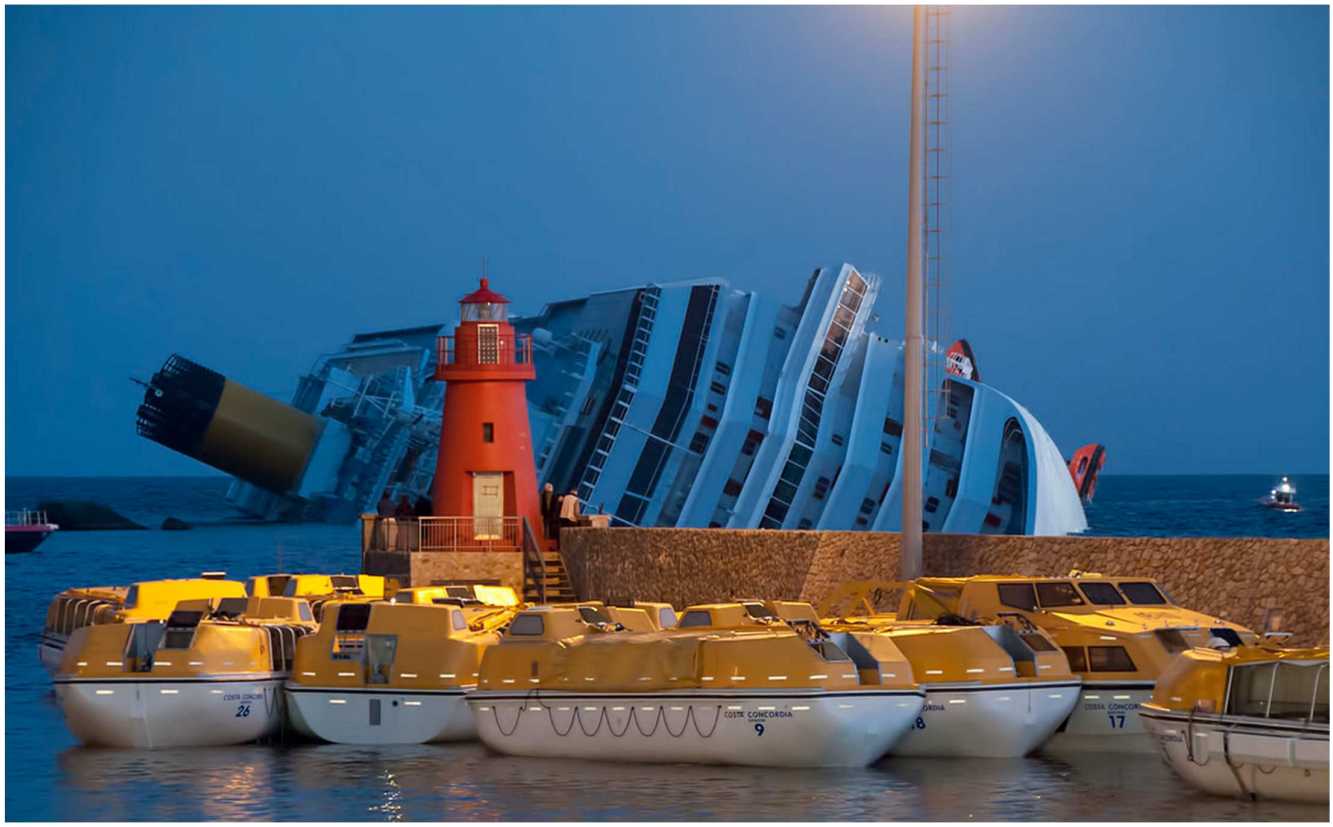
Erilaiset turvallisuudet

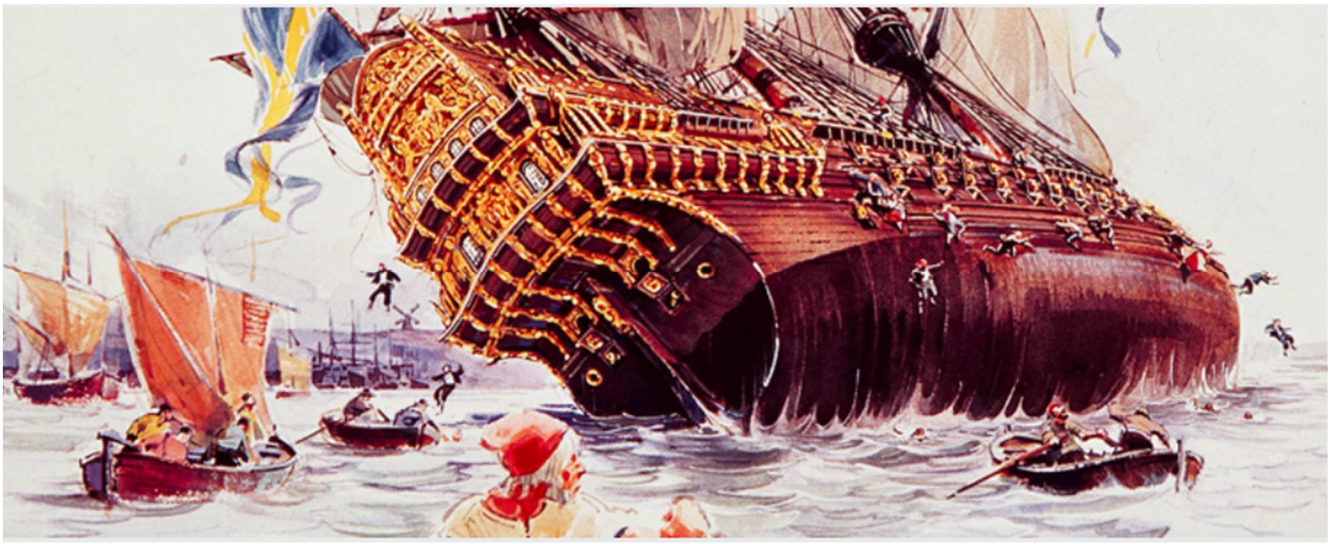
- prosessiturvallisuus
- työsuojelu
- ympäristöturvallisuus
- paloturvallisuus
- reaktoriturvallisuus
- sairaanhoidon turvallisuus
- compliance-riskit
- cyber security
- etc.

From assets to liabilities

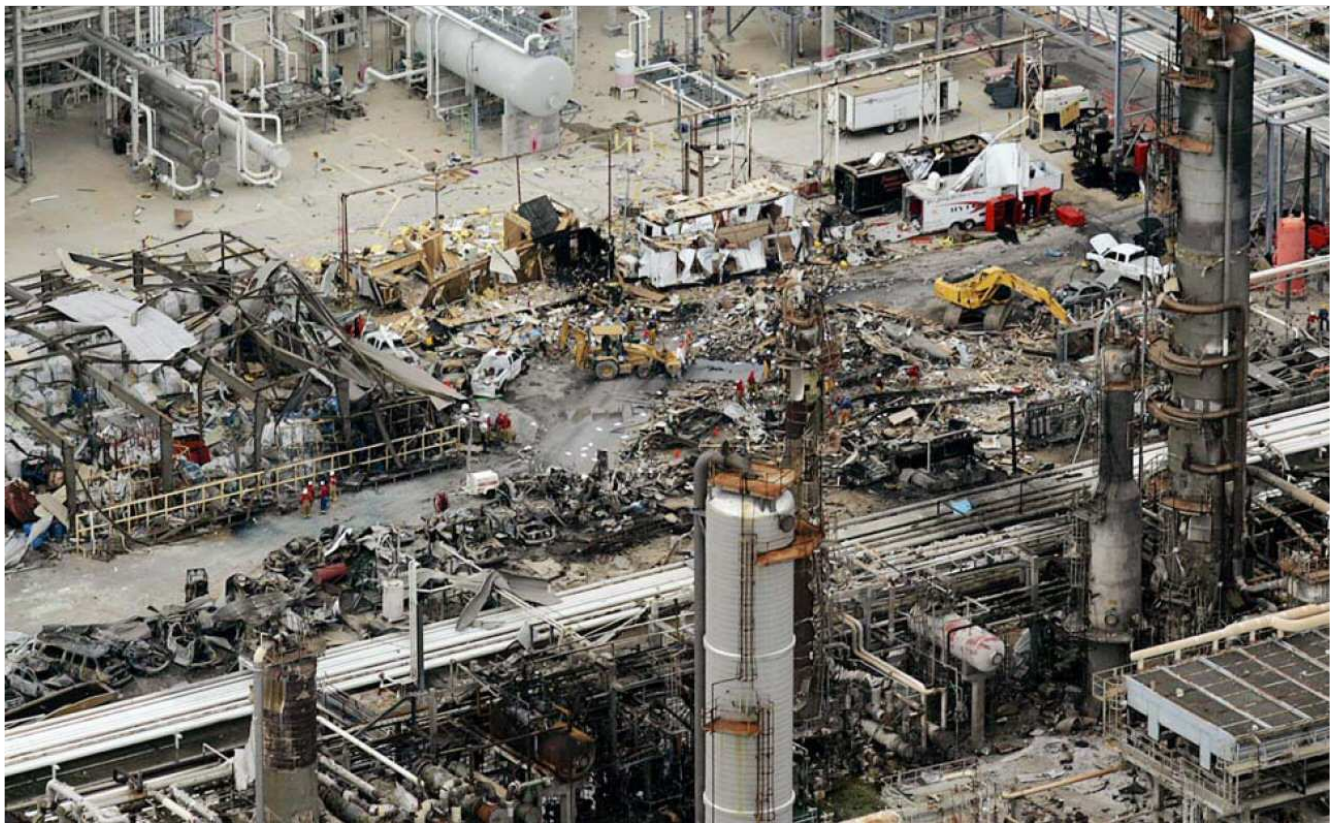


Costa Concordia was a cruise ship built in 2004, which operated from 2005 until 2012. It was wrecked off the coast of Isola del Giglio in Italy on 13 January 2012. It was lifted in 2014 and scrapped in Genoa.

Vasa laivan uppoaminen



Neitsytmatkallaan Vasa laiva upposi sunnuntaina kymmenes elokuuta 1628. Laiva yritettiin nostaa kuitenkin onnistumatta, jonka jälkeen se unohdettiin. Se löydettiin uudestaan vuonna 1956 ja nostettiin 1961. Nyt laiva voidaan nähdä Vasa-museossa Tukholmassa.



BP Texas City – 15 kuollutta, 180 loukkaantunutta, > 1,5 G$ suorat vahingot

http://www.csb.gov/assets/1/19/csbfinalreportbp.pdf

Piper Alpha in 6 July 1988

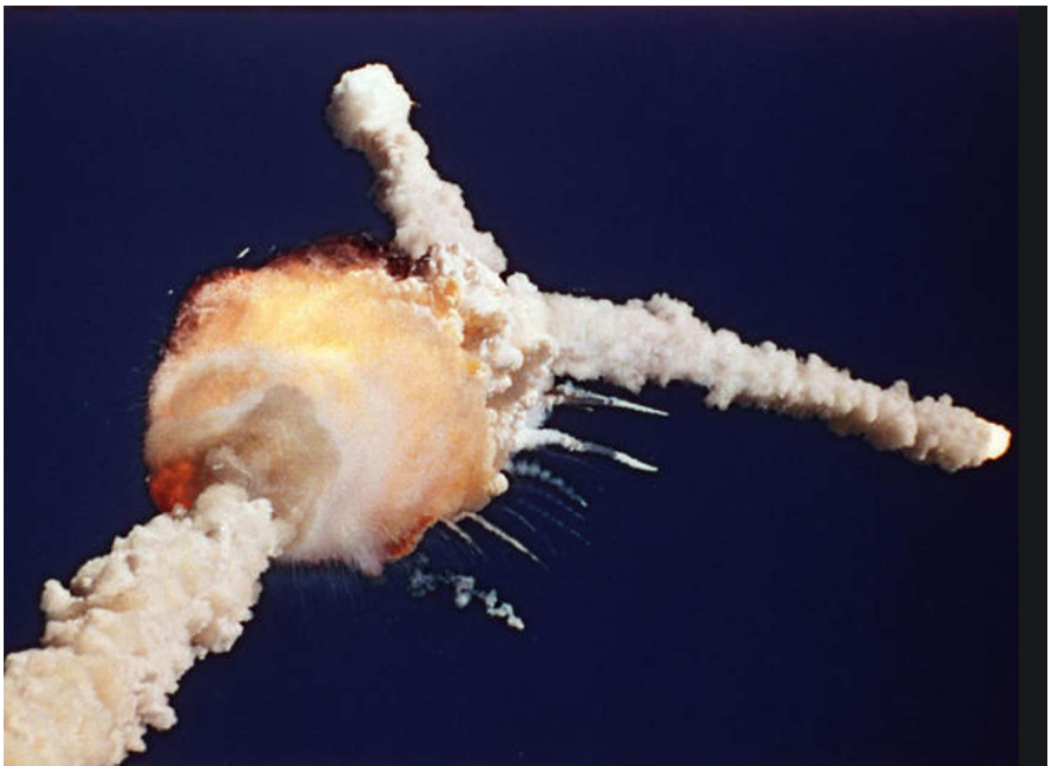
Piper Alpha was a North Sea oil production platform. The platform began production in 1976, first as an oil platform and then later converted to gas production. An explosion and the resulting oil and gas fires destroyed it killing 167 men leaving only 61 survivors.

July 09, 2006 Location: Irkutsk, Russia Aircraft: Airbus A-310-324ET Reg: F-OGYP Airline: Sibir (S7) Flight No: 778. On board 203 (passengers:195 crew:8), Fatalities**:** 125 (passengers:120 crew:5)

Air France Flight 4590

Air France Flight 4590 was an Aérospatiale-BAC Concorde, registration F-BTSC, on a scheduled international flight from Paris, France, to New York City, on 25 July 2000, local time 16:43 CET. While taking off, the aircraft ran over debris on the runway, blowing a tyre and puncturing a fuel tank, leading to fire and engine failure. All 100 passengers and nine crew members aboard the Concorde died when it crashed into a hotel nearby.

Challenger, January 28, 1986



Disintegration of the vehicle began after an O-ring seal in its right solid rocket booster failed at liftoff.

The launch of STS-107, Columbia's 28th mission a piece of foam insulation broke off from the Space Shuttle external tank and struck the left wing.

TMI onnettomuus tapahtui 28 maaliskuuta 1979. Reaktorisydän vaurioitui ja joitakin radioaktiivisia kaasuja pääsi ilmaan. Kukaan ei kuollut eikä loukkaantunut.

Tshernobyl 1986

onnettomuuden syyt

- reaktorin rakenne
- henkilökunnan osaaminen
- organisaation puutteita

Seuraukset

- 28 kuolutta 30 päivän sisällä
- >1800 kilpirauhassyöpää
- paljon käyttökelvotonta maata

Fukushima Daiichi nuclear disaster occurred when the plant was hit by a tsunami that had been triggered by an magnitude 9.0 earthquake on 11 March 2011. Substantial amounts of radioactivity was released from damaged reactors and spent fuel pools.

Sayano Shushenskayan pato Venäjällä

10 generaattoria, 650 MW, eli huipputeho 6500 MW
nimellinen vesivirtaus 358,5 m^3/s per turpiini
putouskorkeus 194 m
generaattoreiden nimellinen kierrosluku 142,86 rpm
laitos käyttöönotettu 1978

Sayano Shushenskaya, 17.8.2009

Pohdintaa

- Miksi tapahtuivat?
- Miten niitä olisi voitu estää?
- Mitä niistä voimme oppia?
- Onnettomuuksien vakavuus?
  - kuinka usein tapahtuvat?
  - seurausten vakavuus?

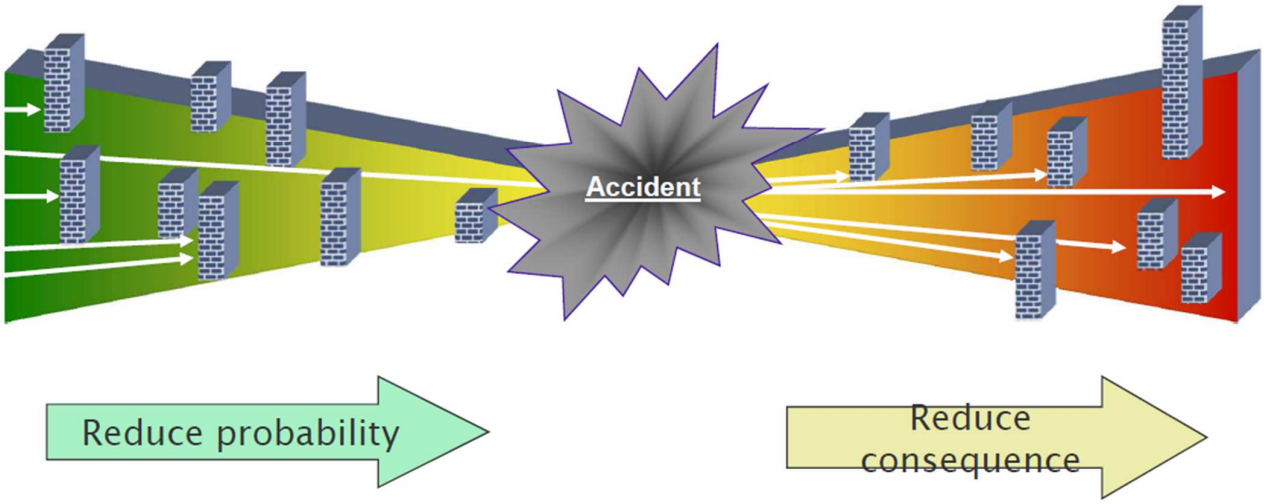
Miksi onnettomuudet tapahtuvat?

Systeemisiä puutteita
- teknillinen systeemi
- ihminen kone liitäntä
- organisaatio
- informaatiojärjestelmä

mutta myös ihmisen toiminnasta systeemissä
- ajattelemattomuutta
- inhimmillisiä virheitä
- vastuutonta toimintaa
- tahallista vahingontekoa

Oikeastaan voidaan ihmetellä kuinka hyvin systeemit useimmiten toimivat!

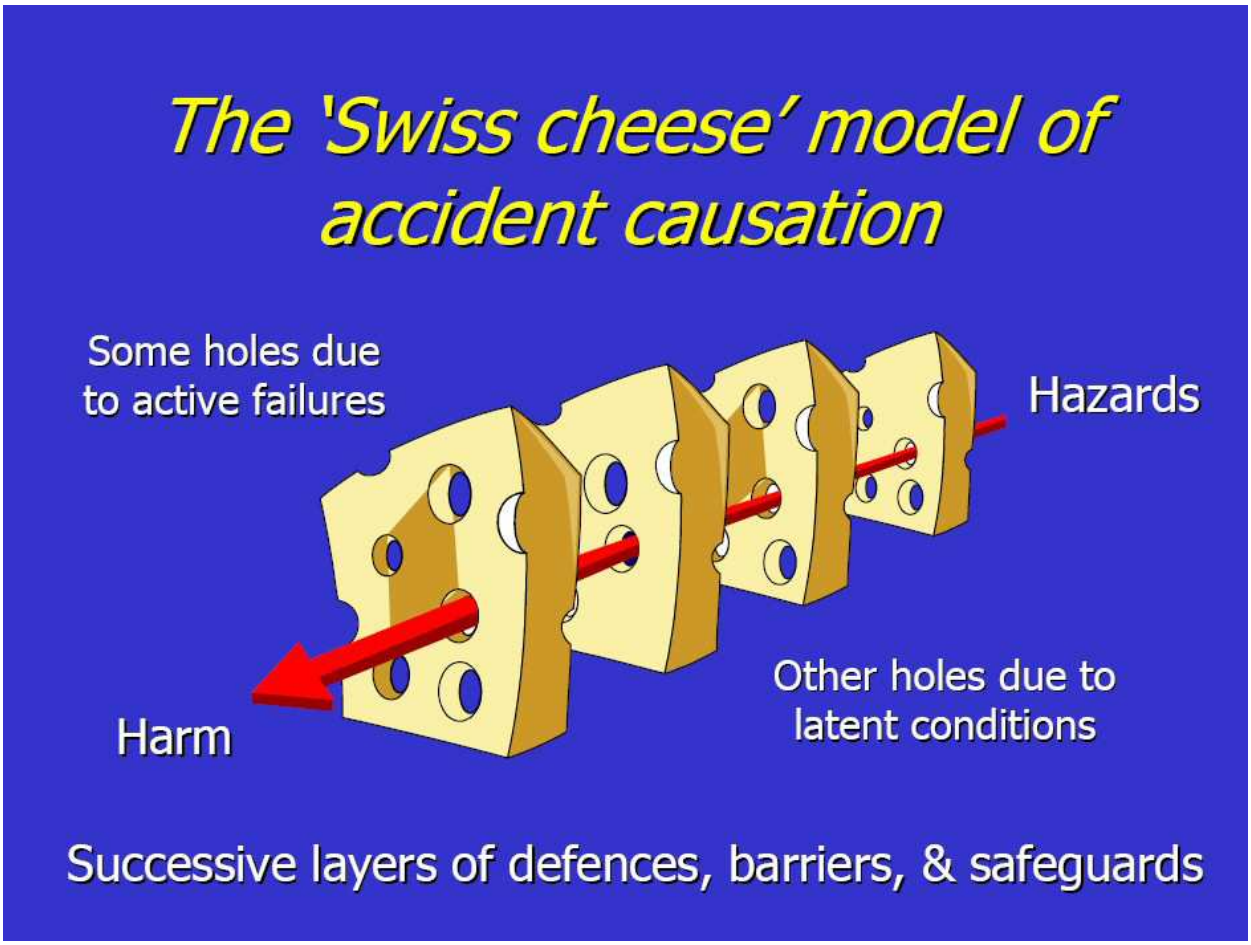
The bow-tie model of accidents



Mitä voidaan tehdä?

- ennen
  - riskianalyysillä varmistaa että merkittävimmät uhat on ottettu huomioon
  - varmistaa että tarkoituksenmukaisia toimintasuunnitelmia on olemassa hätätilanteita varten
- aikana
  - käyttää ennalta laadittuja hätäsuunnitelmia
  - improvisoida kohtuullisesti tilanteen mukaan
- jälkeen
  - analysoida tapahtumat korjaavien toimenpiteiden ehdottamiseksi
  - viedä muutokset systeemeihin riittävän analyysin jälkeen

Eliminate – Isolate – Control – Mitigate



James Reason (1997). Managing the risks of organizational accidents, Ashgate.

Kaksi teoriaa

High reliability theory

- onnettomuuksia voidaan estää hyvin suunnitelulla organisaatiolla
- turvallisuus on organisaation primäärinen tavoite
- redundanttisuus edistää turvallisuutta; turvallisuutta voidaan rakentaa ei luotettavista komponenteistä
- hajautetulla päätöksenteolla saavutetaan ripeyttä ja joustavuutta yllätyksellisissä tilanteissa
- turvallisuus kulttuuri edistää yhtenäisiä ja oikeita toimenpiteitä
- jatkuva käyttö, kolutus ja simulointi edistää turvallisuutta
- kokemusperäistä oppimista voidaan tukea mielikuvituksella ja simuloinneilla

Normal accidents theory

- kompleksisissa ja tiukasti kytketyissä systeemeissä tapahtuu onnettomuksia
- turvallisuus on vain yksi monesta kilpailevasta tavoitteesta
- redundanttisuus lisää kompleksisuutta ja edistää riskien ottamista
- kompleksisuus edellyttää hajautettua organisaatiota, mutta kytketyissä systeemeissä tarvitaan keskittämistä
- militaarinen organisaatio ei tue demokraattisia arvoja
- käsittämättömiä vaarallisia tilantita ei voida kouluttaa organisaatioissa
- vastuun kieltäminen, virheellisen raportoinnin ja historian uudelleen-kirjoittaminen lamaannutta oppimista

Mukautettu kirjasta Scott D. Sagan (1993). The limits of safety, Princeton University Press.
Roberts, K. H. (1990). Some Characteristics of High-Reliability Organizations. Organization Science, 1, 160-177.
Perrow, C. (1984). Normal Accidents: Living with High-Risk Technologies. New York: Basic Books.

Hallinnan romahtaminen

Säädön tai ohjauksen onnistumisen neljä ehtoa

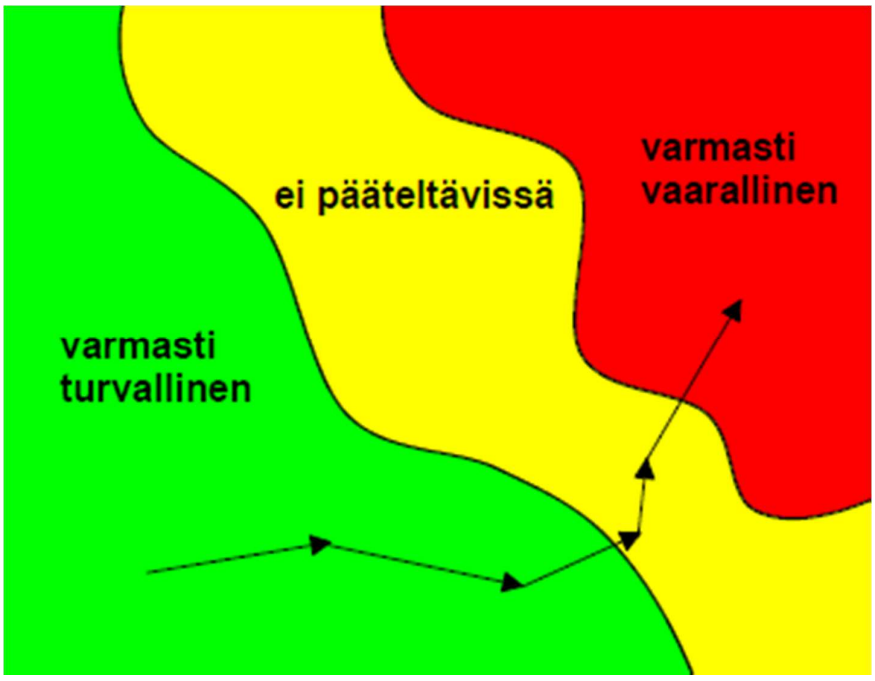
1. Tiedetään mitä halutaan (hyvyyskriteeri)
2. Systeemimallin olemassaolo
3. Tarkailtavuus (systeemin tila voidaan havaita)
4. Ohjattavuus (systeemin tilaan voidaan vaikuttaa)

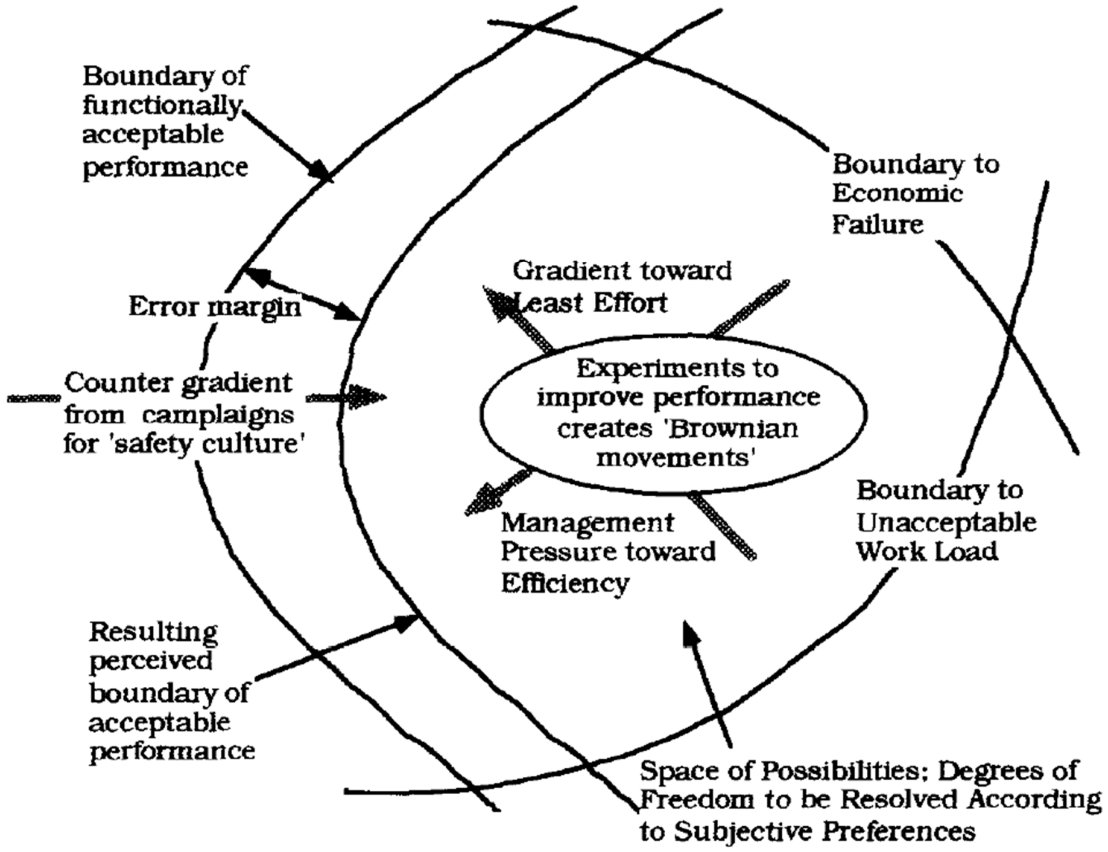
Turvallisuusjohtamisen kaksi tehtävää

1. Pitää systeemiä turvallisessa tilassa (esteet)
2. Ohjata systeemiä turvalliseen tilaan (aktiiviset suojaukset)

B. Wahlström, C. Rollenhagen; Safety management – A multi-level control problem, Safety Science 69 (2014) 3–17

Tila-avaruuden kolme aluetta





Jens Rasmussen (1997). Risk management in a dynamic society:a modelling problem, Safety Science Vol. 27, No. 2/3, pp. 183-213.

Kurssin keskeiset käsitteet

- Uhat ja niiden toteutumisen kustannukset
- Onnettomuuden tapahtumat
  - ennen, aikana, jälkeen
- Erilaiset esteet
  - aidat, barriäärit, lukitukset
  - aktiiviset turvallisuusjärjestelmät
- Ohjaustehtävän onnistumisen edellytykset
  - tavoite, malli, tarkkailtavuus, ohjattavuus
- Suunnittelua ohjaavat tapahtumat
  - mihin pitää varautua (tapahtumat, todennäköisyydet)

Uhan toteutuminen ja sen seuraukset

- Kuinka usein uhka toteutuu?
  - kerran yhdessä, kymmenessä tai sadassa vuodessa
  - populaatiossa yhdelle, kymmenelle tai sadalle yksilölle per vuosi
- Mitkä ovat seuraukset?
  - kustannukset per onnettomuus
    - ihmisiä (heti, viivästyneet, altistuneet ryhmät)
      kuolemantapauksia, loukkantuneita
    - päästöt ympäristöön (ilma, vesi, maaperä)
    - taloudelliset vahingot
    - ei aineelliset vahingot
- Epävarmuuden hallintaa (frekvenssi, kustannus)

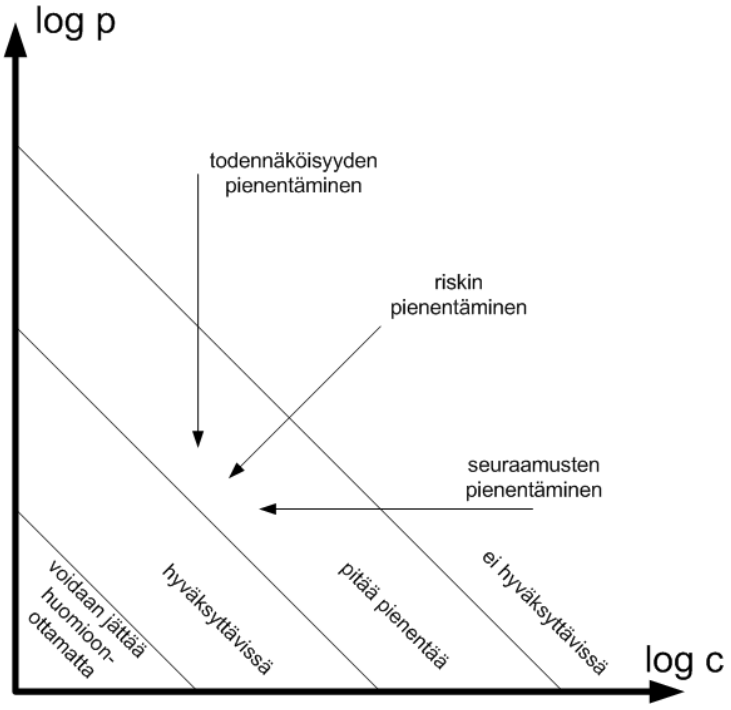
Riskikäsite

$R = c * p$

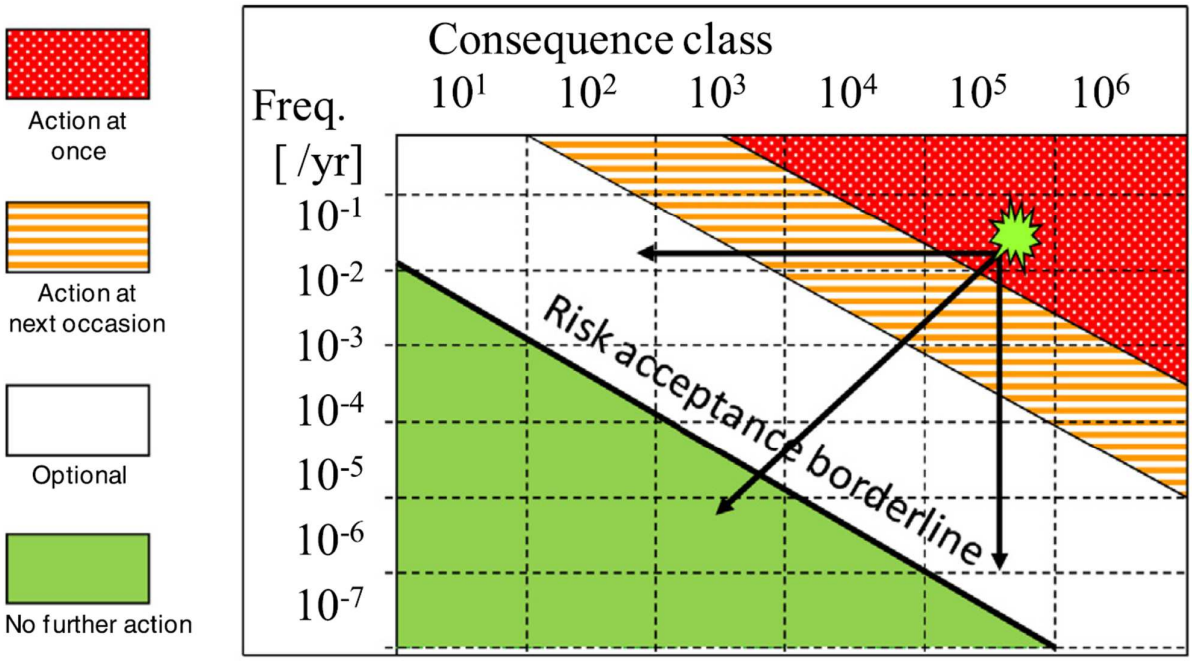
Ongelmana suuri kustannus ja pieni todennäköisyys

$R = \infty * 0 = ?$

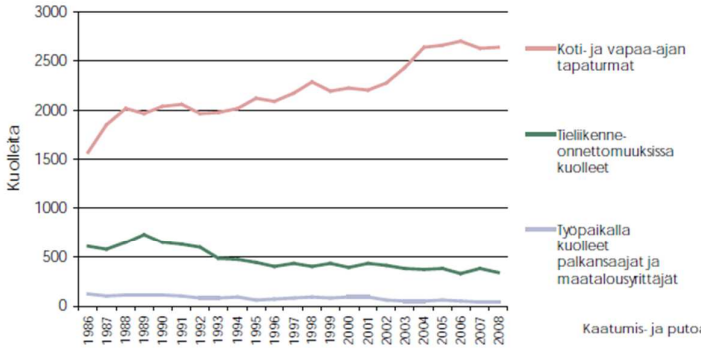
Miten saada uskottavat estimaatit c:lle ja p:lle?



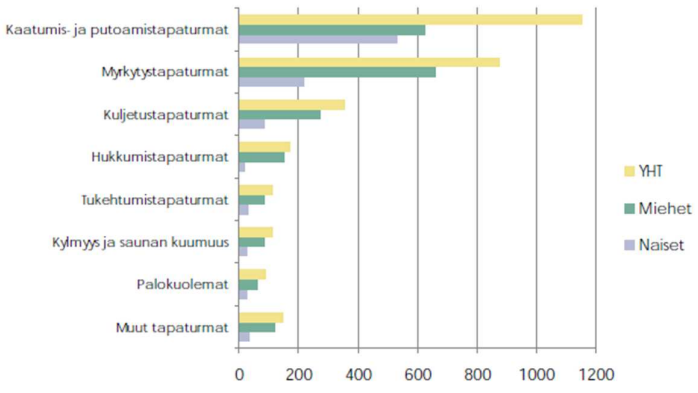
Riskien hyväksyttävyys



Tapaturmat tilastojen mukaan



Kuvio 2. Tapaturmaisesti kuolleet (lkm) 1986–2008. Lähde: Til
Kuolemansyytilasto.



Kuvio 3. Tapaturmiin kuolleiden yleisimmät kuolinsyyt sukupuolen mukaan (lkm) 2008. Lähde: Tilastokeskus SVT: Kuolemansyytilasto.

Riskien olemus

- Miten epävarmuutta pitää mallintaa?
  - todennäköisyydellä
    - frekventistinen tulkinta
    - Bayesilainen tulkinta (subjektiivinen todennäköisyys)
  - mahdollisuudella (possibility theories)
- Aleatoorinen ja episteeminen epävarmuus
- Avenin ja Krohnin argumentit
  - riskin käsitteellistäminen
  - teoria, käsitteet ja menetelmät
  - laatuajattelun ideat ja käsitteet
  - tietoisuuden edellytykset (mindfulness)

Terje Aven, Bodil S.Krohn (2014). A new perspective on how to understand, assess and manage risk and the unforeseen, Reliability Engineering and System Safety, 121, 1–10.

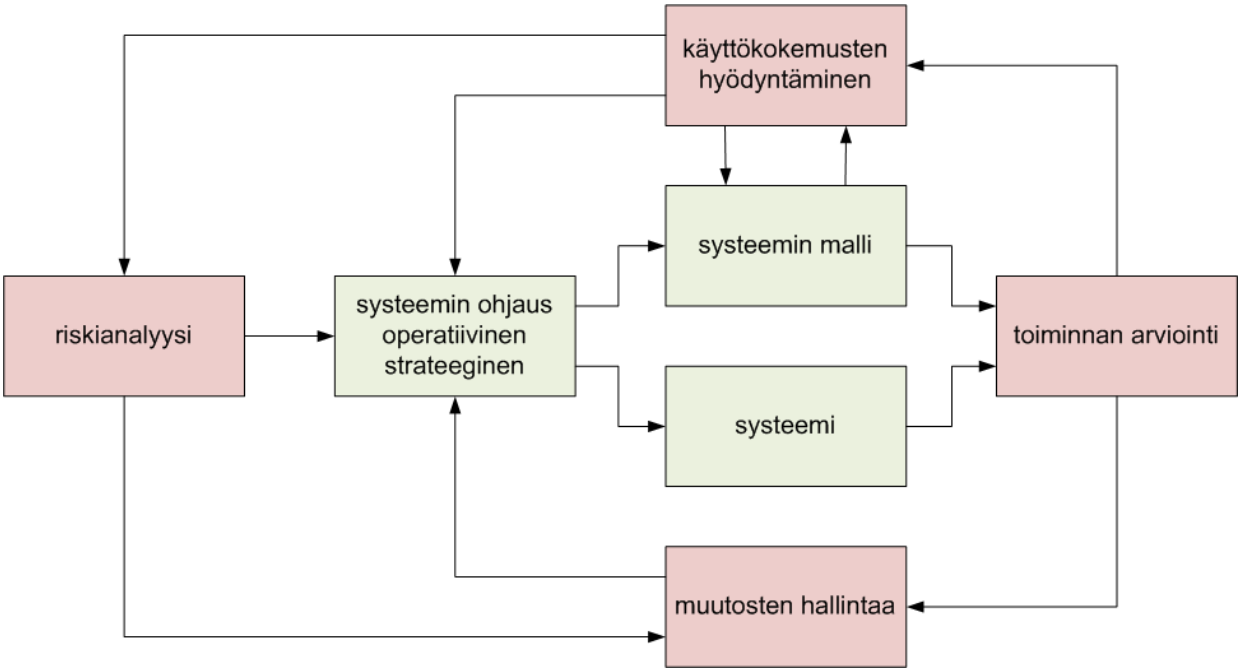
Turvallisuusjohtaminen

Millaisia toimintoja siihen kuuluisi?

- ennen tapahtumaa
  - mitä voi tapahtua?
  - millä tavalla sitä voidaan estää?
  - jos kuitenkin tapahtuu, millä tavalla voidaan seurauksien vakavuutta pienentää?
- tapahtuman aikana
  - toimitaan valmiussuunnitelmien mukaan
- tapahtuman jälkeen
  - mitä tapahtui?
  - miten voimme siitä oppia?
  - miten syysteemiä tai johtamisjärjestelmää pitää muuttaa?

Johtamisjärjestelmä antaa organisaatiolle puitteet toimia ennen, aikan ja jälkeen

Turvallisuusjohtamisen periaate



Turvallisuustyön tehtävät

- Riskianalyysi

  tunnistetaan uhat, arvioidaan kuinka usein ne toteutuvat, päätetään mitä eri uhkien kohdalla tehdään

- Käyttökokemusten keräys ja analysointi

  suunnittelu ja seuranta, omat tapahtumat, samankaltaiset organisaatiot, toimintaympäristö

- Muutosten suunnittelu ja läpivienti

  muutostarpeet, muutosehdotukset, riskien analysointi, päätöksenteko, toteutussuunnittelu, läpivienti

- Toiminnan arviointi

  toimitaanko suunnitelmien mukaisesti, saavutetaanko asetetut tavoitteet, mitä pitäisi muuttaa

Riskianalyysin suorittaminen

Uhkien tunnistaminen
- luonnolliset (sääilmiöt, tulvat, maanjäristykset, ...)
- vikaantumiset (kuluminen, transientit, ...)
- inhimilliset virheet (käyttö, kunnossapito)
- suunnitteluvirheet (prosessi, automaatio)

Riskien arviointi
- kvalitatiivinen, tapahtuma- ja vikapuut
- kvantitatiivinen (SIL, PRA)

Uhkien käsittely
- poistaminen (eliminate)
- eristäminen (isolate)
- hallinta (control)
- pienentäminen (mitigate)

Riskianalyysin vaiheet

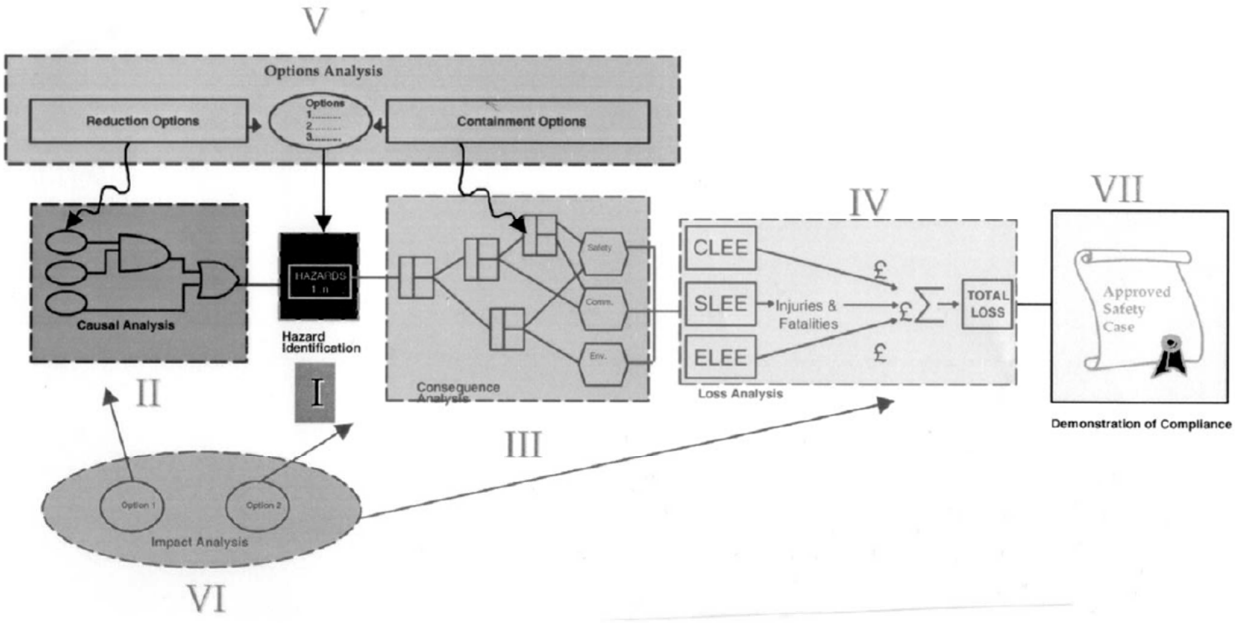


Figure 1 The seven-stage systematic risk assessment framework.

A. G. Hessami: Risk Management: A Systems Paradigm, Syst Eng 3: 156-167, 1999

Hazard and operability analysis (HAZOP)

- Uhkien systemaattinen tunnistamismenettely
  - aivoriihimuotoinen prosessi, johon usean alueen asiantuntijoita osallistuvat
  - analyysissa käytetään systeemin prosessi- ja instrumentointikaaviot
    - käydään läpi toiminnan kannalta tärkeät komponentit käyttäen avainsanoja kuten

      ei, enemmän, vähemmän, sekä että,osa siitä, päinvastoin,toinen kuin, liian aikaisin, liian myöhään, ennen, jälkeen
    - yhdistettyinä prosessisuureisiin kuten virtauksiin, paineisiin, lämpötiloihin, pinnankorkeuksiin, jne.
  - pohditaan niihin johtavia tilanteita tai tapahtumia

J. Dunjóa,. V. Fthenakisb, J. A. Vílcheza, J. Arnaldosa (2010). Hazard and operability (HAZOP) analysis. A literature review, Journal of Hazardous Materials 173, 19–32.
P. Baybutt (2015). A critique of the Hazard and Operability (HAZOP) study, Journal of Loss Prevention in the Process Industries, 33, 52-58.

Probabilistinen riskianalyysi (PRA)

Vikapuu

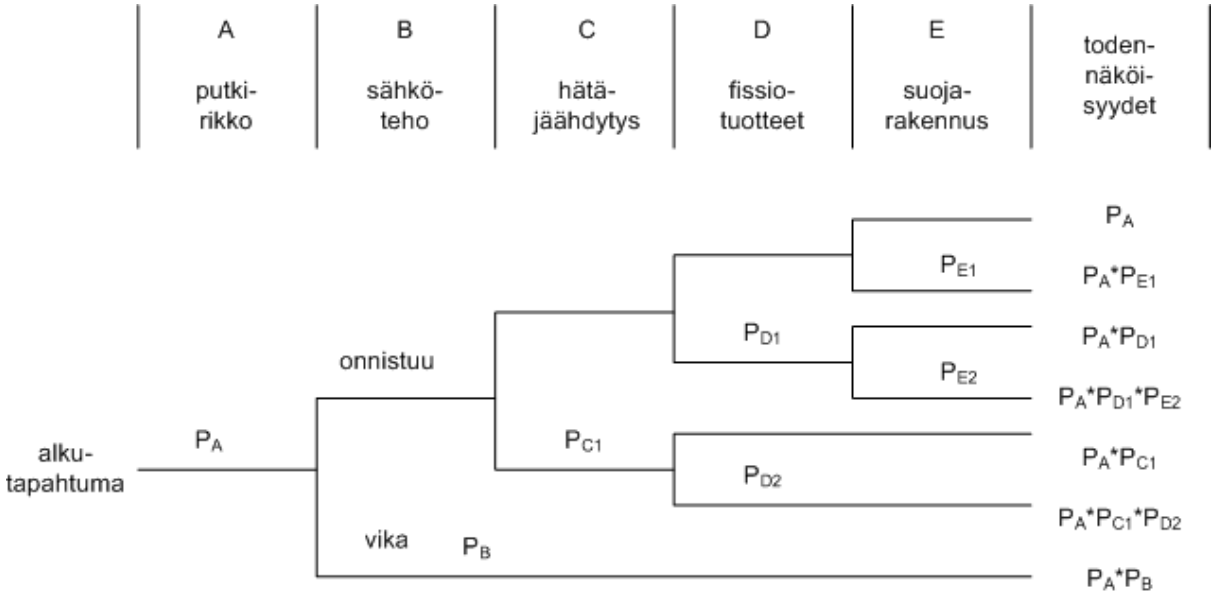
- toiminto tai komponentti vikaantuu jostain syystä
- siitä seuraa ... josta seuraa ...
- jne.

Tapahtumapuu

- lähdetään likkeelle onnettomuudesta
- se voi tapahtua jos ... ja ... tai ...
- jne.

Arvioidaan todennäköisyydet ja summataan kaikkien riskien yli

Todennäköisyysperusteinen riskianalyysi (PRA)



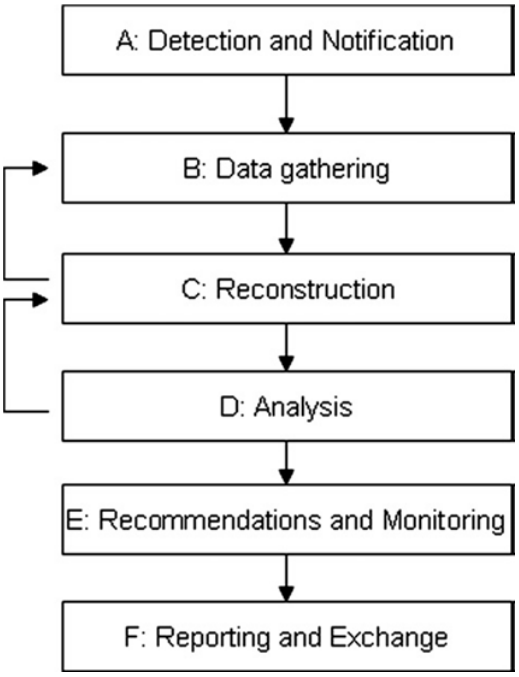
IAEA (2010). Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide No. SSG-3

Käyttökokemusten keräys ja analysointi

- Normaali suunnittelu- ja seurantakäytäntö (vuosi, strateginen)
- Tapahtumien analysointi
  - laajuus, syvällisyys
  - omat tapahtumat, muiden tapahtumat
- Toimittajien käyttökokemusryhmät
- Tutkimuksen seuranta
- Suositusten antaminen

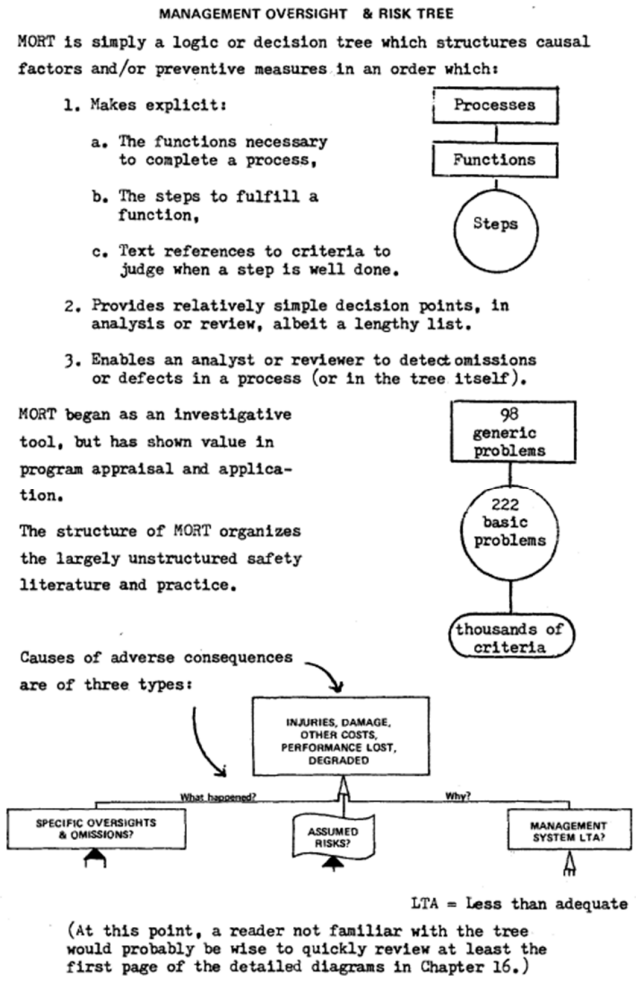
J. Lundberg, C. Rollenhagen, E. Hollnagel (2009). What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals, Safety Science 47, 1297–1311.

Root cause analysis



- Perussyyanalyysi on huono nimi. Miksi?
- Vaiheet B ja C
  - aikajanan laatiminen
  - syiden löytäminen
- Vaihe D ja E
  - miten tapahtumaa olisi voitu estää
- Vaihe F
  - raportointi ja dokumentointi
  - muutosten toteuttaminen

Milos Ferjencik (2011). An integrated approach to the analysis of incident causes, Safety Science, 49, 886–905.
Sverre Roed-Larsen, John Stoop (2012). Modern accident investigation – Four major challenges, Safety Science 50, 1392–1397
S. Chuang1, P.P. Howley:Beyond Root Cause Analysis: An Enriched System Oriented Event Analysis Model for Wide Application, Systems Engineering Vol. 16, No. 4, 2013.



Management Oversight and Risk Tree (MORT)

- menetelmä analysoida tapahtumia
- pitkä lista avainsanoja , jotka tukevat analyysia
- melkein 600 sivua paksu ohjekirja vuodelta 1973 on samalla johdatus riski-analyysiin
- osa ohjekirjasta keskitty johtamiseen ja tuo siitä oma ihannemallinsa
- lähinnä kiinnostava tekniikan historian kannalta

http://rsearch.hitechsvc.com/sesa/corporatesafety/aip/docs/reports/MORT_SAN_8212_1973.pdf

Stegen

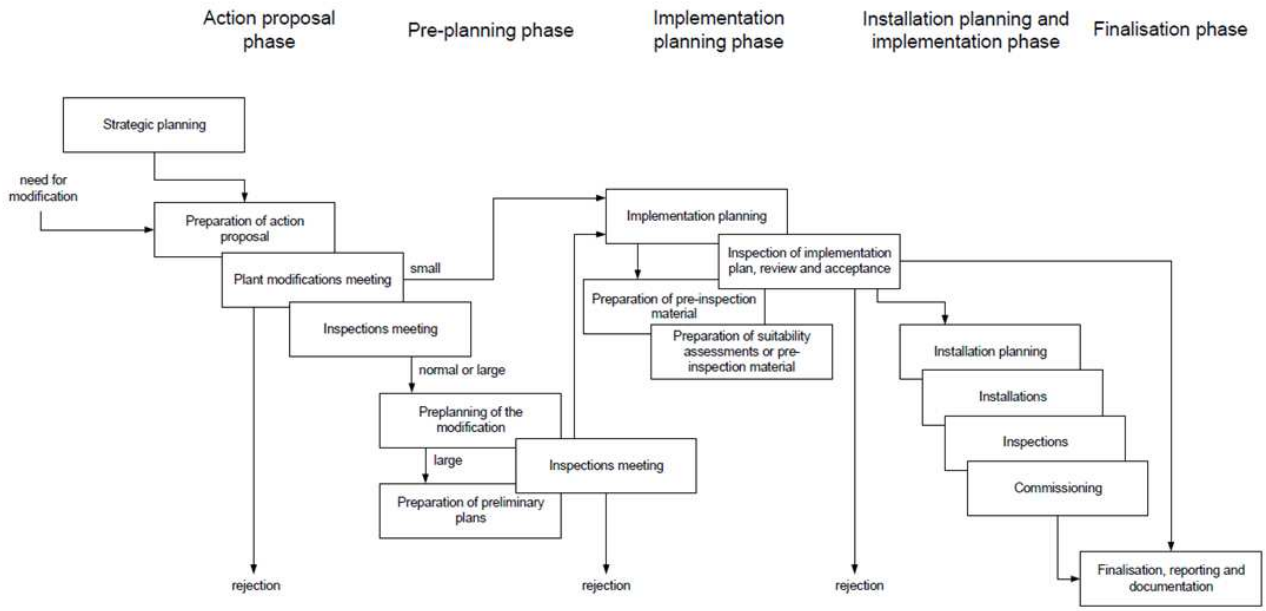
Carl Rollenhagen
Björn Wahlström

→Stegen.ppt

Muutosten suunnittelu ja läpivienti

- Erilaiset inputit
  - käyttökokemusten hyödyntäminen
  - ehdotustoiminnan tulokset
  - uutta tietoa (toimittajat, onnettomuudet, tutkimus)
- Vaiheet
  - muutosehdotuksen konkretisointi ja analysointi
  - projektisuunnitelman laatiminen
  - päätös hylätä tai toteuttaa muutosprojekti
  - muutoksen suunnittelu
  - hankinnat ja implementointi
  - toteutus
  - projektin sulkeminen

Muutoksen suunnittelu ja toteutus



Toiminnan arviointi

- Arvioinnin sisältö

  toimitaanko suunnitelmien mukaisesti, saavutetaanko asetetut tavoitteet, mitä pitäisi muuttaa

- Arvioinnin menetelmät

  auditoinnit, katselmukset, peer review, benchmarking

- Mihin arviointi perustuu

  johtamisjärjestelmän esittämiin vaatimuksiin, alan normisto, kokemuksiin

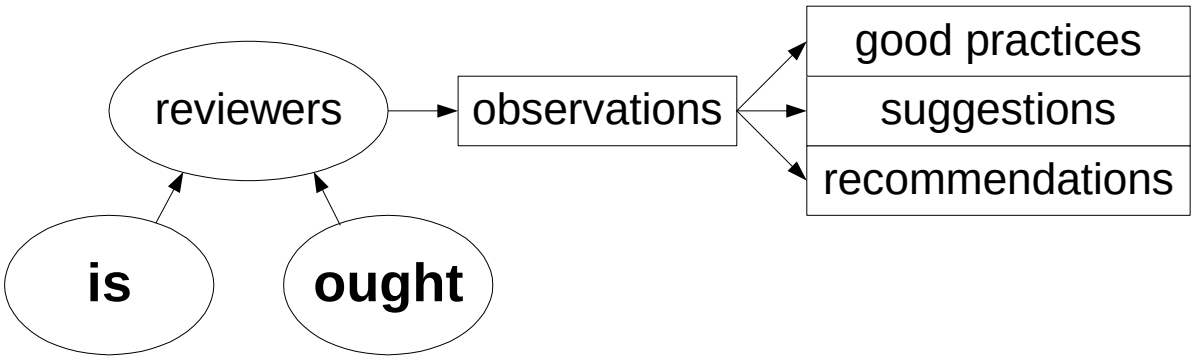
- Arvioinnin tulos

  puutteet, huomautettavat asiat, muutosehdotukset

Arvioinnit ja tarkastukset

- Auditoinnit, katselmukset, peer review, benchmarking
  - määrävälein
  - tapahtuman jälkeen
- Suoritetaan tavallisesti muutaman henkilön ryhmässä
  - auditoinnin asiantuntija
  - auditoitavan alueen asiantuntija
  - käyttäytymistieteiden asiantuntija

Peer review tarkastus



Usean onnettomuuden sarja

- BP Grangemouth, Scotland, three incidents from May 29 to June 10, 2000
- BP Texas City refinery, a catastrophic process accident on March 23, 2005
- Prudhoe Bay oil spill was discovered on March 2, 2006 at a pipeline owned by BP Exploration, Alaska in western Prudhoe Bay, Alaska
- BP Deepwater Horizon drilling rig in the Gulf of Mexico, an explosion that destroyed the rig and initiated a blow out on April 20, 2010

Ensimmäinen harjoitustehtävä

- Olette nyt saaneet käsityksen BPn toiminnasta
  - millaisia turvallisuuspuutteita näette BPn organisaatiossa?
  - mitä niille olisi pitänyt tehdä?
  - paljonko aikaa pitäisi varautua parannusten viemiseen käytäntöön?
  - voidaanko syyllistä nimittää tapahtumasarjassa?
  - voidaanko edellyttää että konseernijohtaja tietää mitä organisaation alemmilla tasoilla tapahtuu?