Kapittel 19 – Risikostyring

Risiko defineres ofte ved å besvare følgende tre spørsmål:

* Hva kan gå galt?
* Hvor sannsynlig er det? (eller hvor ofte skjer det?)
* Hva er konsekvensene?

# Risikostyring

«Å hindre at det som gå galt gjør det»

«The process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure» (Institute of Risk Management»

Prosess betyr her måten man jobber på – støttet av : prosedyrer, planer, verdier, holdninger, kultur, ledelsesfokus osv.

# Årsaker (til feil)

Årsakene kan være knyttet il:

* Prosjektgjennomføring
* Finansielle vurderinger
* Egenskaper ved produkter som kan skade personer og miljø
* Hendelser som kan påvirke en bedrifts leveranseevne
* Hendelser som kan medføre store ulykker
* ++

# Hvorfor er risikostyring viktig?

Storulykkesperspektivet

* Vi ønsker å unngå store ulykker som kan gi tap av menneskeliv, skade på miljø og skade på verdier av stor viktighet for samfunnet.

Produktsikkerhet

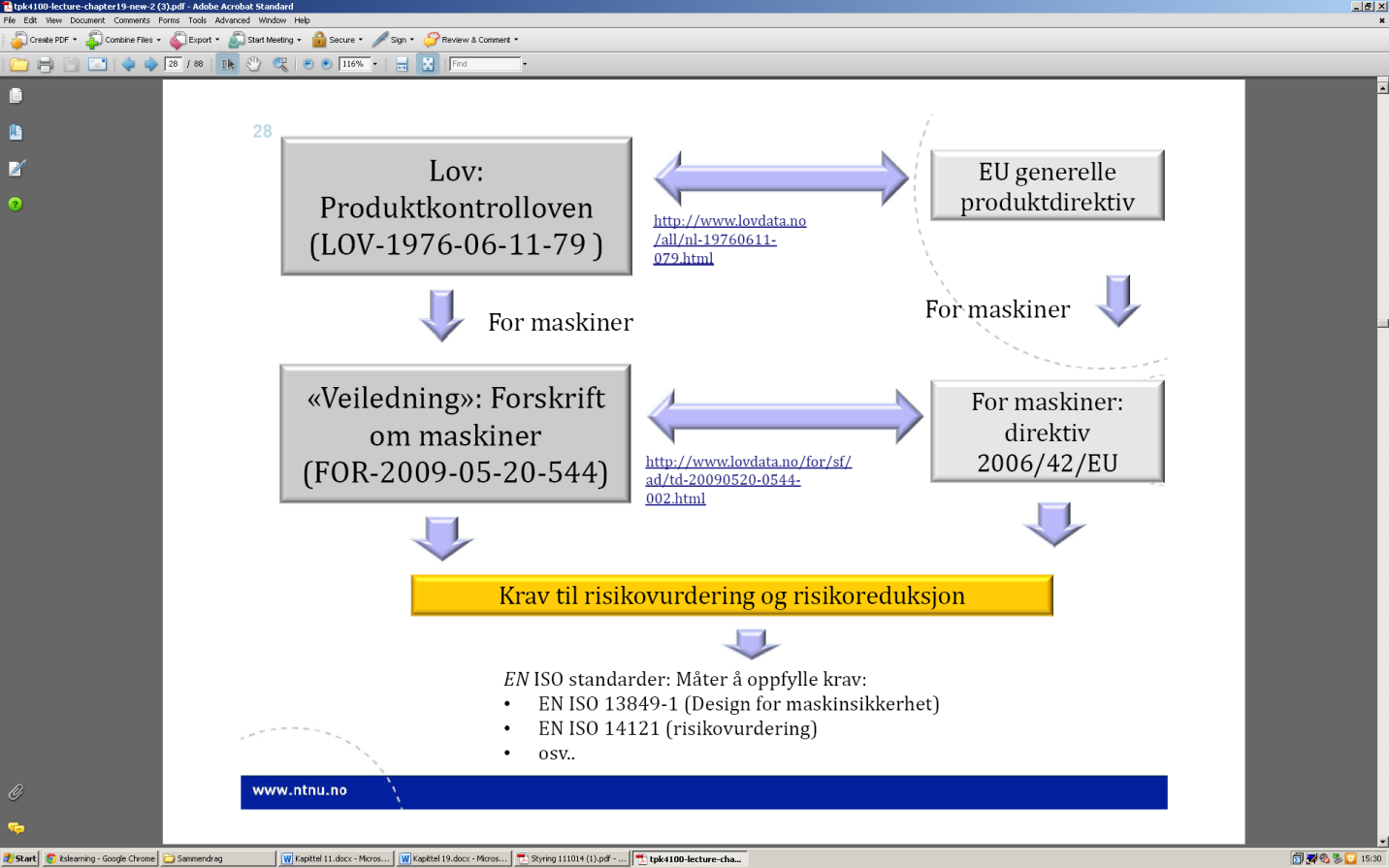
* Vi ønsker å beskytte forbrukere fra å bli skadet av produkter som sendes ut på markedet

Arbeidernes sikkerhet

* Vi ønsker å beskytte arbeidstakere fra å bli skadet under produktfremstilling

# Risikostyring i bedrifter

Risikostyring (produktsikkerhet og sikkerhet for arbeidstakere) er påkrevd i bedrifter gjennom lover og gjennom standarder som er referert i lover.



# Prinsipper for risikostyring

Risikostyring er ingen enmannsjobb og må bakes inn i måten bedriften drives på.

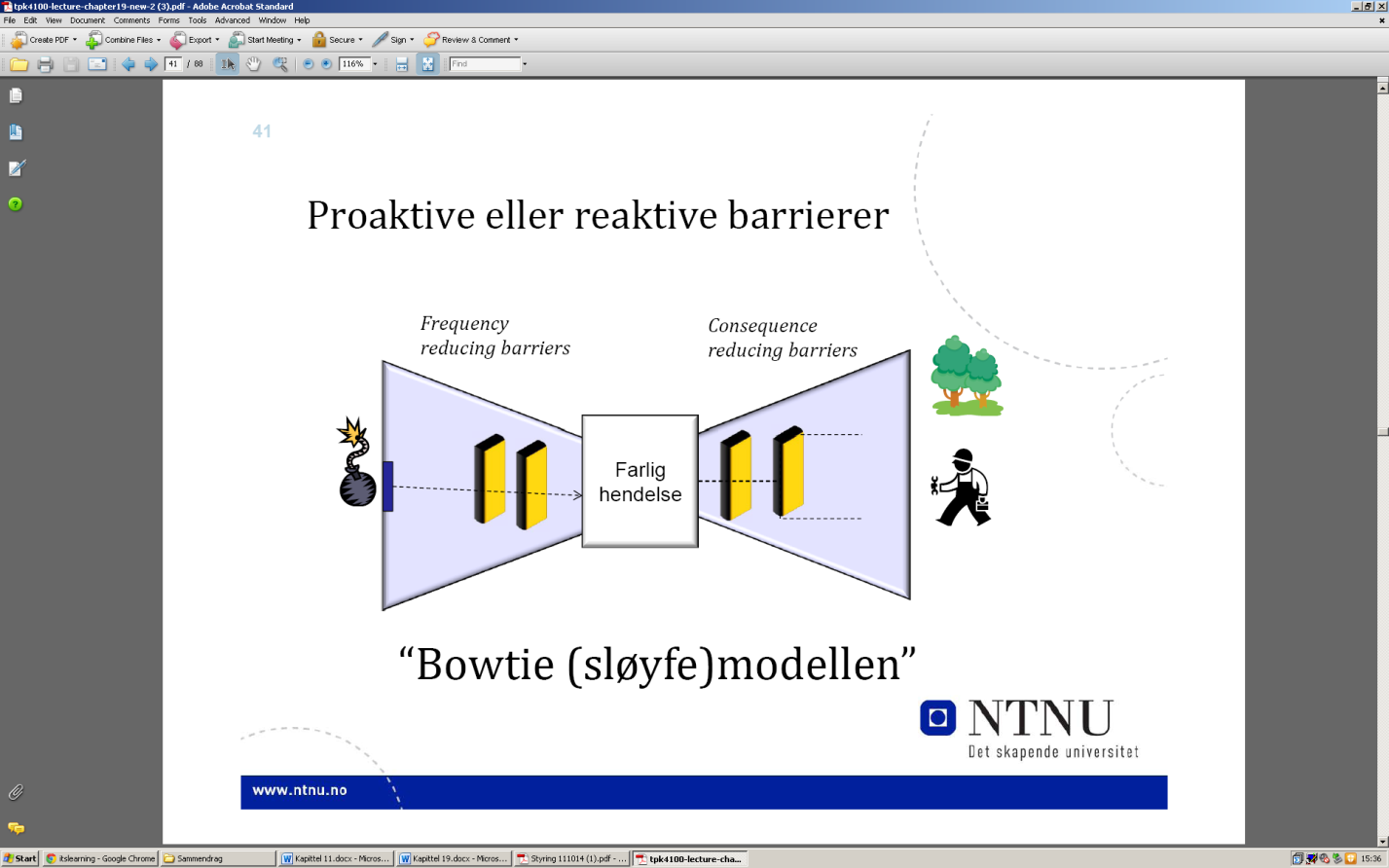
Syv prinsipper foreslås:

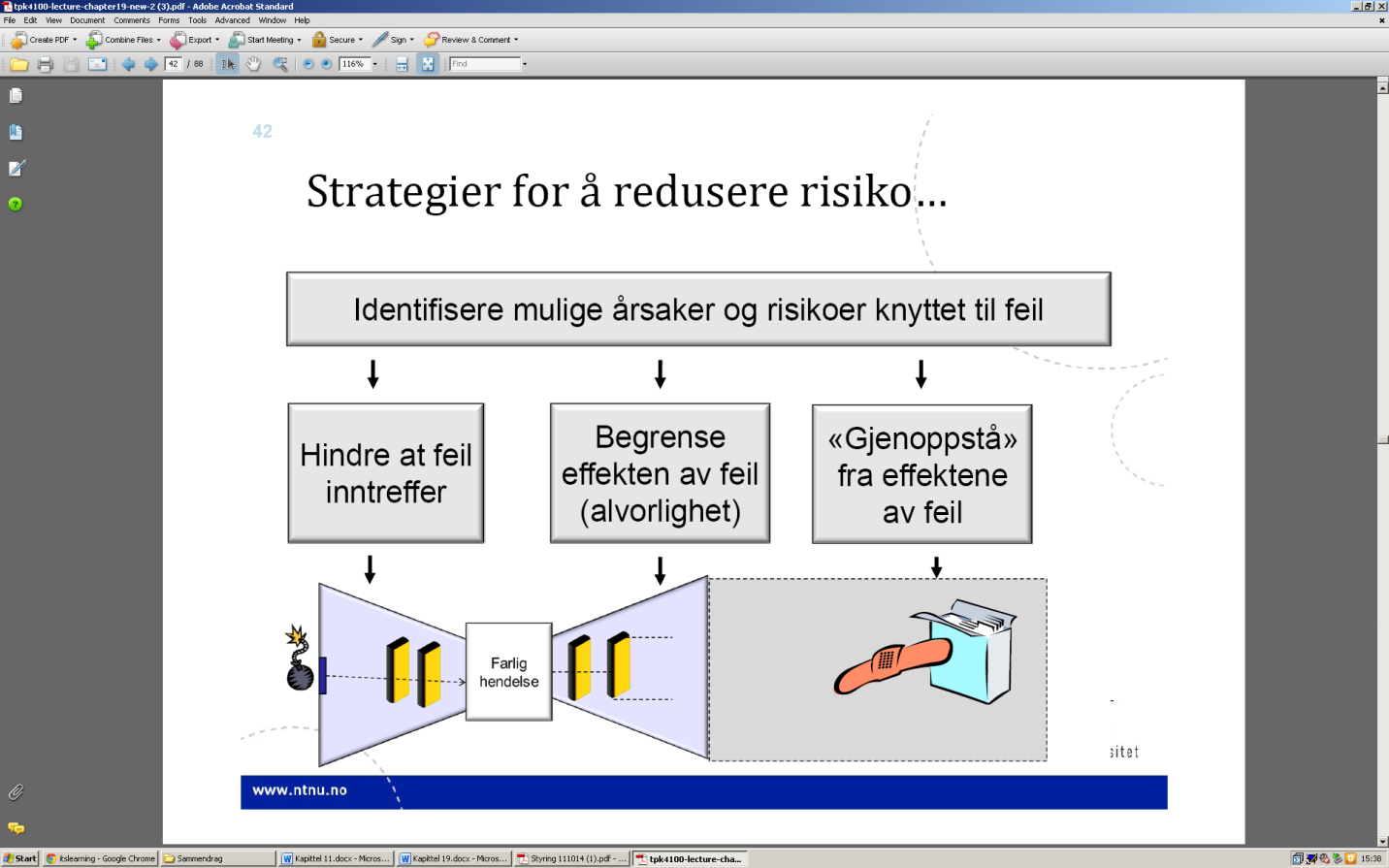
1. Bedriftsperspektiv
   * Se på utvikling som i konteksten til strategiske mål
   * Ledelsen og bedriften ser viktigheten av å ha kontroll med risiko («oppside» og «nedside»
2. Fremtidsrettet syn
   * Vurderer usikkerhetsmomenter frem i tid og tar dette inn i bedriftens aktiviteter og prosjekter
3. Åpen kommunikasjon
   * Oppmuntre til fli flyt av informasjon i og mellom nivåer
   * Legge til rette for formell, uformell og improvisert kommunikasjon.
   * Bruke prosesser som verdsetter den individuelle stemmen
   * Identifikasjon og kontroll med risiko krever «fri flyt» av kommunikasjon – opp og ned i organisasjonen
4. Integrert med øvrige aktiviteter
   * Risikostyring kommer ikke i tillegg, men er innbakt i både formelle prosesser og kultur
   * Bruke metoder og verktøy for risikostyring i prosjekters infrastruktur
5. Kontinuerlig prosess
   * Risikostyring er ikke en «av og på»-aktivitet, men må foregå kontinuerlig
   * Indentifisere og styre risikoer gjennom alle endringsfaser
6. Delt visjon
   * Gjensidig visjon basert på felles mål, delt eierskap og kollektiv kommunikasjon
   * Alle må ha en delt forståelse av hvorfor risikostyring er viktig og se resultater som god risikostyring (eller mangel på dette) medfører.
   * Fokus på resulater
7. Teamarbeid
   * Få til en kultur der man jobber sammen om risikostyring. Krever også ferdigheter i forhold til dette.

# Strategier for å redusere risiko

Risiko kan reduseres ved bruk av **barrierer**. Men barrierer er ikke perfekte. Vi trenger derfor å bestemme påliteligheten til barrierene.

Vi kan kategorisere barrierer som enten proaktive eller reaktive, som enten forhindrer at hendelser oppstår eller som reduserer konsekvensene av dem – Bowtie-modellen.



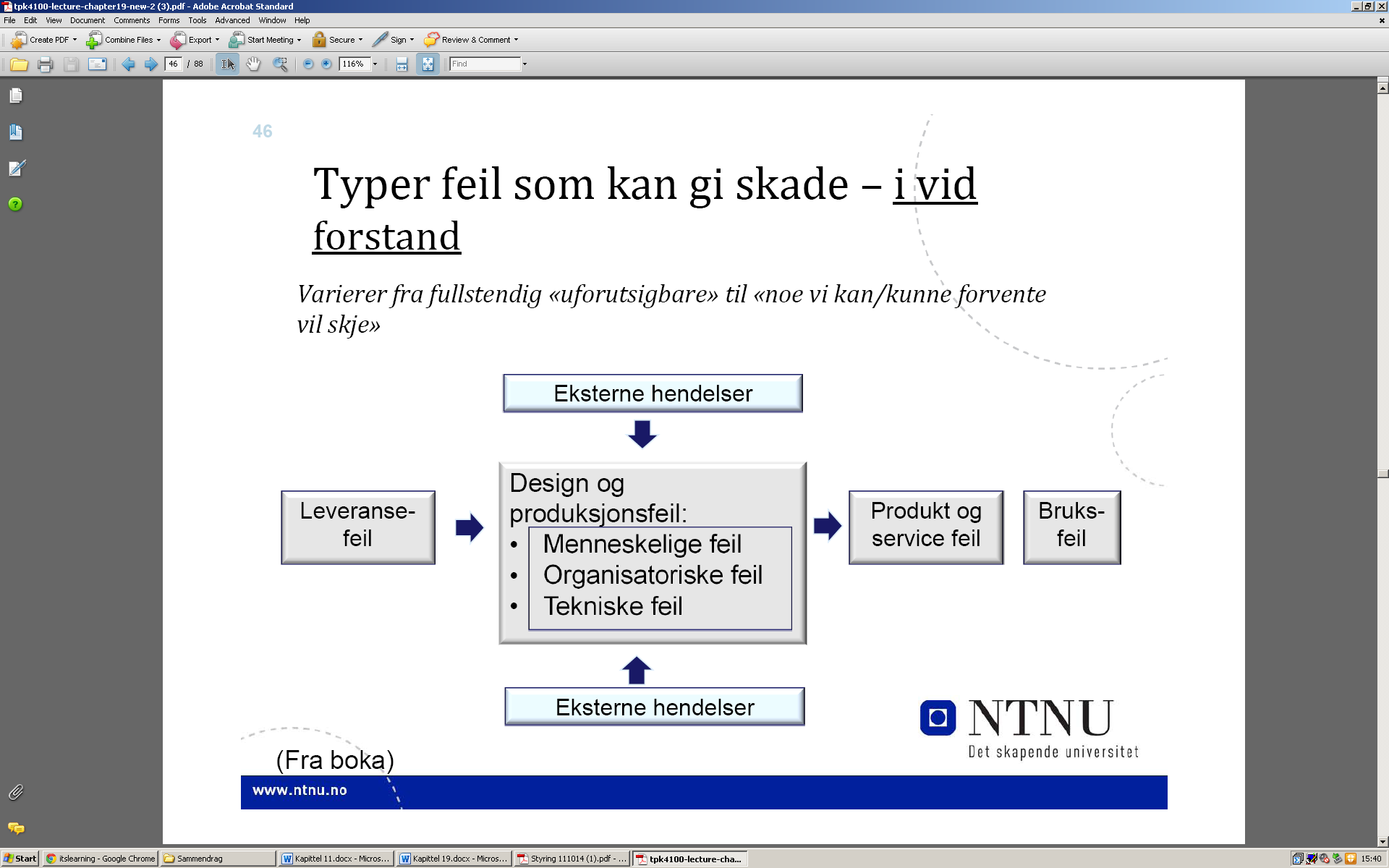


Tiltak må bygge på grundige analyser

* Hva kan gå galt?
* Hvor ofte skjer det?
* Hva er konsekvensene?

# Analysere hva som kan gå galt

Typer feil som kan gi skade varierer fra fullstendig uforutsigbare til noe vi kan /kunne forvente vil skje. De fleste feil forårsakes av noe som kan unngås. Som et minimum startpunkt vil en enkel sjekkliste for årsaker til feil være nyttig. Roten til feil er vanligvis menneskelig feil av en type.



**Leveransefeil** er feil i timing eller kvalitet på varer og tjenester som leveres til operasjonen. Global sourcing betyr vanligvis at deler sendes rundt om i verden på reisen gjennom verdikjeden. Samtidig opplever mange industrier økt flyktighet i etterspørsel. Det mest signifikante er muligens en tendens til at det stadig blir mindre lagre i verdikjeder som kan fungere som buffer for forstyrrelser i leveranser.

«Potentially the risk of disruption has increased dramatically as the result of a too-narrow focus on supply chain efficiency at the expense of effectiveness» (Christopher, 2002).

Leveransefeil omhandler også tidsforsinkelser på grunn av transport og tap av kritiske systemer (Energi, IT).

**Menneskelig svikt**

Det er to hovedtyper menneskelig feil. Den første er når nøkkelpersonell slutter, blir syk, dør eller på en annen måte ikke kan gjøre sin rolle. Den andre er når mennesker gjør jobben sin, men gjør feil. Å forstå risikoen ved den første feilen vil være å identifisere nøkkelpersonene som operasjonen vil slite uten. Menneskelige feil gjennom «mistakes» kommer også i to typer: errors og violations.

* Error
  + Feiltolkning
  + Personen burde gjort noe annerledes
* Violation
  + Overtredelse/unnlatelse
  + Handlinger som klart står i motsetning til definerte prosedyrer for operasjonen.

Katastrofale feil kommer ofte av en kombinasjon mellom errors og violations.

Andre menneskelige feil er:

* Error of commissioning: Gjør det, men gjør det feil
* Error of omission: Lar være å gjøre det
* Onsinnet handling
* Å overse relevant informasjon

**Organisatoriske feil**

Er feil ved prosedyrer og prosesser og feil som kommer fra en virksomhets organisatoriske struktur og kultur. Er en stor potensiell kilde til feil og inkluderer nesten all operasjon- og prosesstyring. Spesielt trengs feil i design av prosessen og feil i ressursbruken til prosessene å undersøkes.

* Underliggende forhold som kan medføre at mennesker gjør feil
* Mangel på prosedyrer
* Mangel på god kultur og verdier
* Mangelfull allokering av ressurser
* Mangelfull opplæring

**Tekniske (produksjonsrelaterte) feil**

* Alt av tekniske feil som kan bidra til produktet feiler
  + Feil i IT-systemer
  + Feil i maskiner og ustyr
  + Feil i styringssystemer
  + Feil innstilling av maskiner

**Feil ved design til produkt eller tjeneste (Produktfeil)**

I desingstadiet kan et produkt eller tjeneste se fin ut på papirer og feil bli tydelige når den kommer ut i virkeligheten. I løpet av designprosessen skal potensiell risiko for feil identifiseres og designes ut, men er ikke alltid dette skjer. Noen ganger kommer dette av trade-off mellom rask produkjon- og leveringstid til markedet og risikoen for at produktet eller tjenesten feiler i operasjonen. Ingen virksomheter kan holde på et produkt eller tjeneste uendelig lenge for å eleminere en hver risiko for feil….

* På grunn av designfeil, men oppdaget etter det er kommet på markedet
* Mangelfull testing og analyse
* Medfører ofte behov for tilbakekalling
* Forbundet med høye kostnader

**Forbrukerfeil**

* Ikke utstyret som er feil, men bruken av det medfører feil
  + Har ikke lest bruksanvisning
  + Bruker bevisst produktet feil
* Produsent ikke fri for ansvar
  + Må påse nok informasjon og kundeveiledning
* Produsenter vil uansett rammes dersom forbrukere anser produkter som «dårlige»

**Miljøpåførte skader/eksterne forhold**

Inkluderer alle årsaker til feil som ligger utenfor en operasjons direkte påvirkning.

* Ikke utstyret som er feil, men eksponering fra miljø og eksterne hendelser
* Utenfor produsentens kontroll
  + Terrorisme
  + Store miljøkatastrofer
  + Uvær
  + Politiske hendelser
  + Datavirus

**Feil og tap på grunn av manglende IT-sikkerhet**

* Feil påført produktet eller produsent med hensikt
  + Spionasje
  + Terror
  + Introdusere feil – oppnå status
  + Introdusere feil – påføre konkurrenter skade
* Er en trade-off mellom å tilby bedre tilgang gjennom internett og sikkerhetsspørsmålene det genererer.
* Tre utviklinger har forsterket spørsmål ved e-sikkerhet
  + Økt «connecitvity» betyr at alle potensielt kan «se» alle andre. Operasjoner ønsker å gjøre systemer og informasjon mer tilgjengelig for interne ansatte, business-partnere og kunder (ERP)
  + Tap av perimeter-sikkerhet når flere mennesker jobber hjemmefra eller gjennom mobil kommunikasjon.
  + For noen nye (av og til uregulerte) teknologier, som mobile nettverk, tar det tid å oppdager alle mulige risikokilder. Internett er et åpent system og den raske utviklingsraten av nytt software og systemer betyr ofte at brukerne ikke har tilstrekkelig kunnskap om softwaren og systemers arkitektur. Dette gjør brukere ikke nødvendigvis er klar over potensielle sårbarheter som lede til betydelige sikkerhetsbrudd.

# Hvordan identifisere hva som kan gå galt?

For å finne frem til hva som kan gå galt kan man bruke sjekklister, for eksempel med utgangspunkt i standarder (ISO)

Failure modes, effecs and critical analysis (FMECA). Identifiserer hvordan utstyr kan feile (feilmode) i ulike operasjonsmodi, tilhørende feilårsaker, muligheter for deteksjon og feileffekter (konsekvenser).

Risk priority number (RPN) kan brukes for å rangere kritikaliteten av en feilmode og dermed prioritering av tiltak

# Analysere hvor ofte det skjer (eller sannsynlighet for feil)

Feilestimater basert på historisk informasjon kan måles hovedsakelig på tre måter: feilrater – hvor ofte en feil inntreffer, pålitelighet – sjansene for at feil skjer, og tilgjengelighet – mengden tilgjengelig operasjonstid.

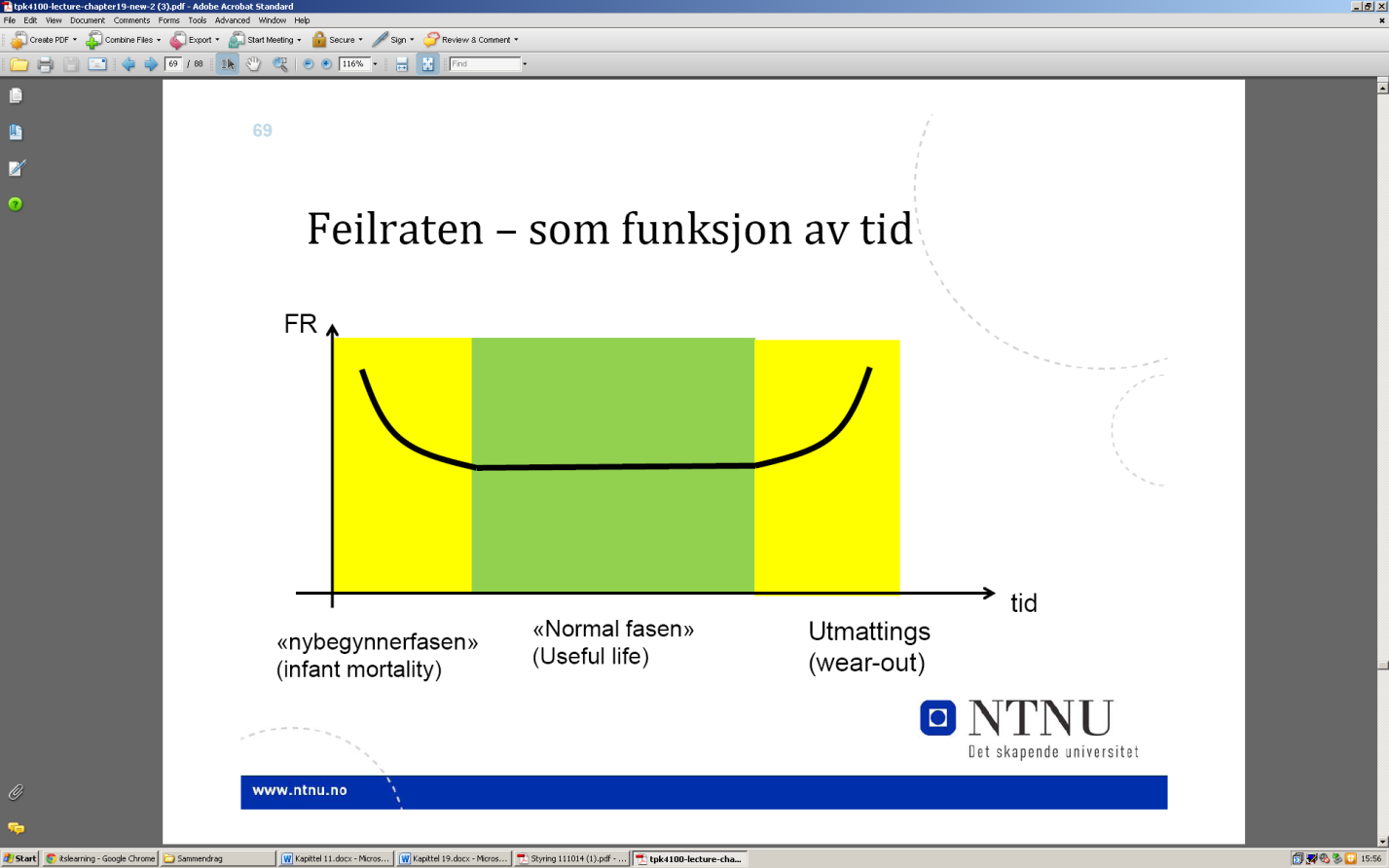
Feilrate og pålitelighet måler begge tilbøyeligheten en operasjon eller en del av en operasjon har til å feile .Tilgjengeligheten er et mål på konsekvensene av feil for operasjonen.

## Feilrate

**Feilrate (FR)** brukes for å si noe om hvor ofte noe feiler. Beregnes først for hver komponent, deretter for hele systemet. Kan måles enten som prosent av totalt antall produkter som testes eller som antall feil over tid.

### Badekar-kurver

Når funksjon er en funksjon av tid. Kurven beskriver sannsynligheten for denne typen feil. I begynnerfasen oppstår feil på grunn av defekte deler eller upassende buk. I normalfasen er feilraten normalt lav og mer eller mindre konstant og feilene kommer av normale og tilfeldige faktorer. I utmattingsfasen øker feilraten når delen går mot slutten av sitt fungerende liv og feil oppstår på grunn av aldringen og slitasjen til delene.



Når vi gjør pålitelighetsvurderinger, antar vi ofte at vi er i normalfasen. Det vil si at FR er konstant og uavhengig av tid. Når feilraten er konstant vil vi samtidig kunne anta at

## Pålitelighet

Pålitelighet måler evnen til å prestere som forventet over tid. Vanligvis vil alvorlighetsgraden til en feil bestemmes delvis av hvor avhengig de andre delene av systemet er. Vi har et behov for en pålitelighetsmodell – det vil si et diagram som sammenstiller årsaker til feil, eventuelt en modell for betingelser for at funksjonen virker. Dette kalles pålitelighetsnettverk.

Med interdependence vil en feil i en komponent gjøre at hele systemet feiler. Så dersom et interdependent system har *n* komponenter med hver sil pålitelighet, Ri vil påliteligheten til systemet være gitt ved:

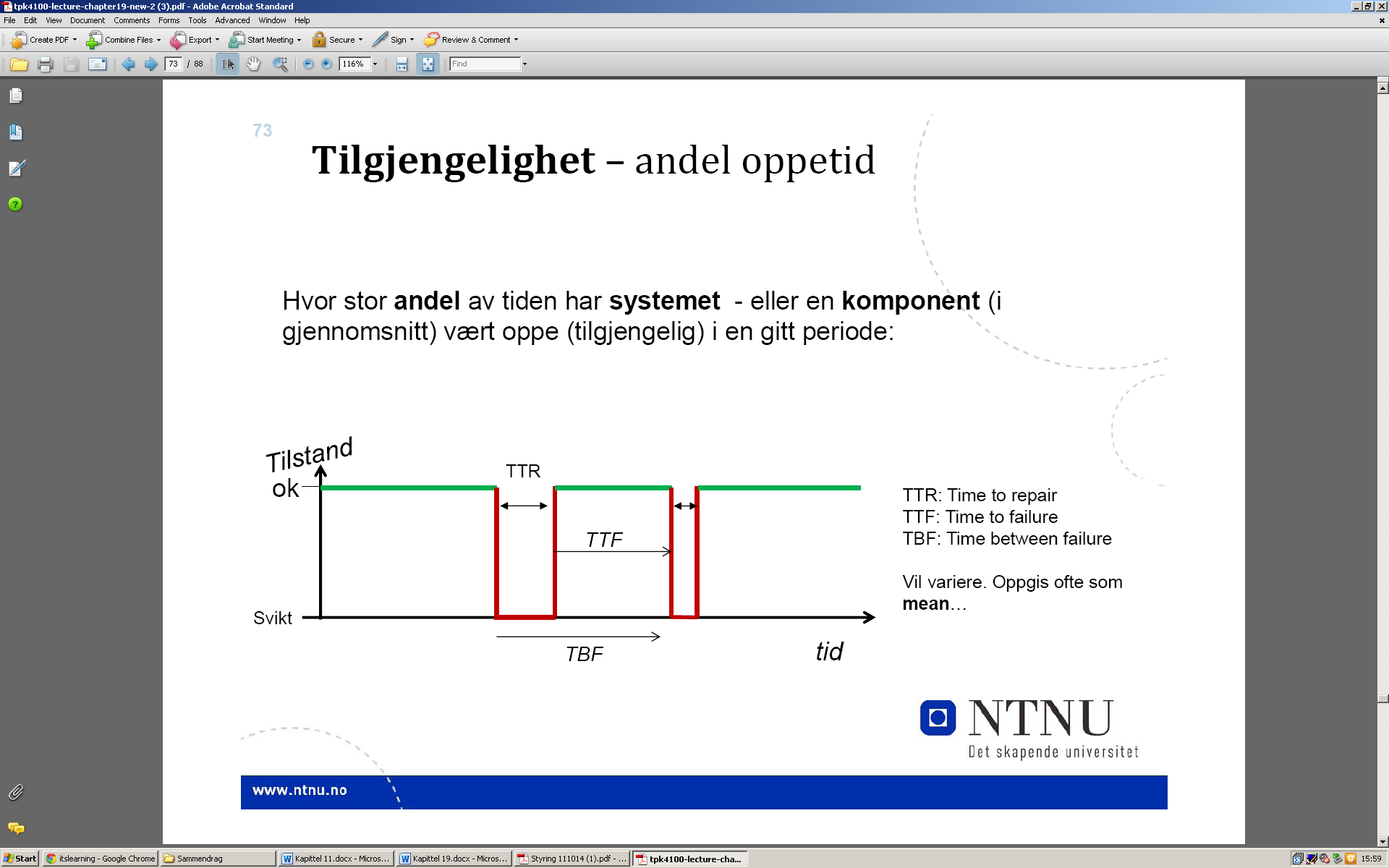
Ved parallelkoblede systemer får vi:

## Gjennomsnittstid mellom feil (MTBF)

Et vanlig mål på failure. MTBF er den inverse til feilrate (i tid)

## Tilgjengelighet

Hvor stor andel av tiden har systemet eller en komponent i gjennomsnitt vært oppe (tilgjengelig) i en gitt periode. En operasjon er ikke tilgjengelig viss den har feilet eller blir reparert på grunn av feil. Gjennomsnittlig tilgjengelighet brukes for å indikere operasjonstid ekskludert konsekvensene ved feil:

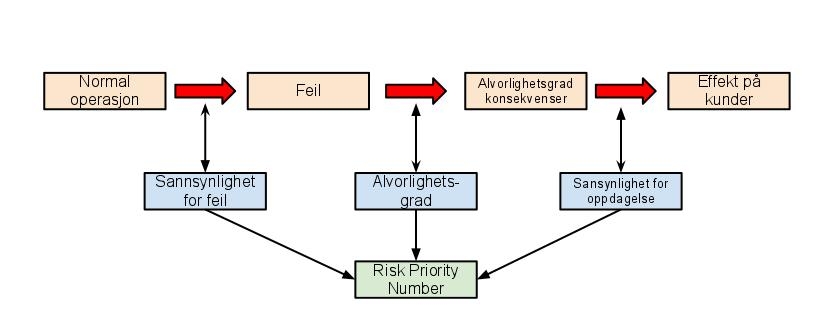


# Failure mode and effect analysis (FMEA)

Er en av de mest kjente tilnærmingene til å vurdere den relative signifikansen til feil. Dens mål er å identifisere faktorer som er kritiske for ulike typer feil for å kunne identifisere feil før de inntreffer. Dette gjør den ved en sjekkliste-prosedyre som er bygget rundt nøkkelspørsmålene for en hver mulig årsak til feil

* Hva er sannsynligheten for at feil vil skje?
* Hva vil være konsekvensene av feilen være?
* Hvor sannsynlig er det at en slik feil oppdages før den når kundene?

Basert på en kvantitativ evaluering av disse spørsmålene vil en risk priority number (RPN) kalkuleres for hver potensiell årsak til feil. Korrigerende handlinger rettet mot å forhindre feil blir så innført for de årsakene som RPN indikerer at krever prioritet.



# Analysere konsekvenser

Vi må starte med å spørre om for hvem eller for hva gjør konsekvensene seg gjeldende (personer, miljø, økonomi, kritisk infrastruktur, politiske forhold).

Personer er ikke en kategori

1. person: arbeidstakere
2. person: midlertidig «besøkende»
3. person: de som bor rundt
4. person: fremtidige generasjoner

Graden av hva vi aksepterer reduseres når graden av frivillighet minker. Aksepterer større ulykkesrisiko for arbeidstakere enn for fremtidige generasjoner.

# Tiltak som kan redusere alvorlighet

* Deteksjon før det som kan gå galt inntreffer
* Deteksjon før hendelsen utvikler seg til en alvorlig konsekvens

Vet deteksjon kan man

* Korrigere feil før de får en fatal konsekvens
* Igangsette konsekvensreduserende tiltak (evakuering, informasjon til forbrukere, tilbakekallinger)

# Forhindre at feil skjer

Når en god forståelse av årsaker og konsekvenser av feil er etablert er ansvaret til operasjonens managers å prøve å forhindre at feil skjer. Den åpenbare måten å gjøre dette er å systematisk vurdere en hver prosess som er involvert og designe ut alle feilpunkt. Mange av tilnærmingene brukt i kapittel 4, 5 og 17 kan brukes til dette.

## Redundans

Å bygge inn en redundans i en operasjon betyr å ha et back-up system eller komponenter i tilfelle feil. Det kan være kostbart og brukes generelt når breakdown kan ha kritiske konsekvenser. Det betyr å doble eller triple noen deler av prosessen eller systemet i tilfellet en komponent feiler. Påliteligheten til en komponent sammen med dens back-up er gitt av summen av pålitelighetene til den originale komponenten og sannsynligheten for at back-up komponenten vil trenges og virker.

)

Redundans brukes ofte for servere hvor tilgjengelighet til systemet er spesielt viktig. Industrien bruker tre typer redundanser:

* Hot standby
  + Når både primær- og sekunder (back-up) systemer går samtidig. Data kopieres til sekundær server slik at begge systemene inneholder identisk informasjon
* Warm standby
  + Det sekundære systemet går i bakgrunnen til hovedsystemet. Data kopieres til sekundær server ved gjevne mellomrom
* Cold standby
  + Det sekundære systemet brukes bare når primærsystemet feiler.

## Fail safe - Å feile sikkert

Konseptet kommer fra Japanske metoder for operasjonsforbedrelser. Kalles poka-yoke (yokeru – forhindre, poka, utilsiktede feil) og er basert på prinsippet om at menneskelige feil til en grad er uunngåelig. Det som er viktig er å forebygge at de blir defekte. Poka-yokes er enkle verktøy eller systemer som inkorporeres i prosesser for å at uunngåelige operatørfeil resulterer i defekter.

Et viktig prinsipp for design av sikkerhetskritiske systemer, for eksempel jernbane signalanlegg, er å bytte systemet «fail safe». I praksis betyr dette at systemet og anlegget det beskytter automatisk går til en feilsikker tilstand. For signalanlegg betyr det at alle feil skal medføre rødt lyssignal.

Fail-safeing

* Et konsept som går utover «fail safe»-design
* Poenget er å redusere effekten av menneskelige feil
* Omfatter virkemidler i vid forstand som kan redusere sannsynligheten for skade eller økonomiske tap i forbindelse med bruk av produkter/utstyr:
  + Tydelig merking
  + Interlock som hindrer feil rekkefølge i utførelse av aktiviteter
  + Prosedyrer – krysslister
  + Lydsignal/alarmer
  + +++

For en del systemer er «feil safe» ikke helt rett frem.

* Airbag
  + Sikker tilstand er ikke vel definert
  + På den ene siden ønsker man å bygge det mest mulig pålitelig med hensyn på å løse ut
  + Men det å løse ut uten at det er behov for funksjonen kan være farlig.

## Vedlikehold

Vedlikehold er hvordan organisasjoner forsøker å forhindre feil ved å ta vare på sine fysiske fasiliteter. Fordelene med bra vedlikehold inkluderer økt sikkerhet, økt pålitelighet, høyere kvalitet, lavere operasjonskostnader, lengre levetid for prosessteknologi og høyere sluttverdi for maskinene.

### Tre hovedtilnærminger til vedlikehold

**Bruk til break-down** involverer å tillate at fasilitetene opererer til de feiler. Vedlikeholdsarbeid utføres bare etter at feil har skjedd. Feil under slike forhold er ikke katastrofale eller så frekvente at det er nødvendig med kontinuerlig vedlikehold.

**Forebyggende vedlikehold** forsøker å eliminere eller redusere sjansene for feil ved å service fasilitetene ved planlagte intervall. Konsekvensene ved feil i tjeneste vil gjerne være høyere her.

**Tilstandsbasert vedlikehold** forsøker å utføre vedlikehold vare når det kreves. Forutsetter kontinuerlig overvåking som kan avgjøre om vedlikehold trengs.

## Miksede vedlikeholds-strategier.

RTB brukes ofte når reparasjoner er relativt rett frem, når jevnlig vedlikehold er relativt kostbart eller hvor feil ikke er forutsigbare (like sannsynlig at feil inntreffer før vedlikehold som etter). Forebyggende vedlikehold brukes hvor kostnadene ved feil er høye og hvor feil ikke er helt tilfeldig. Tilstandsbasert vedlikehold når vedlikeholdsaktiviteter er dyre, enten på grunn av kostnadene ved vedlikeholdet i seg selv, eller på grunn av avbrytelsen som vedlikeholdsaktivitetene fører til i operasjonen. De fleste operasjoner har en miks av strategiene.

### Breakdown versus preventivt vedlikehold.

Balansen mellom preventiv og breakdown vedlikehold settes normalt til å minimere de totale kostnadene ved breakdown. Ujevne preventiv vedlikehold vil koste lite å utføre, men vil resultere i større sannsynlighet for breakdown vedlikehold (store kostnader) og omvendt. De totale vedlikeholdskostnadene ser ut til å minimere et optimumnivå for preventivt vedlikehold, men kostnadene ved å gjøre preventivt vedlikehold trenger ikke å stige like bratt som indikert på figuren. Kurven antar at vedlikehold utføres av en separat gruppe mennesker og at hver gang vedlikehold skjer kan ikke fasilitetene brukes til produksjon. Dette er imidlertid ikke alltid tilfellet. Kostnadene ved breakdown kan også være høyere enn indikert. Ved å putte disse innvendingene sammen får vi den andre kurven.

# Total productive maintenance (TPM)

Er «the productive maintenance carried out by all employees through small group activities», hvor productive maintenance er «maintenance management which recognizes the importance or reliability, maintenance and economic efficiency in plant design». Kommer fra Japan og sees på som en naturlig forengelse av evolusjonen fra run-to-breakdown til preventive vedlikehold. TPM tar til seg noen av team-arbeid og empowerment prinsippene fra kapittel p, i tillegg til kontinuerlig forbedrings tilnærming som diskutert i kapittel 18. Ser også på vedlikehold som en spørsmål for hele organisasjonen hvor ansatte kan bidra. Det er analogt til TQM.

**De fem målene ved TPM**

TPM forsøker å etablere gode vedlikeholdspraksiser i operasjoner gjennom jakten på de fem målene:

1. Forbedre effektiviteten til utstyr ved å eksaminere alle tap som skjer
2. Oppnå autonom vedlikehold ved å få ansatte til å ta ansvar for en del av vedlikeholdsoppgavene og for forbedringer av vedlikeholdsprestasjoner.
3. Planlegg vedlikehold med en fullt utarbeidet tilnærming til alle vedlikeholdsaktiviteter.
4. Tren ansatte i relevante vedlikeholdsferdigheter slik at både vedlikeholdsansatte og operatører har ferdighetene for å utfylle rollene sine
5. Oppnå tidlig «equipment management» ved forebyggende vedlikehold, som involverer å vurdere årasker til feil og vedlikehold av utstyr i design, produksjon, installasjon og bestilling.

# Pålitelighets-sentrert vedlikehold (Reliability-centered maintenance)

Bruker feilmønsteret for hver type feilmode til et system eller del for å diktere tilnærmingen til dens vedlikehold. Tilnærmingen til RCSM refereres gjerne til som «dersom vi ikke kan hindre det i å skje, bør vi stoppe det fra å bety noe». Altså, dersom vedlikehold ikke kan forutsi eller forhindre feil og feilen har en viktig konsekvens, må innsatsen rettes mot å redusere konsekvensene av feilen.

# Mitigating the effects of failure

Risk, eller failure, mitigation betyr å isolere en feil fra dens negative konsekvenser. Det er en innrømmelse av at ikke alle feil kan unngås. Men i noen operasjonsområder er styring basert på mitigation i stedet for forebygging utdatert. For eksempel vil en inspeksjons-praksis i kvalitetsledelse være basert på antagelsen om at feil er uunngåelige og må oppdages før de fører til skade. Moderne TQM vektlegger i større grad forebygging. Men i andre operasjoner kan mitigation være viktig når det brukes sammen med forebygging for å redusere total risiko.

### Risk mitigation actions

Handlingen som tas for å begrense (mitigate) feil vil være avhengig av risikoen. I de fleste industrier har tekniske eksperter etablert en klassifisering av risikobegrensnings-handlinger som er passende for sannsynlig type risiko.

**Mitigation planlegging** er aktiviteter som sørger for at alle mulige feil mitigation-aktiviteter har blitt identifisert. Det er den overordnede aktiviteten som omgir de andre aktivitetene, og kan beskrives som en form for løsningstre eller retningslinjer.

**Økonomisk mitigation** inkluderer handlinger som forsikringer mot tap på grunn av feil og å spre de finansielle konsekvensene.

**Containment (spatial)** betyr å stoppe feilen fra å fysisk spre seg og påvirke andre deler av den interne eller den eksterne verdikjeden.

**Containment (temporal)** betyr å begrense spredningen av feil over tid. Brukes spesielt når informasjon om en feil må videresendes uten forsinkelser

**Tapreduksjon** dekker mange handlinger som reduserer katastrofale konsekvenser av feil ved å fjerne ressursene som trolig vil lide av disse konsekvensene.

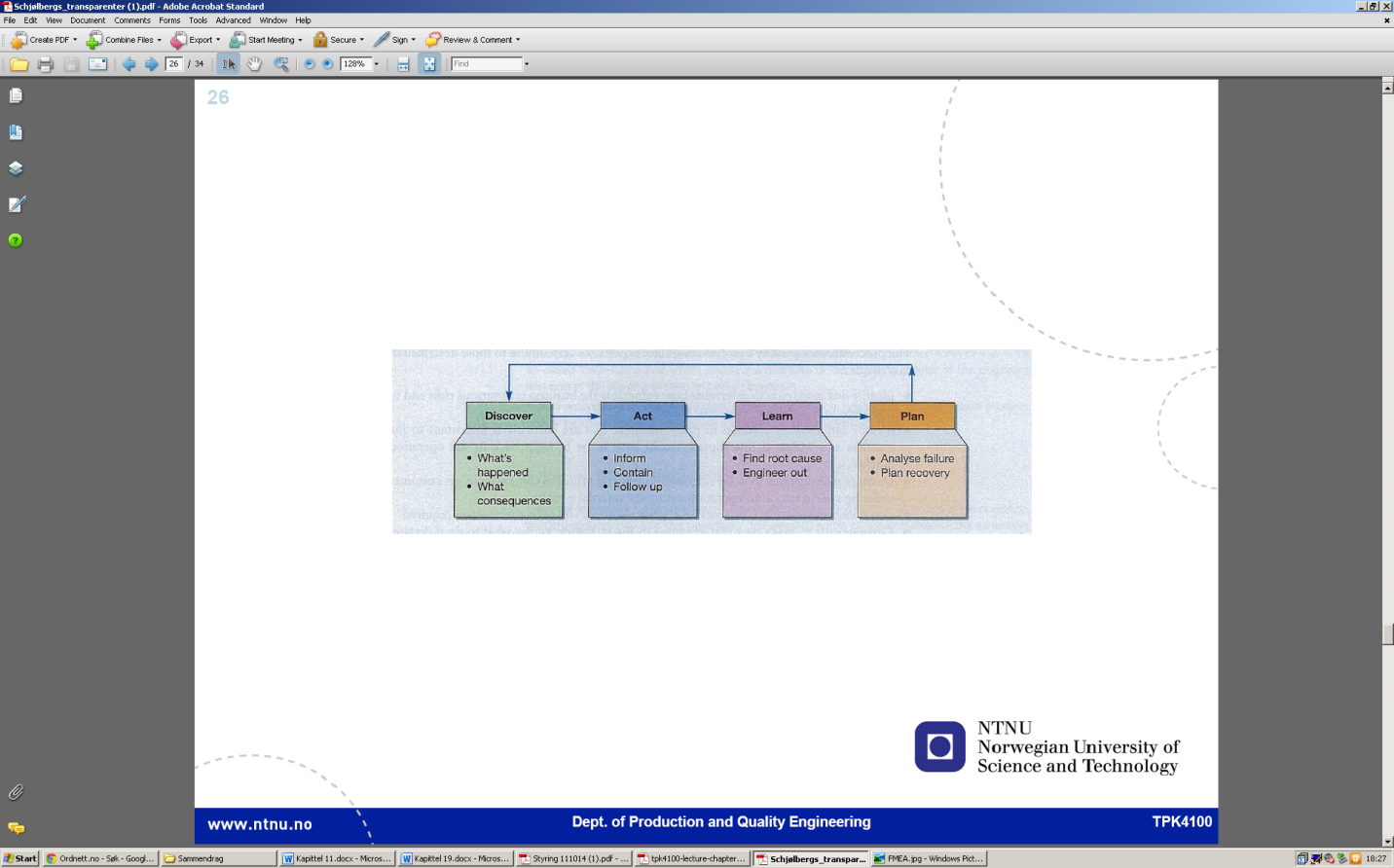
**Substituering** betyr å kompensere for feil ved å tilby andre ressurser som kan substituere dem som har blitt mindre effektive på grunn av feil. Minner litt om redundans-prinsippet.

# Recovering from the effects of failure

En god recovery kan gjøre sinte og frustrerte kunder til fornøyde og lojale kunder.

**Recovery i high-visibility tjenester**Alle kunder har forventninger til recovery som de vil at operasjoner skal møte. Recovery må være en planlagt prosess. Organisasjoner må derfor utvikle en passende respons til feil, linket til kostnadene og ubeleiligheten for kunden som møter kundenes behov og forventninger.

### Failure planlegging

Å identifisere hvordan organisasjoner kan recover fra en feil er spesielt interessant for tjenesteoperasjoner fordi de kan minimere effektene feil har på kunden eller til og med gjøre feil til en positiv opplevelse. Er også av interesse for andre industrier, spesielt for dem hvor konsekvensene av feil er veldig alvorlige. **Failure planning** er aktiviteten ved å utforme prosedyrene som gjør at en operasjon kan recover fra feil. Representeres ofte av en steg-modell.

**Discover.** Finn ut eksakt hva feilen dreier seg om. Hva har skjedd? Hvem vil påvirkes av feilen? Hvorfor skjedde feilen?.

**Act.** Dersom konsekvensene er store må man bevege seg rast til dette stadiet. Dette betyr å gjøre tre handligner: Først må vi fortelle signifikante mennesker innvolvert hva man foreslår å gjøre med feilen slik at alle kan starte sine egne recovery planer. Så må effektene av feilen begrenses for å hindre at konsekvensene sprer seg og fører til videre feil. Til slutt må det vær en form for oppfølging for å være sikker på at begrensningshandlingene virkelig har begrenset omfanget. De første to stegene kan bytte rekkefølge.

**Learn.** Læring involverer å se på feilen for å finne ut årsakene for så å eliminere ut årsakene for å forhindre at det skjer igjen.

**Plan.** Operations managers må formelt inkorporere leksene som er lært i fremtidige reaksjoner til feil. Gjøres ofte ved å jobbe gjennom hvordan de vil reagere til fremtidige feil i teorien. Dette involverer å først identifisere alle mulige feil (FMEA). Så må man formelt definere prosedyrene som organisasjonen skal følge ved hvert tilfelle.

## Business continuity

Mangen av ideene bak feil, forebygging og recovery er inkorporert i det voksende feltet «business continuity». Dett har som mål å hjelpe operasjoner med å unngå og recover fra katastrofer samtidig som de holder virksomheten i gang. Når operasjoner blir økende integrert kan kritiske feil resultere av en serie relaterte og urelaterte hendelser og kombiner totalt avbryte en virksomhets business.

Prosedyrene minner om de som tidligere er beskrevet

* Identifiser og vurder risiko for å avgjøre hvor sårbar virksomheten er for ulik risiko og for å ta steg for å minimere eller eliminere dem
* Identifiser kjerneprosesser for å prioritere de som er spesielt viktige for virksomheten og som fort må bringes tilbake til aktivitet viss avbrutt
* Kvantifiser recovery tid for å sørge for at ansatte forstår prioriteringer
* Avgjør behøvde ressurser for å sørge for at ressurser er tilgjengelig når de trengs
* Komuniser for å sørge for at alle i operasjonen vet hva de skal gjøre viss en katastrofe inntreffer