Sikkerhetsdilemmaer
-Tar man de riktige beslutningene?

Jan A. Pappas
Sjefskonsulent
LR Consulting
ESRA Jubileumsseminar 11.6.2014

Lloyd's Register Consulting

Working together
for a safer world

Dilemma

- Dilemma: Valgsituasjon hvor alternativene på en eller annen måte står i motsetning til hverandre, er i konflikt på en eller annen måte

- Sikkerhetsdilemmaer: konflikt mellom f.eks
  - Sikkerhetstiltak og økonomi (produksjon, kostnader)
  - Ulike prioriteringer av risiko uavhengig av økonomi. Sikkerhetstiltak som ikke er entydig gunstige.
  - Regelverk/krav og optimal ressursbruk
  - HMS styringsdilemmaer

Temaer

- Ny kunnskap om gamle anlegg – hva er bra nok?
- Sikkerhet vs produksjon
- HMS/sikkerhetsstyring
- ALARP
- Risikobasert styring
- Rene sikkerhetsdilemmaer
- Usikkerhet og sjeldne hendelser
- Tar man de riktige valgene?

Ny kunnskap om gamle anlegg – hva er bra nok?
(men verden er ikke helt som vi trodde den var..)

- Eks: Ny kunnskap om brannlaster.
  - Gamle anlegg er bygget iht API RP 520/521 med lave brannlaster.
  - I dag vet vi at HC branner blir vesentlig varmere enn det, så anlegget har for lite brannisolasjon eller for dårlig trykkavlastningskapasitet
  - Eskalering av en brann er derfor mer sannsynlig enn man trodde.

- Hva gjør man?
  - Går man inn i problemet - eller lar man være:
    - Argumenterer formalistisk med gjeldene regelverk på byggetidspunktet
  - Reanalyserer hele anlegget? Kostbart, men nødvendig for å vite hvor man står.
  - Endrer design: Påføring av mer brannisolasjon.
    - Ønsker så lite som mulig men allikevel nok: Kostbart og kan gi korrosjonsproblemer.
  - Driftsmessige kompenserende tiltak:
    - Automatisk trykkavlastning ved brann? Løser noe men ikke alt. Feilutløsning koster tapt produksjon.

Ny kunnskap om gamle anlegg – hva er bra nok?
(men slik har vi jo alltid gjort det…?)

- Brønnbarrierer mot utblåsning:
  - WO/Wireline BOP er ofte en totalt selvstendig lokalt operert pakke.
    - Har ikke ekstern nødforsyning på kraftsiden
    - Kan kun utløses lokalt
    - Kontrollenhet står ute i brønnområdet der utblåsningen kommer, da med HC umiddelbart
  - Hvor ellers aksepterer man en NAS barriere som ikke har nødkraft, ikke er fail safe og som må opereres lokalt ute i ulykken?
  - “Slik har alle alltid gjort” – men hva gjør man med det?

Vi prioriterer sikkerhet foran økonomi

- eller…?

- Gassdeteksjon:
  - Hvor mye stenges ned?
    - Stenges alt utstyr man ikke trenger?
    - eller minst mulig (for å starte raskt) – alt er jo Ex uansett…
  - Hvor lenge venter man med å stenge tennkilder?
    - Kan miste sikkerhetskritisk utstyr men som er fail safe
    - Tar risiko for å ”redde” brønn. Større villighet til å bruke BOP?

- Ikke ha fail-safe hvis det er for dyrt eller komplisert
  - shunt releer på høyspenningsmotorer, hydraulisk retur på NAS ventiler
- Tester det som er rimelig enkelt å teste, ikke nødvendigvis det som er best,
  - Full NAS test?
  - Full brannvannstest?

Vi prioriterer sikkerhet foran økonomi
- eller…?

- Hvor lenge opprettholder man produksjon ved delvis svikt i sikkerhetssystemene?
  - Eks: Automatiske NAS aksjoner ute av funksjon, hvor lenge driver man?
- ”Upraktisk” å opprettholde doble barrierer:
  - Isolasjon av prøvetakingsstasjoner mot prosessen – tungvint med 2 ventiler
- Sikker operasjon tar så lang tid…
  - Drenering av separator – venter man til den er helt trykkavlastet eller begynner man ”litt” før – dvs med potensiale for trykk i closed drain?

HMS styring: ”Vi følger jo bare kravene…..”

- Å følge regelverk er ikke det samme som om at alt er sikkert nok
- Bare følger kravene selv om man må skjønne at det ikke er godt nok.
- ”Sikkert område” på plattformen: Utslippet eller ulykken følger ikke områdeklassifieringen
  - Sikkerhetskritisk utstyr plassert “safe by location”. LIR rom med NAS funksjoner. NAS funksjon kan svikte ved behov, hva gjør man med det?
  - Ubeskyttede tennkilder i åpent “sikkert” område
  - Wireline/WO BOP kontrollenhet utenfor områdeklassifisering, men hva så?

-og følger kravene uansett om det er optimalt eller ikke…

- Vi gjør det fordi Ptil sier det, selv om det ikke nødvendigvis alltid er det beste
- Eks: Ptils krav til brannvannsdekning (10/20 l/m2min) følges uansett. Nyere forskningsresultater tilsier at det ikke nødvendigvis bare er vannmengden som er poenget. Allikevel vil man møte kravet, men er det optimal bruk av ressurser?
- Modifikasjoner på gamle anlegg etter nye regler:
  - Brannisolerer nye rør iht nye krav, men hva hvis det ikke hjelper noe på sikkerhetsnivået? (f.eks der nye og gamle rør ligger i nærheten av hverandre). Skal man heller bruke ressursene på noe annet eller oppgradere også alt gammelt?

Rene sikkerhetsdilemmaer

Når sikkerhetstiltak har en risiko

- Brannisolere prosessutstyr – korrosjon under isolasjon.
- Åpne områder gunstig for eksplosjon, lukkede områder gunstig for brann
- Tennkildekontroll:
  - Trippe ved gass i luftinntak til nødtavler. Eliminerer tennkilder men mister nødkraft (kun UPS).
  - Gass i luftinntak: Kobler ut alt elektrisk innenfor . Fail safe, men kan miste PSD, ekstern radiokommunikasjon etc
- Skip på kollisjonskurs: Trykkavlaste prosessen, men via NAS trippes radar.
- Trykkavlastning: Venter til alle seksjoneringsventiler er lukket. Feil hindrer dermed trykkavlastningen. (Løsning: Start uansett)

HMS-styring: Løser sitt eget problem men ikke virkeligheten…

- Skal man sette fokus på et sikkerhetsproblem eller ignorere det?
  - Tenk om det går bra allikevel, så unngår man kostnadene og ubehagelig fokus.
- Et designproblem oppstår under prosjektering. Nødvendig endring er dyr eller forsinker. Overfører problemet til drift , men det finnes ingen god løsning.
- Gjør man realistiske forutsetninger for designen ?
  - Eks: PFP på rør, påføringsprosedyrer og korrosjon.
- Bruk av ny teknologi:
  - Alle vil ha den men ingen tør å være først ute

- Kunde-leverandør:
  - Alle ser at løsningen er for dårlig og vet hva som bør gjøres, men ingen vil betale (mener den andre bør)
  - Skal man uansett følge kontraktuelle spilleregler eller er det situasjoner som krever at man først løser problemet og deretter diskuterer regningen?

HMS – styring: Bedre kunnskap om design

Hva gjør man da?

- Begrenset kunnskap tilsier mer konservatisme
- Øket kunnskap tilsier bedre sikkerhet eller….?
  - Eks: Øket kunnskap om materialer og bedre strukturelle beregningsprogrammer medfører lavere sikkerhetsfaktorer.
  - Øket kunnskap kan brukes til å fjerne ekstra robusthet – “slankere design” – men mindre sikkert

- Vel og bra så lenge man har kontroll på det som fjernes. Men hva hvis man tar feil?
  - Enkle analyser – få feilmuligheter men de kan være store.
  - Kompliserte analyser – mange feilmuligheter
  - Forutsetningene sviktet (men analysen var korrekt)
  - Kan medføre redusert robusthet overfor det uforutsette

ALARP – ”kost-nytte” vurderinger av sikkerhetstiltak

- Mange av dilemmaene er egentlig en variant av ALARP (gitt at man følger regler og krav).
- Typisk for situasjonen:
  - Kostnadene kommer med en gang og “belaster” f.eks engineering. Motivasjon?
  - Man ser ikke nødvendigvis gevinsten, for det gikk jo ikke galt, den kommer kanskje aldri….
  - Hvis ulykken kommer er det lenge etter kostnadene og drift får “regningen”, og hadde ingen påvirkning.

Risikobasert styring – tveegget sverd…..?

- Er det tilstrekkelig å styre etter risikonivået (dvs gjennomsnittet)? Hva hvis det er hendelser med svært stor konsekvens og svært lav frekvens?
  - Eks: Innløfting av en ny modul over en lang trykksatt rørledning. Selv om RA viser aksept ift kriterier, skal man likevel trykkavlaste rørledningen?
  - Hva hvis konsekvensen av drop betyr at selskapet er ”out of business”?

Risikoparametre kan lure….

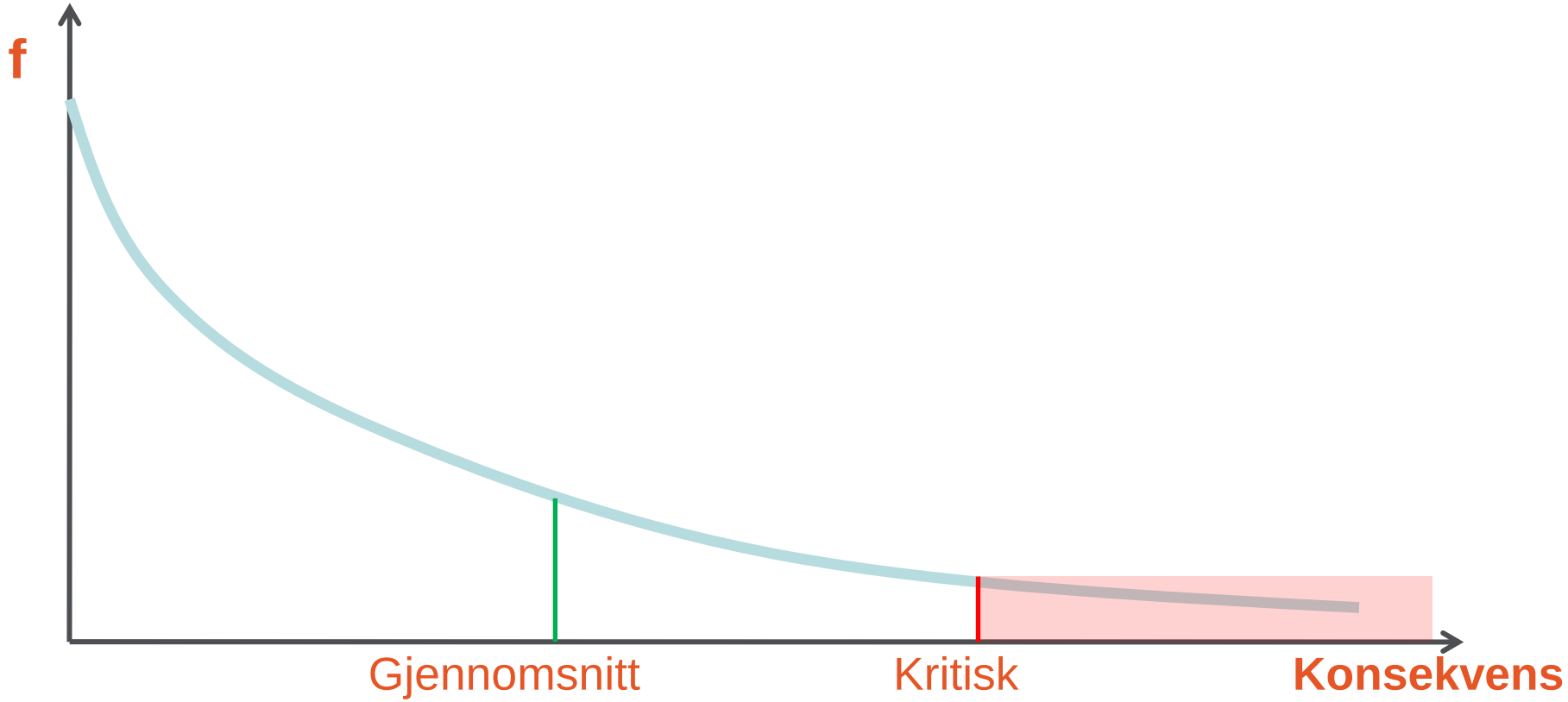
- Er risikobildet nyansert nok – bruker vi de relevante risikoparametrene?
- Har risikobildet de riktige trendene?

  Eks: Øket bemanning i boligkvarteret på en installasjon:

  - Flere personer om bord – potensielt flere drepe ved ulykker (PLL)
  - Men gjennomsnittelig dødsrate (FAR) avtar fordi bemanningsøkningen kommer i et lavrisiko område

- Hva gir egentlig en RA et bilde av?
  - Ulykkesfrekvens over en stor samling av anlegg f – 10^{-n} som om ulykker er probabilsitiske
  - Men ulykker er deterministiske - for det anlegget der ulykken skjer var egentlig P = 1 før ulykken, RA tror f er 10^{-n}.

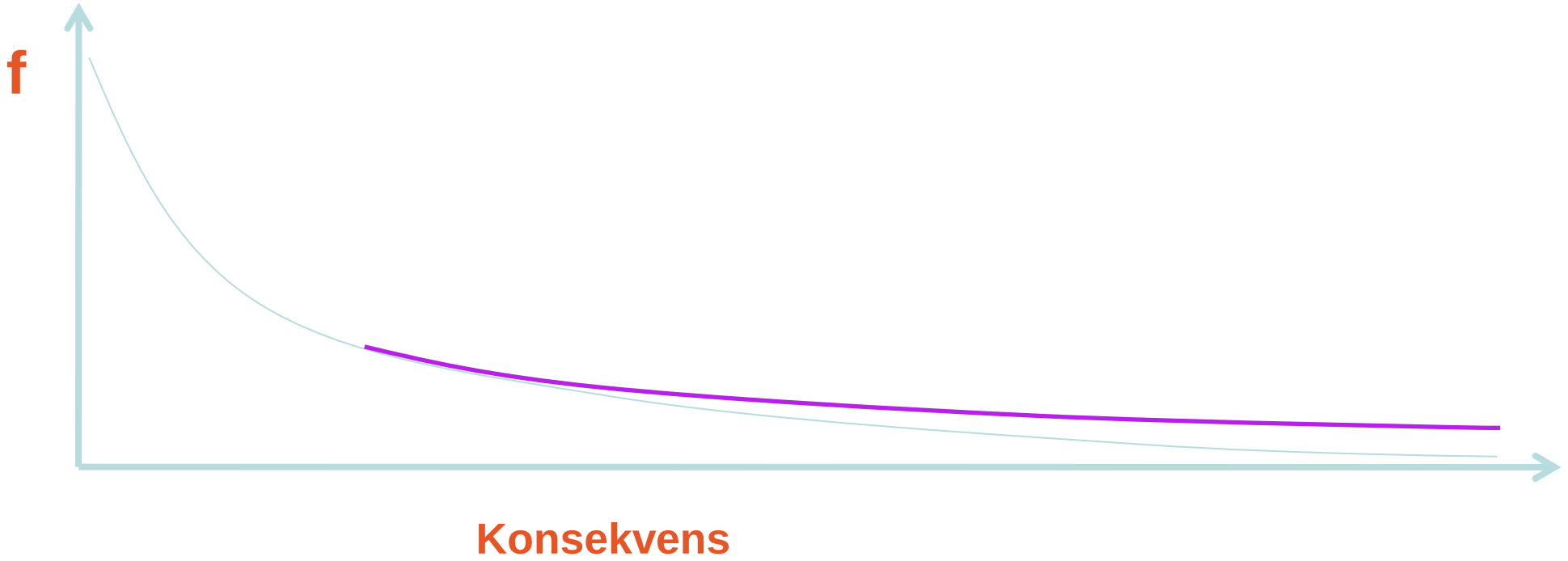
Gjennomsnittsverdier - fallgruber



Sjeldne hendelser -usikkerhet

- RA har en iboende usikkerhet – RA gjør man fordi man ikke vet….
- Usikkerhet pga kjente situasjonener som er eksludert pga “lav sannsynlighet”
  - “Dobbelt jeopardy” fallgruben – de fleste storulykker har “multiple jepoardy”.
- Ukjente eller uventede hendelser som derfor aldri er tatt med som likvel har vist seg å kunne skje – “Black Swans”, the “Unknowns Unkowns”
  - RA reflekterer bare historien – det man har erfart kan skje.
  - Det uventede kan være en overraskelse for RA også.
  - Hvordan klare å prediktere når man avviker fra historien?

Underestimering av ”multiple jeopardies”

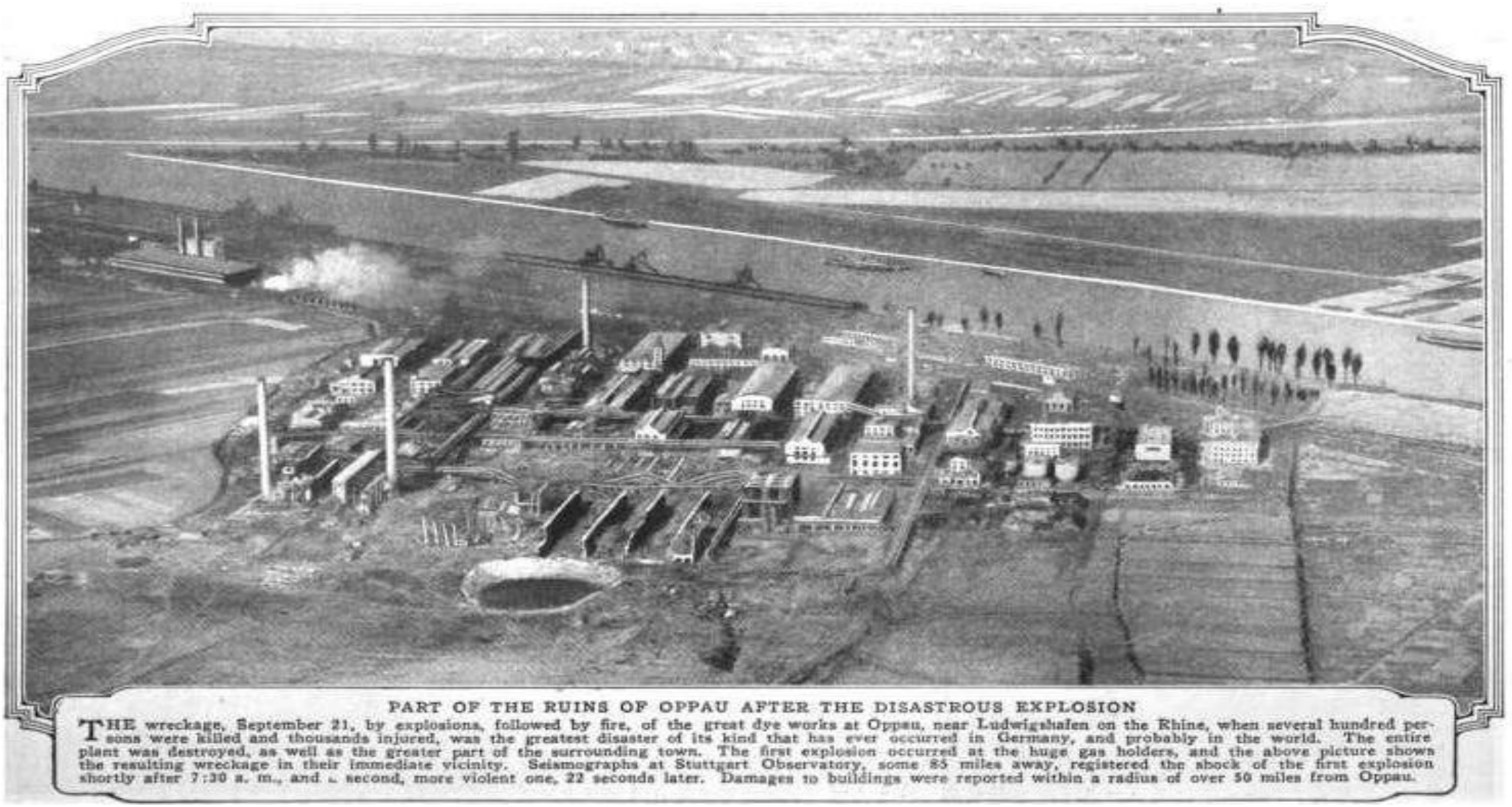


UFA eksplosjon (1989) – 565 drepte

”Black Swans” – de ukjente usikkerhetene

- Noe helt uforutsett - helt utenfor vanlig erfaring da ingen ting i fortiden kan indikere muligheten på en overbevisende måte
- Ekstrem konsekvens
- I etterpåklokskapens lys var alt forutsigbart
- Men ofte var det noen ett eller annet sted som likevel visste..

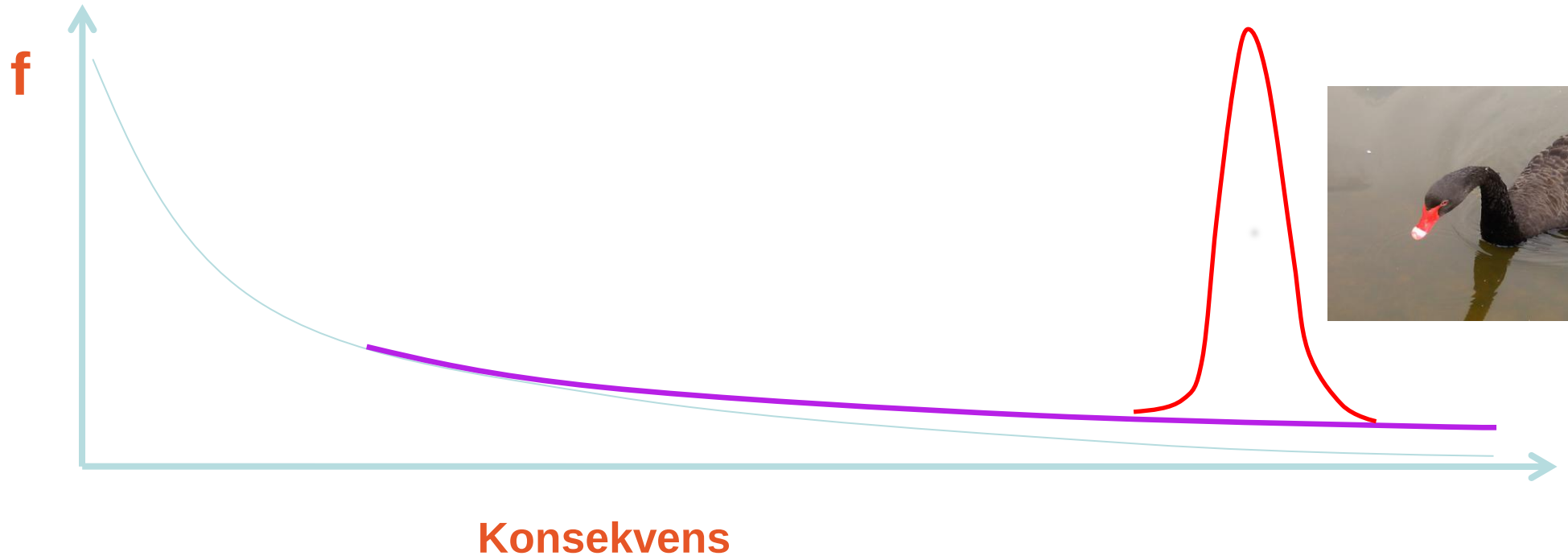
Oppau, Germany 1921. 561 drepte
4500 tonn ammonium sulfate/nitrate



PART OF THE RUINS OF OPPAU AFTER THE DISASTROUS EXPLOSION

THE wreckage, September 21, by explosions, followed by fire, of the great dye works at Oppau, near Ludwigshafen on the Rhine, when several hundred persons were killed and thousands injured, was the greatest disaster of its kind that has ever occurred in Germany, and probably in the world. The entire plant was destroyed, as well as the greater part of the surrounding town. The first explosion occurred at the huge gas holders, and the above picture shows the resulting wreckage in their immediate vicinity. Seismographs at Stuttgart Observatory, some 85 miles away, registered the shock of the first explosion shortly after 7:30 a. m., and a second, more violent one, 22 seconds later. Damages to buildings were reported within a radius of over 50 miles from Oppau.

Black Swans – De ”ukjente” usikkerhetene



Robusthet

- Risikobasert styring gir ikke robusthet overfor uforutsette hendelser, for de er ikke identifisert eller med i risikobildet.
- Skal man legge inn ekstra robusthet selv om det ikke synes i risikoblidet?
- Sunne designprinsipper gir derimot ofte robusthet, f.eks:
  - Etabler et minimum av tekniske barrierer uansett risikobilde
  - “Inherently safe”
  - 2 funksjonelt forskjellige og uavhengig barrierer vs 2 like barrierer.
  - Uavhengighet mellom kontroll og sikkerhetssystemer i motsetning til integrert system.
  - Fullt shutintrykk på manifold i stedet for pålitelighet av 20 stengeventiler og PSV?
- Beredskap: Tren også på at noe helt uforutsett og “utenkelig” skjer.

Tar man så de riktige valgene?

- Det er ikke alltid entydig hva som er riktig, rettferdig eller optimalt.
- I realiteten er det et verdivalg, og hvor står man da?

  Det er holder ikke alltid å gjemme seg bak at man følger regler/krav fordi:
  - Disse er ikke alltid entydige, man må ta standpunkt til hvor i gråsonen man vil være.
  - Krav og regelverk plukker ikke opp alt, dvs man må gjøre en selvstendig vurdering allikevel.
- Enkel retningslinje….?:
  - Er man villig til å ta risikoen selv?
    - Eks: Testing av russiske jernbanebroer
  - Er man villig til å la sine nærmeste ta risikoen ?
    - Eks: Lokalisering av bolig for ICI fabrikkdirektører

- ”Riktig” valg forutsetter tilstrekkelig kunnskap om og forståelse av risikoforholdene:
  - Har man de riktige spesialistene eller skal alle være generalister?
  - T. Kletz: ”De visste ikke hva de ikke visste…”

For more information, please contact:

Jan A. Pappas
Sjefskonsulent

LR Consulting AS, Sandvika

T +47 9527 6232
E jan.pappas@lr.org
W www.lr.org
w

First name Last name
Position
Unit/ Department
T +xx xx E xxxxx.xxxxx@lr.org

Lloyd's Register Consulting
www.lr.org/consulting

Working together
for a safer world