To av tre oppgaver skal besvares

Oppgavene vektes likt

NB: Det er mulig å tegne figurer for hånd på egne ark. Disse må merkes godt og leveres til eksamensvaktene.

Oppgave 1

Resilience Engineering er et av flere perspektiver på sikkerhet.

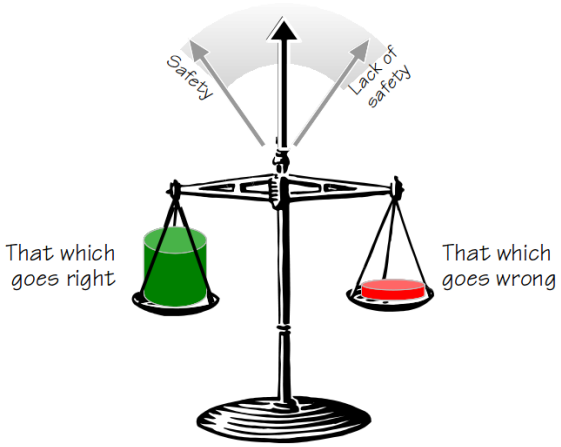
- Forklar først hva som menes med resilience og Resilience Engineering.
- Redegjør for begrepene Safety I og Safety II.
- Work as imagined / work as done (WAI/WAD), efficiency-thoroughness trade-off (ETTO), variabilitet og funksjonell resonans er begreper som kan knyttes til Resilience Engineering. Forklar disse begrepene og hvordan de er relevante for sikkerhet.

Resilience er en metafor som brukes i sikkerhetslitteraturen og som er inspirert av måten resilience har blitt brukt for å beskrive økologiske systemer. Resilience handler om evnen til å tilpasse seg varierende omstendigheter, til å tåle og absorbere påkjenninger og sjokk og gjenopprette funksjonen – 'bounce back from failure'.

Resilience Engineering er en retning innenfor sikkerhetsfaget som fokuserer på hva som gjør organisasjoner og sosiotekniske systemer 'resiliente'. I utgangspunktet har man i RE rettet fokus mot mye av de samme typer komplekse systemer som man adresserer innen NAT og HRO. Det som skiller RE fra disse retningene er at man særlig er opptatt av å forstå *det som går bra* i forbindelse med 'normalarbeid' – altså ikke nødvendigvis de mest spektakulære operasjonene. Dette med å forstå det som går bra, skiller RE fra NAT, som er særlig opptatt av å forstå hvorfor ulykker oppstår, samt HRO, som forklarer mekanismne bak såkalte høypålitelige organisasjoner som presterer *særdeles* godt. Man snakker også gjerne om fire hjørnesteiner:

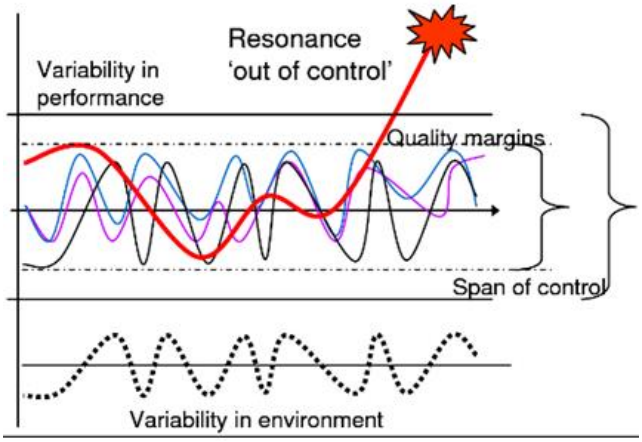
- Kunnskap om *hvordan en skal håndtere både regulære og irregulære forstyrrelser*/problemer, ved å iverksette planlagte prosedyrer, eller ved å justere vanlig praksis eller ved improvisasjon
- Å vite *hva en skal se etter*: d.v.s. å overvåke det som er eller kan utgjøre en trussel, både innenfor systemet/organisasjonen og i omgivelsene
- Å vite *hva en kan vente* seg; d.v.s. å forutse mulige trusler og muligheter
- Å forstå hva som har hendt: d.v.s. ha evnen til å *lære av erfaringer*

Safety II har blitt presentert som en utvidelse av det tradisjonelle fokus på sikkerhet, som man omtaler som Safety I. Safety I adresserer sikkerhet som fravær av uønskede hendelser og ulykker, «freedom of unacceptable risk». Safety II snur på dette og adresserer sikkerhet som evnen til å lykkes under variende forhold, og om å forstå mekanismene bak dette. Det handler med andre ord om å forklare hvorfor ting går bra:



Et argument for Safety II er at det er mye mer som går bra enn som ikke går bra, og art det er veldig mye erfaringsgrunnlag som går tapt dersom man bare fokuserer på unntakene der ulykker inntreffer.

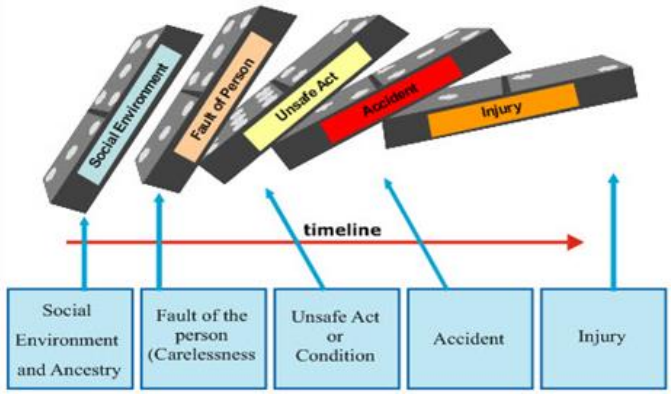
Work as imagined er organisasjonens formelle virkemåte, og fremstiller gjerne organisasjonen fra et ledelsesperspektiv. Work as done handler om arbeidet slik det utføres i praksis. Blant de mekanismene som forekommer i normalarbeid er ETTO – efficiency-thoroughness trade-off. Dette er avveininger mellom grundighet og effektivitet som er nødvendig for å få arbeidet til å flyte på en god måte. ETTO gir opphav til variabilitet, som er kilde både til det som går bra og det som går galt. Variabilitet er med andre ord et naturlig forekommende fenomen, og betraktes i utgangspunktet ikke som avvik. I RE forklares ulykker ved funksjonell resonans, altså variabilitet i ulike deles av systemet, med lignende frekvens og bølgelengde, som samvirker og bringer systemet ut av kontroll.



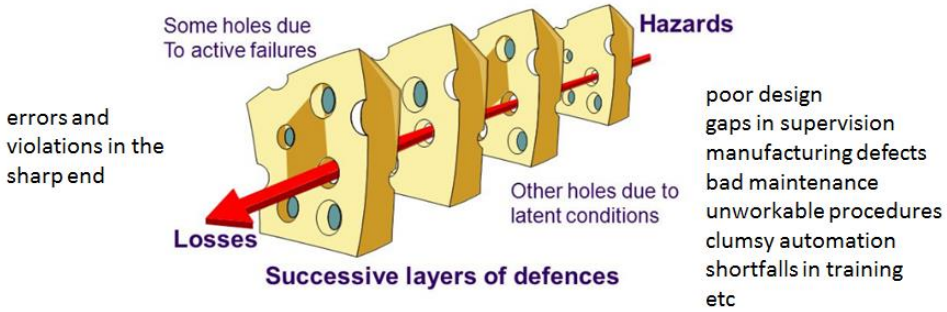
Oppgave 2

I sikkerhetslitteraturen finnes det ulike måter å tenke om hendelsesforløp/ulykkesforløp på. Forklar hva som menes med enkle lineære forløp, komplekse lineære forløp og systemiske forløp/prosesser for ulykker. Beskriv en modell for hver av de tre typene hendelsesforløp/ulykkesforløp.

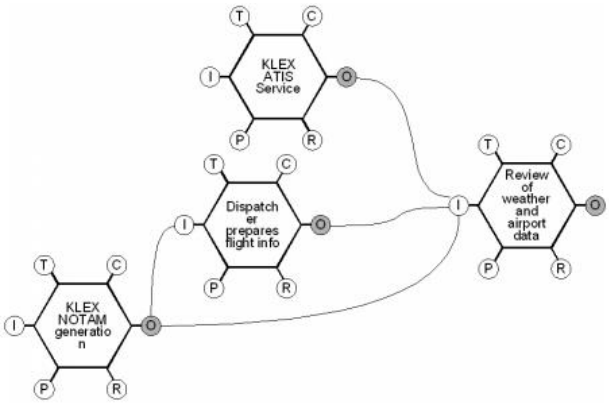
Enkle, lineære hendelsesforløp er forløp der en uønsket hendelse kan spores bakover til en rotårsak gjennom flere kausale, sekvensielle ledd. Ser man på hendelsesforløpet, finner man gjerne bakenforliggende faktorer (eksterne faktorer) som påvirker lokale faktorer på arbeidsplassen, som igjen tilrettelegger for menneskelige feil med påfølgende ulykker. En kjent modell som fremstiller dette er Dominomodellen:



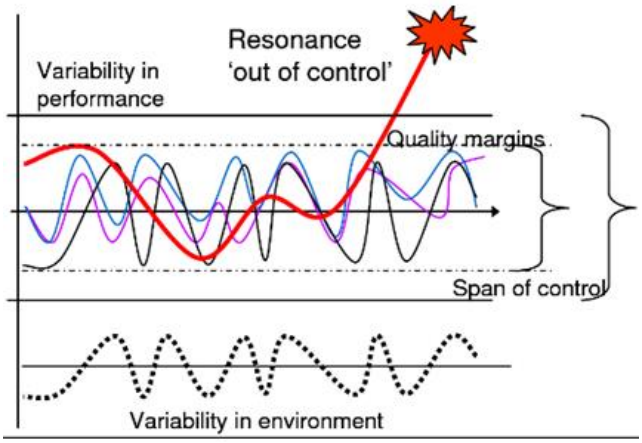
I komplekse, lineære forløp fremstiller man hvordan slike sekvensielle hendelsesforløp lar seg påvirke og hindre ved hjelp av barrierer i dybden. Dette kan være barrierer av ulike typer, og barriereredundans er et stikkord. Når uønskede hendelser likevel skjer henger det gjerne sammen med svekkelse av barrierene. Barrierer kan svekkes både pga latente feil og akive feil. Latente feil oppstår gjerne over tid og kan være vanskelige å oppdage (eks design, dårlig ledelse, dårlig vedlikehold, mangelfull trening osv), mens aktive feil oppstår mer akutt som følge av feilhandlinger i den skarpe enden. Komplekse, lineære forløp fremstilles gjerne gjennom den såkalte sveitserostmodellen:



Systemiske hendelsesforløp er ikke-lineære, og forekommer ikke som sekvensielle forløp. Her kan man ikke lete seg tilbake etter en rotårsak; uønskede hendelser forklares derimot vanligvis som emergente, det vil si at flere deler av systemet spiller sammen på måter som ikke beskrives som kausale forløp. Med bakgrunn av beskrivelse av variabilitet i sosiotekniske systemer kan uøsnekde hendelser i systemisk forløp beskrives som resultat av resonans mellom flere funksjoner i systemet (som beskrevet i oppgave 1).



En modell som fremstiller dette er FRAM – functional resonance analysis method / accident model.

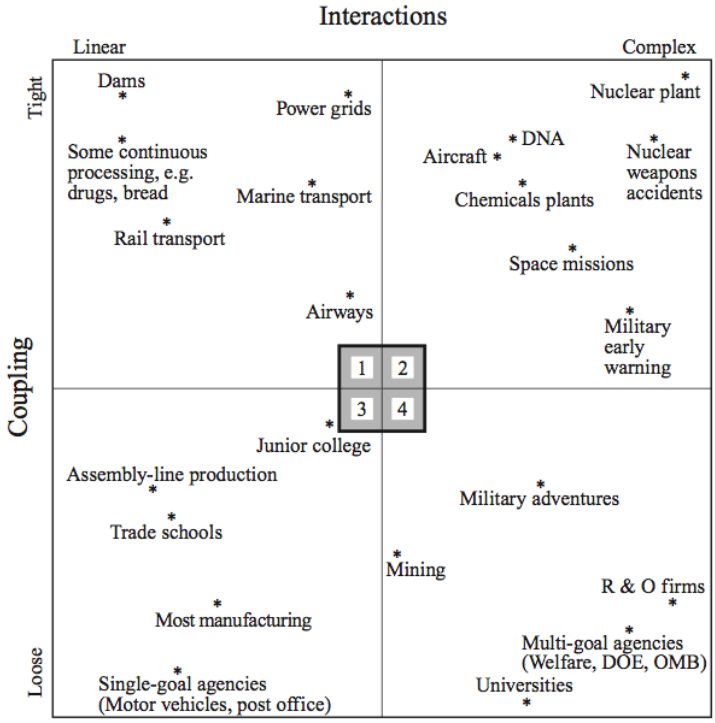


Oppgave 3

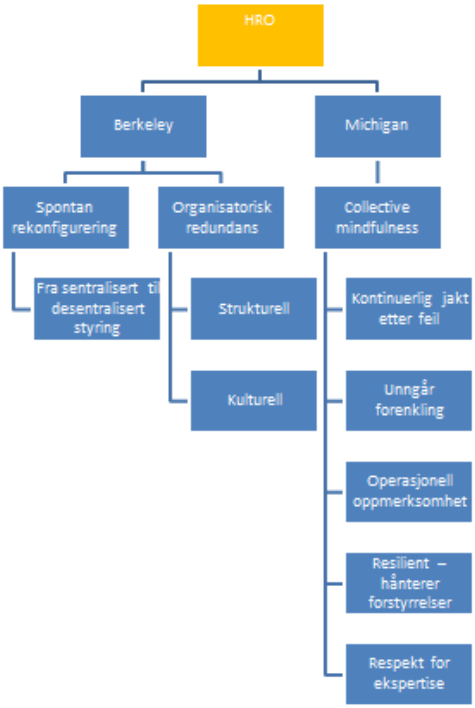
Redegjør for de grunnleggende elementene og konklusjonene i Normal Accident Theory (NAT) og High Reliability Organisations (HRO). Sammenlign deretter de to perspektivene/teoriene og vis likheter og forskjeller.

Normal Accident Theory fremstiller systemer ut fra hvor løst eller tett de er koblet, samt hvorvidt interaksjoner er lineære eller komplekse.
Et system er tett koblet hvis forstyrrelser forplanter seg hurtig gjennom systemet og det er lite slakk og rom for improvisasjon for å «temme» forstyrrelsene. Det motsatte er tilfelle med løst koblede systemer.
Et system med komplekse interaksjoner oppfører seg uforutsigbart og byr gjerne på overraskelser. Det motsatte er tilfelle for systemer som preges av lineære interaksjoner.
Et system med tette koblinger krever sentralisert styring for å kunne kontrolleres tilfredsstillende. Et system med komplekse interaksjoner krever derimot desentralisert styring. Paradokset oppstår når organisasjoner eller sosiotekniske systemer med komplekse interaksjoner også er tett koblede og har komplekse interaksjoner – da er det ifølge NAT ikke mulig å innfri begge krav samtidig og samtidig garantere tilfredsstillende sikkerhet over tid. For slike systemer anbefaler teorien at man enten løser

opp koblingene eller gjør systemet mindre komplekst. Er dette ikke mulig, anbefales det å ikke drive videre.



HRO-forskningen studerte lignende organisasjoner som NAT, men kom frem til en annen konklusjon. Bl.a. gjennom å vektlegge sterkere en del kulturelle forhold, fant man at enkelte organisasjoner presterer godt til tross for tette koblinger og komplekse interaksjoner. HROer kjenntegnes ved følgende egenskaper:



HRO og NAT teoretiserer samme typer høyrisikoorganisasjoner, men kommer likevel til ulike konklusjoner. Der NAT er opptatt av strukturer og teknologi, og fremstilles som struktur-/teknologideterministisk, er HRO mer opptatt av organisasjonskulturelle forhold, og fremstilles gjerne som sosialkonstruktivistisk. Det kan legges til at begge disse karakteristikkene er noe unyanserte.

For øvrig finnes en del andre forskjeller mellom NAT og HRO:

High Reliability Theory	Normal Accidents theory
Accidents can be prevented through good organisational design and management.	Accidents are inevitable in complex and tightly coupled systems.
Safety is the priority organizational objective.	Safety is one of a number of competing objectives.
Redundancy enhances safety: Duplication and overlap can make "reliable systems out of unreliable parts."	Redundancy often causes accidents: it increases interactive complexity and encourages risk-taking.
Decentralised decision-making is needed to permit prompt and flexible field-level responses to surprises.	Organizational contradiction: Decentralization is needed for complexity, but centralization is needed for tightly coupled systems.
A "culture of reliability" will enhance safety by encouraging uniform and appropriate responses by field-level operators.	A military model of intense discipline, socialisation, and isolation is incompatible with democratic values.
Continuous operations, training, and simulations can create and maintain high reliability organizations.	Organizations cannot train for unimagined, highly dangerous, or politically unpalatable operations.
Trial and error learning from accidents can be effective, and can be supplemented by anticipation and simulations.	Denial of responsibility, faulty reporting, and reconstruction of history cripples learning efforts.