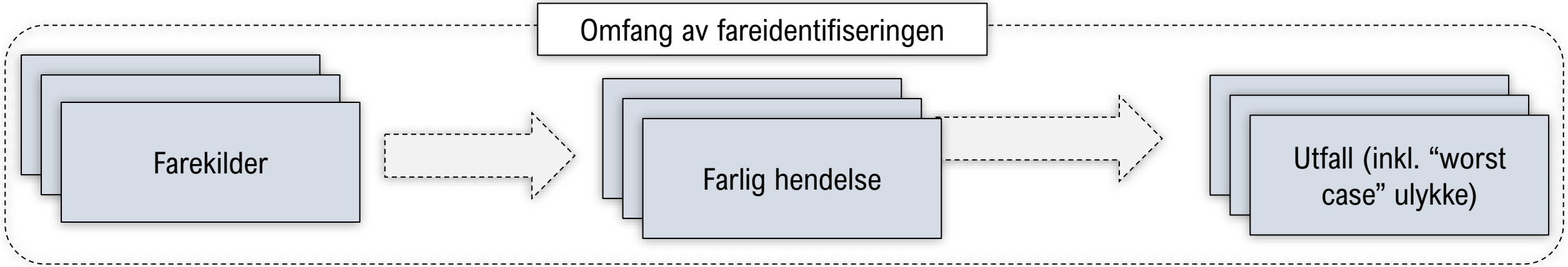
Operasjonsvinduet til kontrollsystemet (process control)

Fareidentifisering

Sentrale begrep:

- **Fare ("Hazard"):** Kilde til skade (egenskaper ved systemet, drifts- og miljømessige forhold, hendelser...)
- **Farlig hendelse ("Hazardous event"):** Første *betydelige* hendelse som, hvis den ikke stoppes, kan utvikle seg til en ulykke
- **Utfall:** Mulige konsekvens*er* av den farlige hendelsen, gitt typen inngrep og forhold som påvirker hvert enkelt utfall
  - **Utfallsrom:** En liste av mulige utfall for en spesifikk farlig hendelse
  - **Ulykke ("accident"):** "worst case" utfall som fører til død, skader, tap av system eller forsyning, eller miljøskade (hvis det er mindre alvorlig, kan vi kalle det uønsket hendelse)

En fareidentifisering vil i tillegg til å identifisere farer og farlige hendelser også identifisere mulige utfall og alvorlighet av disse. Utføres ofte i arbeidsmøter (workshops) som samler personer med kunnskap

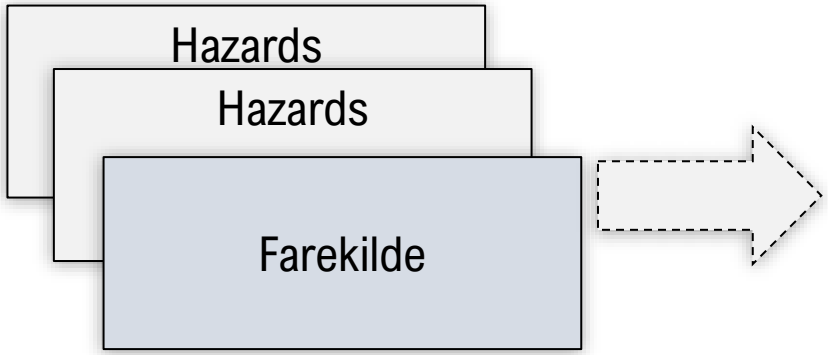


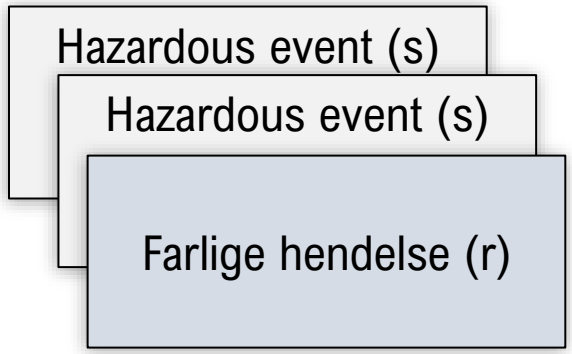
Flere ulike metoder for fareidentifisering

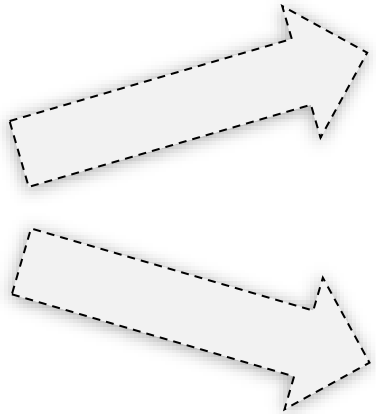
Metodeeksempler	Kommentar	Dekkes i
Feilmode, Effect, and Criticality Analysis (FMECA /FMEA)	Primært brukt for å identifisere farer og feil forbundet med enkeltutstyr, men kan tilpasses andre anvendelser (software FMECA, logistic FMECA,…)	TTK 4175, TTK32
Hazards and Operability Study (HAZOP)	Primært utviklet for fareidentifisering i prosessanlegg (delsystemer), men kan tilpasses andre anvendelser (control HAZOP).	TTK 4175 (delvis)
Hazards Identification – HAZID	Ikke en spesifikk metode, men omfatter fareidentifisering der man ofte baserer seg på sjekklister. Sjekkliste-basert fareidentifisering der sjekklister er tilpasset kontekst og fokus for analyse	TTK2
Systems Theoretic Process Analysis (STPA)	Systemfokus – spesielt utviklet for software intensive systemer og systemer der ulike aktører (og kontrollere) samhandler	TTK32

TTK2

Fareidentifisering







- Ingen
- Andre utfall, ranger etter alvorlighet
- Andre utfall, ranger etter alvorlighet
- Ulykke(r) (“worst case”) (Accidents)

Type farekilde	Eksempler
Prosessavvik	Årsaker knyttet til for eksempel: • For høyt/lavt nivå, trykk, flow, temperatur • Feil (i betydning ikke tatt hensyn til valg av utstyr og kapasitet) i komposisjon av prosessmedium
Mekaniske farer	• Fallende gjenstander • Roterende eller bevegelige deler • Skarpe deler og utstyr • Varme overflater
Elektriske farer	• Strømbrudd • Tap av kommunikasjon • Jordingsfeil
Design og utformingsrelaterte farer	• Uhensiktsmessig /feil plassering av utstyr • Mangelfull beskyttelse av utstyr (fysisk, digitalt, avstand til annet utstyr) • Mangelfull eller feil installasjon • Underdimensjonert utstyr eller kapasiteter • Ikke hensyntatt ex-beskyttelseskrav
Eksterne forhold	• Brann • Værforhold (snø, is, lave temperaturer, høye temperaturer, fuktighet, vind,....) • Ekstern strømforsyning og digital infrastruktur (IKT, internett) • (Cyberangrep)
Menneske og organisatoriske faktorer	• Mangelfull opplæring/trening/kompetanse • Mangelfull prosedyrer • Mangelfull dokumentasjon (ikke oppdatert) • Feiloperering (utilsiktet) • Mangelfull allokering av ressurser, roller, ansvar

Bruker ofte **sjekkliste** for å stimulere til å tenke bredest mulig

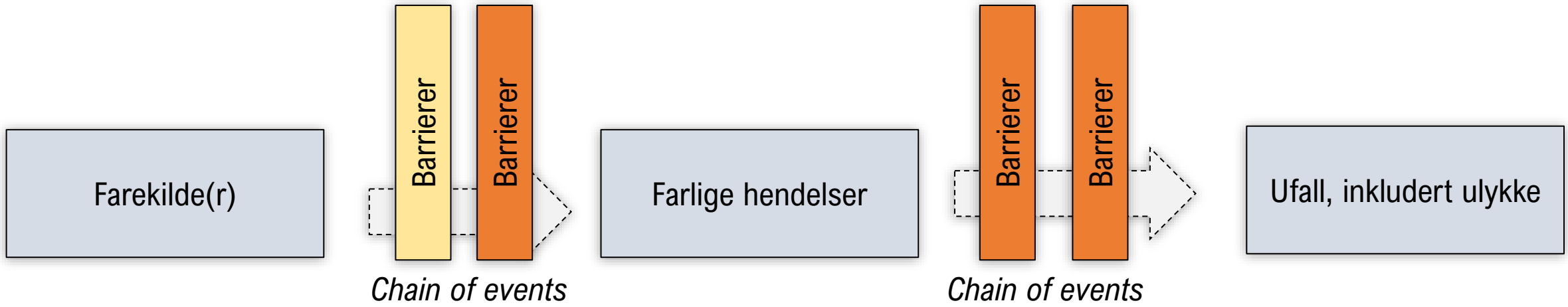
Ved analyse av dokumentasjon, driftserfaring og bruk av deltagernes kunnskap avdekkes mulige farlige hendelser som følger tap av kontroll med farekilder

Bruker ofte **kategorisering** for å skille alvorlighet av utfall

Utfall	Eksempler	Konsekvens for menneskeliv	Konsekvens miljø	Alvorlighets-kategori (eksempler)
Ulykke (eller storulykke)	Worst case utfall, slik som eksplosjon og brann som eskalerer og berører hele anlegget	Potensielt mange dødsfall	Irreversibel miljøskade, eller skade som tar lang til å gjenopprette	Katastrofalt
«Mellomutfall»	Avgrenset eksplosjon og brann	Ingen eller få dødsfall, kritiske skader	Kortvarig utslipp med mindre konsekvenser	Alvorlig til kritisk, avhengig av hvor mye skadeomfanget begrenses og isoleres
Ingen	Utvikling av den farlige hendelsen stanses eller håndteres så raskt at normaltilstand gjenopprettes etter kort tid	Ingen	Ingen eller veldig små	Neglisjerbar

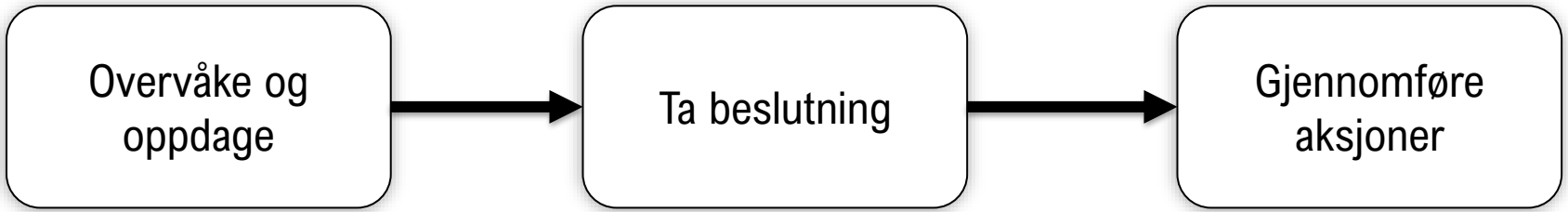
Roller til sikkerhetssystemer (også omtalt som barrierer)

- Gripe inn og enten stanse utvikling av eller begrense utfallet av en farlig hendelse
- Kan være tekniske eller operasjonelle:
  - Tekniske: Fysiske, mekaniske, instrumenterte
  - Operasjonelle: Menneskeinvolverte aksjoner som ikke er tilfeldige, men følger prosedyrer



Sikkerhetsbarrierer Andre barrierer (eksempelvis reguleringssystemet)

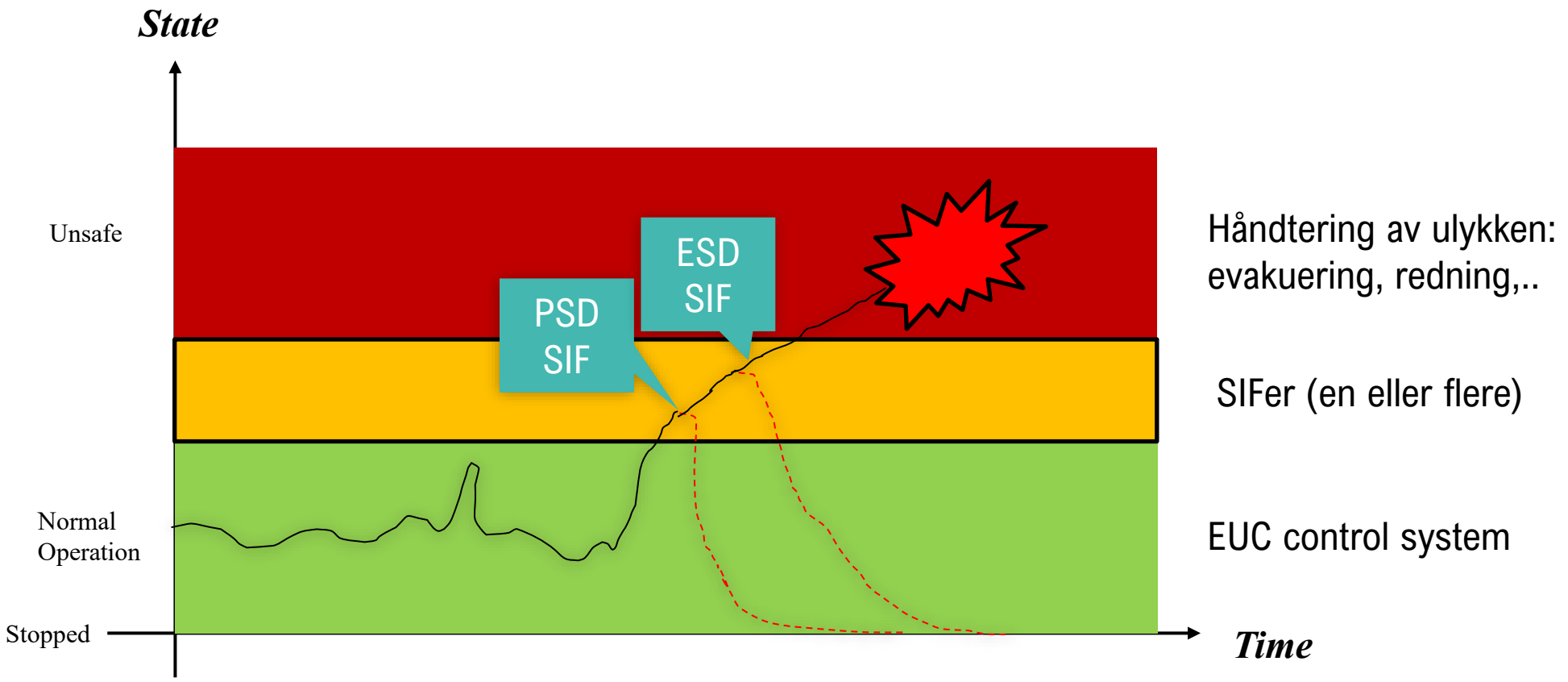
Funksjoner forbundet til *aktiverte* barrierer



Barrierer må bidra til **sikker tilstand** for anlegget eller isolert for et EUC:

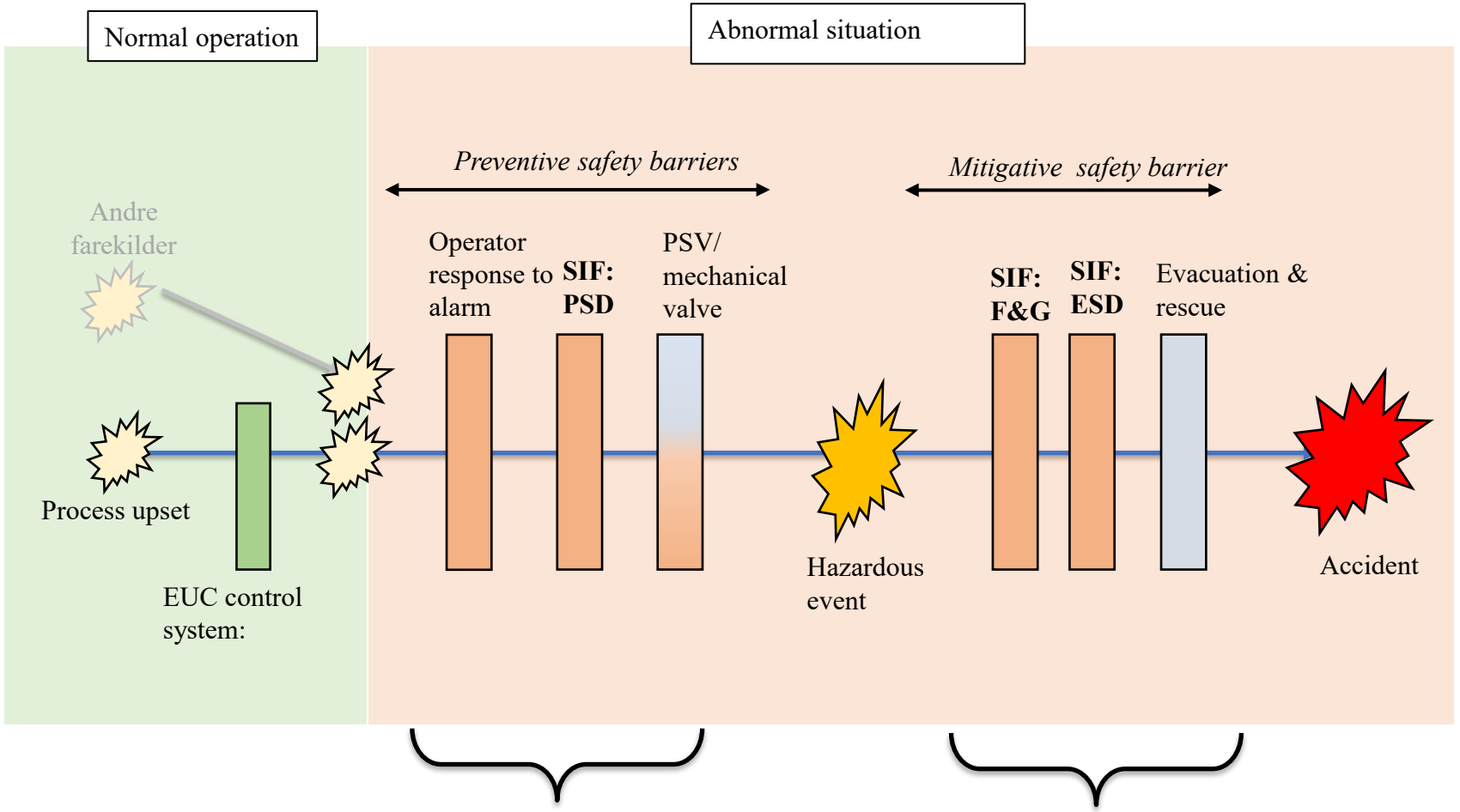
- For mange fabrikker betyr det ofte å stenge ned (stanse produksjonen)
- Men det kan også være å stenge ned først etter at en kjemisk reaksjon er kjørt ferdig
- Eller det kan være å opprettholde kjølevannstilførsel (kjernekraft)
- Eller å opprettholde motordrift tilstrekkelig til å lande (fly) eller komme seg til kai (skip)
- Osv.

Hvordan oppnå eller bevare sikker tilstand



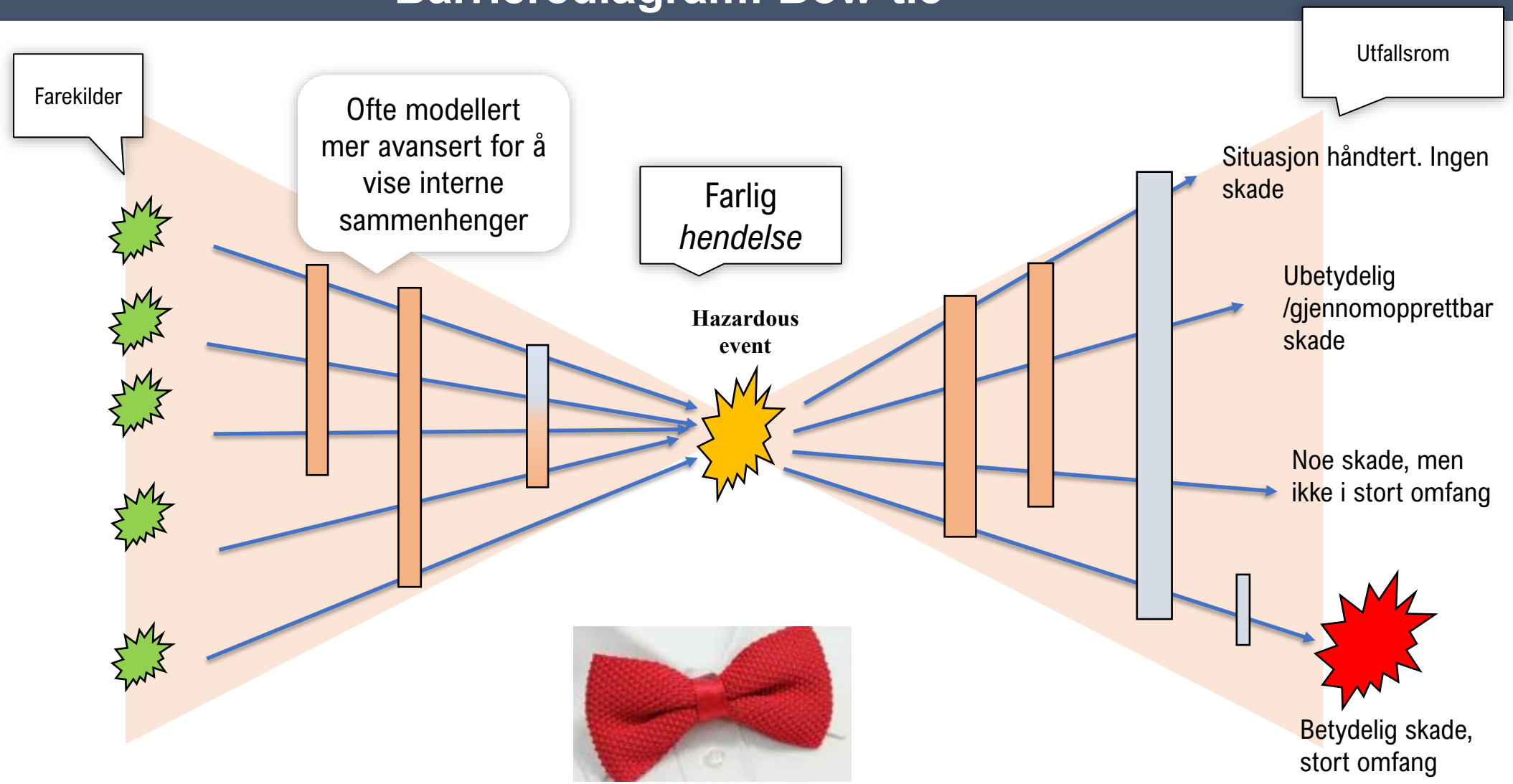
PSD: Process shutdown system, ESD: Emergency shutdown system

Barrierediagram: Barrieresti/løp



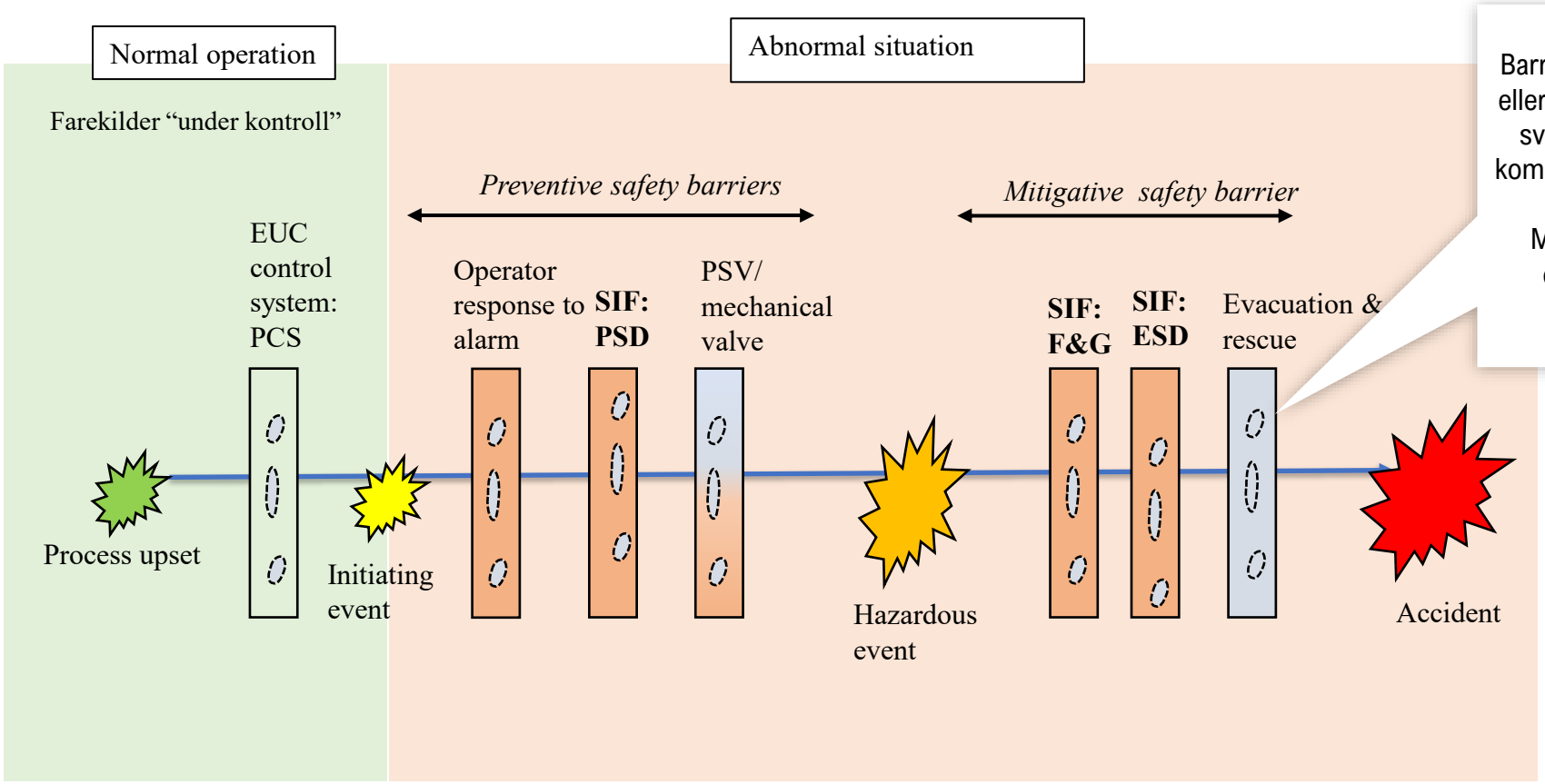
Hazards og intierende hendelser

Barrierediagram: Bow-tie



Denne måten å vise sammenhengen mellom årsaker og utfall av farlige hendelser kalles **Bowtie modellen**.

Barrieresti/løp tilpasset Sveitserostmodelen

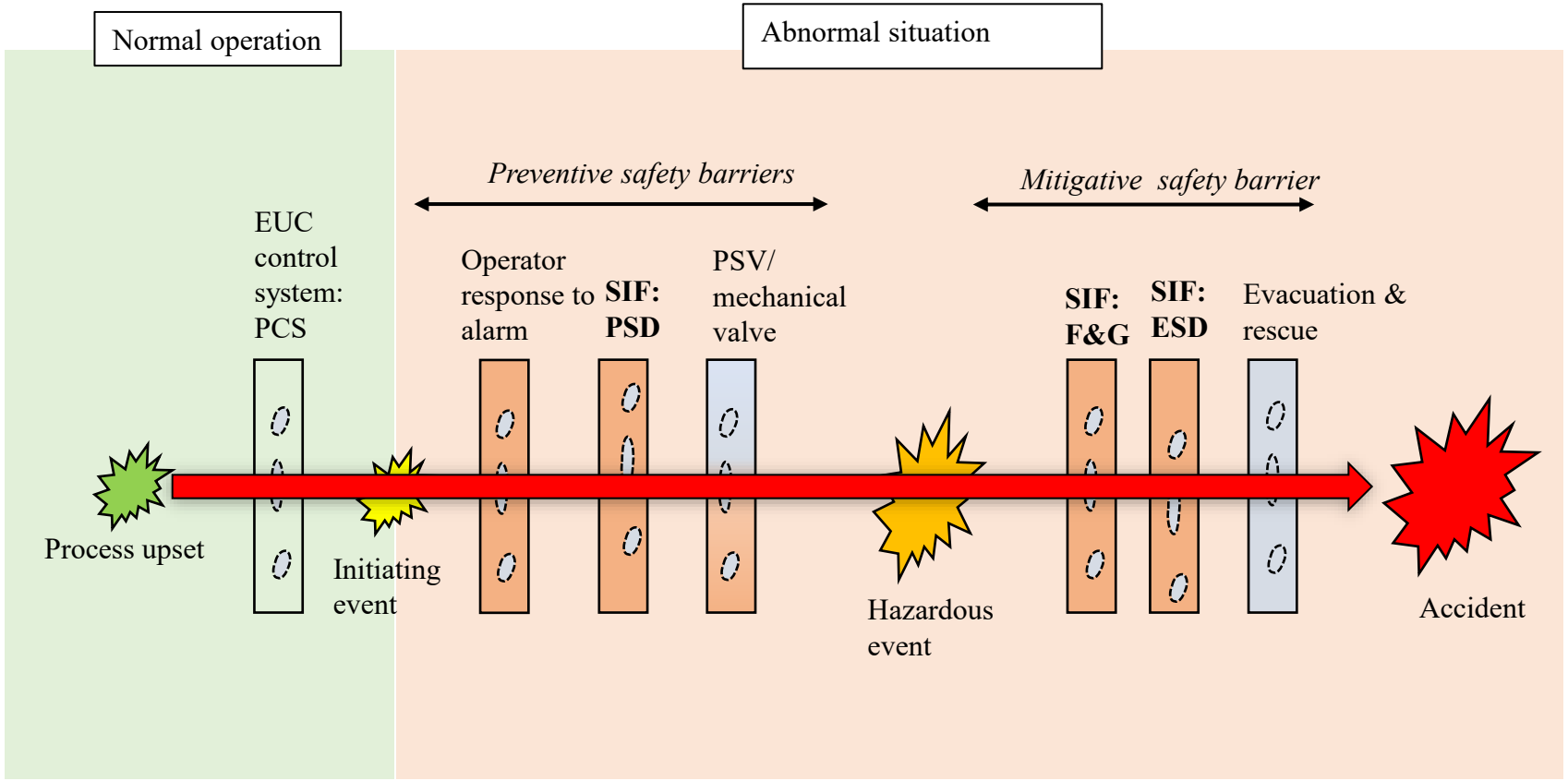


Barrierer kan ha **svekkelser** – enten tekniske eller organisatoriske – som gjør at barrierene svikter som resultat av tekniske feil eller i kombinasjon med menneskelig feilhandlinger.

Menneskelig feilhandlinger skyldes ofte organisatoriske forhold, ikke uvilje og overlegg!

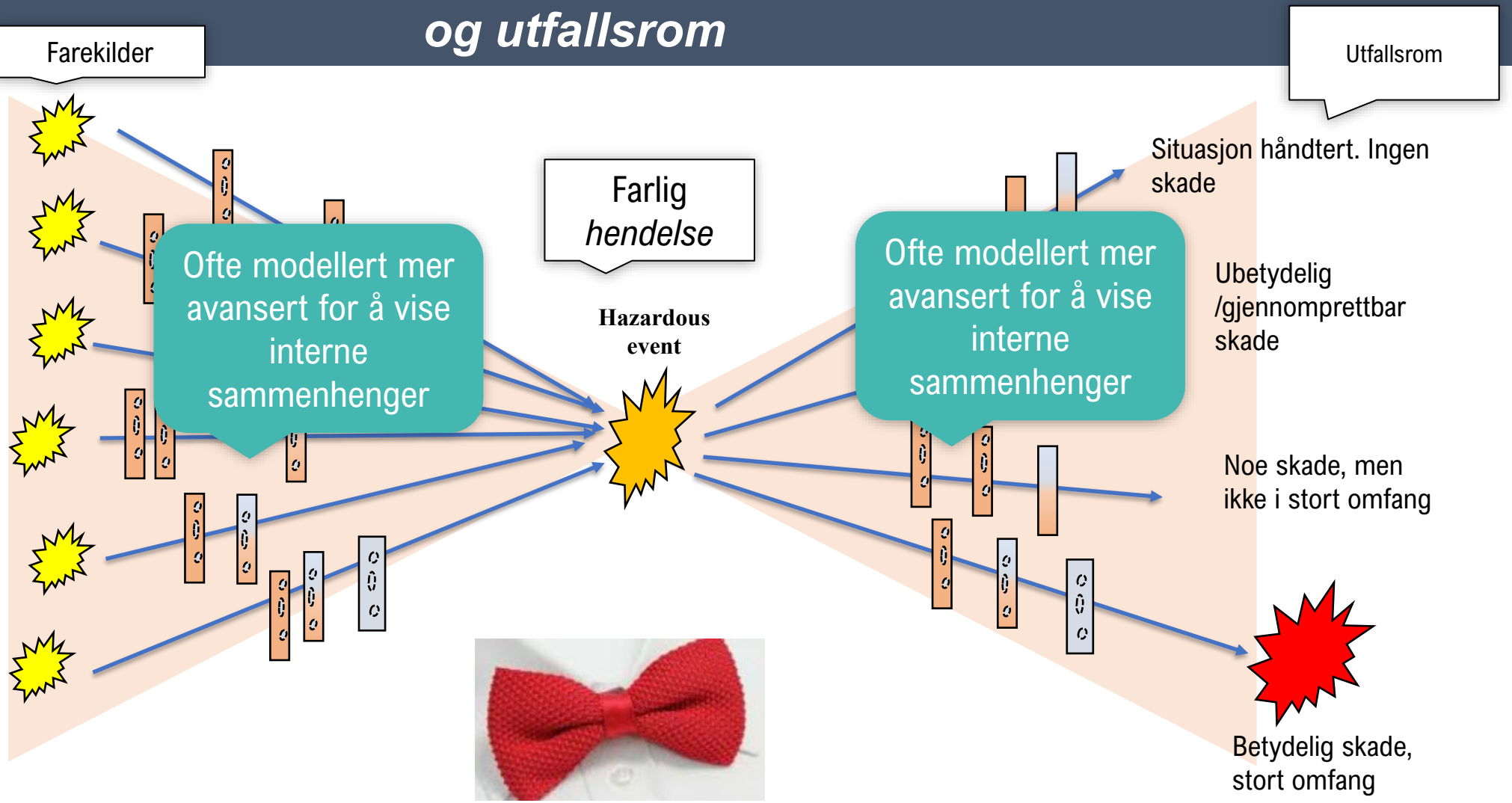
Ofte vist som **hull** i barrierene med referanse til James Reason (1997) «Swizz cheese model»

Ulykker skjer når «hullene» liner opp



Når større ulykker skjer, er det ofte et resultat av at mange ting har gått galt.

Barrieremodel «Bowtie» som forbinder en spesifikk farlig hendelse med farekilder og utfallsrom



Denne måten å vise sammenhengen mellom årsaker og utfall av farlige hendelser kalles **Bowtie modellen**.

Et (forenklet) eksempel

1373 personer om bord, mange eldre

Nærme land

Uvær og høy sjø

Lavt nivå smøreoljesystem gir motorstans

Algoritme prioriterer alltid maskin-beskyttelse, ikke situasjonen skipet er i

Båtens rulling og stamping gjør at smøreoljenivået går lavere enn settpunktet

Alle fire smøreolje-systemer opplever det samme

Strengere restriksjoner for å seile i uvær

Høyere min nivå smøreolje

Supervisory system som ikke tillater samtidig stans av ALLE motorer

Hazardous event

Restart motorer (fikk ikke til i situasjonen). Omstendig prosedyre)

Slippe anker (det gjorde man)

Evakuere personer om bord (storstilt aksjon)

Situasjonen (ble) håndtert. Ingen forulykket. Kanskje noen mindre personskader. Skip ikke skadet.

Noe fatale personskader, skip ok (kunne skjedd)

Noen fatale personskader, skap utsatt for mindre skader pga grunnstøting (kunne skjedd)

Skip kantrer. Mange forulykkede (kunne skjedd).

Motorstans alle fire motorer
Viking sky 2019 Hustadvika

Hvordan håndterer vi risiko for storulykker?

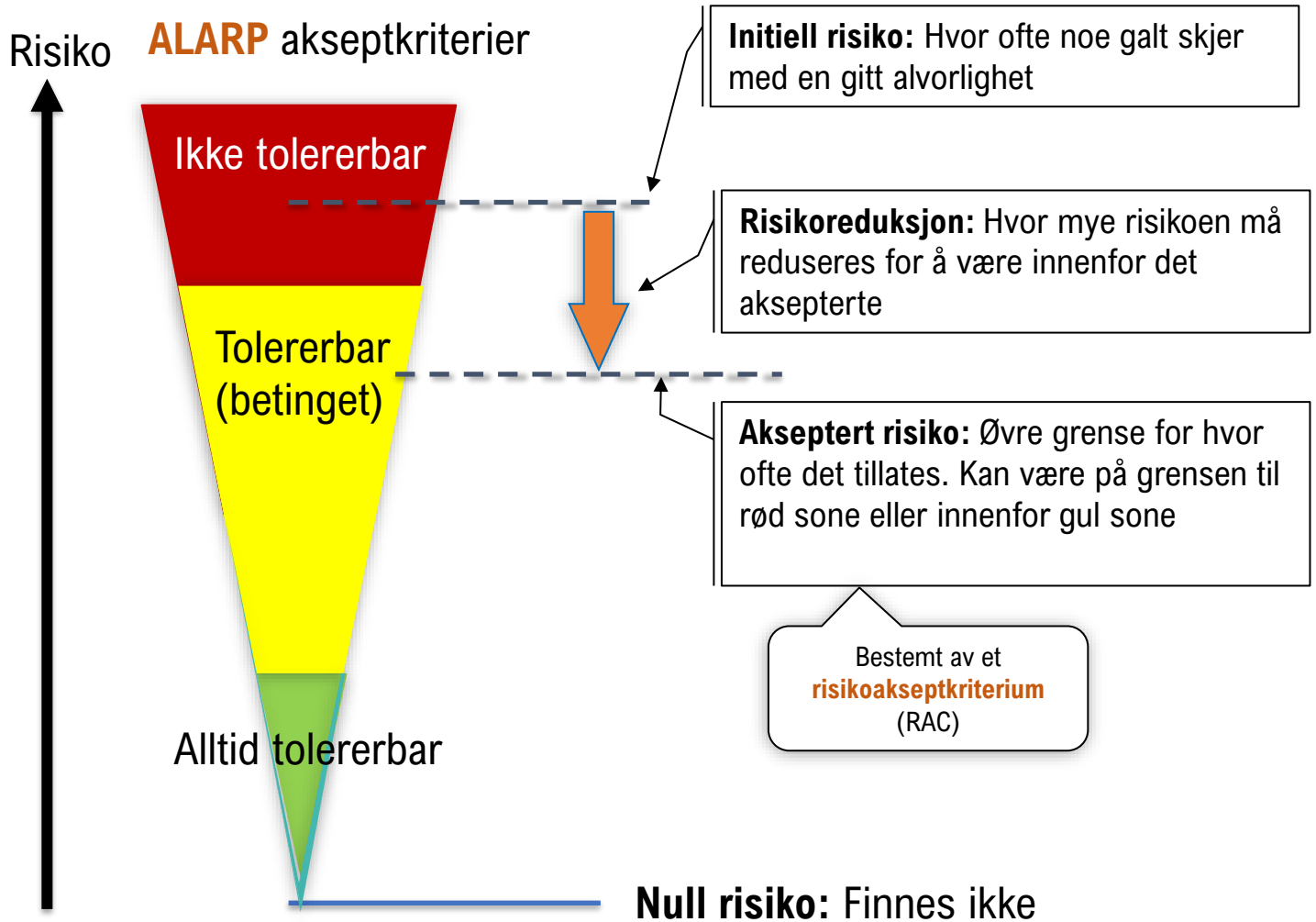
Først: Hva mener vi med risiko?

Risiko defineres ofte med følgende **tre spørsmål**:

- Hva kan gå galt?
- Hvor sannsynlig er det/ofte skjer det? (Fr or Pr)
- Hva er konsekvensene(C)

$$R=Fr \times C \text{ or } Pr \times C$$

Ny definisjon av risiko i ISO 31000 stiller krav til eksplisitt å adressere og dokumentere **usikkerhet** – hvor mye innsikt har jeg. Hvor mye erfaring har vi fra lignende situasjoner?

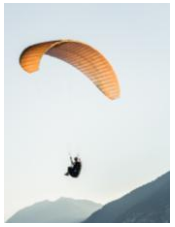


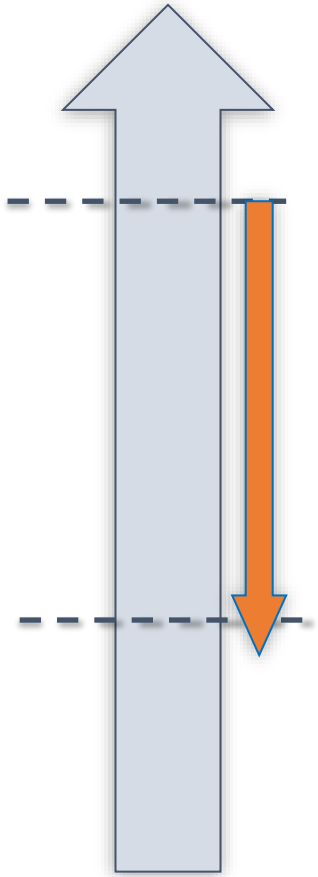
Fr: Frequency, Pr: Probability

ALARP: As low as reasonably practicable

Risikoreduksjon

Risiko for død (individ)

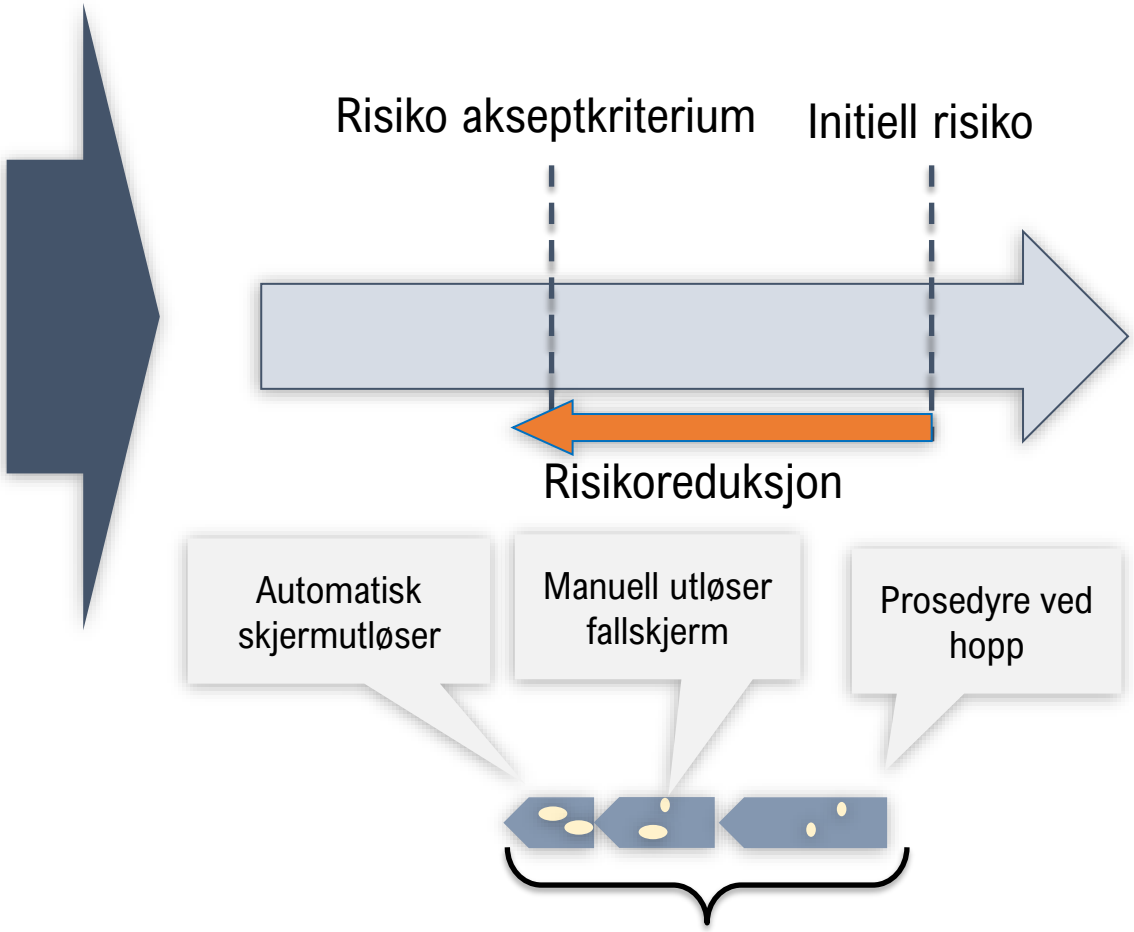




Kanskje 0.01/år hvis jeg driver med mye fallskjermhopping

Jeg må få til risikoreduksjon på i alle fall 100 ganger hvis jeg ikke vil utsettes for ekstra risiko pga fallskjermhoppingen

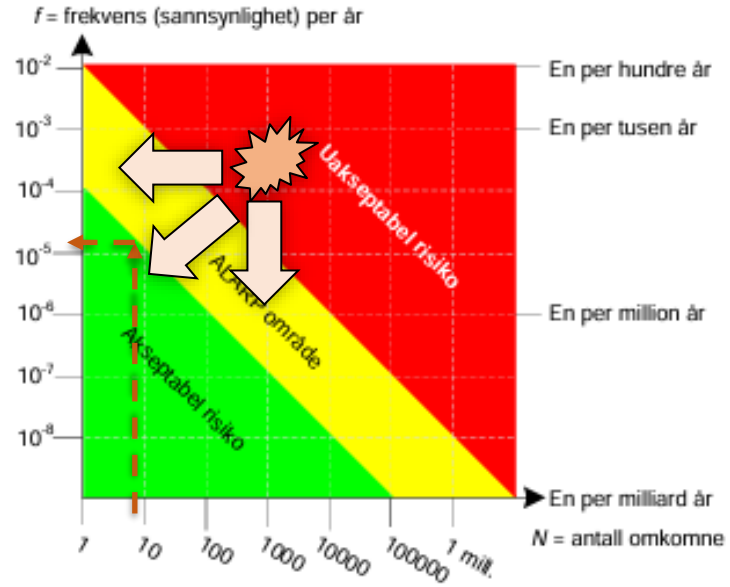
0.0001/år –individuell risiko som en utsettes for i et gjennomsnittsliv – og som vi av den grunn aksepterer



Hvor mye risikoreduksjon relevante sikkerhetsbarrierer må bidra med – samlet og hver for seg.

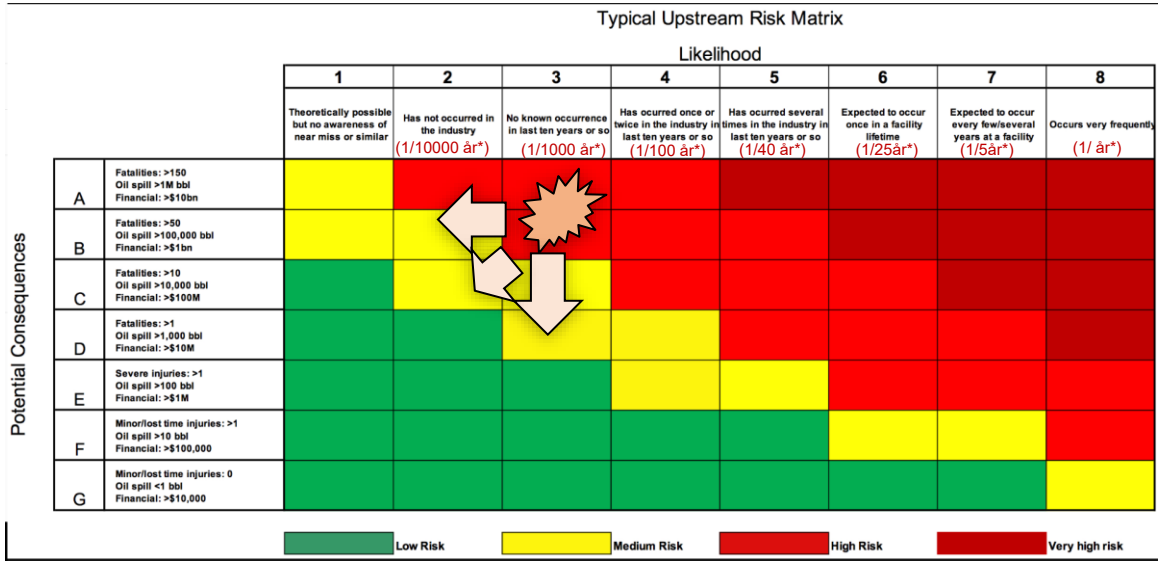
Fra initiell risiko til risikoreduksjon

F-N kurve brukt i caset



Figur 2 Lyse sine risikoakseptkriterier for samfunnsrisiko

Risikomatrise (en alternativ og ofte brukt måte å vise risiko og risikoaksept på)

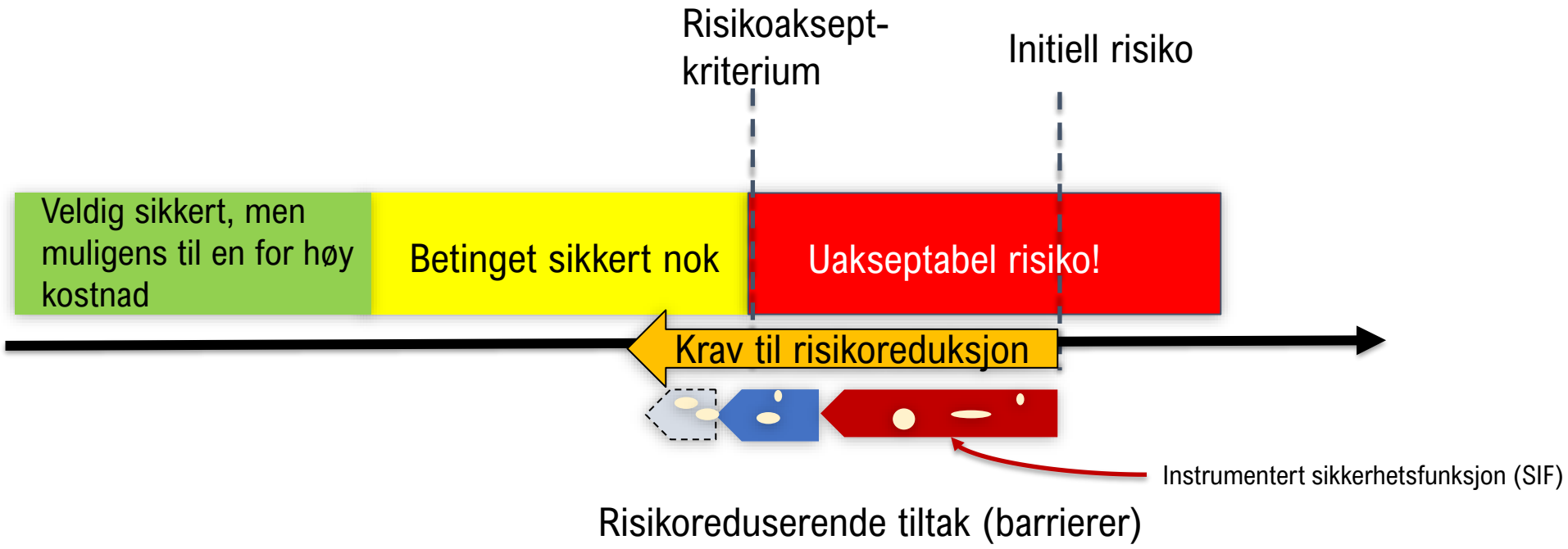


Slike matriser kalibreres ofte av selskapene
Og i forhold til type sektor/industri.

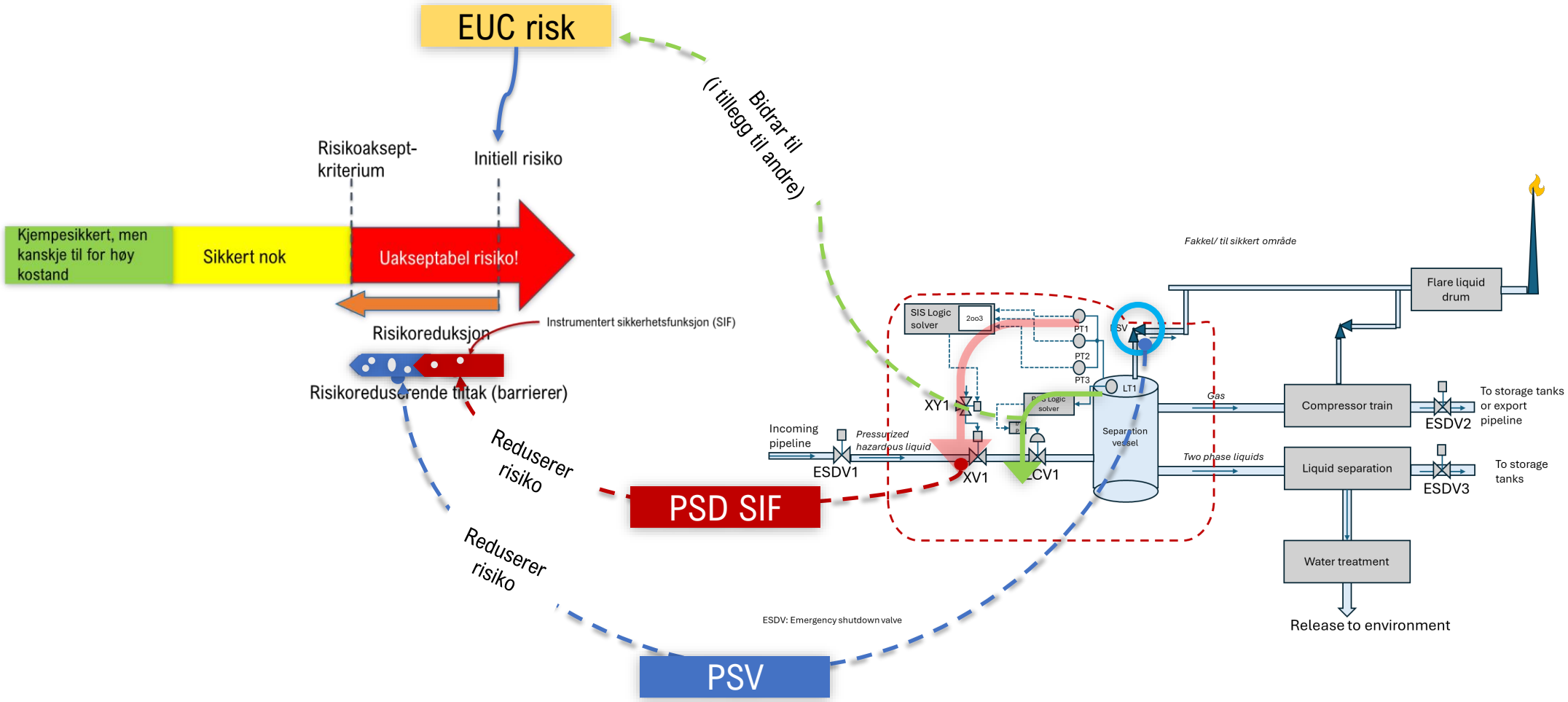
Functional safety (funksjonell sikkerhet)

Funksjonell sikkerhet (functional safety): Den sikkerheten (i praksis risikoreduksjonen) som oppnås der SIFer er en del av bidraget.

Standarder for funksjonell sikkerhet har primært fokus på hvordan man utfører stiller krav til, designer, verifiserer, samt overvåker, drifter og vedlikeholder SIS systemer. Å utføre pålitelighetsanalyser av SIFer inngår som en del av kravene.

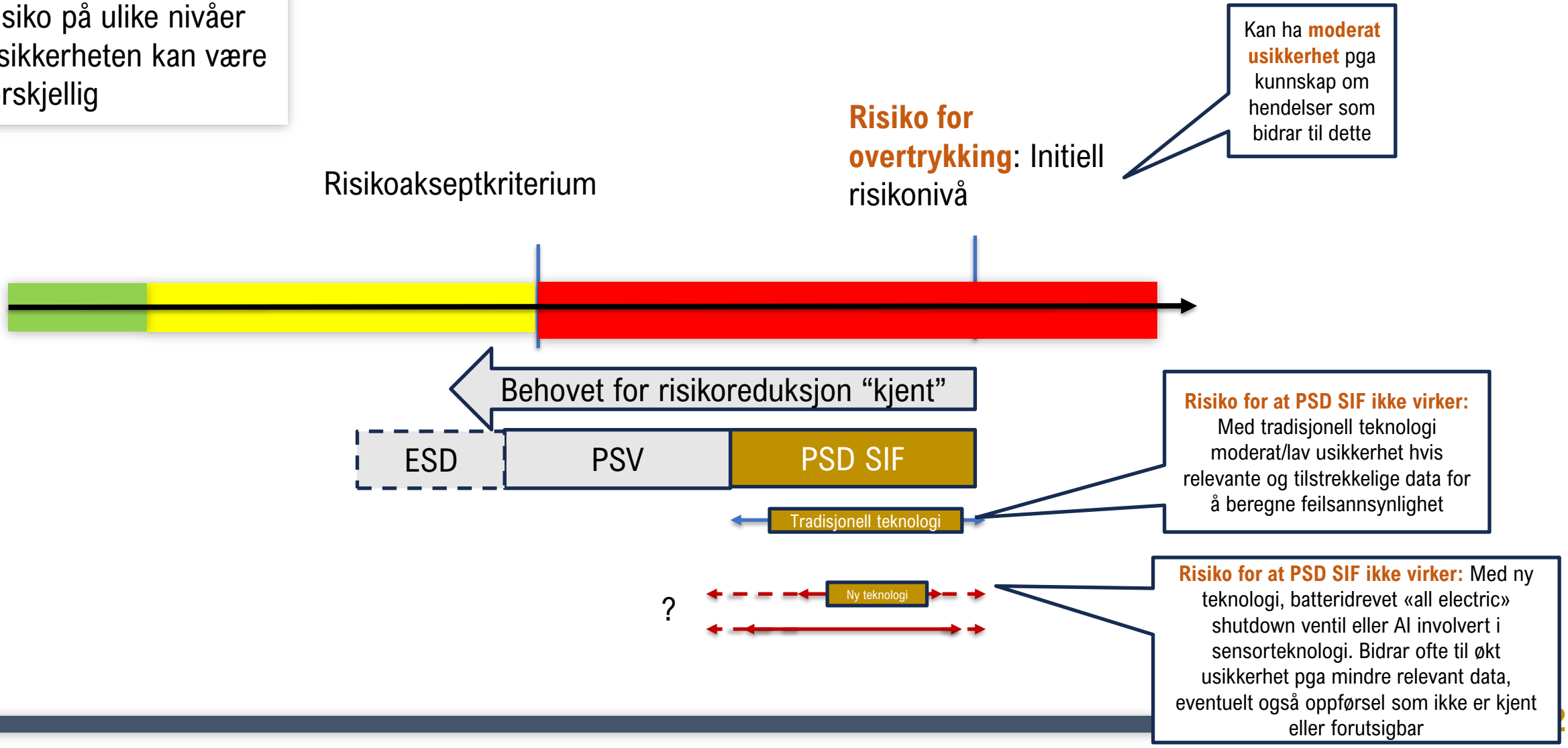


Hvordan sikkerhetsfunksjoner bidrar til risikoreduksjon



Risiko og usikkerhet

Stikkord:
- Risiko på ulike nivåer
- Usikkerheten kan være forskjellig

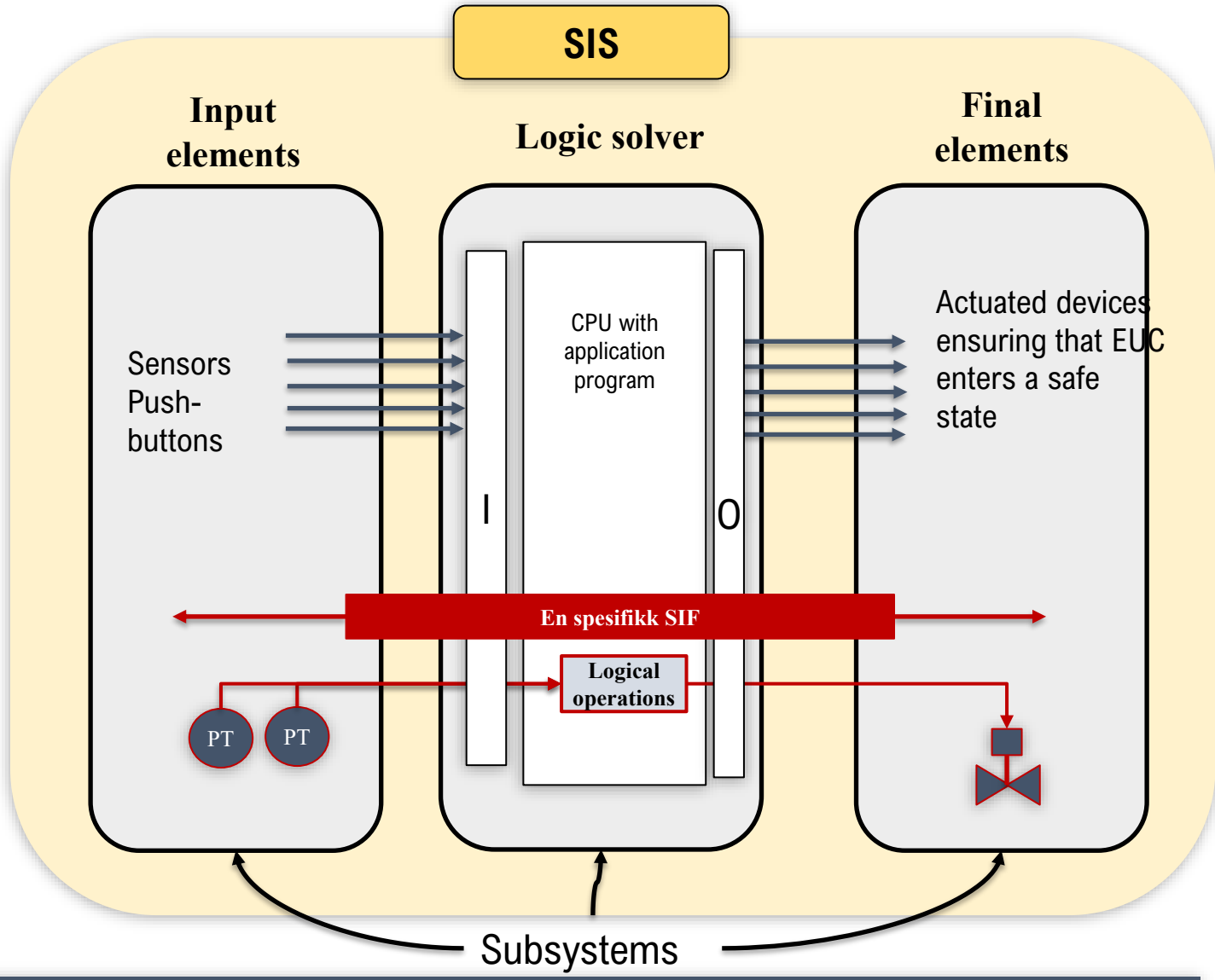


Safety instrumented *function* (SIF) og Safety instrumented *system* (SIS)

SIF: En sikkerhetsfunksjon som utføres med:

- En eller flere sensorer
- Logisk operasjon i kontroller
- Aktivert utstyr
- Kommunikasjon i mellom

SIS: Alt utstyr med hardware, software og kommunikasjon som er nødvendig for å utføre SIFer med «lignende oppgaver».

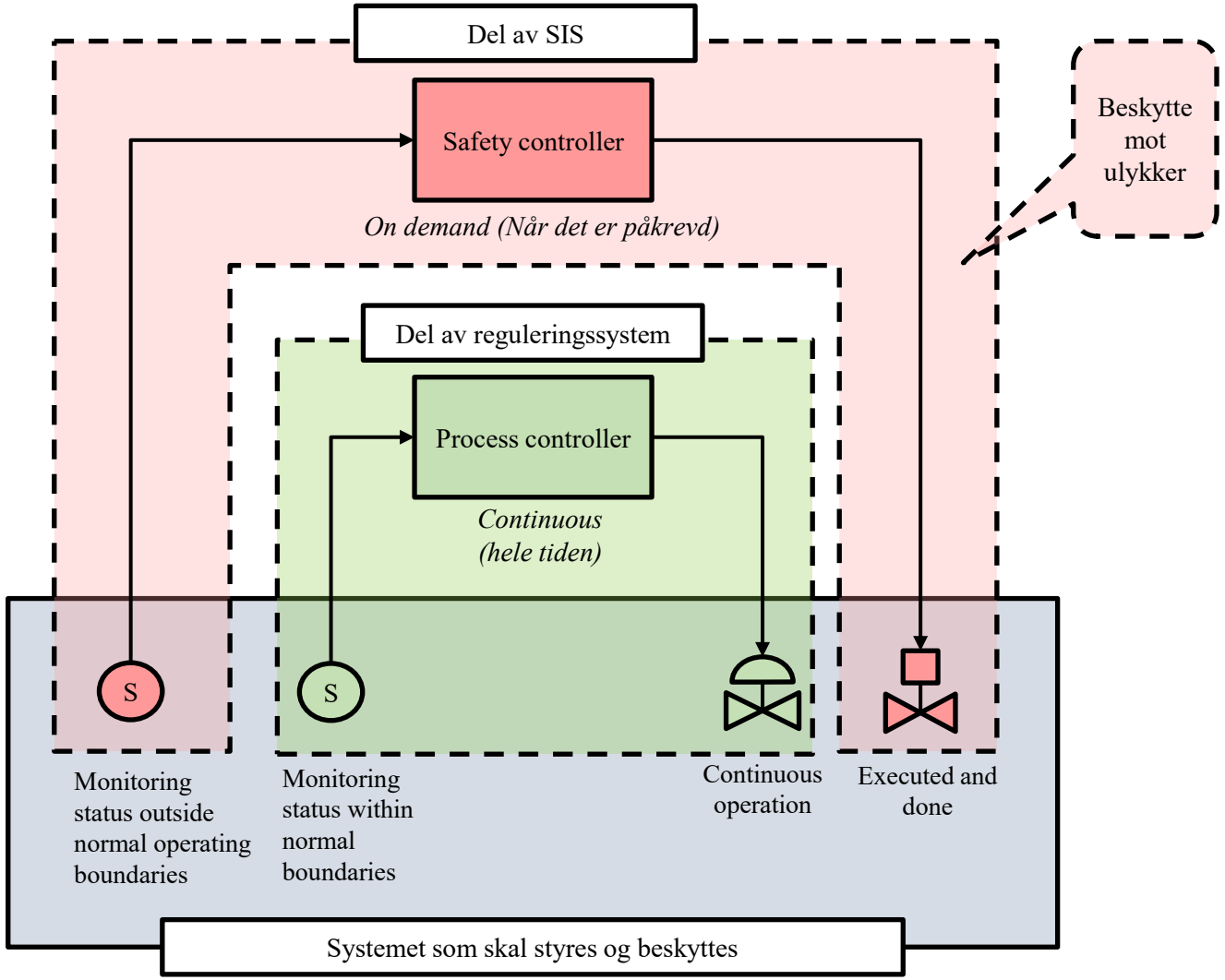


SIS i forhold til andre automatiserte systemer

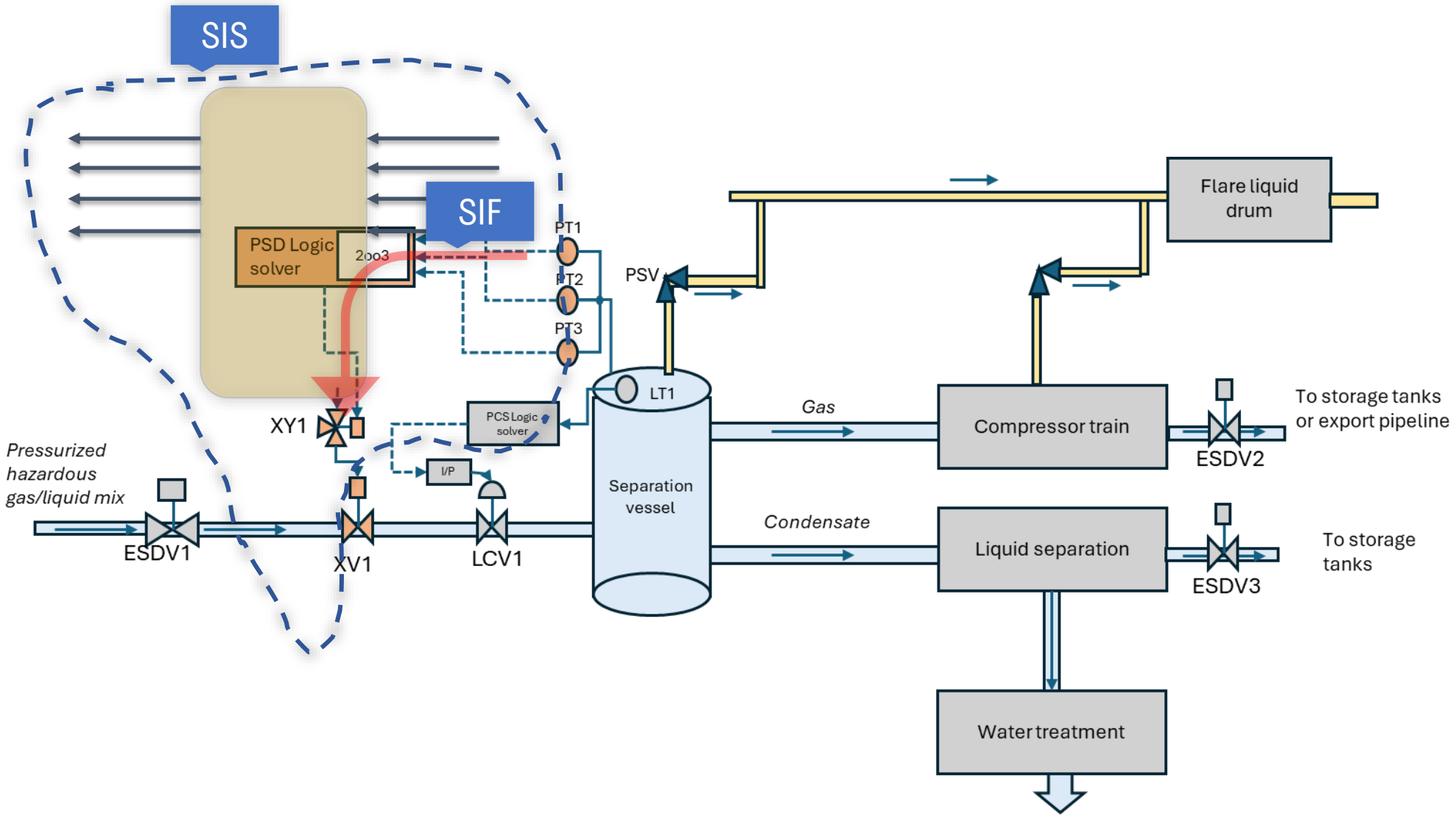
- **SIS:** Håndtere ulike **type oppgaver** i forbindelse med tilløp til ulykker og skadebegrensning.
- **Reguleringssystem:** Håndtere normal drift

- **SIS:** Tilstrekkelig **uavhengig** til å kunne ta over når kontrollsystemet feiler

- Ofte flere **SIS** for at også SIFer av en type er uavhengig av andre typer::
  - Prosessnedstengning (PSD)
  - Nødavstengning (ESD)
  - Brann- og gassdeteksjon (F&G)
  - Brannslukkingssystemer (Brannpumper, vanntåke,…)



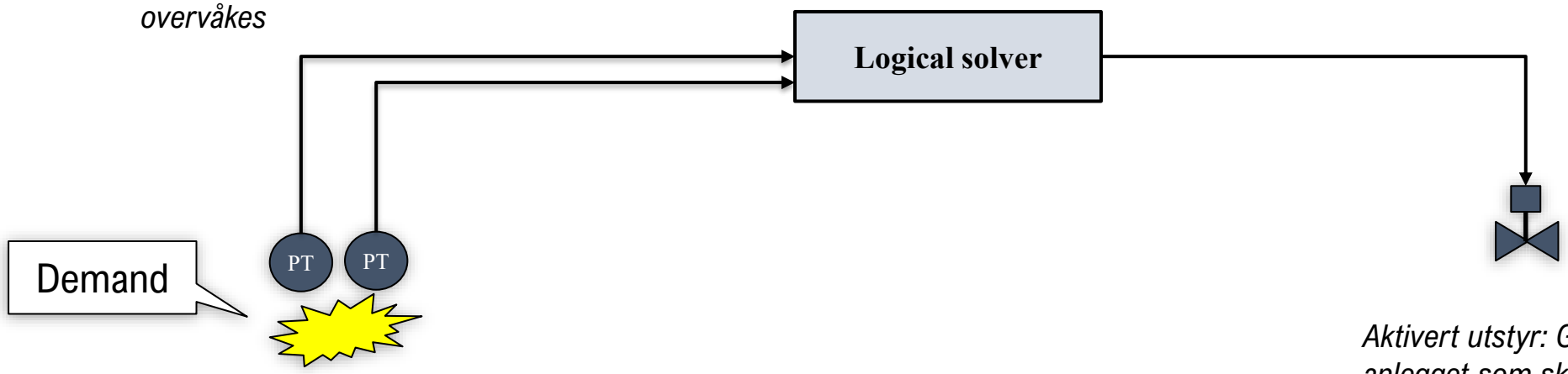
SIS vs SIF


SIS
SIF
PSD Logic solver
2oo3
PT1
PT2
PT3
PSV
Flare liquid drum
LT1
XY1
PCS Logic solver
I/P
Pressurized hazardous gas/liquid mix
ESDV1
XV1
LCV1
Separation vessel
Gas
Compressor train
ESDV2
To storage tanks or export pipeline
Condensate
Liquid separation
ESDV3
To storage tanks
Water treatment

Demand and mode of operation

Logikk:
- *Sammenligner måling med settpunkt*
- *Voterer målingene for å avgjøre om aksjon skal utføres*

Sensorer/trykkbrytere: Måler tilstand som skal overvåkes

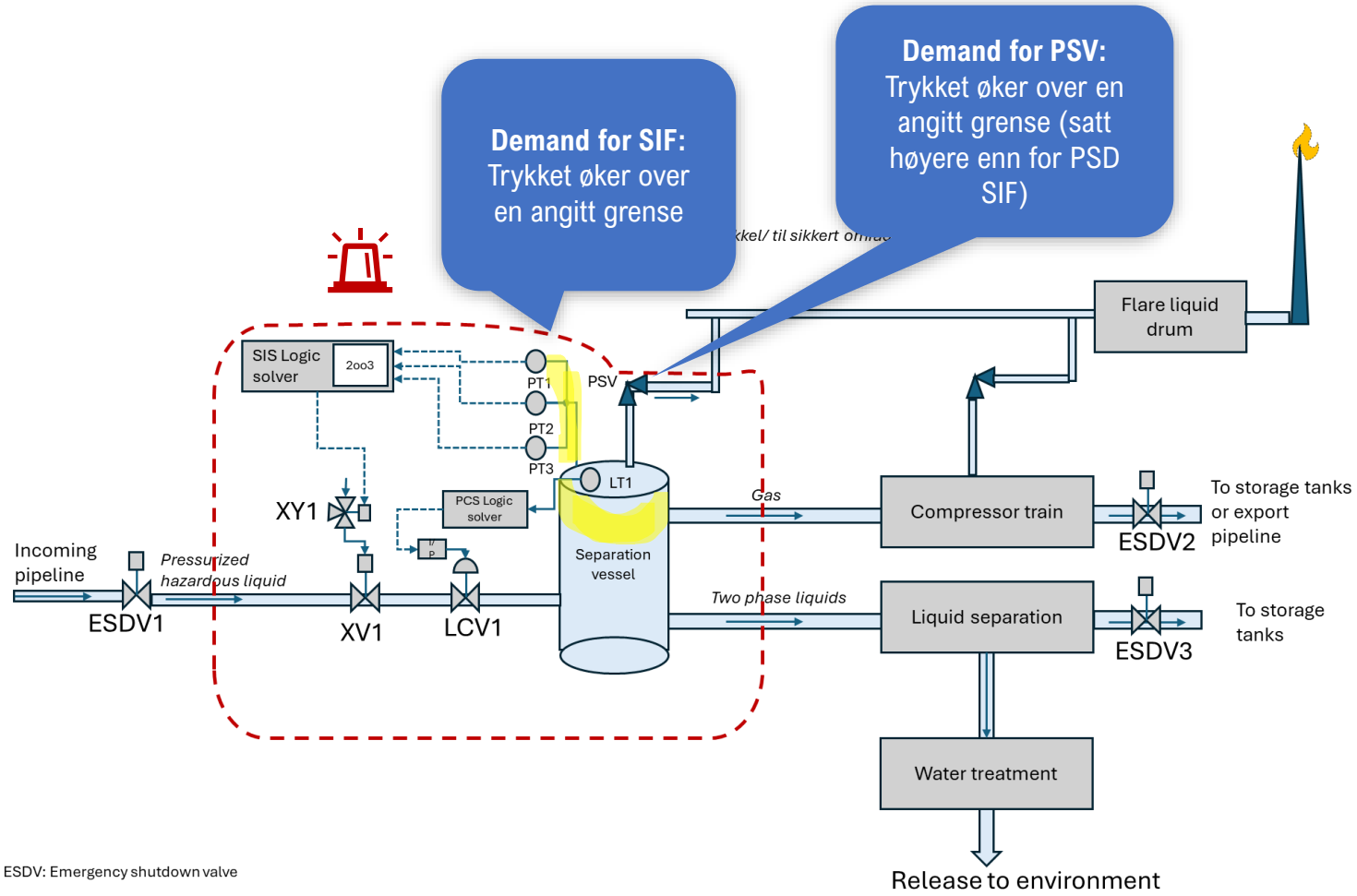


Aktivert utstyr: Griper inn i anlegget som skal beskyttes slik at sikker tilstand oppnås.

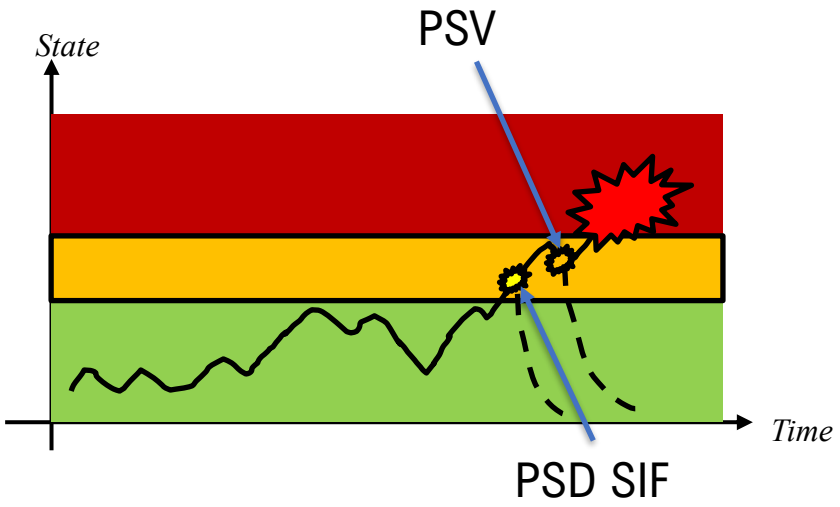
Demand: Tilstand /situasjon som krever at SIFen utfører sin aksjon:

To **operasjonsmodi** (mode of operation):
- Low demand → PFD valgt pålitelighetsmål
- High-demand/continuous mode → PFH valgt pålitelighetsmål

Demand for PSD SIF



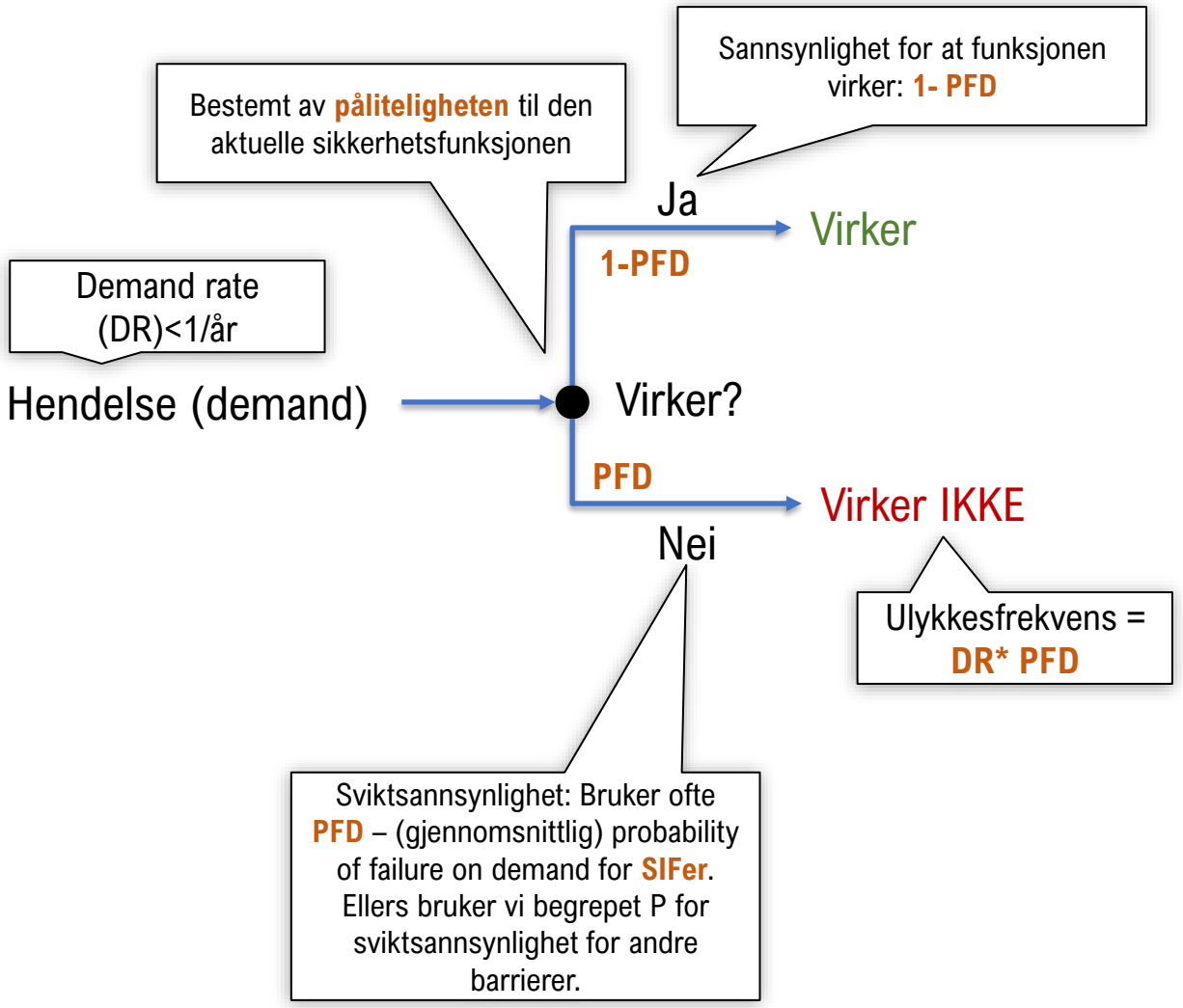
ESDV: Emergency shutdown valve



Hvordan skjer risikoreduksjon?

For low-demand:

- Behov for funksjonen er **sjelden**
- Vi ønsker å vite ***OM*** funksjonen svikter **dersom** det skjer **samtidig** som det er en demand

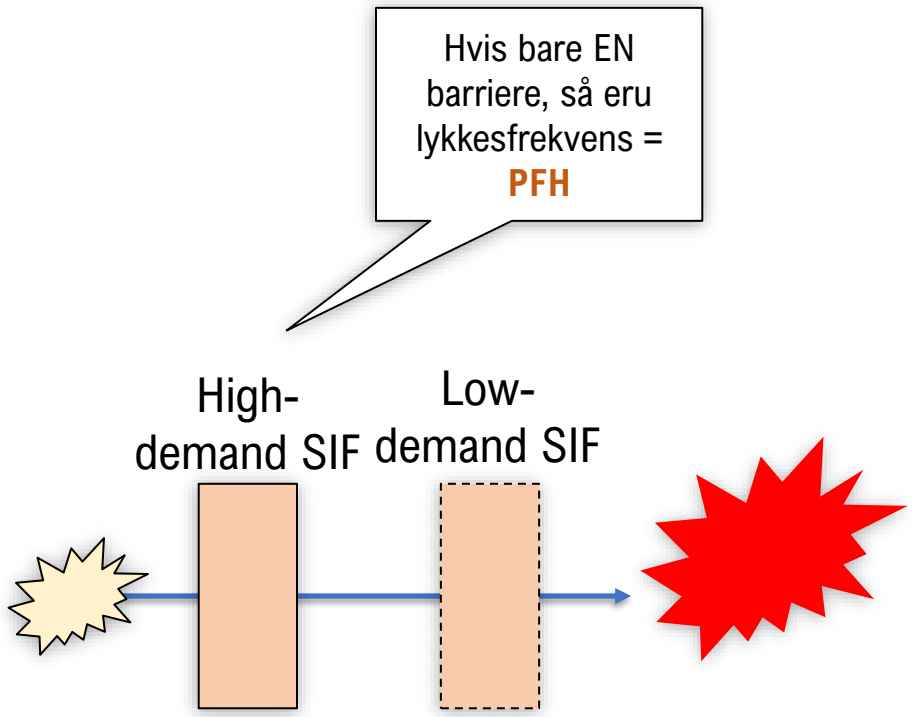


Vi ser bare på *en* barriere her

Risikoreduksjon for high/continuous demand mode

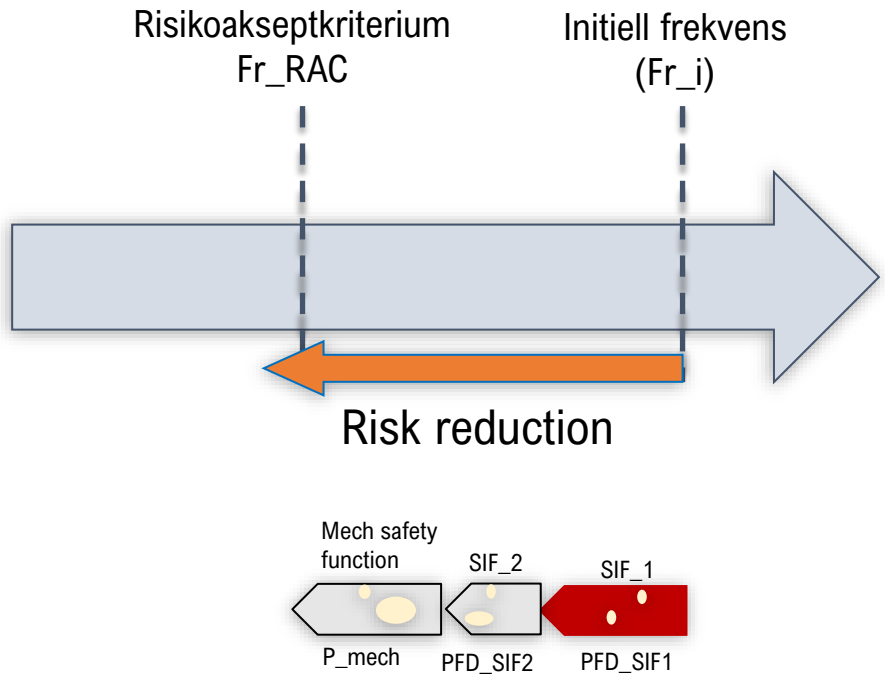
For high-demand/continuous mode:

- Behov for funksjonen **ofte** eller **hele tiden**
- **Enhver svikt** av SIFen blir dermed en farlig hendelse
- Maksimal PFH SIFen (PFH krav) må derfor være mindre eller lik akseptkriteriet satt for den farlige hendelsen.



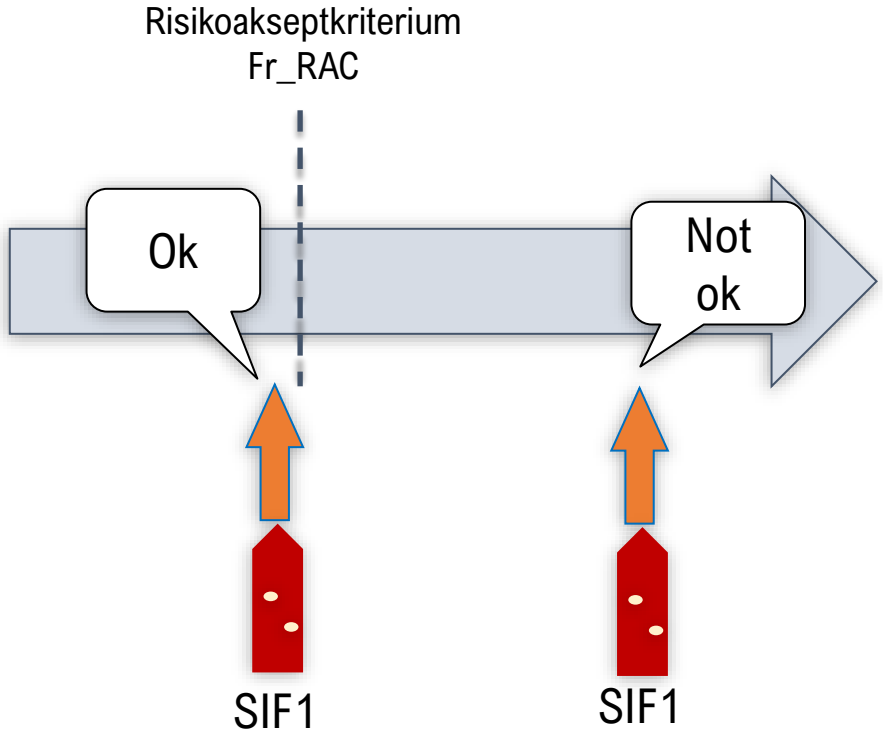
Oppsummert om PFD og PFH

Low demand/PFD



Fr_RAC≥ Fr_i * **PFD_SIF1*** PFD_SIF2 * P_mech

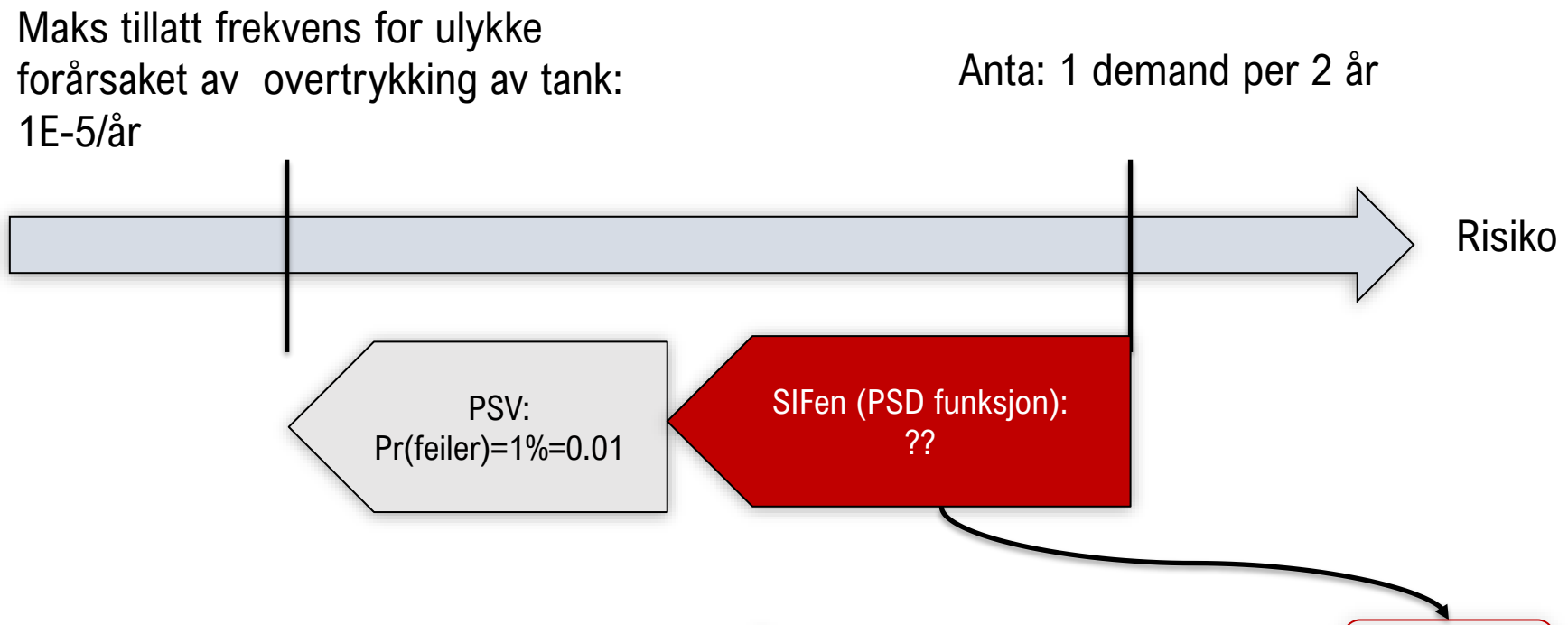
High demand/PFH (hvis bare en barriere)



Fr_RAC ≥ **PFH_SIF1**

Maks tillatt PFD og tilhørende SIL krav til en SIF

Med litt andre antagelser enn case



1E-5 (per år) ≥0.5 (per år) * 0,01 * **PFD_SIF**

PFD_SIF ≤ 1E-5/(0.5*0.01) = 0.002=2E-3

Kan vi designe en SIF i henhold til en PFD verdi alene?

Nei. De som *har nytte* av PFD direkte er:

- ✓ Pålitelighetsingeniører
- ✓ Risikoanalyseingeniører
- ✓ Systemansvarlig kan følge med på hvordan verdiene endrer seg

De som **ikke** kan bruke PFD som input direkte er:

- ? Programmere (av logikken som skal inn i sikkerhetssystemene)
- ? Systemdesignere (som skal velge utstyr og stille krav til funksjonalitet)
- ? Prosjektledere som skal vite hvordan og hvilke krav som stilles til verktøy og prosesser

Løsningen for SIS ligger i SIL

- **SIL: Safety Integrity Level**
- Gjelder **bare** for SIFer
- Totalt fire nivåer – SIL 1 til SIL 4
- Hvert SIL nivå **gir løfte om en viss pålitelighet** (eks maks og min for feilsannsynlighet)
- **Maks tillatt PFD** for å oppnå risikoreduksjon **omformes** til et **SIL krav** for SIFen

SIL kravet utløser en del regler for hvordan man designer en SIF

- Reglene finnes i internasjonale standarder (som IEC 61508, IEC 61511 og IEC 62061)
- Dekker blant annet:
  - Bruk av sertifiserte funksjonsblokker som konfigureres (eller krav til hvordan sertifiserte blokker lages)
  - Krav til utviklingsverktøy (kompilator) og programmeringsspråk og tillatt funksjonalitet
  - Krav til votering og diagnostikk
  - Krav til hva som skal gjøres når i en designprosess
  - Krav til kompetanse på de som jobber med sikkerhetssystemer
  - Krav til hva som skal være med i pålitelighetsanalysen og når de skal utføres

Safety integrity level (SIL)

SIL:

- Et uttrykk for et pålitelighetsnivå for en sikkerhetsfunksjon (SIF)
- Delt inn i fire nivå: SIL 1, SIL 2, SIL 3 og SIL 4

SIL	Sviktsannsynlighet (PFD) (brukes for low demand SIFer)	Sviktfrekvens (PFH) (per time) (brukes for high-demand SIFer)
4	0.00001≤PFD <0.0001	1E-9 ≤PFH <1E-8
3	0.0001≤PFD <0.001	1E-68≤PFH <1E-7
2	0.001≤PFD <0.01	1E-7 ≤PFH <1E-6
1	0.01≤PFD <0.1	1E-6 ≤ PFH <1E-5

SIL 2: SIF må ikke svikte oftere enn en gang hvis utsatt for 100 demands

SIL 2: SIF må ikke svikte oftere enn (ca) 1 gang per 100 år

TTK2 dekker bare pålitelighetsbiten av SIL

Men standarder for funksjonell sikkerhet utløser altså mange flere krav som er knyttet til SIL kravet. Her er bare ett av mange eksempler!

NEK IEC 61508-2:2010

Table A.15 – Techniques and measures to control systematic failures caused by hardware design

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Failure detection by on-line monitoring (see Note 4)	A.1.1	R low	R low	R medium	R high
	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
	Standard test access port and boundary-scan architecture	A.2.3	R low	R low	R medium	R high
	Code protection	A.6.2	R low	R low	R medium	R high
	Diverse hardware	B.1.4	– low	– low	R medium	R high

At least one of the techniques in the light grey shaded group, or one of the techniques specified in Table A.3 of IEC 61508-3, is required.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text immediately preceding this table.

NOTE 2 The measures can be used to varying effectiveness according to Table A.18, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annexes A, B and C of IEC 61508-7. The relevant subclause is referenced in the second column.

NOTE 4 For E/E/PE safety-related systems operating in a low demand mode of operation (for example emergency shutdown systems), the diagnostic coverage achieved from failure detection by on-line monitoring is generally low or none.

NEK IEC TR 61511-4:2020

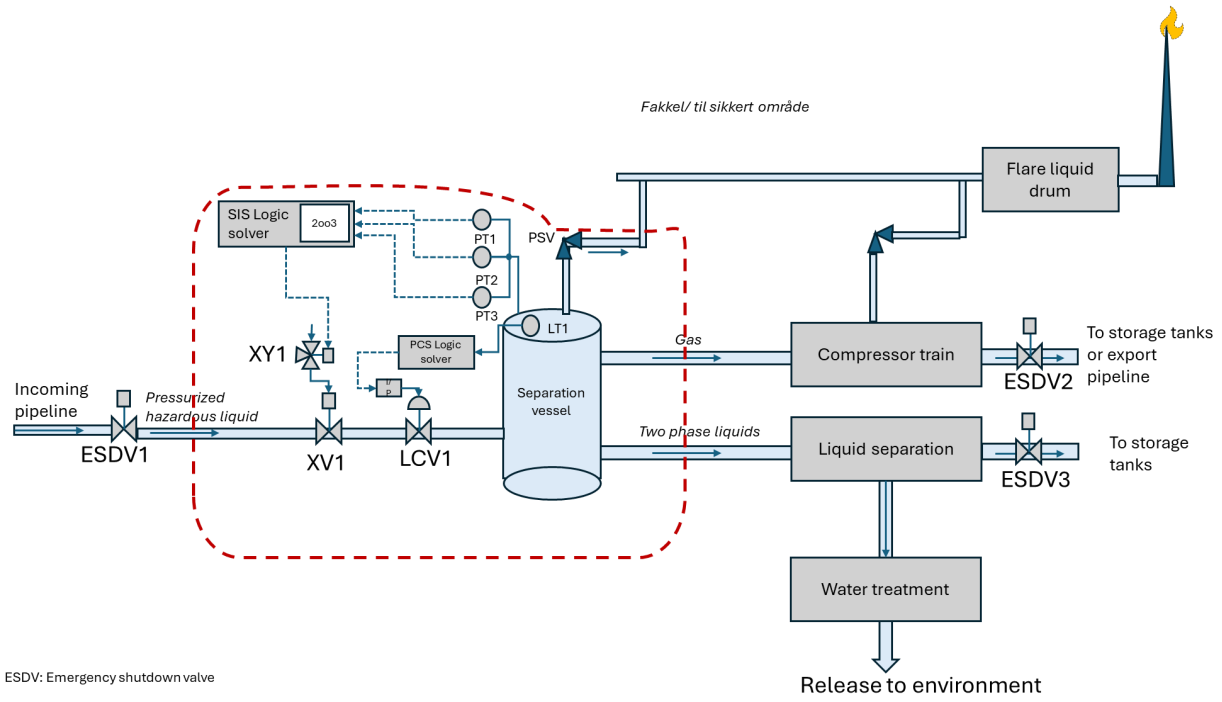
INTRODUCTION

IEC 61511 (all parts) addresses safety instrumented systems (SIS) for the process industry sector. It is written to use terminology that is familiar within this sector and to define practical implementation requirements based on the sector-independent clauses presented in the IEC 61508 basic safety standard. IEC 61511-1 is recognized as a good engineering practice in many countries and a regulatory requirement in an increasing number of countries.

Nevertheless, standards evolve with the application experience in the affected sector. The second edition of IEC 61511-1 was edited based on a decade of international process sector experience in applying the requirements of the first edition of IEC 61511-1:2003. The changes from Edition 1 to Edition 2 were initiated by comments from National Committees representing a broad spectrum of users of the standard worldwide.

In Edition 1:2003 (Ed. 1) [1], the requirements addressing the avoidance and control of systematic errors that occur during design, engineering, operation, maintenance and modification were adapted primarily to support independent safety functions up to a SIL 3 performance target. In contrast, Edition 2:2016 (Ed. 2) needed to address a prevailing trend of sharing automation systems across multiple safety functions.

Feilkategorier av betydning for pålitelighet av SIF



For komponenter som inngår i en SIF

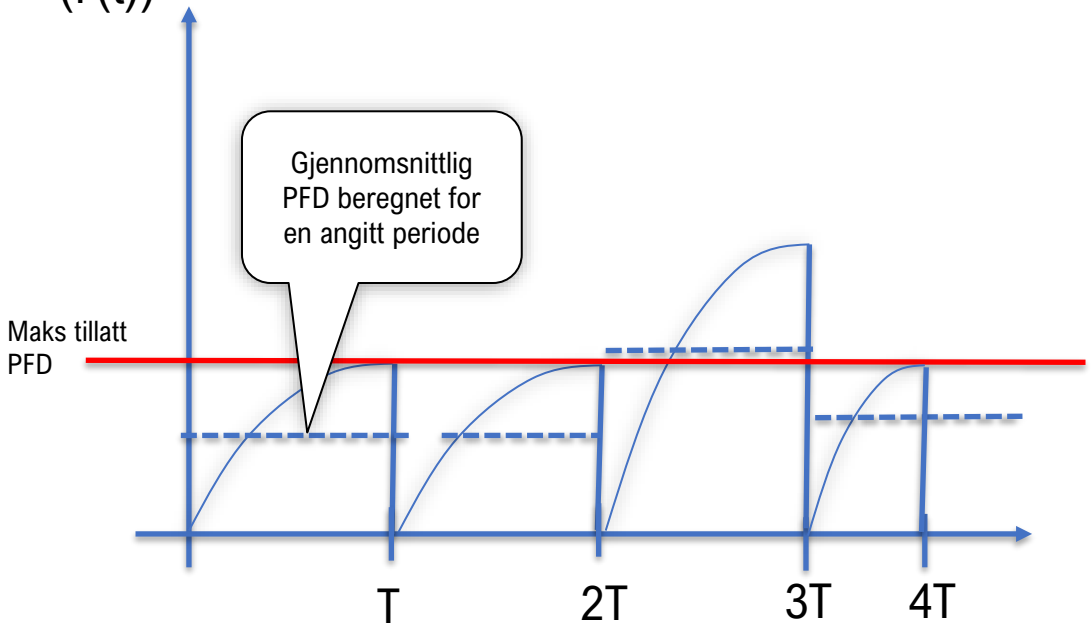
- Kritikalitet
  - **Farlig** (dangerous - D) feil:
    - **Udetektert: DU**
    - **Detektert: DD**
  - Sikker feil

Hovedbidrag et til **PFD** og **PFH**

- Årsaker og tiltak:
  - **Tilfeldige feil** (skyldes slitasje og andre årsaker som gjør at feil skjer på nytt
  - **Systematiske feil** (Feil som er introdusert og som teoretisk sett kan rettes slik at de ALDRI skjer igjen)

PFD vs PFH

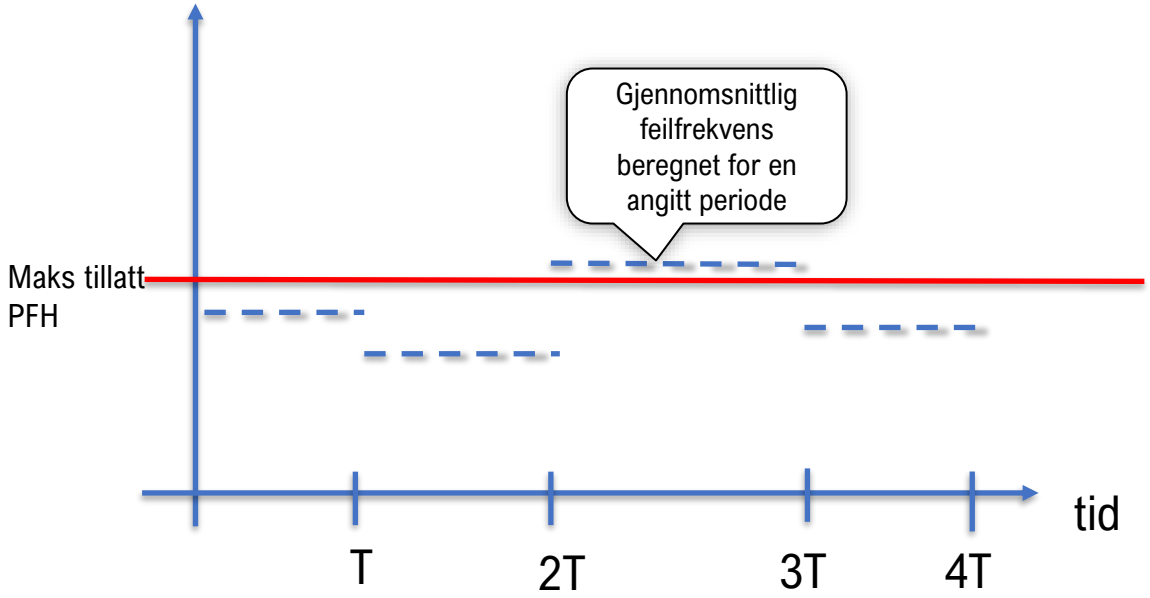
Feilsannsynlighet
(F(t))



(Utregnet) PFD: - - - - -

- Gjennomsnittsverdi av F(t) innenfor hver periode T, der T er intervallet mellom hver gang funksjonen testes for å avdekke DU feil.
- Noen metoder inkluderer også DD feil, men de får vanligvis ikke mye å si

Gjennomsnittlig feilfrekvens PFH
(per time)



(**Utregnet) PFH:** - - - - -

- Gjennomsnittsverdi for frekvensen av DU feil (og noen ganger også med DD feil inkludert)
- Tilnærmes F(T)/perioden i timer hvis perioden ikke er for lang

Oppgave 1

4 Oppgave 1 (seminar 1) – Bestemme krav til sikkerhetsfunksjoner

I oppgave 1 er formålet å gjennomføre en risikoanalyse og komme frem til et pålitelighetskrav til sikkerhetsfunksjonen SIF1.

a) Foreslå en naturlig avgrensning av EUC for hendelsen «overtrykking av separator», og gi eksempler på utfordringer eller problemstillinger man må ta hensyn til for å gjøre denne avgrensningen.

b) Bruk en sjekkliste til å identifisere mulige årsaker til overtrykking og identifiser hvilke som PSD-systemet og PSV-ventilen kan stanse.

c) Lag et hendelsestre som identifiserer mulige utfall av hendelsene, der rollen til ESD og F&G systemet vises

d) Overfør informasjonen fra forrige deloppgave til et bowtie-diagram og angi hvor sikkerhetsfunksjoner implementert via PSD, ESD og F&G, samt trykkavlastningsventilen PSV, vil plassere seg.

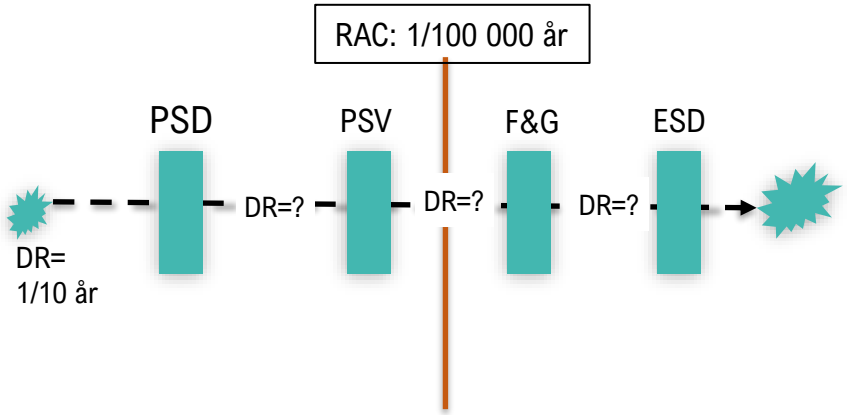
e) Regn ut pålitelighetskravet, uttrykt som PFD, for PSD SIF-en dersom vi antar en demand-rate for PSD SIF på 1/10 år, et akseptkriterium på 1/100 000 år og at PSV-ventilen har en feilsannsynlighet på 1%. Illustrer grafisk og vis utregning.

f) Regn også ut demand-ratene for PSV-ventilen, ESD-systemet og F&G-systemet, dersom vi for dette eksempelet legger til at funksjonene i ESD- og F&G-systemene er designet for å oppfylle SIL 2-krav. Tegn opp et barrierediagram med alle demand-ratene.

g) Anta at man ønsker å introdusere en ny sensorteknologi for overtrykksdeteksjon i PSD SIF som bruker KI (AI).

   i. I hvilken grad påvirker dette usikkerheten forbundet med risikoreduksjonen for PSD SIF-en isolert sett, og hvilken konsekvens kan dette ha for risikoreduksjonen totalt sett?
   ii. Hvordan vil ALARP-prinsippet kunne påvirke hvordan man håndterer dette? (ikke utregninger, her er det ment å resonnere litt frem og tilbake)

Bare separatoren eller også deler av innløpsrør?



Neste gang: Seminar 2

- Feil og feilklassifsering
- Pålitelighetsnettverk
- Formler for PFD og PFH for et utvalg av subsystem med votering
- Hva parametrene betyr
- Hvordan PFD beregnes – per subsystem og for en SIF totalt

Forberedelser:

- Les tilhørende litteratur til seminar 2 (se filen «TTK2_Detaljert temaoversikt med litteratur)