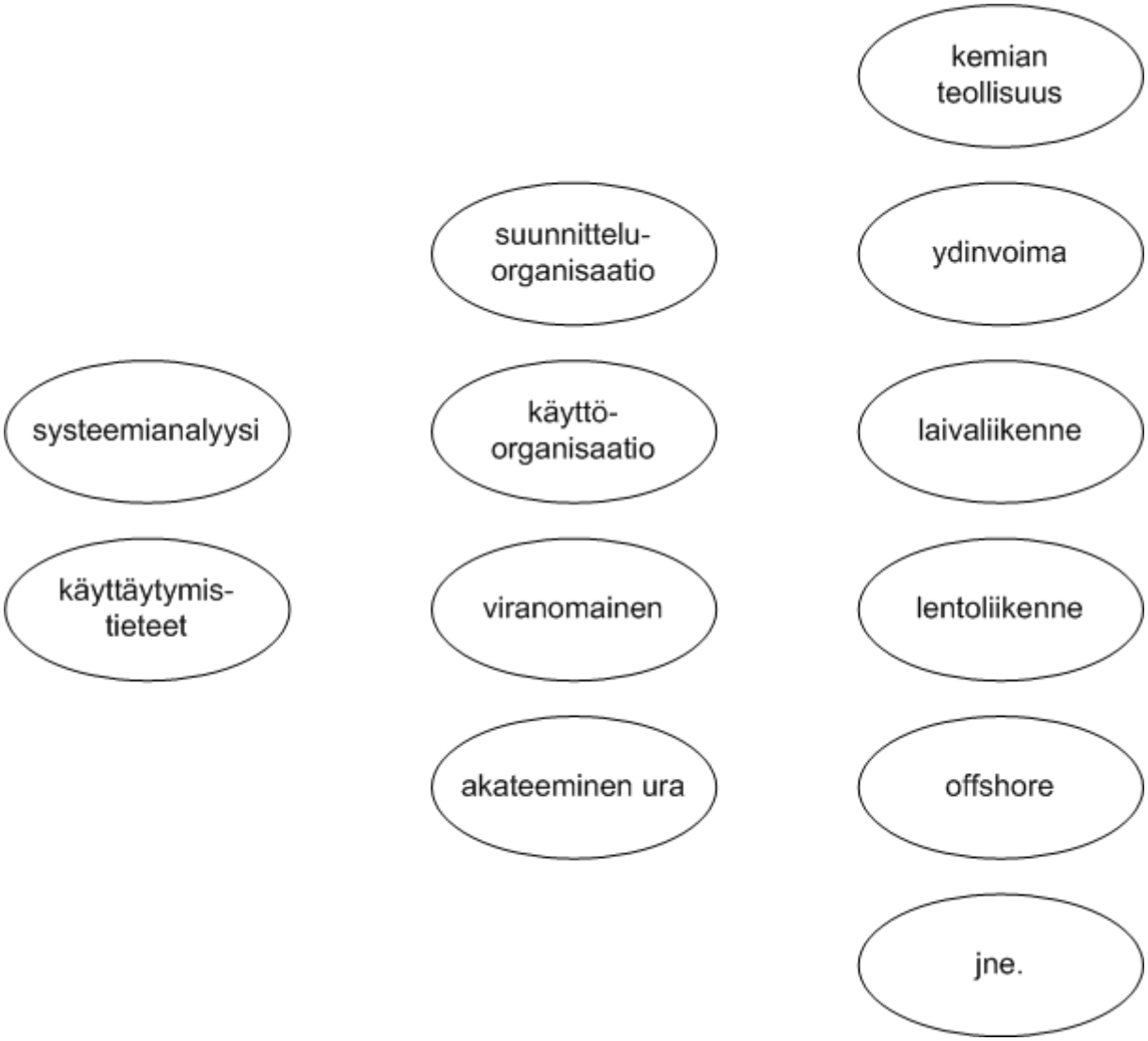
Ensimmäinen päivä, 29.8

- ap, 9.00-12.00
  - kurssikokonaisuus
  - muutama onnettomuus
    meriliikenne, kemiallinen teollisuus, offshore, lentoliikenne, avaruus, ydinvoima, padot
  - miksi onnettomuudet tapahtuvat
    muutama onnettomuusmalli, hallinnan romahtaminen, kurssin keskeiset käsitteet, riskien olemus
  - turvallisuusjohtaminen
    turvallisuusjohtamisen periaatteet
  - turvallisuusjohtamisen tehtävät
    riskianalyysi, käyttökokemusten hyödyntäminen, muutosten hallintaa, toiminnan arviointi
- ip, 13.00-16.00
  - tapahtuma-analyysin esimerkki
  - HTOI- malli
    miten mallia käytetään, onnettomuuksien syyt
  - systems of systems (SoS)
    SoS tyypit, kompleksisuuden haasteet
  - onnettomuuksien sarja
  - harjoitustehtävä 1

Turvallisuustekniikan suuntaukset



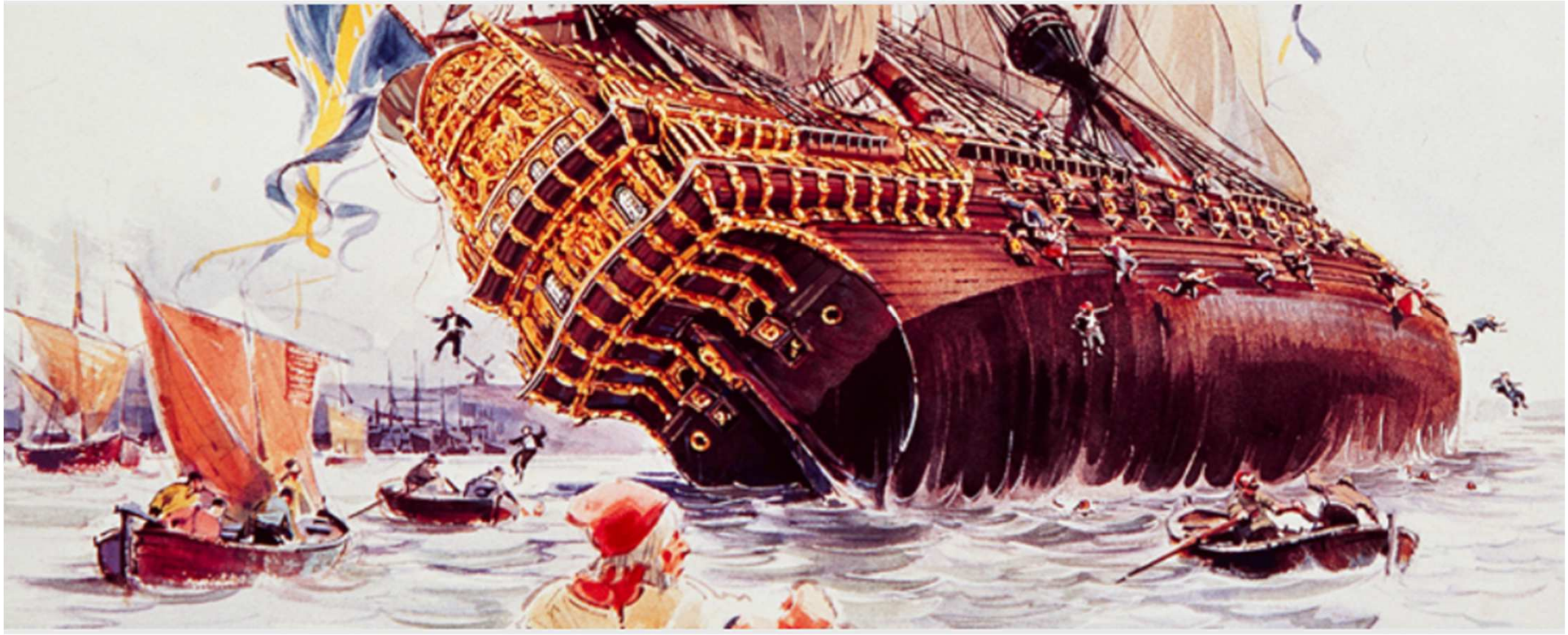
Erilaiset turvallisuudet

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

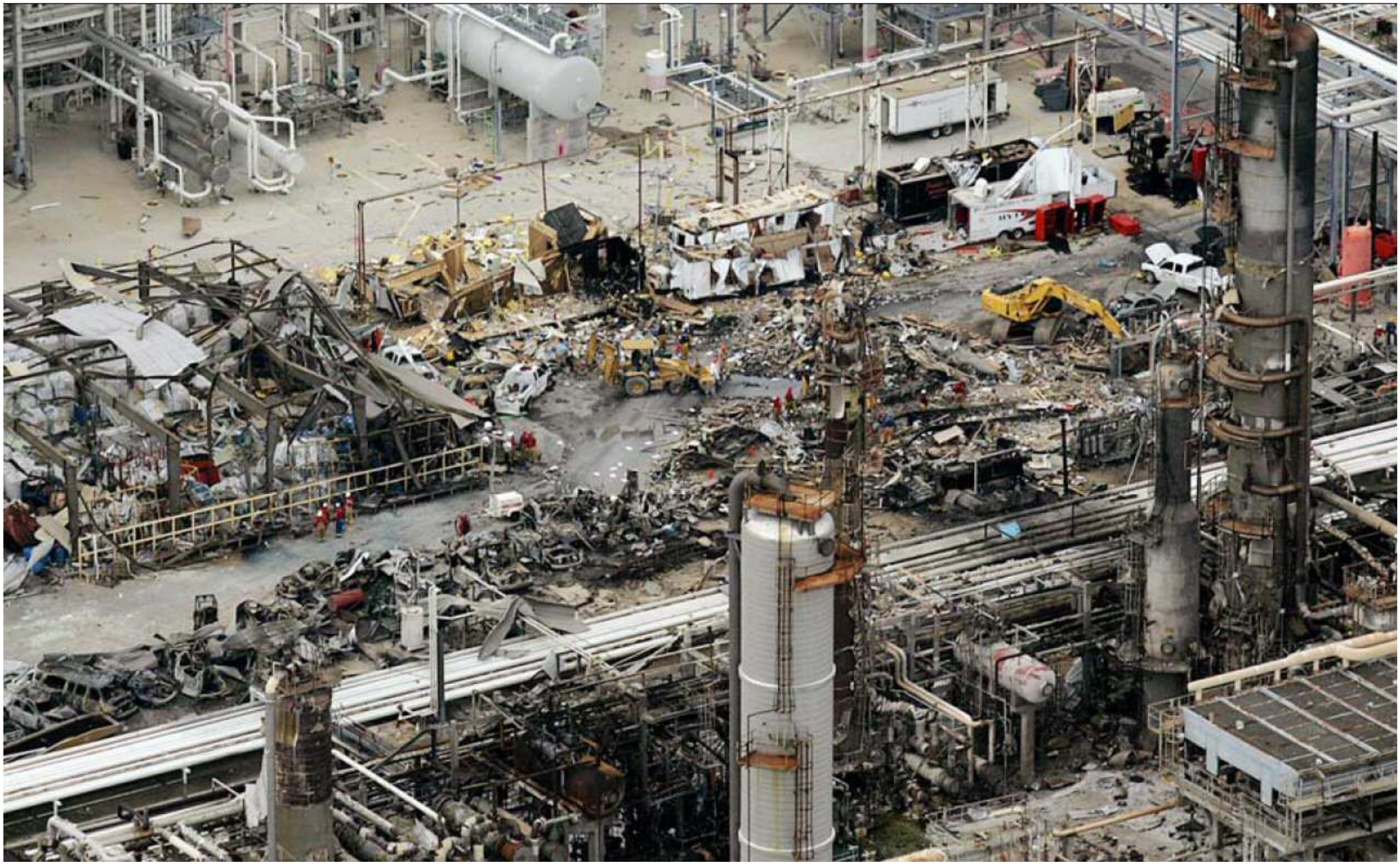
From assets to liabilities

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

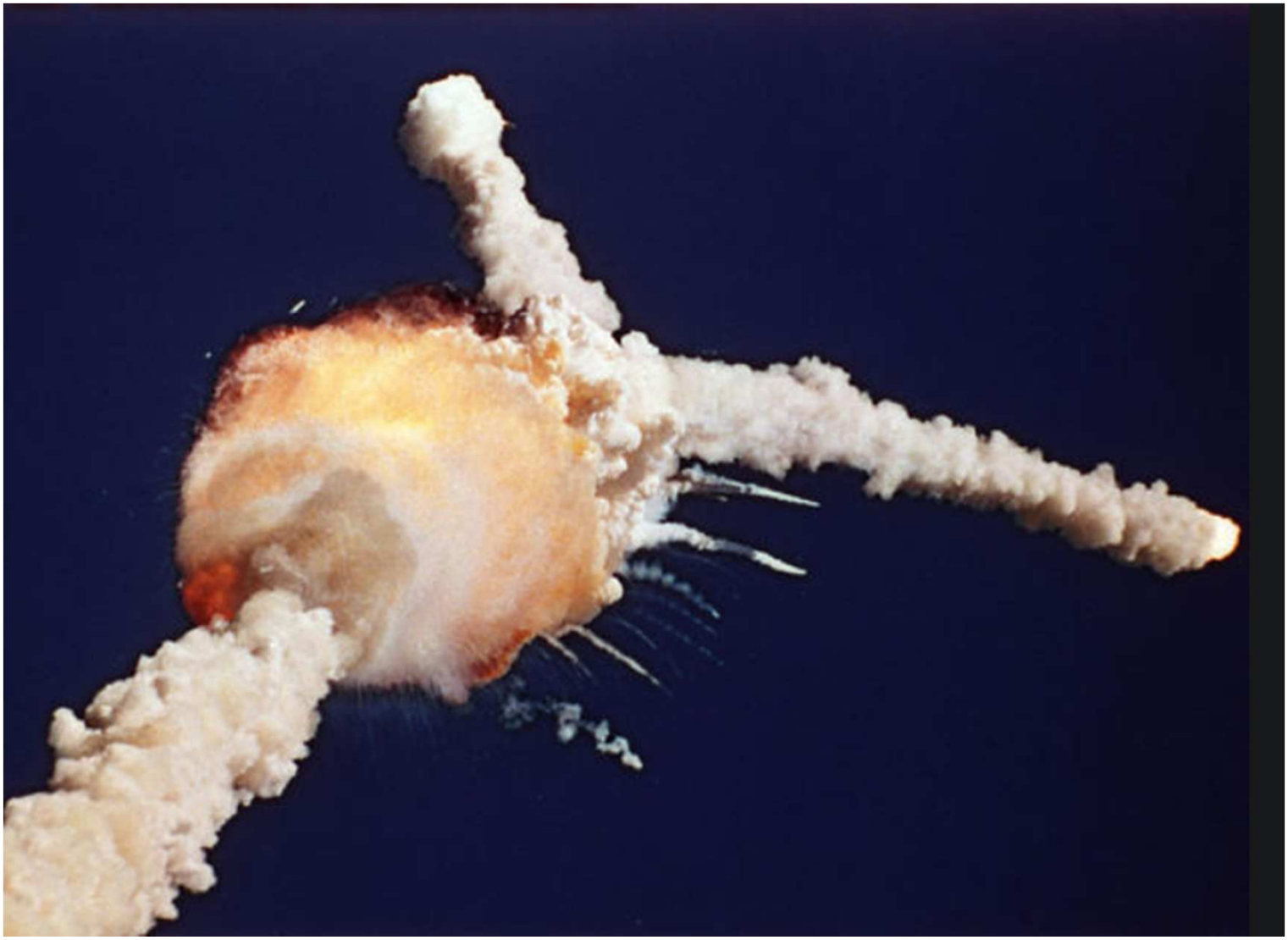
Piper Alpha was a North Sea oil production platform. The platform began production in 1976, first as an oil platform and then later converted to gas production. An explosion and the resulting oil and gas fires destroyed it killing 167 men leaving only 61 survivors.

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.

Tsernobyl 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

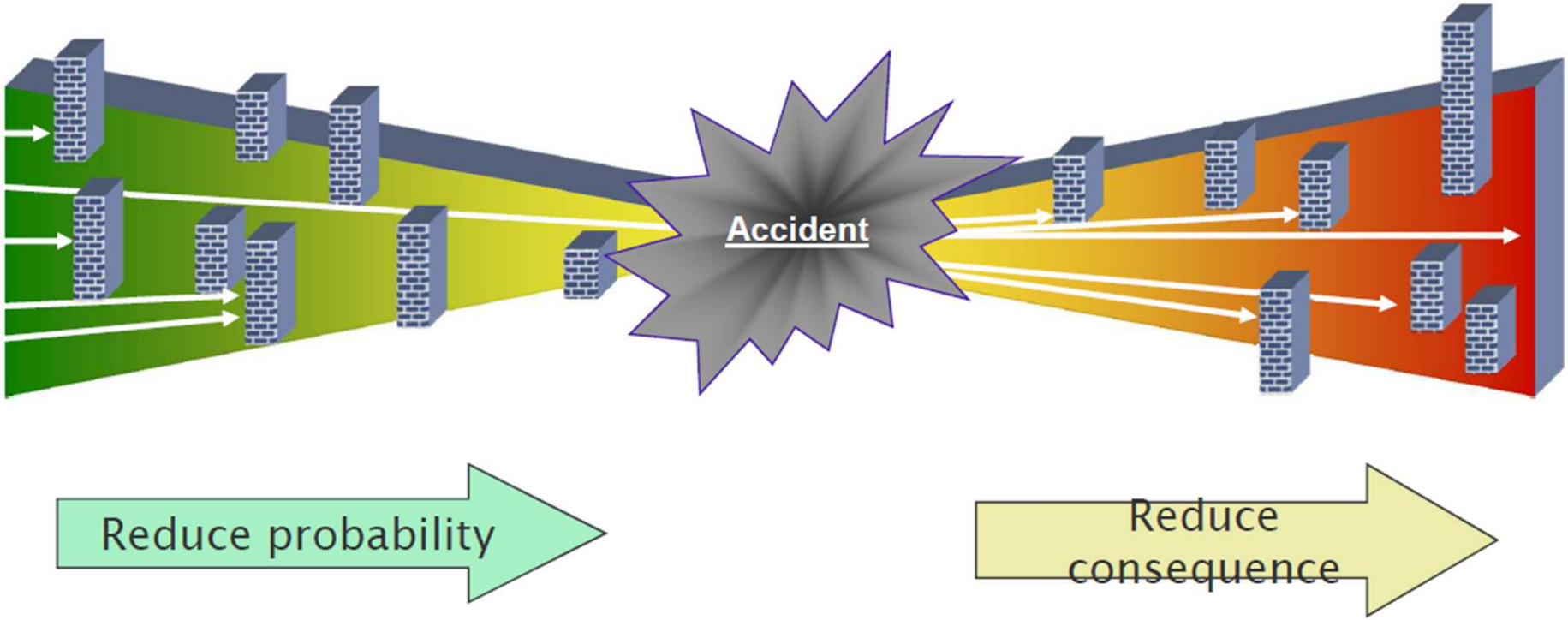
- tekninen systeemi
- ihminen kone rajapinta
- organisaatio
- informaatiojärjestelmä

mutta myös ihmisen toiminnasta systeemissä

- inhimmillisiä virheitä
- ajattelemattomuutta
- vastuutonta toimintaa
- tahallista vahingontekoa

Oikeastaan voidaan ihmetellä kuinka hyvin systeemit useimmiten toimivat!

The bow-tie* model of accidents



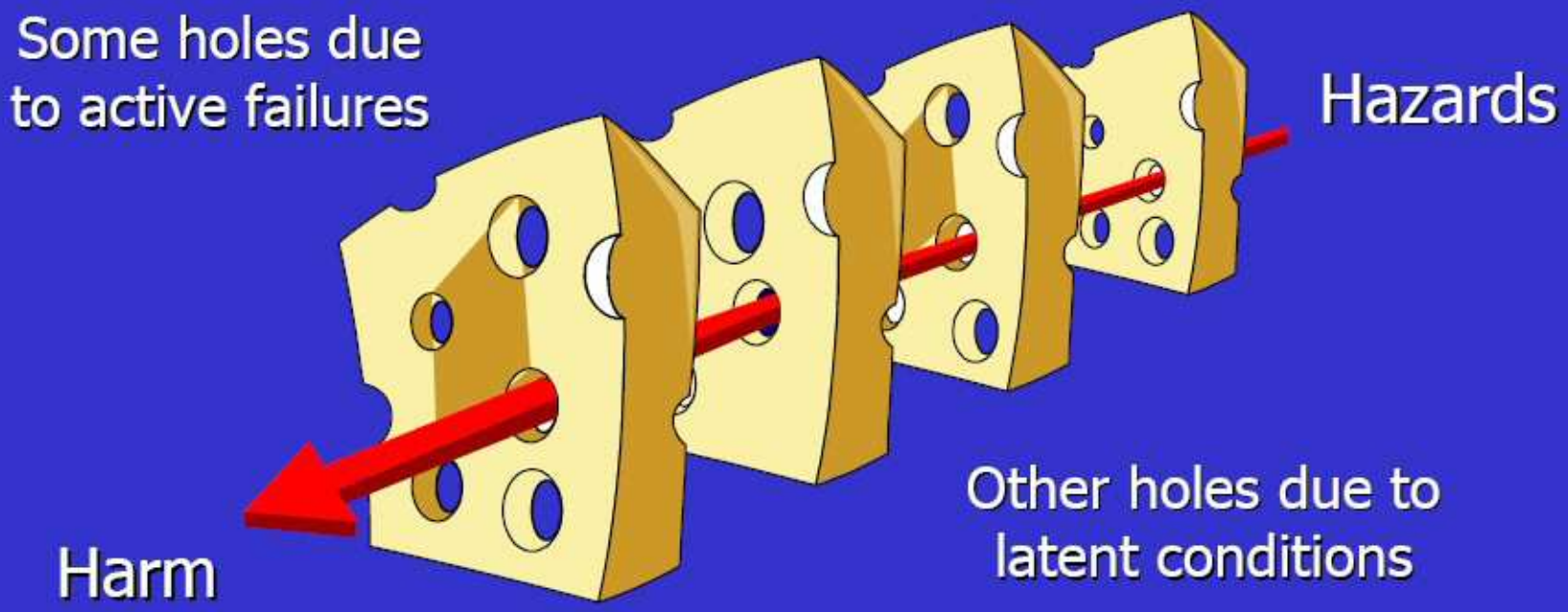
*bow-tie (suomeksi : solmuke, rusetti)

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

The 'Swiss cheese' model of accident causation



Successive layers of defences, barriers, & safeguards

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
- turvallisuuskulttuuri 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 keskittämista
- 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

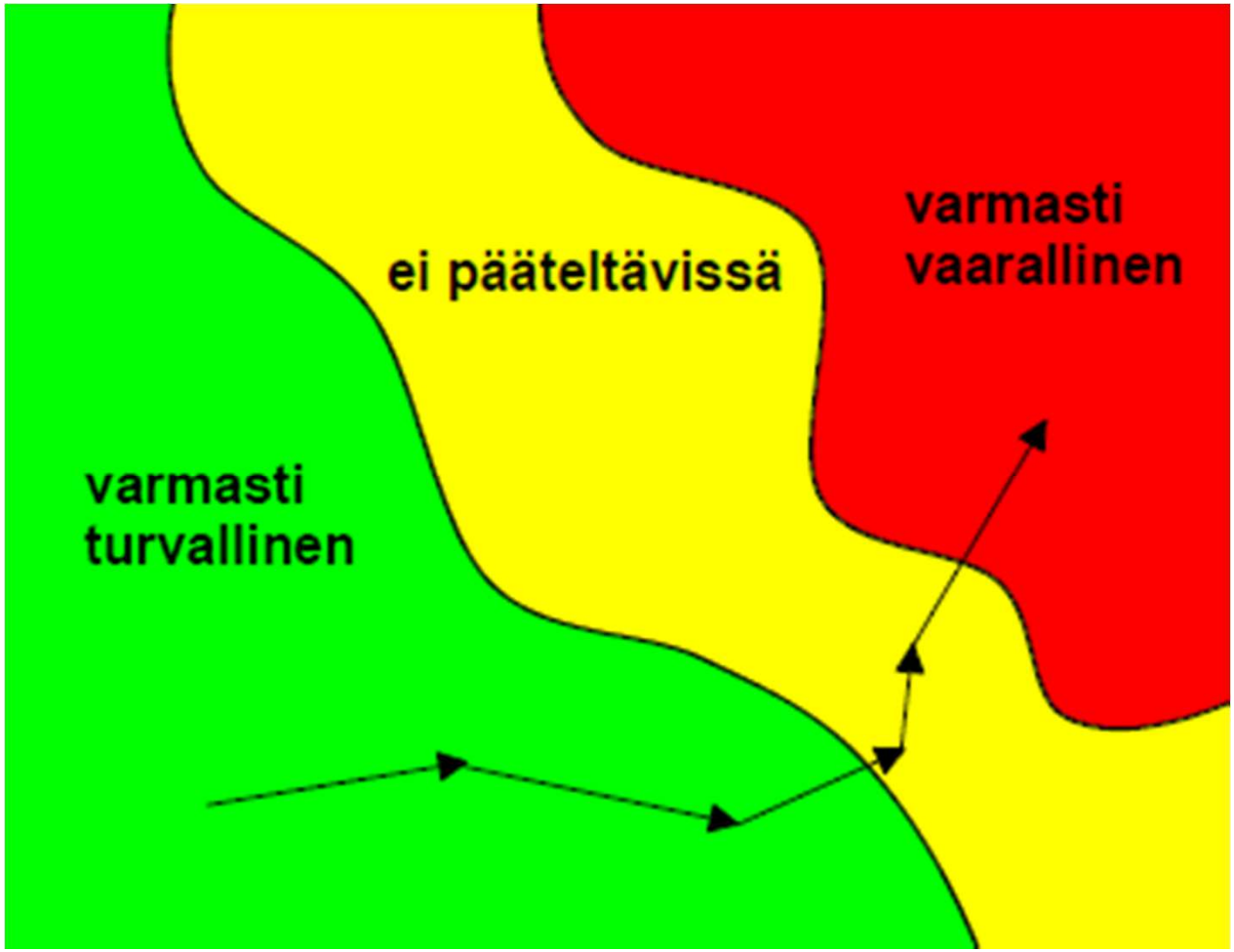
1. Tiedetään mitä halutaan (hyvyyskriteeri)
2. Systeemimallin olemassaolo
3. Tarkkailtavuus (systeemin tila voidaan havaita)
4. Ohjattavuus (systeemin tilaan voidaan vaikuttaa)

Turvallisuusjohtamisen kaksi tehtävää

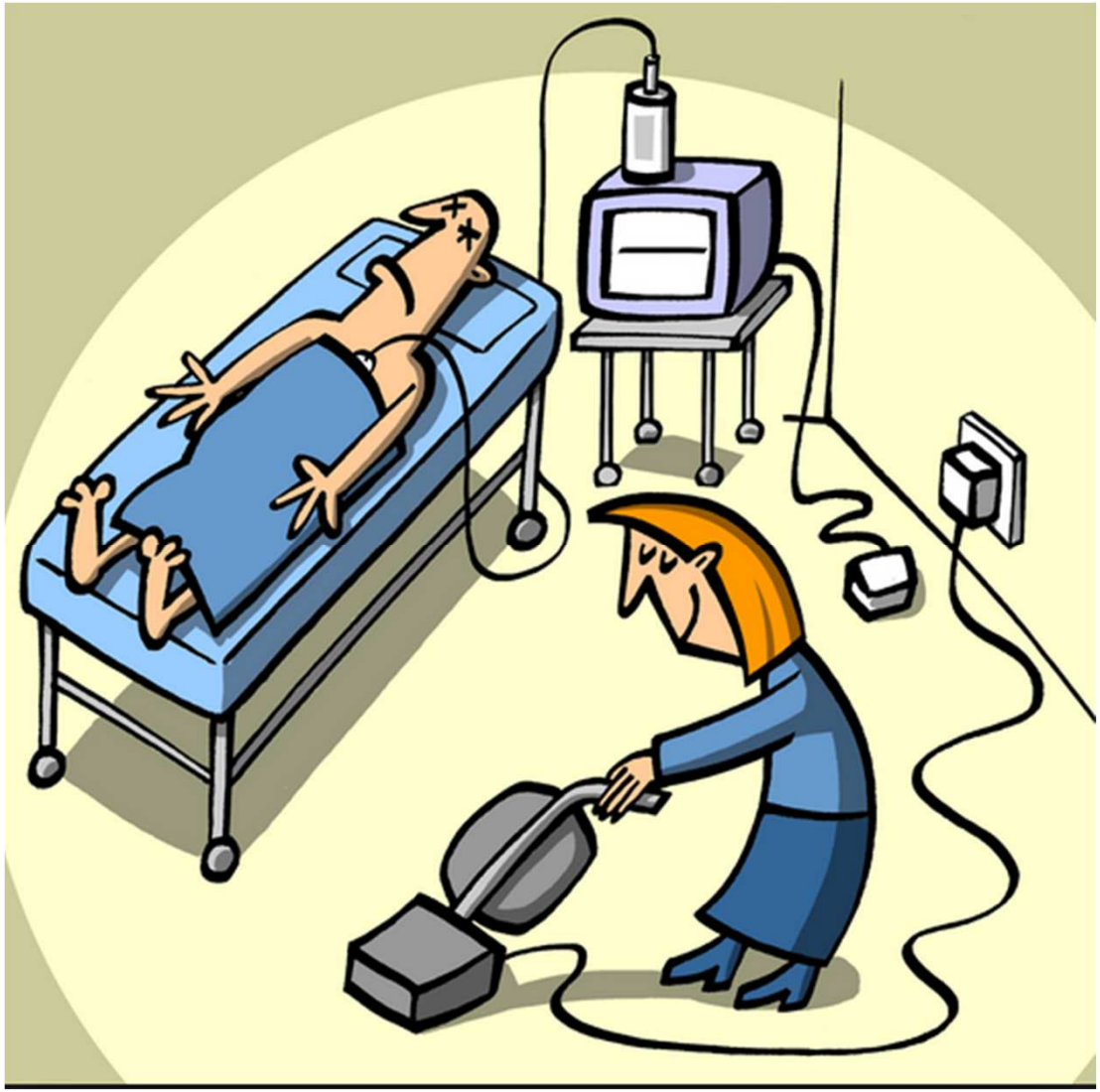
1. Pitää systeemiä turvallisessa tilassa (esteet)
2. Ohjata systeemiä turvalliseen tilaan (aktiiviset suojaukset)

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

Tila-avaruuden kolme aluetta



Toimenpide ja sen seuraukset!



Kurssin keskeiset käsitteet

- Uhat ja niiden toteutumisen seuraukset
- Onnettomuuden tapahtumat
  - ennen, aikana, jälkeen
- Erilaiset esteet
  - aidat, esteet, lukitukset, hallinolliset säännöt
  - 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)

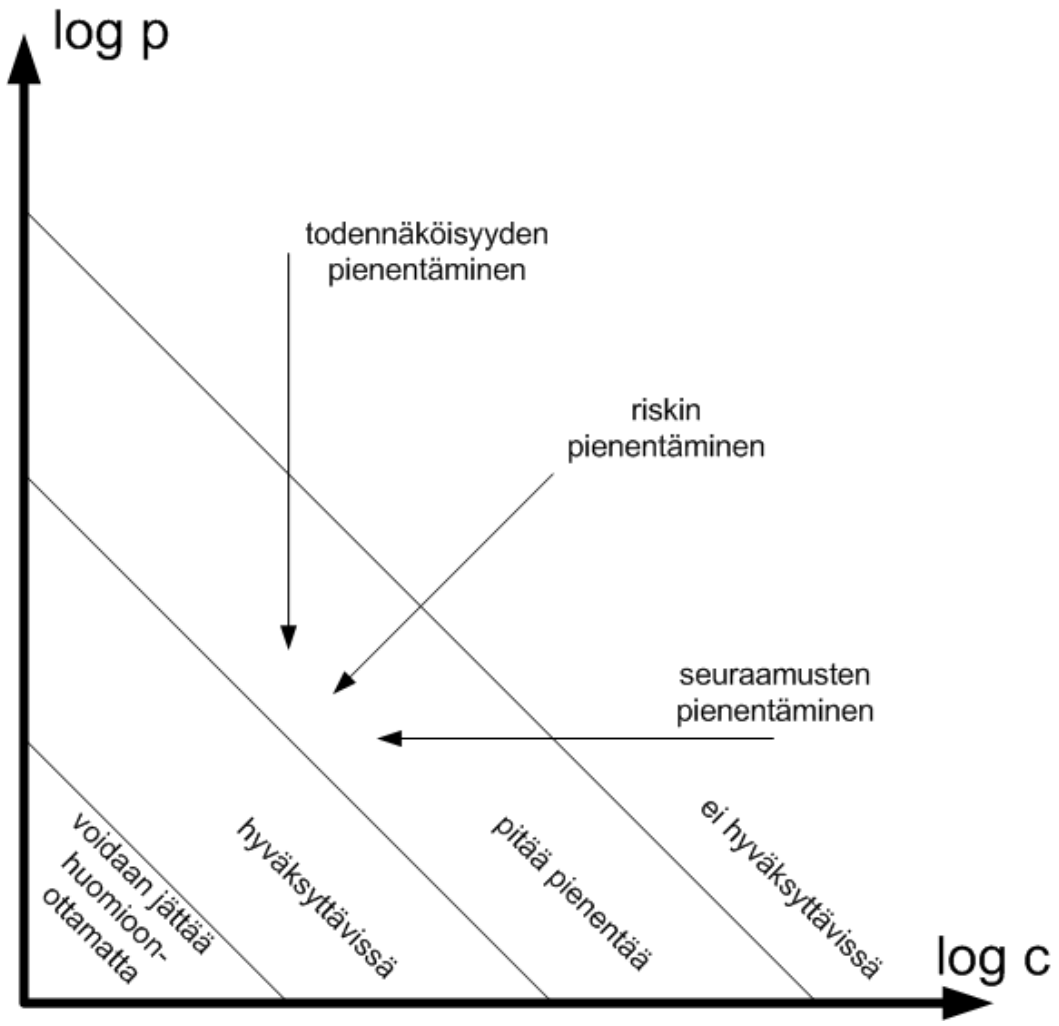
Riskikäsite

R = c * p

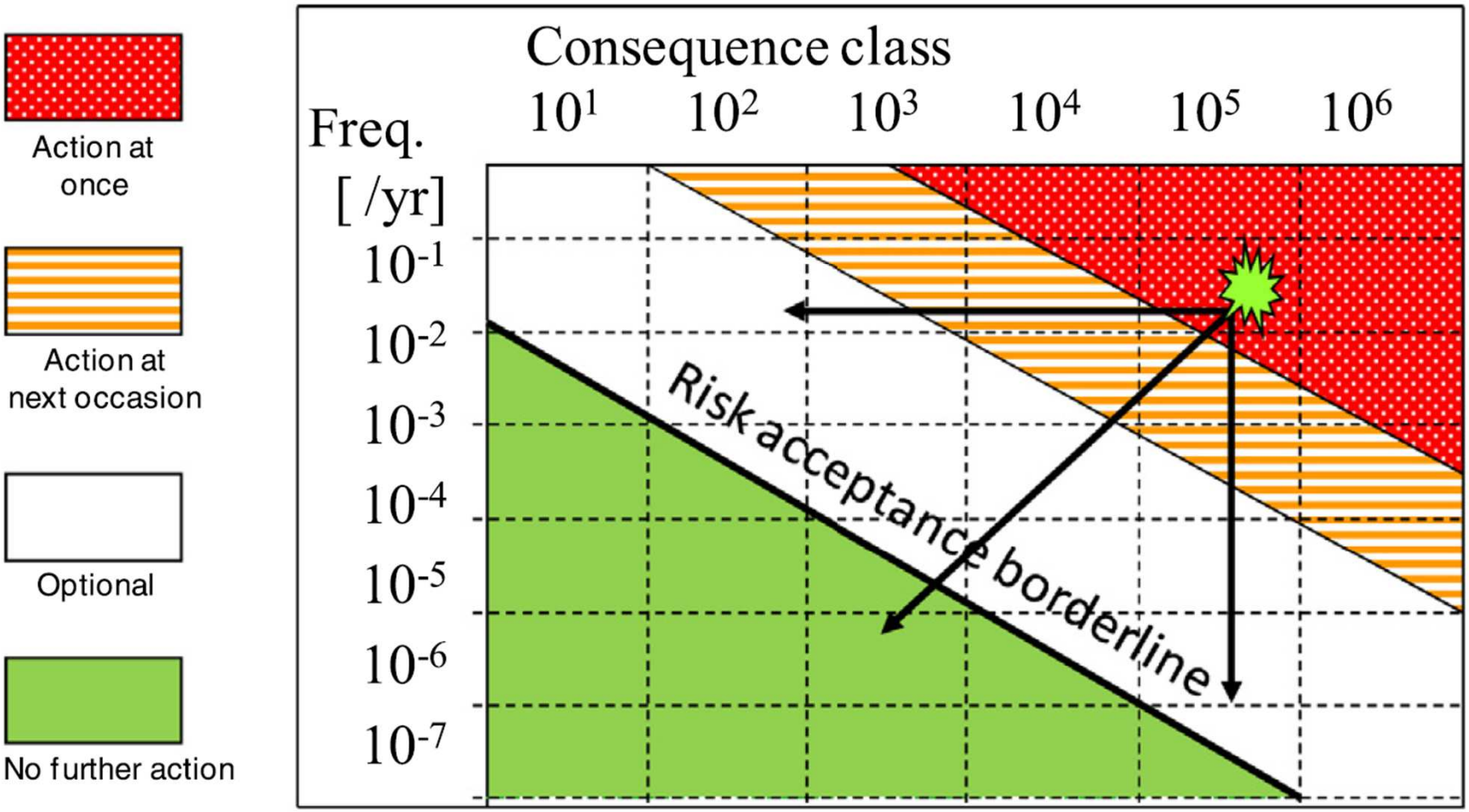
Ongelmana suuri kustannus ja pieni todennäköisyys

R = ∞ * 0 = ?

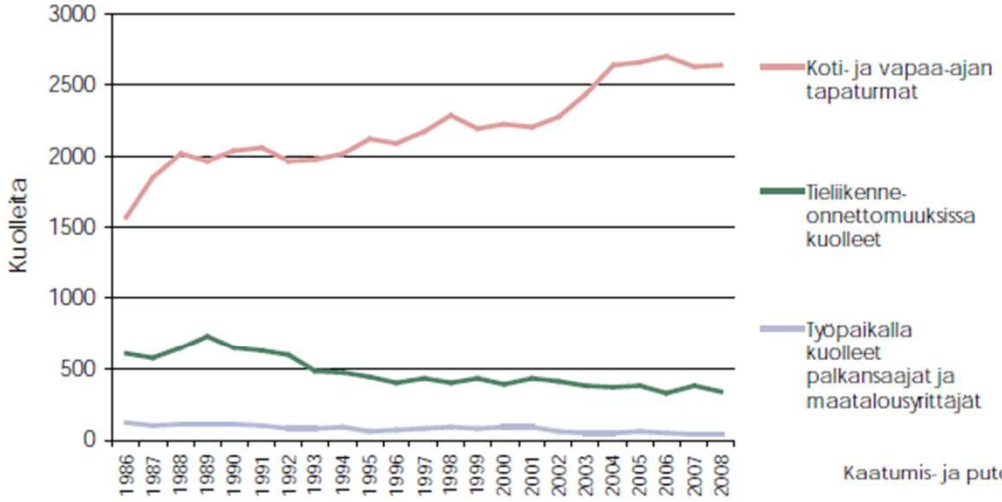
Miten saada uskottavat estimaatit c:lle ja p:lle?



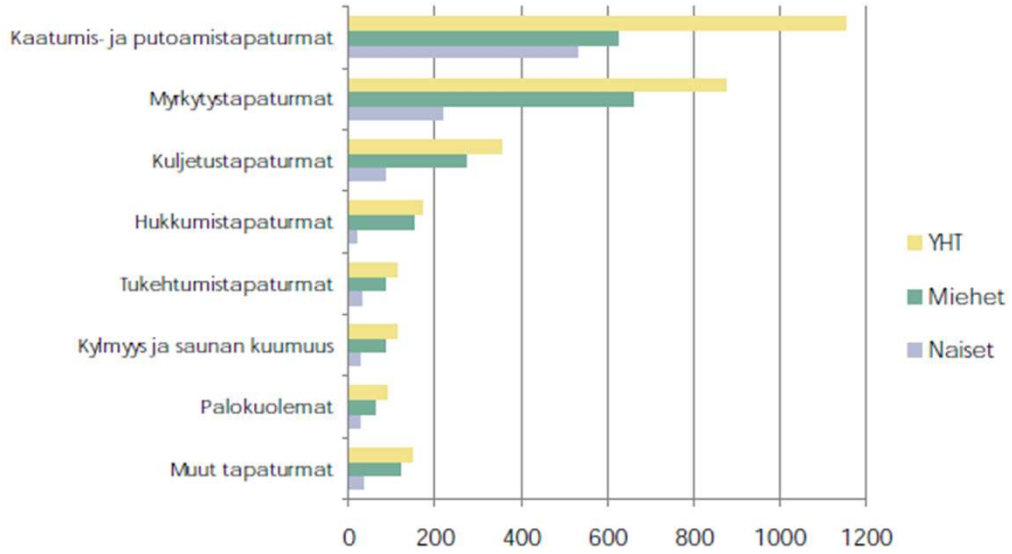
Riskien hyväksyttävyys



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.

Kesäloman suuret riskit: **viina ja puun poltto**

Ulkoiset uhat muodostavat pienemmän riskin kuin lomalaisen omat valinnat.

Johanna Junttila HS

GRILLIRUOASTA ja auringonpolttamista voi saa syövän, punkista taudin ja susi voi viedä marjastajan hengen.

Suomalaisten hinku viettää kesäpäiviä ulkoilmassa, tai vieläpä luonnon helmassa, tuntuu olevan vaaroja täynnä.

Vaara on onneksi eri asia kuin riski. Esimerkiksi lentokoneen putoaminen on hengenvaarallista, mutta yksittäisen matkustajan riski joutua tähän onnettomuuteen on hyvin pieni. Riski siis kertoo, miten todennäköisesti vaara toteutuu.

KUOLEMANSYITÄ tarkastellessa on oikeastaan nurinkurista, että suomalainen lahtaa pihasta kyykäärmeen ja pelkää metsäretkellä sutta. Sitten hän rentoutuu juomalla alkoholia ja lämmittää puusaunan.

Alkoholista johtuviin sairauksiin ja alkoholimyrkytykseen kuoli vuonna 2015 vajaat 1 700 suomalaista. Se on noin kolme prosenttia kaikista kuolleista.

Välillisesti alkoholi surmaa suomalaisia vielä enemmän. Samana vuonna 2015 tapaturmaisesti kuolleista vajaasta 2 200 suomalaisesta 300 oli vahingon sattuessa päihtynyt. Hukkuneista noin puolet oli humalaisia. Alkoholi edesauttaa myös joidenkin syöpien ja elintapasairauksien kehittymistä.

HS.fi
Kesän vaarat -digilehti kertoo lisää tietoa siitä, mitä kannattaa pelätä ja mitä ei.
HS.fi/kesanvaarat

PALAMISESSA syntyvät pienhiukkaset ovat suomalaisille melkein yhtä turmiollisia kuin alkoholi.

Ne aiheuttavat Terveyden ja hyvinvoinnin laitoksen arvion mukaan joka vuosi 1 600 kuolemaa, lähinnä siksi, että pienhiukkaset vaikuttavat hengitys-, sydän- ja verenkiertosairauksien syntyyn.

Eniten pienhiukkasia leijailee Suomessa naapurustoissa, joissa lämmitetään puulla takkoja, kiukaita ja uuneja. Pienet tulisijat ovat vastuussa noin 250 kuolemasta vuosittain. Loput menevät pääasiassa voimalaitosten ja autojen polttomoottoreiden piikkiin.

Satunnaisesti takkaa polttavia mökkiläisiä pelotellaan häkäkaasulla. Todennäköisemmin suomalainen menehtyy saunan kuumuuteen. Vuonna 2015 häkämyrkytyksiin kuoli vain 6 mutta saunakuolemiin 31.

KOTIEN puunpoltto on riskinä samaa luokkaa kuin liikenne.

Viime vuoden tilastot eivät ole vielä valmistuneet, mutta vuonna 2015 liikenteen tapaturmissa kuoli 268 ihmistä. Heistä 34 oli pyöräilijöitä, joista arviolta 10 olisi jäänyt henkiin käyttämällä kypärää.

Liikenne selittää myös sen, miksi hirvi on Suomen tappavin eläin. Samana vuonna hirvikolareissa menehtyi 4 suomalaista.

Satunnaisia kuolonkolareita tulee myös törmäyksissä porojen, peurojen, hevosten ja koirien kanssa.

ELÄINTEN kohdalla pelätyimmät ovat harvoin vaarallisimpia. Hirven jälkeen kakkossijaa pitää hevonen. Sen kontolle lasketaan myös onnettomuudet, jotka sattuvat ratsastajille ja ohjastajille.

Eläinten levittämistä taudeista myyräkuume surmaa enemmän kuin punkin levittämät borrelioosi ja puutiaisaivotulehdus yhteensä.

Suomalaisen tappaa kahdeksan kertaa todennäköisemmin salamanisku kuin kyy tai karhu. Salaman aiheuttamia kuolemia ei riitä edes tilastoiksi kaikkina vuosina.

PELKOMME osuvat harhaan, koska aivomme arvioivat riskejä enemmän intuitiivisesti kuin loogisesti järkeillen.

Lento-onnettomuus tai terrori-isku väkijoukkoon herättävät voimakasta pelkoa, koska niissä kuolee äkillisesti useita ihmisiä. Saksalainen psykologian tutkija Gerd Gigerenzer kutsuu tätä ilmiötä kammoriskiksi.

KAMMORISKEJÄ on helpompi pelätä kuin riskejä, jotka toteutuvat vasta vilveellä tai jothin joutuu yksi onneton ihminen kerrallaan.

Kesäloman aloitus automatkalla tai jokailtainen viininlipitys mökillä eivät tunnu vaarallisilta. Silti liikenteessä kuolee melkein yksi sadasta suomalaisesta ja alkoholiin noin yksi kymmenestä.

Suurin uhka suomalaisille ovat epäterveelliset elämäntavat.

Maailman terveysjärjestö WHO listaa kehittyneiden maiden isoimmat kuolemien riskitekijät tässä järjestyksessä: kohonnut verenpaine, tupakka, korkea kolesteroli, ylipaino, hedelmien ja kasvisten vähäinen käyttö ja liikunnan puute. Perässä tulevat alkoholi ja ilmansaasteet.

Fakta

Suomen tappavimmat eläimet 1998–2015

- Hirvi 101
- Hevonen 41
- Peltomyyrä 30
- Ampiainen 23
- Koira 21
- Nauta 12
- Punkki 12
- Kissa 3
- Karhu 1
- Kyy 1
- Mehiläinen 1
- Pässi 1
- Susi 0

► Lähde: Tilastokeskus

Suomen tappavimmat eläimet 1998–2015

- Hirvi 101
- Hevonen 41
- Peltomyyrä 30
- Ampiainen 23
- Koira 21
- Nauta 12
- Punkki 12
- Kissa 3
- Karhu 1
- Kyy 1
- Mehiläinen 1
- Pässi 1
- Susi 0

► Lähde: Tilastokeskus

Riskien olemus

- Miten epävarmuutta pitää mallintaa?
  - todennäköisyydellä
    - frekventistinen tulkinta
    - Bayesilainen tulkinta (subjektiivinen todennäköisyys)
  - mahdollisuudella (possibility theories)
- Aleatorinen 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.

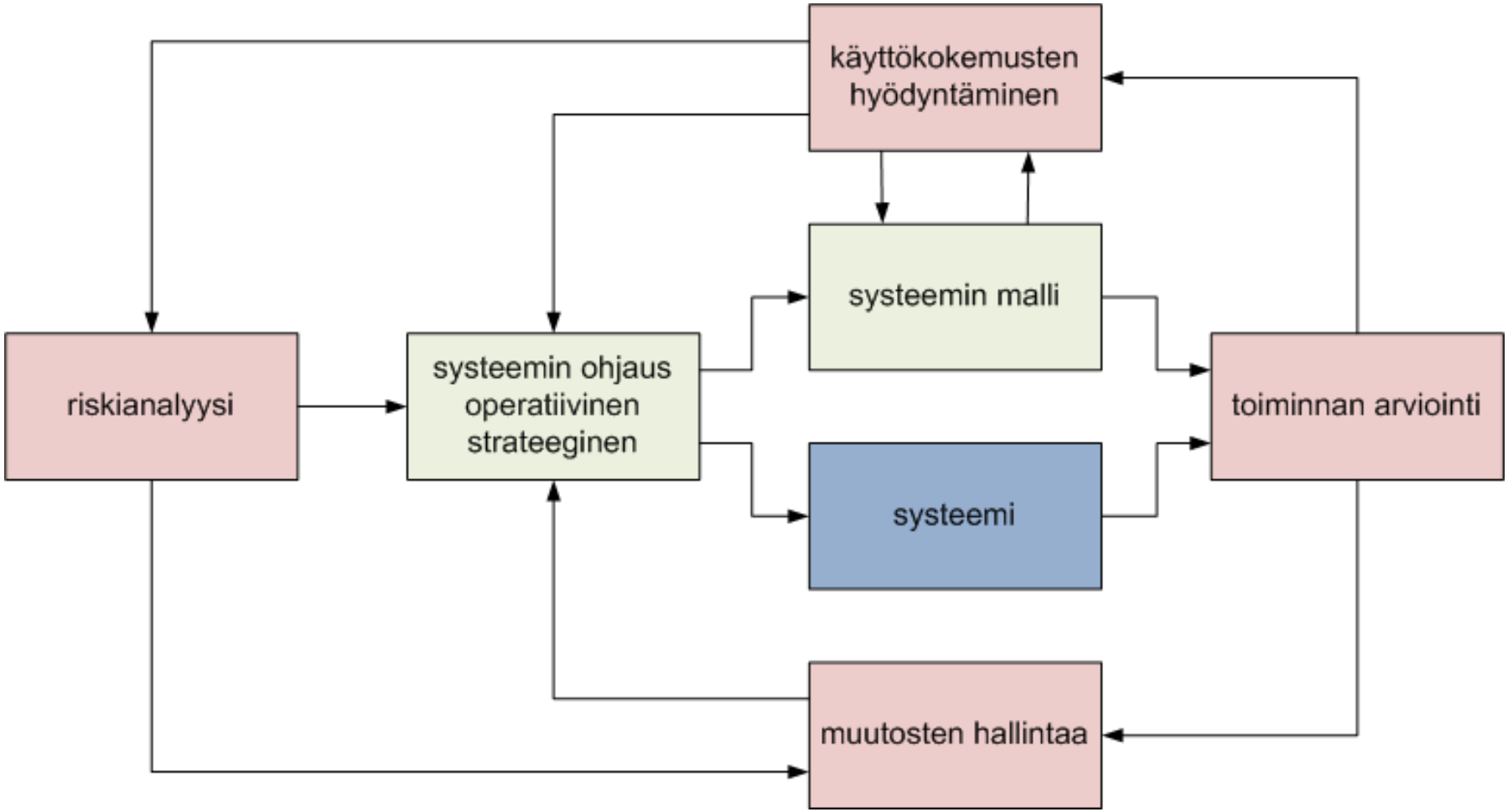
Turvallisuusjohtaminen

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
  - toimitaan innovatiivisesti
- tapahtuman jälkeen
  - mitä tapahtui?
  - miten voimme siitä oppia?
  - miten syysteemejä tai johtamisjärjestelmää pitäisi muuttaa?

Johtamisjärjestelmä antaa organisaatiolle puitteet toimia ennen, aikana ja jälkeen

Turvallisuusjohtamisen periaateet



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 (kvalitatiiviseen maallin liitetään todennäköisyydet haaroitumispisteissä)

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

Riskianalyysin vaiheet

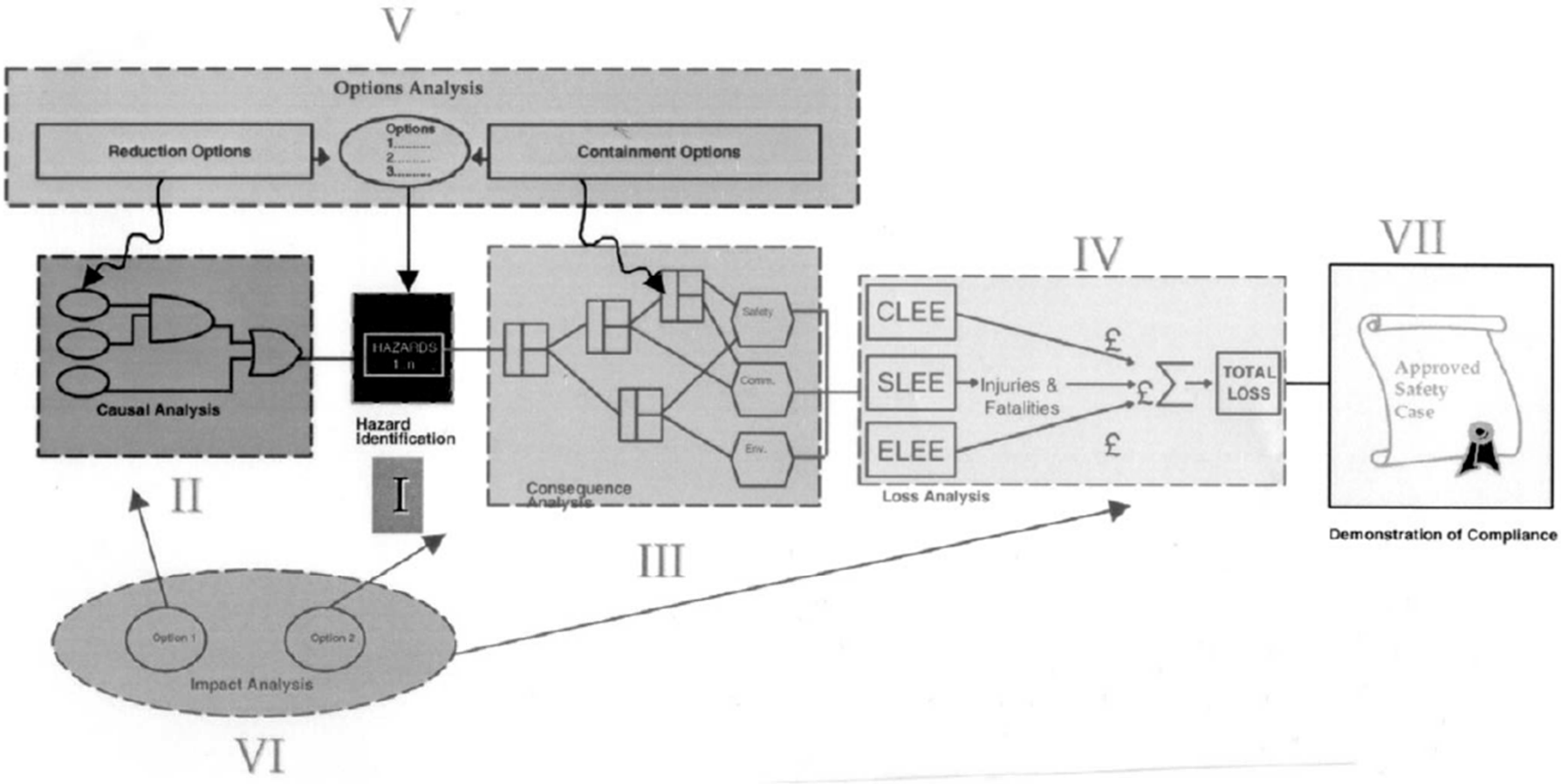


Figure 1 The seven-stage systematic risk assessment framework.

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

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 (ennen)
  - niistä johtuvia seurauksia

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 (2014). Requirements for improved process hazard analysis (PHA) methods, Journal of Loss Prevention in the Process Industries 32, 182-191.

Probabilistinen riskianalyysi (PRA)

Vikapuu (viottumisen todenäköisyys)

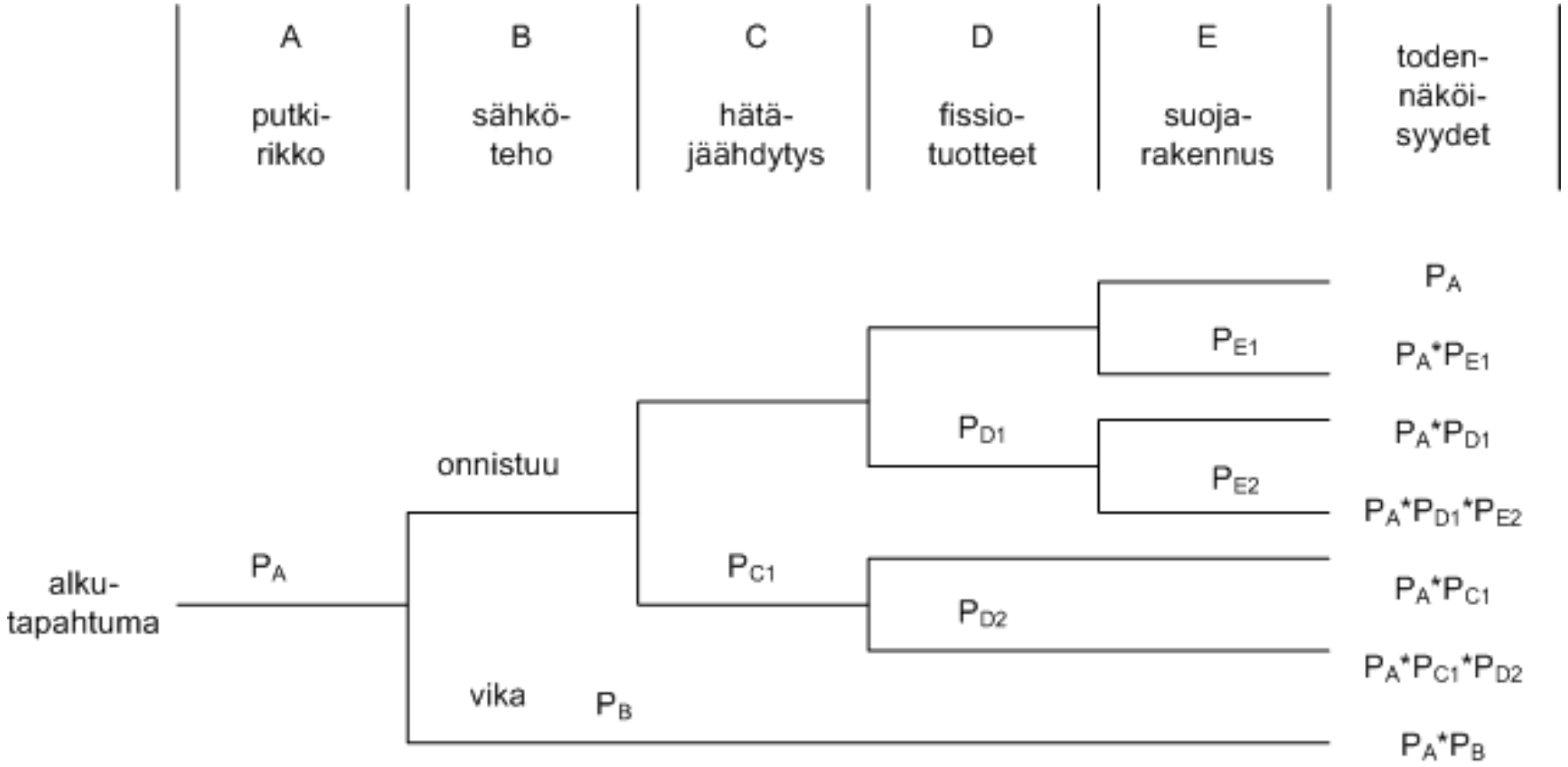
- toiminto tai komponentti vikaantuu jostain syystä
- siitä seuraa ... josta seuraa ...
- jne.

Tapahtumapuu (tapahtuman todennäköisyys)

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

Arvioidaan todennäköisyydet ja summataan kaikkien riskien yli

Todennäköisyysperusteinen riskianalyysi (PRA)



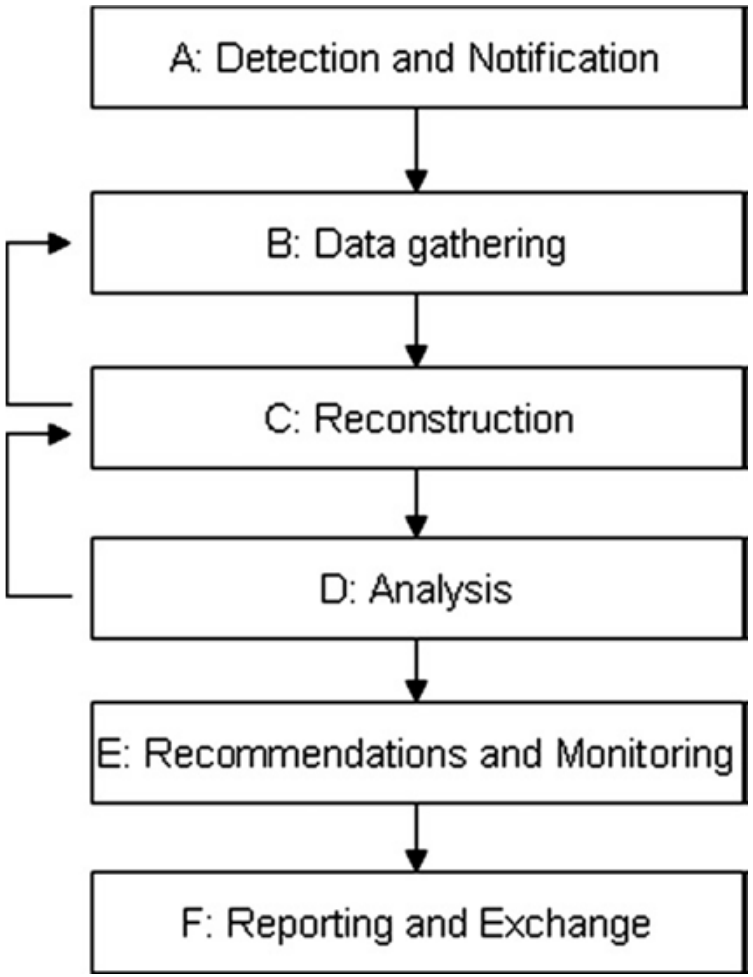
IAEA (2010). Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide No. SSG-3

Käyttökokemusten keräys ja analysointi

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

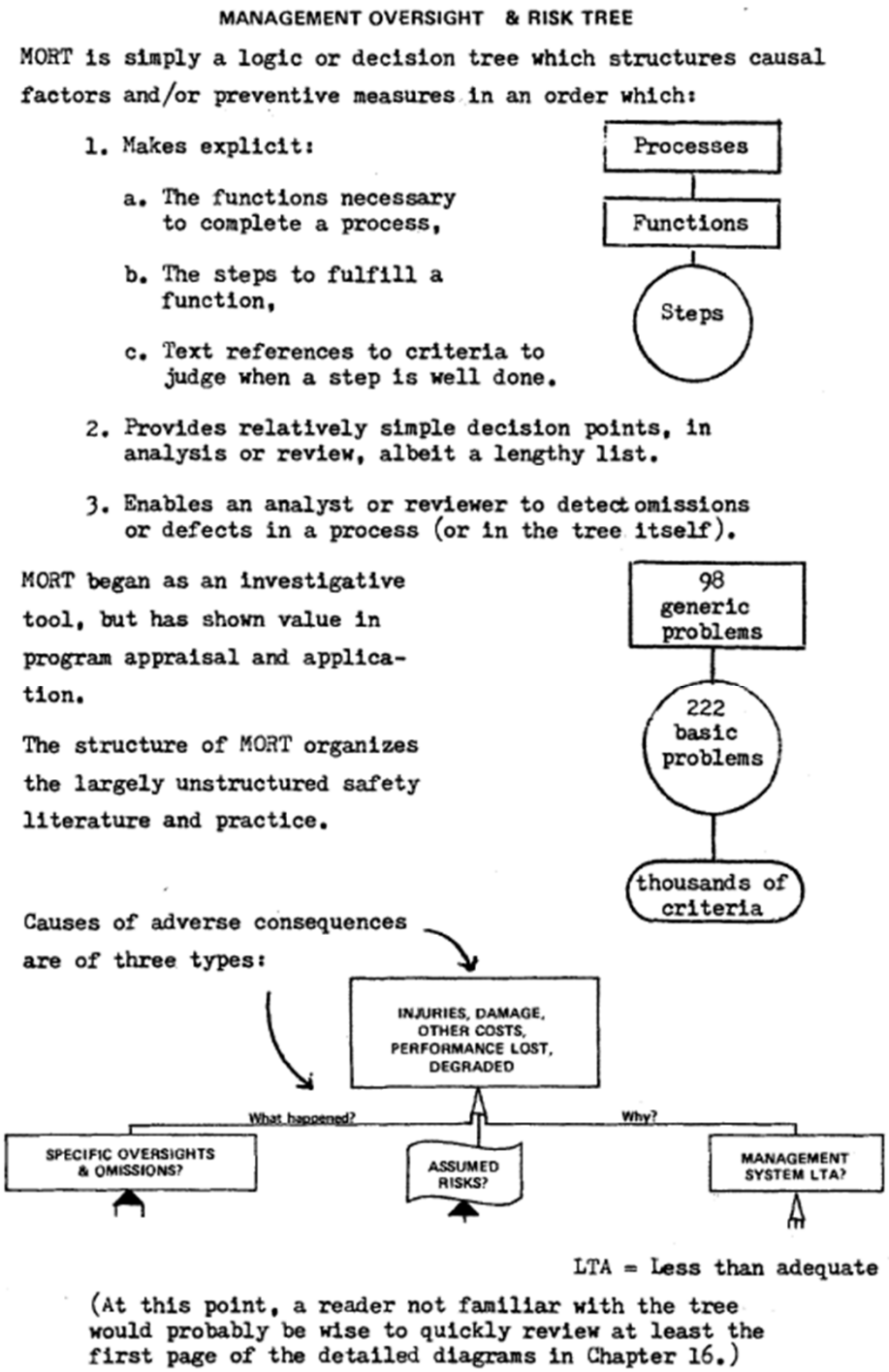
J. Lundberg, C. Rollenhagen, E. Hollnagel (2009). What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals, Safety Science 47, 1297–1311.

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 (2013). Beyond Root Cause Analysis: An Enriched System Oriented Event Analysis Model for Wide Application, Systems Engineering Vol. 16, No. 4.



Management Oversight and Risk Tree (MORT)

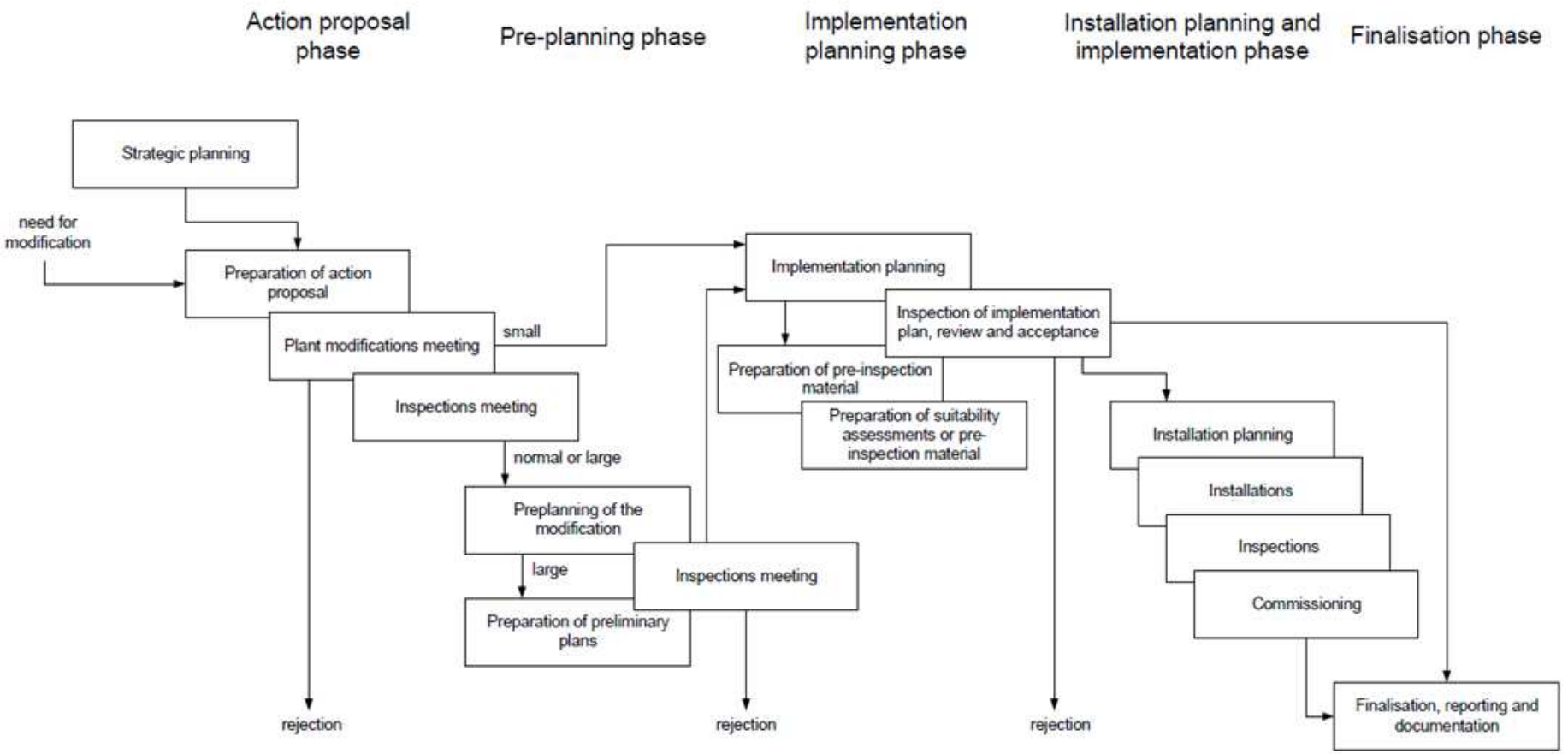
- menetelmä tapahtumen analysoitiin
- pitkä lista avainsanoja , jotka tukevat analyysia
- melkein 600 sivua paksu ohjekirja vuodelta 1973 on samalla johdatus riski-analyysiin
- osa ohjekirjasta keskitty johtamiseen ja tuo siitä oma ihannemallinsa
- lähinnä kiinnostava turvallisuustekniikan historian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

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

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

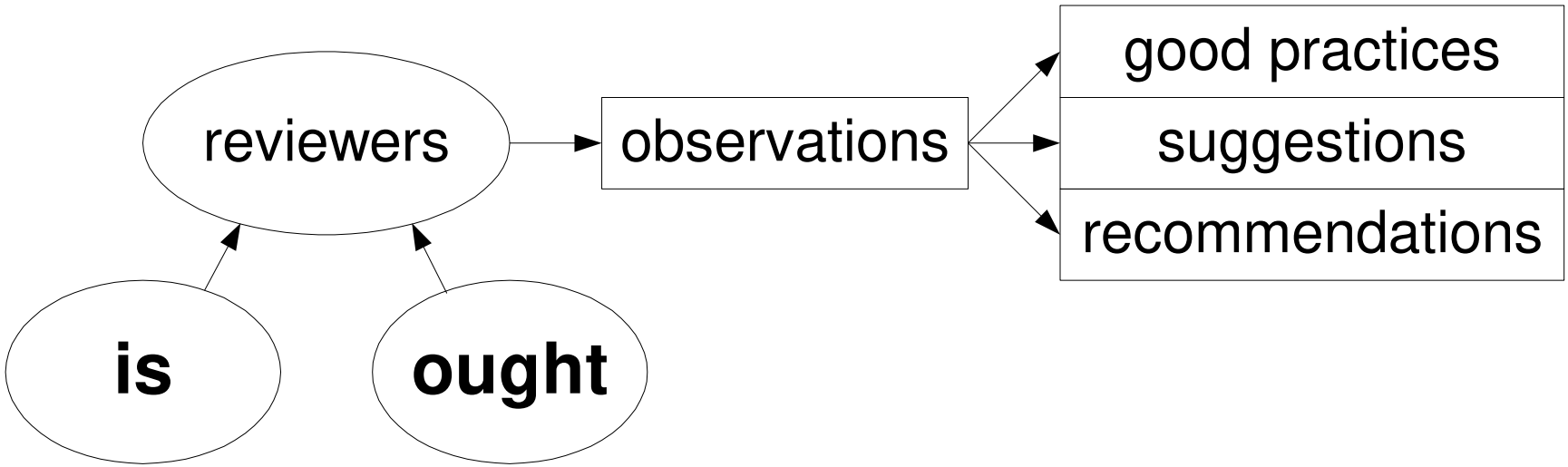
- Arvioinnin tulos

  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



Stegen

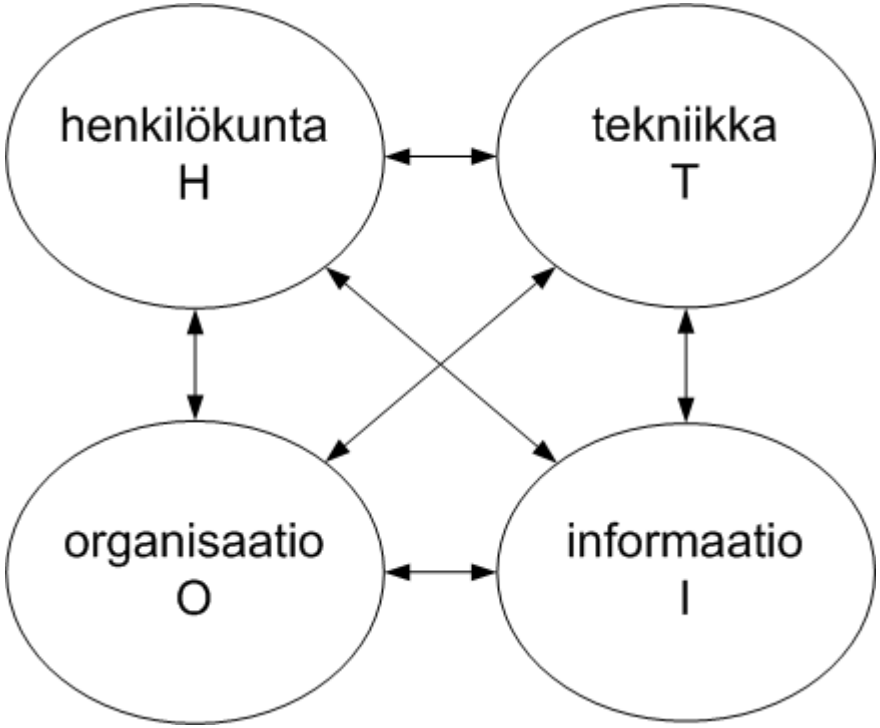
Carl Rollenhagen

Björn Wahlström

→Stegen.ppt

HTOI-malli

- Human
- Technology
- Organisation
- Information



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

HTOI-mallin käyttö

Tilakomponenttien turvalliset alueet määrittelevät turvallisuuden välttämättömät ehdot

- H, ammattitaitoinen, osaava ja motivoitunut henkilökunta
- T, hyvin suunniteltu ja ylläpidetty laitos
- O, riittävät resurssit, toimiva johtamisjärjestelmä, turvallisuustyön neljä tehtävää hoidetaan kunnolla
- I, kattava ja toimiva informaatiojärjestelmä, käyttöohjeet ja dokumentointi pidetään ajan tasalla

Puutteita HTOI-mallin mukaan?

- Henkilöstö

  puutteellinen koulutus, liian vähän resursseja, huono ikäjakauma

- Teknillinen järjestelmä

  laitos on huonosti suunniteltu, kunnossapito on laiminlyöty

- Organisaatio

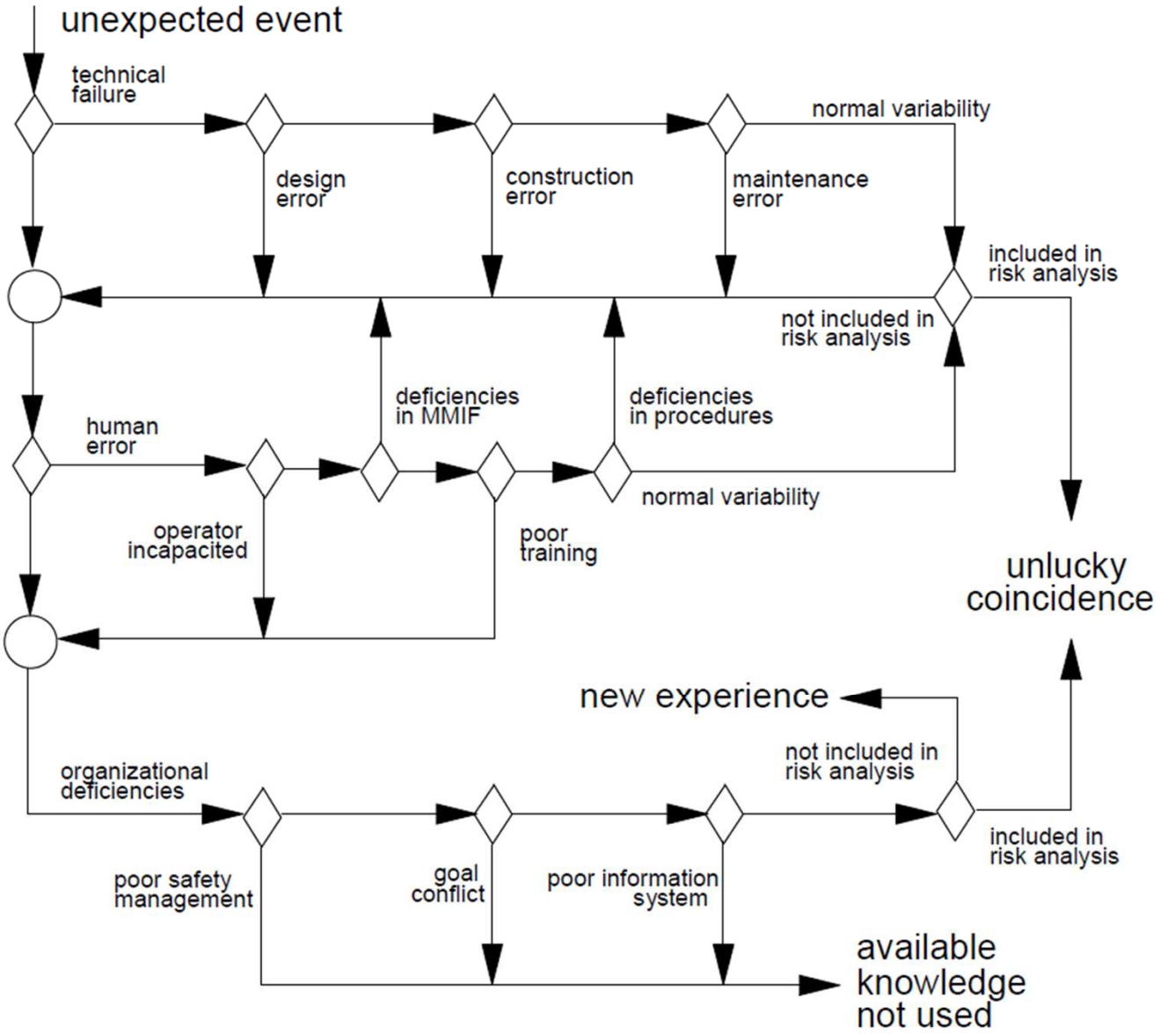
  johtoon ei luoteta, tehoton itsearviointi, identifioituja puutteita ei korjata

- Informaatio

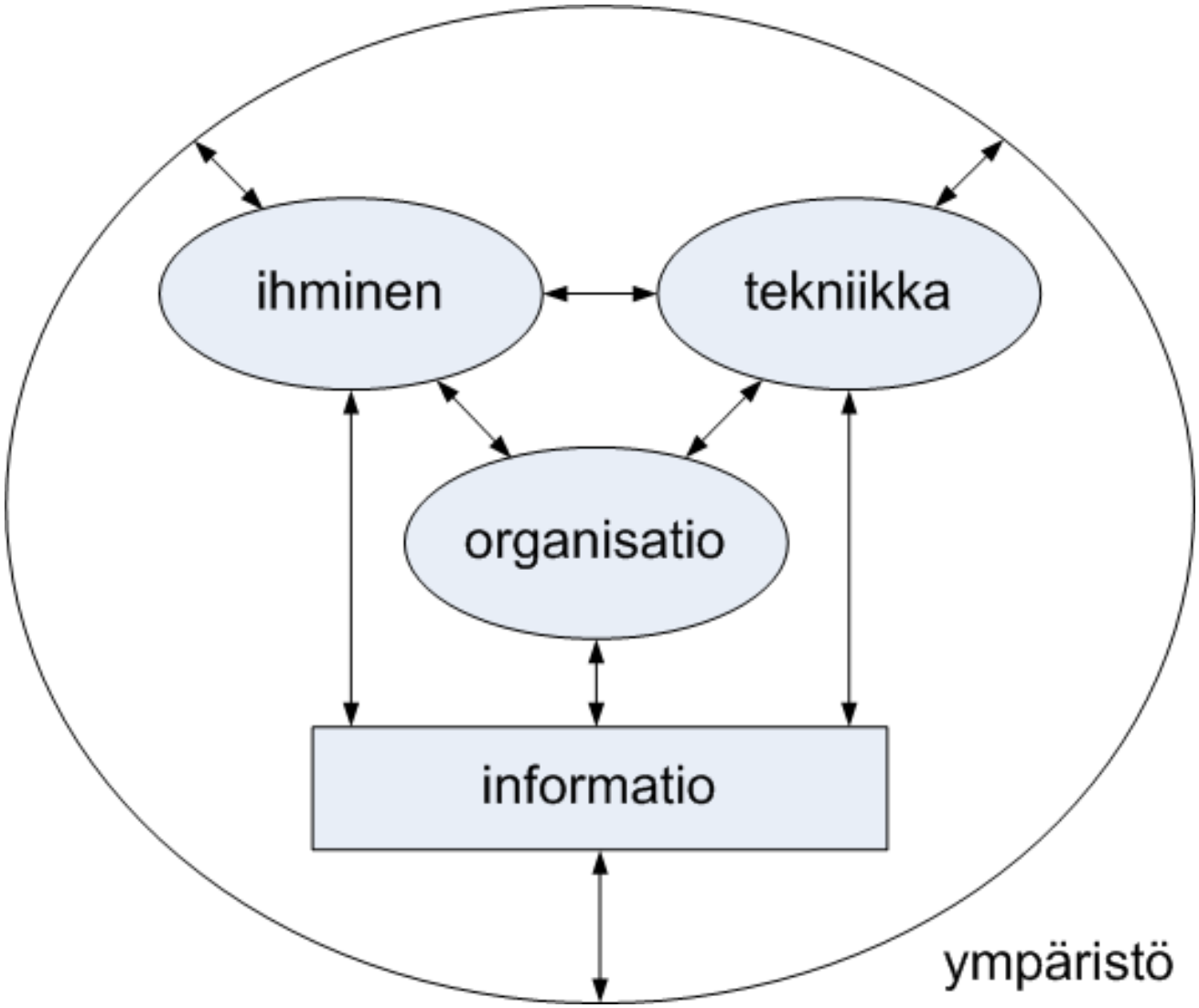
  informaatio ei kulje vertikaalisesti ja/tai horisontaalisesti, tärkeä informaatio ei päivitetä

Miksi? ... Miksi? ... Miksi? ... Miksi? ... Miksi? ...

Onnettomuuksien syyt?



Toinen tapa nähdä HTOI-mallia



Systems of System (SoS)

- Osasysteemien koordinointi

  johdettu ylhäältä, yhteiset hyväksytyt tavoitteet, yhteistoimintaa, virtuaalinen SoS

- Kompleksisuus (vaikeita ymmärtää ja mallintaa)

  sisäisiä takaisinkytkentöjä, monta tilamuuttujaa, epälineaariset vuorovaikutukset

- Riskien hallintaa

  ohjausrakenteiden mallintaminen, erilaiset muutospaineet, standardien käyttö, informaatiokanavat, henkilöstön ja resurssien hallintaa, ympäristöhuolet

C.N. Calvano, P. John: Systems Engineering in an Age of Complexity, Systems Engineering, Vol. 7, No. 1, 2004

Kompleksisuuden juuret

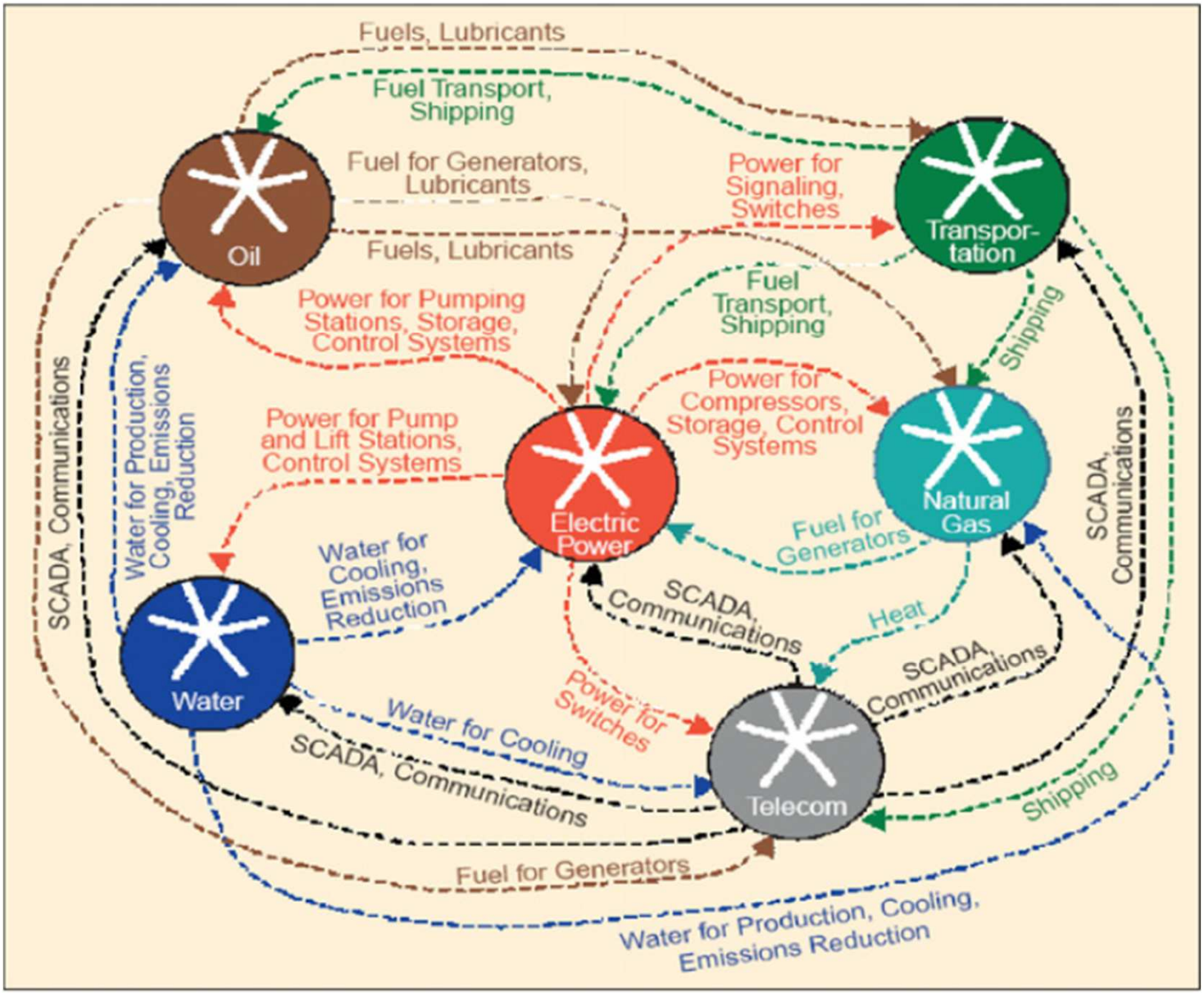
- Tila-avaruuden dimensio
- Liitäntöjen lukumäärä (osasysteemien sisällä ja niiden välillä)
- Epälineaaristen liitäntöjen esiintyminen ja niiden lukumäärä
- Erisuuruiset aikavakiot osasysteemien sisällä ja niiden välissä
- Erilaiset mallinnustavat ja erityyppisten mallien liittämistä toisiinsa
- Tavoitteiden identifiointi ja mallintaminen eri osasysteemeissä
- Eri ympäristöjen huomioonottaminen

SoS tyypit

- Virtual SoS
  - no central management authority
  - no centrally agreed-upon purpose
  - systems can enter/exit dynamically based on mission requirements
  - potential for emergence of large scale system behavior (which may be desirable)
  - relies on relatively hidden mechanisms for maintenance
  - examples: Stock market, national economies
- Collaborative SoS
  - component systems interact more or less voluntarily to fulfill agreed upon central purposes
  - e.g., internet is a collaborative SoS; the Internet Engineering Task Force defines but can't enforce standards
  - central players collectively decide how to provide/deny service (some means to enforce and maintain standards)
  - examples: World-wide web, multi-robot systems
- Acknowledged SoS
  - has recognized objectives, a designated manager, and resources; however,….
  - constituent systems retain independent ownership, objectives, funding, development and sustainment
  - changes in the system are based on collaboration between the SoS and the system
  - example: DoD's Ballistic Missile Defense System
- Directed SoS
  - integrated SoS is built and managed to fulfill specific purposes
  - centrally managed during long-term operation to fulfill purposes and any new ones set by system owners
  - component systems maintain ability to operate independently, but their normal operational mode is subordinated to the central managed purpose
  - example: JPL's Deep Space Network

A.M. Madni, M. Sievers: System of Systems Integration: Key Considerations and Challenges, Systems Engineering, 17:2, 2014

Interdependent infrastructures



I. Eusgeld,C.Nan, S.Dietz: "System-of-systems" approach for interdependent critical infrastructures, Reli. Eng. & Syst Safety 96 (2011) 679–686

SoS themes and key challenges

- Network structure
  - Challenge 1: socio-technical–organisational interactions
- Complexity and external influence
  - Challenge 2: complexity
  - Challenge 3: openness
- An emergent whole
  - Challenge 4: emergent behaviour
  - Challenge 5: unpredictability
- Information transfer across boundaries
  - Challenge 6: boundaries
  - Challenge 7: responsibility
- Continual change and culture
  - Challenge 8: change
  - Challenge 9: legacy (and longevity)
  - Challenge 10: culture (and climate)

C. Harvey, N.A. Stanton: Safety in System-of-Systems: Ten key challenges, Safety Science 70 (2014) 358–366

SoS changes

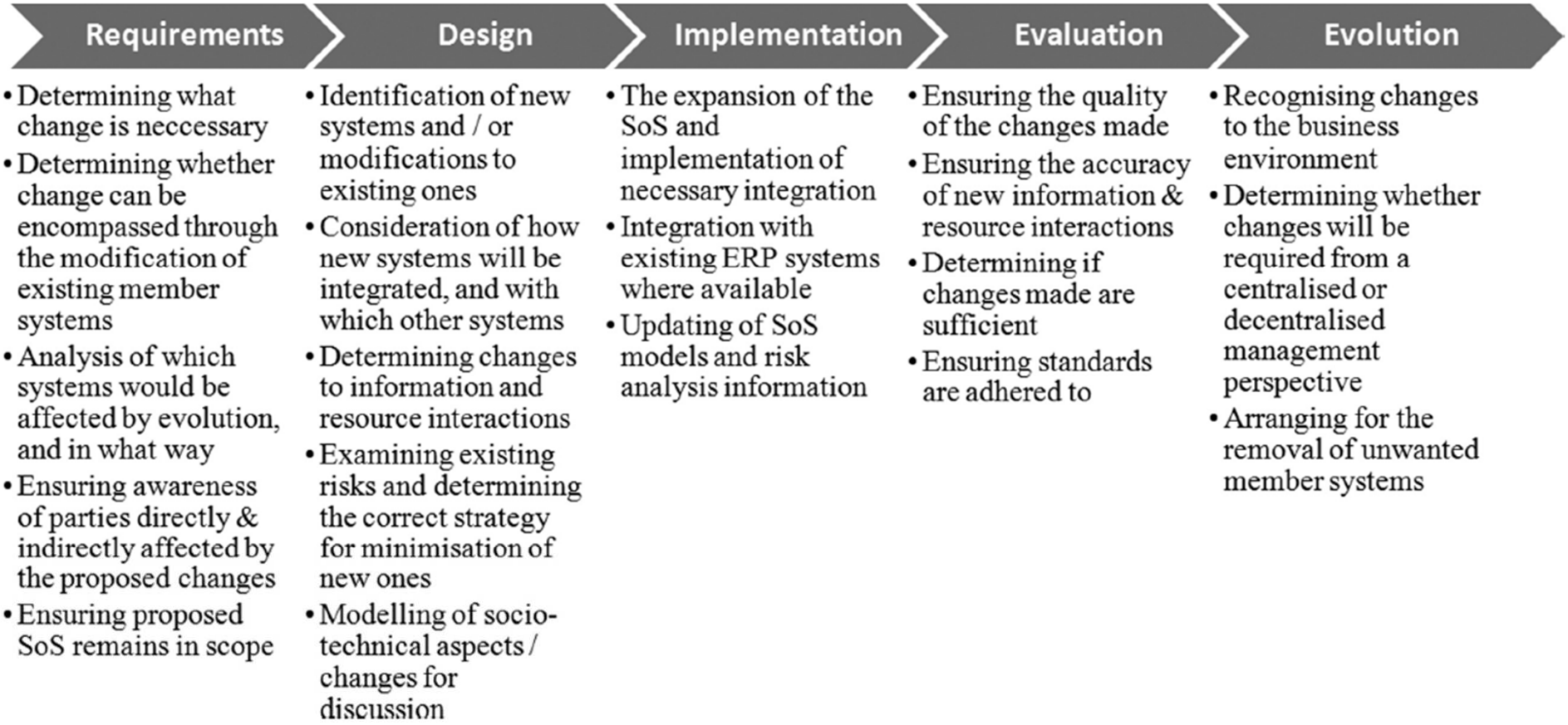


Figure 2. Adapted SoS development model.

R. Lock (2012). Developing a Methodology To Support the Evolution of System of Systems Using Risk Analysis, Systems Engineering, 15:1.

Design Questions Related to Highly Integrated Systems

Question	How well understood
What are our objectives?	Dynamic complexity does not make this difficult, although rapid development of technologies encourage other trends.
What must our solution do?	Relatively clear based largely on previous architectures
What solution options may be appropriate?	There are many solution options available, not because technological development in each individual engineering domain, but also at a system level because of ITC technologies
What option is best?	This evaluation is very difficult to conduct since the behaviors ofthe multiple options emerge from systemic interactions.
What constraints apply?	The range of potential constraints is broad and varied given the multitude of options and hence the are difficult to establish
What priorities are appropriate?	Priority judgments must be made with knowledge of implications of decisions and they are difficult to make
How will we know when we are done?	This is difficult to establish since there are greater risks of un-envisaged behaviors arising from strong lateral interactions
How confident are we?	Relatively clear, based largely on previous knowledge of the contributing technologies

C.N. Calvano, P. John: Systems Engineering in an Age of Complexity, Systems Engineering, Vol. 7, No. 1, 2004

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?