Risikoanalyse, kompleksitet og usikkerhet - noen refleksjoner

Kenneth Pettersen (UiS)

Kenneth Pettersen, Universitetet i Stavanger

15. mars 2016

Universitetet i Stavanger

Agenda - fire tema

- Teknologidefinisjon
- System ulykker – kompleksitet og kopling (Perrow)
- Risikoanalyse og usikkerhet – mot et bredt rammeverk
- Håndtering av avdrift og pålitelighetseksperter

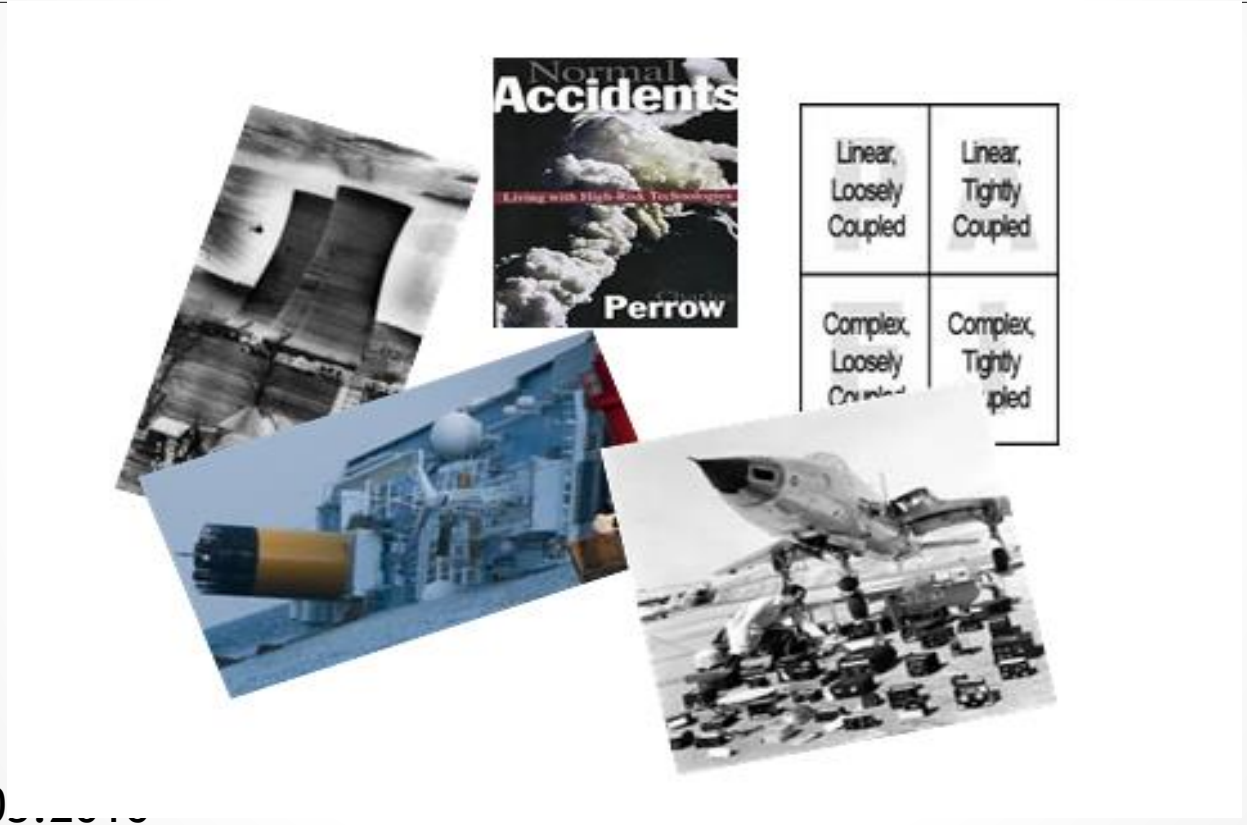
Universitetet i Stavanger

1. Teknologidefinisjon – Fra *Perspektiver på samfunnssikkerhet*

Med teknologi forstår vi de materielle objekter, teknikker og kunnskap som gir oss mennesker mulighetene til å endre og kontrollere den materielle verden (basert på Westrum 1991 s.9). Teknologi er derfor både konkret og abstrakt. Det er både tastaturet jeg skriver på og kunnskapen om hvordan det lages. Mange teknologier omtales i dette kapittelet som teknologiske system. Med *teknologiske systemer* mener vi de tilfellene hvor teknologier er integrerte nettverk av mennesker, kunnskap og apparater, i organisasjoner eller sektorer som for eksempel den sivile luftfarten, petroleumsindustrien og kjernekraftindustrien (Bijker et al. 2012). Andre teknologier, slik som genteknologi eller asbest materialer er ikke avhengig av slik organisatorisk og systemisk oppbygning og fungerer som uavhengige deler (Westrum 1993).

Universitetet i Stavanger

2. Perrow: Complexity, Coupling, and Catastrophe



Universitetet i Stavanger

17.0

Fokuserer på egenskaper ved systemene, ikke ved den som behandler dem

- 1.nivå – DEL (minste enheten i systemet, f eks en ventil)
- 2.nivå- ENHET (samling av deler som f eks til sammen utgjør en generator)
- 3.nivå- SUBSYSTEM (samling av enheter som til sammen utgjør et system – f eks et kjølesystem bestående av generator, pumper, motorer og rør)
- 4. Nivå – SYSTEMET (det totale systemet – f eks kjernekraftverket).

Logikken hos Perrow

- System er delt opp i fire nivå: del, enhet, subsystem og system.
- «Incidents» er begrenset til deler eller enheter i systemet, selv om det kan stoppe produksjonen.
- Ulykker medfører ødeleggelse i subsystem eller systemet som helhet og medfører stopp i produksjon.
- Komponentfeilulykker involvere en eller flere komponentfeil (del, enhet, subsystem) som er koplet på forventede måter.
- Systemulykker involverer ikke forventede koplinger av flere feil. Systemulykker må ha multiple feil og de må oppstå i rimelig uavhengige enheter eller subsystem.
- Systemulykker starter vanligvis i deler, f eks en ventil…
- Det er ikke kilden som avgjør skillet mellom de to ulykkestypene, men om det er eller ikke er multiple feil som interagerer uforutsett.

Komplekse systemer	Lineære systemer
Nærhet	Segregert
Mange komplekse sammenhenger	Kjente sammenhenger
Subsystemer innbyrdes forbundet	Segregerte subsystem
Vanskelig å erstatte deler	Lett å erstatte deler
Tilbakeføringssløyfer	Få tilbakeføringsløyfer
Kontroll mangefoldig og Med gjensidig påvirkning	Kontroll entydig og adskilt
Indirekte info	Direkte info
Begrenset forståelse	

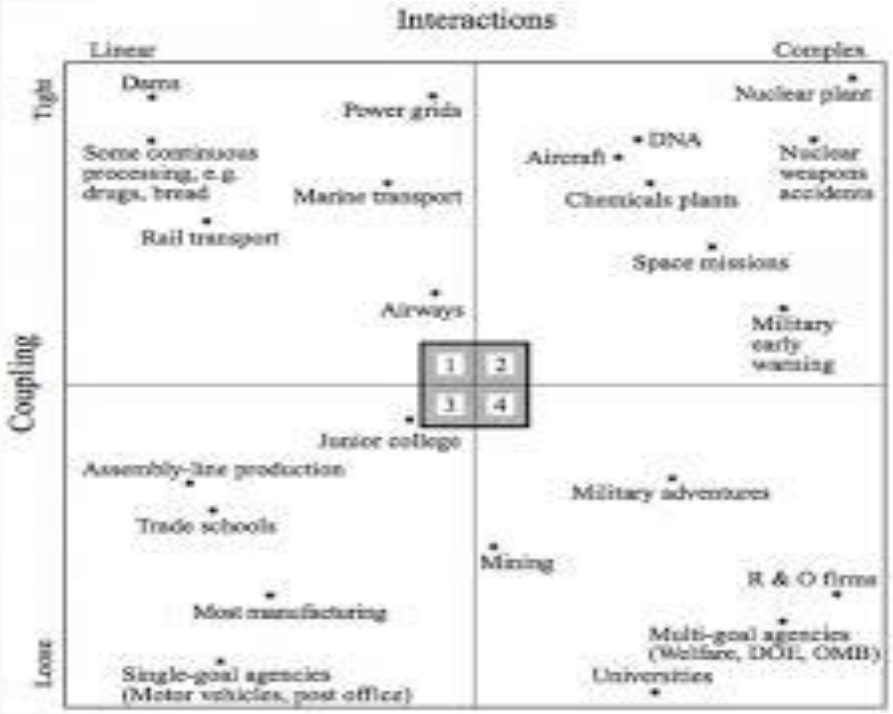
Universitetet i Stavanger

Kobling

- Tett koplede system har mer tidsavhengige prosesser, de kan ikke vente. Produksjons-prosessen tåler ikke stans.
- Sekvensene kan vanskelig endres
- Prosessdesign tillater bare en fremgangsmåte for å nå produksjonsmål
- Tett koplede system har liten slakk: antall må være presist, ressurser kan ikke erstattes av andre, svikt i utstyr fører til nedstegning av produksjonen.
- I tett koplede system må buffere, slakk og erstatninger bli designet inn i systemet på forhånd
- I løst koplede system er det flere utveier, buffere, slakk i systemet og mulighet for å finne erstatninger selv om de ikke var planlagt.

Tett kopling	Løs kopling
Forsinkelser ikke mulig	Forsinkelse mulig
Rekkefølge fastlagt	Rekkefølge kan endres
Kun en metode for å nå målet	Alternative metoder
Lite slakk i utstyr og personell	Slakk mulig
Buffere innebygget i designet	Buffere finnes tilfeldig
Erstatninger av komponenter	Erstatning finnes
Må planlegges	tilfeldig

Universitetet i Stavanger



Charles Perrow

3. Økt kompleksitet og avhengigheter – implikasjoner for risikoanalyse og kontroll

- Økt kompleksitet og avhengigheter = usikkerhet vil være en karakteristikk ved analyse og kontroll

Hva skal vi så gjøre?

- Alternativ 1: får vi gode nok data og metodene blir presise nok kan vi redusere usikkerhet til risiko
- Alternativ 2: Usikkerhet er et argument for hvorfor teknologisk system design og ledelse har grunnleggende begrensninger og utviklingen av høy-risiko systemer må stoppes
- Alternativ 3: Usikkerhet kan håndteres i teknologiske systemer igjennom et bredt rammeverk som går på tvers av tekniske og samfunnsvitenskapelige fag

Universitetet i Stavanger

Et bredt rammeverk for risikoanalyse - implikasjoner

- Usikkerhet må tilnærmes som noe positivt, ikke bare negativt
- Dette betyr ikke at det upredikerbare kan forutsees eller at vi kan forberede oss på usikkerhet, men…
- Det er alternativer i verktøykassen.

1. Et bredt rammeverk betyr ikke at sannsynlighetsbaserte metoder skal «ut med badevannet», men…
2. Informasjonshåndtering (unknown knowns): Utvikle en organisasjonsmodell som kombinerer analytisk og praktisk kunnskap, og som har flere handlingsalternativer
3. Perspektiv utvikling (unknown unknowns): tilstrekkelig variasjon i ledelse og lytte til ulike meninger for å oppdage svake signaler

Universitetet i Stavanger

4. En hovedutfordring er integreringen av design og tekniske systemer med operatør ferdigheter, erfaring og kunnskap

Universitetet i Stavanger

REALTRANS – en introduksjon

- Transportsystemerer preges av:
  - Ny teknologi
  - Varierende situasjonelle betingelser
  - Standardisering av risiko og sikkerhet.

- Standarder og prosedyrer ikke tilstrekkelige for å møte de oppgaver og krav teknikere, piloter og kapteiner møter i ulike situasjoner

- Organisasjoner og operatører må gjøre tilpasninger…
  - Ofte for å holde systemene i gang og unngå uønskede operative konsekvenser (tilpasning eller resiliens)
  - Andre ganger bidrar tilpasningene til økt risiko for ulykker og katastrofer (avdrift)

  - **Hvordan kan vi skille den ene formen for tilpasning (eks. resiliens) fra den andre (avdrift)?**

Universitetet i Stavanger

Pålitelighetsavdrift (‘reliability drift’)

- Vi finner at avdrift:
  - Er både en atferdsmessig og kognitiv prosess, med endringer i atferd og tilknyttede forandringer i tenkemåte og forståelse
  - kan knyttes til grupper av ansatte, avdelinger, organisasjoner og sektorer, så vel som befolkningen
  - Avdrift har drivere som konkurrerende verdier, målkonflikter og motstridende krav fra omgivelsene

- I den grad endringer i atferd og forståelse plasserer organisasjoners resultat utenfor kjente og forståtte handlingsrom definerer vi dette som pålitelighetsavdrift

Håndtering av avdrift og Widerøe's kortbaneoperasjoner

- Høyrere risiko/mindre sikkerhetsmarginer på kortbanenettet gjør at oppmerksomhet ovenfor pålitelighetsavdrift er særlig viktig for Widerøe
  - Vi finner at:
    - Selskapet bruker store ressurser på å forstå og definere handlingsrommet for pålitelighet og sikkerhet på kortbanenettet
    - Stor variasjon i blant annet topografi, infrastruktur og vær gjør at grensene for dette handlingsrommet er spesielt for hver enkelt flyplass og påvirkes av gjeldende forhold.
    - Operasjoner på kortbanenettet stiller et høyere krav til pilotvurderinger sammenlignet med den sivile luftfarten generelt

‘Drift management’ I

- Rollen til pilot vurderinger kan føre til pålitelighetsavdrift bort fra etablerte standarder,
  - for eksempel ved enkeltpiloter som presses til å levere transport til ellers isolerte områder av landet
  - eller holdninger som gjør at en aksepterer høyere risiko knyttet til eget selvbilde og tro på seg selv.
- Vi finner at Widerøe har en strategi for å opprettholde høy pålitelighet, på tross av at en aksepterer flyforhold som vanligvis ikke forbindes med høy pålitelige operasjoner

Universitetet i Stavanger

‘Drift management’ II

- Selskapet deler organisatoriske betingelsene med høy pålitelighet med kommersiell sivil luftfart generelt
  - For eksempel er det høy kunnskap og forståelse av teknologien
- Pålitelighet i operasjonene bygger på et omfattende og detaljert rammeverk av analytisk og erfaringsmessig kunnskap
- Utviklet egne navigasjonssystemer for å øke påliteligheten i posisjonering og pilotenes kapasiteter til monitorering i nordlig og ukontrollert luftrom
- Pålitelighetseksperter – med spesielle perspektiver på pålitelighet: forpliktet til at ting skal gå bra og har stor sensitivitet ovenfor selskapets handlingsrom, ser systemisk på pålitelighet
  - Kunnskap om handlingsrommet omfattende og svært detaljert
  - Stiller store krav til kommunikasjon og informasjonsflyt

Noen konklusjoner

- Handlingsrommet for høy pålitelighet langt mer differensiert enn hva vi ser i kommersiell luftfart generelt og andre høy pålitelige organisasjoner
  - Stiller store krav til seleksjon, trening av personell.

- Selskapets beskyttelse mot avdrift bygger på en suksessfull fusjon mellom beste praksis og standarder og regulering

- Begrensninger i organisasjoner sin håndtering av avdrift: dekker ikke endringer i samfunnet rundt og eksterne utfordringer som kan undergrave 'drift management'
  - Endringer i samfunnets verdier og politikk
  - Krav om lavere kostnader
  - Endringer i en sektors regulering og standarder
  - Systematiske endringer i ansattes trening og erfaring.

Universitetet i Stavanger