Toinen päivä, 30.8

- ap, 9.00-12.00
  - harjoitustehtävän palaute
  - MTOI- malli
    miten mallia käytetään, onnettomuuksien syyt
  - turvallisuus organisaation tavoitteena
    johtamisjärjestelmä, sen rakenne ja sisältö, organisaation ohjaukset, tehtävät päällikkötasolla, laatuajattelu, elinjakson huomioiminen
  - turvallisuuskulttuuri
    tausta, käsitteen kritiikkiä, turvallisuuskultturin mittauksen ongelma, kulttuuri kausaalisena selityksenä, turvallisuuden myyttejä
- ip, 13.00-16.00
  - organisaation puutteet
    esimerkkejä tutkimuksista, puutteiden syyt
  - organisaatioiden mallintaminen
    eräs kehys, fraktaalinen organisaatio, johtaja tai päällikkö, liian yksinkohtaiset mallit
  - turvallisuuskriittisen systeemin suunnittelu
    vaatimusten hallintaa, modularisointi ja integrointi, ihmisten huomioonottaminen, inhimmillset virheet, systeemin sovittaminen ihmisiin
  - turvallisuuden osoittaminen
    turvallisuusseloste, uusien systeemien turvallisuus, automaation turvallisuus
  - harjoitustehtävä 2

BPn turvallisuusjohtaminen

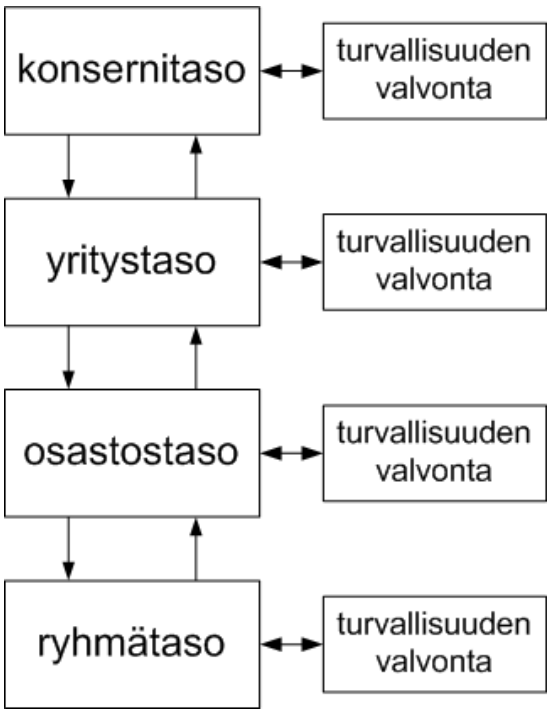
- Millaisia turvallisuuspuutteita näette BPn organisaatiossa?
- Mitä niille olisi pitänyt tehdä?
- Paljonko aikaa pitäisi varautua parannusten viemiseen käytäntöön?
- Voidaanko syyllistä nimittää tapahtumasarjassa?
- Voidaanko edellyttää että konseernijohtaja tietää mitä organisaation alemmilla tasoilla tapahtuu?

Palaute, harjoitustyö 1

Keskustelusta

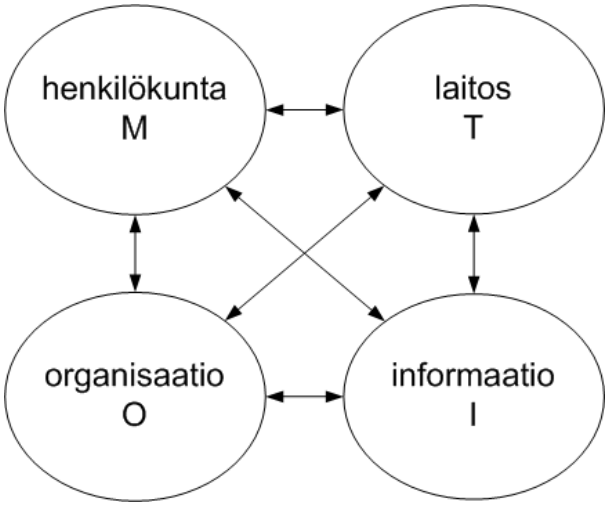
- Metodit riskihallintaan näytti puutuvan konsernitasolta
  - Ei rationaalista toimintaa businessriskien kannalta
- Julkiset ulostulot: toiset yritykset totesivat BPn toiminnan alaarvoiseksi,
  - oliko kommentti rehellinen katsoen heidään toimintaansa?
- Taustatekijänä Amerikkalainen businesskulttuuri
  - Englanti, Ruotsi ehkä toisella tavalla
- viranomainen ja lainsäädäntö oli liian heikko
  - Rikoksilla saatu voitto pitäisi voida tuomita takavarkoitavaksi
- Voidaanko yhtä putkea tarkastamalla todeta että muut ovat kunnossa
- Johtajien ja omistajien sitouttaminen epäonnistui
  - pitää ymmärtää että investointi turvallisuuteen todennäköisesti tuo notkahduksen tulokseen
  - Insentiivit: johtajien henkilökohtainen riski on pieni, vaikkakin sattuu onnettomuus ja tulee potkut eroraha tulee
  - Ylin johto oli fokusoitunut kasvuun, unohti turvallisuus
    - ostettiin konkurssikypsiä yrityksiä halvalla, eikö tarkoitus ollut saada niitä tuottamaan
- Tilanteen sallittiin jatkua kauan
  - Miksi kukaan ei puuttunut? Eikö toimintapaikoista löytynyt toimintaa seuranneita ihmisiä, jotka olisivat pystyneet reagoimaan aikaisemmin
  - Oltiinko epäonnistuttu jo niin pahasti, ettei kunniallista paluuta ollut?
- Salamyhkäisyyden kulttuuri: Epäonnistumisia peiteltiin maksamalla suuria summia sekä sakkoja

Turvallisuuden valvonta



MTOI-malli

- Man
- Technology
- Organisation
- Information



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

MTOI-mallin käyttö

Tilakomponenttien turvalliset alueet määrittelevät turvallisuuden välttämättömät ehdot

- M, 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 MTOI-mallin mukaan?

- Henkilöstö

  puutteellinen koulutus, liian vähän resursseja, huono ikäjakauma

- Teknillinen järjestelmä

  laitos on huonosti suunniteltu, kunnossapito on laiminlyöty

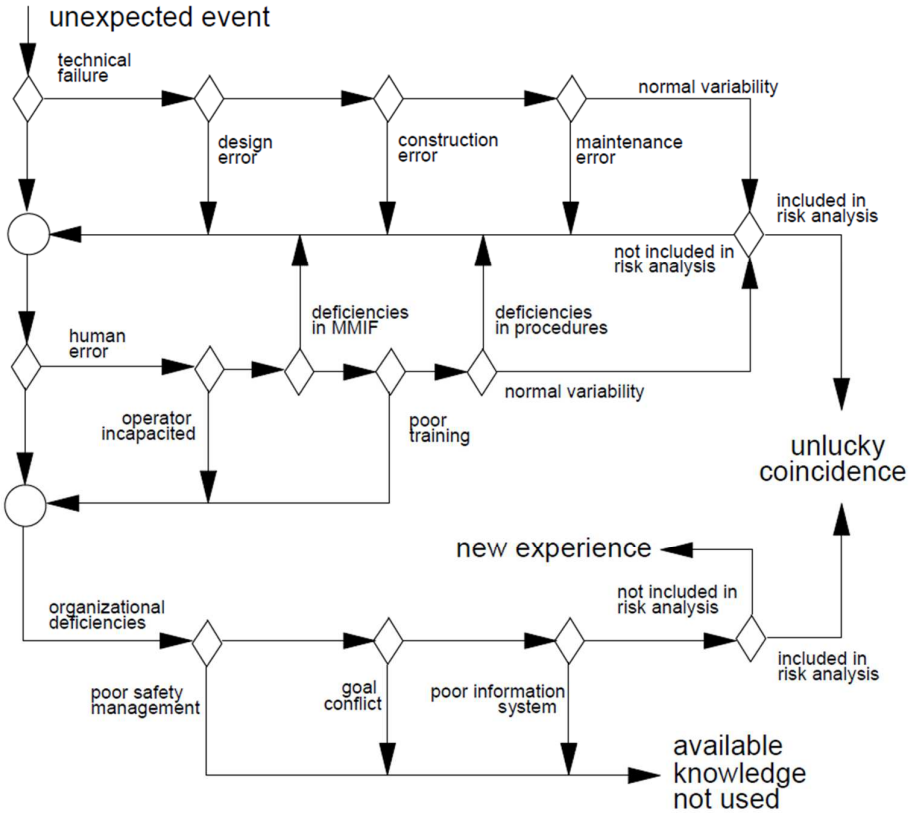
- Organisaatio

  johtoon ei luoteta, tehoton itsearviointi, identifioituja puutteita ei korjata

- Informaatio

  informaatio ei kulje vertikaalisesti ja/tai horisontaalisesti

Onnettomuuksien syyt?



Turvallisuus organisaation tavoitteena

- Johtamisjärjestelmä
  - virallinen organisaatio
  - epävirallinen organisaatio
- Johtamisjärjestelmälle asetettavat vaatimukset
  - on olemassa
  - on dokumentoitu
  - on ymmärretty
  - käytetään
  - pidetään ajan tasalla
- Johtamisjärjestelmän kaksi osaa
  - organisaatio- ja laatukäsikirja (kuka, miten)
  - toimintaohjelmat (mitä, milloin)

Erään yrityksen johtamisjärjestelmä

Management and Quality Handbook
WHO & HOW

Chapter 1 Management and Control
President

Chapter 2 Organization
President

Chapter 3 Quality Requirements
President/ mQ

Chapter 4 Quality Response mX

Chapter 5 Updating and distribution Q

Activity Program
What & When

Chapter 1 Strategy 5 year
Business Plan 1 year
VP

Chapter 2 Departmental Score Cards
incl. Activity Plans mX

Chapter 3 Company Programs mX
- **Reactor Safety**
- **ALARA**
- **Conventional Environmental Issues**
- **HR Program**
- **Industrial safety**
- **House keeping**

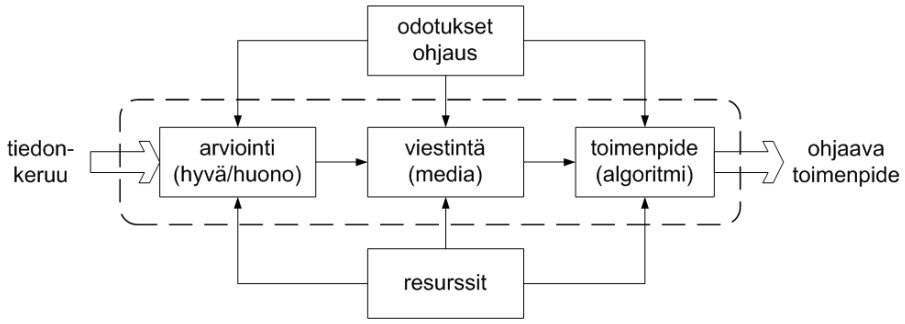
Chapter 4 Company Plans mX
- **Production Plan**
- **Internal Audit Plan**
- **Reporting Plan**
- **Activity Plan/Business Control**

Chapter 5 Investments guidelines mE

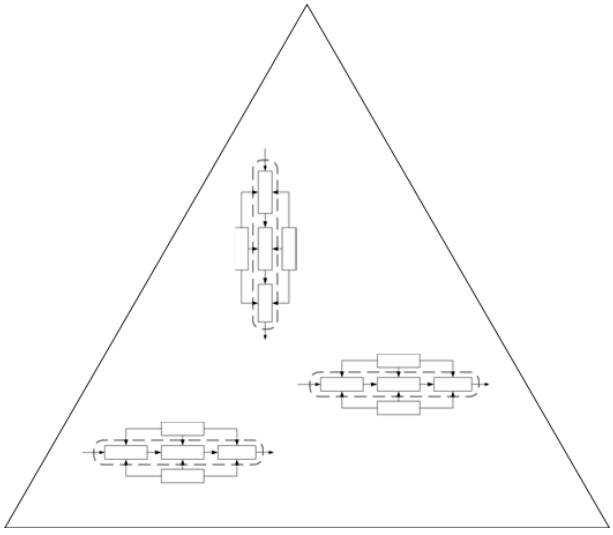
Johtamisjärjestelmän rakenne ja sisältö

- Missio, arvot, tavoitteet, toimintatavat
- Organisaation rakenne (yksiköt, kytkennät)
  vastuut, valtuudet, prosessit, menettelyt, toimintaohjeet
- Turvallisuuteen liittyvät toiminnot
- Toiminnan suunnittelu ja seuranta (operatiivinen, strateginen)
- Vaatimusten hallintaa
- Konfiguraation hallintaa
- Dokumenttien hallintaa
- Johtamisjärjestelmän päivittäminen

Organisaation ohjaukset



Organisaatiomuodot
- linjaorganisaatio
- prosessiorganisaatio
- matriisiorganisaatio
- projektiorganisaatio



Joitakin käytäntöjä

- Työlupakäytäntö
  - valvomo antaa laitoksen työlupia (säteilytyö, tulityö, sähkötyö, jne.)
- Allekirjoitukset
  - dokumentin kirjoittaja, tarkastaja ja hyväksyjä allekirjoittavat
- Prosessin tai käyttöohjeen omistaja
  - pyritään aikaansaamaan parempaa sitoutumista
  - vastaa tarvittavista päivityksistä
- Prejob briefing
  - huolto- tai assennustyötä käydään läpi yksityiskohtaisesti ennen sen tekemistä

Organisaatiotyypit

- process oriented vs results oriented;
- employee oriented vs job oriented;
- parochial vs professional;
- open system vs closed system;
- loose control vs tights control;
- normative vs pragmatic.

Andrew Hopkins (2006). Studying organisational cultures and their effects on safety, Safety Science 44 875–889.

Tehtävät päällikkötasolla

- resurssisuunnittelu (aika, henkilöstö, rahaa)
- menetelmien ja osaamisen kehittäminen
- ohjeiden ajankohtaisuuden varmistaminen
- riskien tunnistaminen ja hallintaa
- toiminnan tehostaminen
- suunnitella, seurata, dokumentoida ja raportoida
- henkilöstön ja työympäristön kehittäminen
- kokemusten keräys ja hyödyntäminen
- kommunikointi muun organisaation kanssa

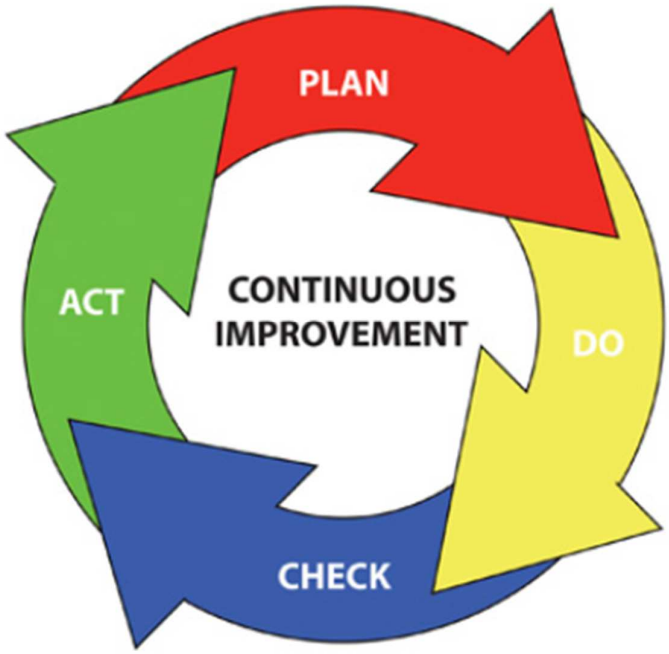
Kuinka samanlaiset ovat johtamisjärjestelmät?

- prosessi- tai henkilöturvallisuus
- epävarmuuden minimointi tai hallinta
- organisaation tunnuspiirteet
  - yksinkertaiset tai kompleksiset vuorovaikutukset
  - löyhä tai kiinteä kytkentä
- ulkopuolinen tai sisäinen valvonta
- standardit ja menettelyt
- turvallisuuskoulutus
- tapahtumien raportointi ja analysointi
- turvallisuuskulttuuri

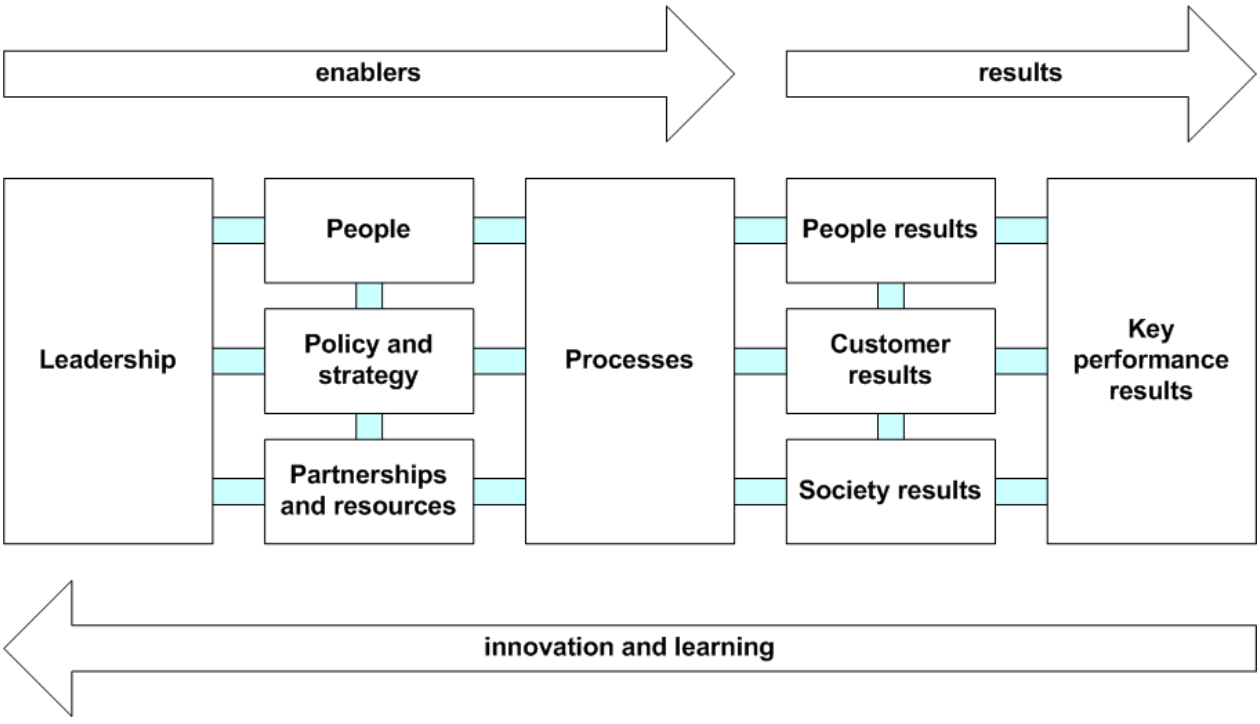
Oscillations between "one size fits all" and "reinventing the wheel"

Gudela Grote (2012). Safety management in different high-risk domains – All the same? Safety Science 50, 1983-1992.

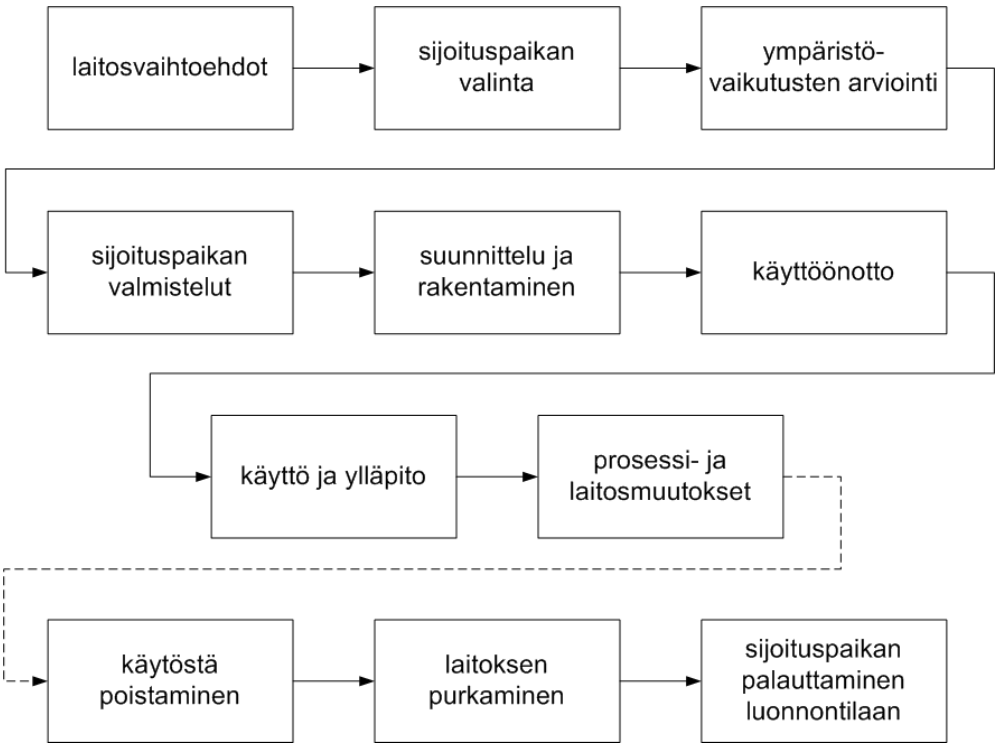
Palautteen käyttö johtamisessa



Laatuajattelu ja laatujärjestelmät



Elinjakson huomioonottaminen



D.G. Woodward: Life cycle costing--theory, information acquisition and application, Int. Jour. of Project Management, 15:6, 335-344, 1997

Turvallisuuskulttuuri

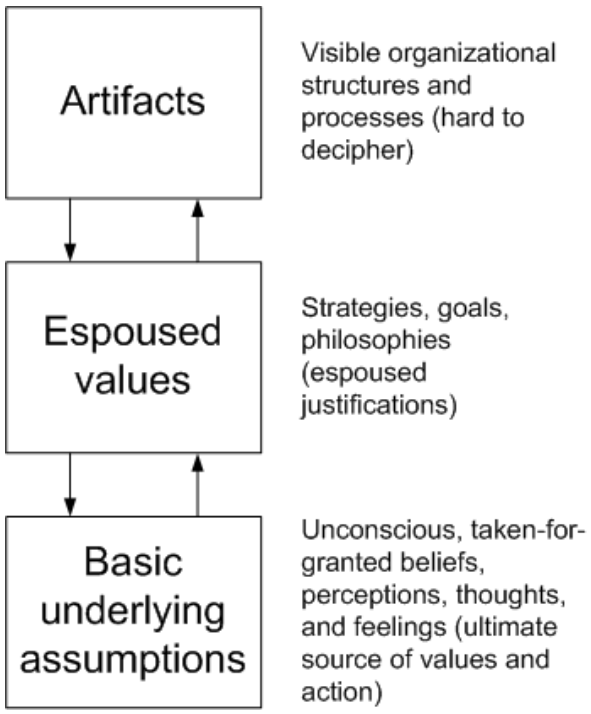
- Nousi teemaksi Tjernobylin onnettomuuden jälkeen
- Muutama ongelma
  - kulttuuri ohjauksen kohteena?
  - kytkentä organisaatiokulttuuriin?
  - organisaatiossa yksi tai monta kulttuuria?
  - kattaa kaikkea vai rajoitetaanko johonkin?
  - oikeako painatus systeemit ja henkilökunta?
- Käsitteen systeeminen tulkinta
  - kokonaisuus ja yksityiskohdat
  - MTOI-systeemikokonaisuus

Guldenmund, F.W. (2000), 'The Nature of Safety Culture: A Review of Theory and Research', Safety Science, Volume 34, pp. 215–257.
C. Rollenhagen (2010). Can focus on safety culture become an excuse for not rethinking design of technology? Safety Science 48, 268–278.

IAEA Normative Safety Culture Framework

IAEA (2009). The Management System for Nuclear Installations, No. GS-G-3.5
B. López de Castro, F.J. Gracia, J.M. Peiróa, L. Pietrantonic, A. Hernández: Testing the validity of the International Atomic Energy Agency (IAEA) safety culture model, Accident Analysis and Prevention 60 (2013) 231– 244

Eräs organisaatiokulttuurin malli



Edgar H. Schein (1992). Organizational culture and leadership, Jossey-Bass

Turvallisuuskulttuurin kehityksestä

- Pathological; Who cares about safety as long as we are not caught?
- Reactive; Safety is important: we do a lot every time we have an accident.
- Calculative; We have systems in place to manage all hazards.
- Proactive; We try to anticipate safety problems before they arise.
- Generative; HSE (health, safety, environment) is how we do business round here.

D. Parker, M. Lawrie, P. Hudson (2006). A framework for understanding the development of organisational safety culture, Safety Science 44 551–562.

Hearts and Minds

Hearts and Minds is a toolkit intended to help organisations to improve their HSE performance by:
1. Leading the way – the 'route to the top' of the HSE culture ladder
2. Providing the process and tools to get everyone involved and to facilitate behavioural change – the necessary components of a solution

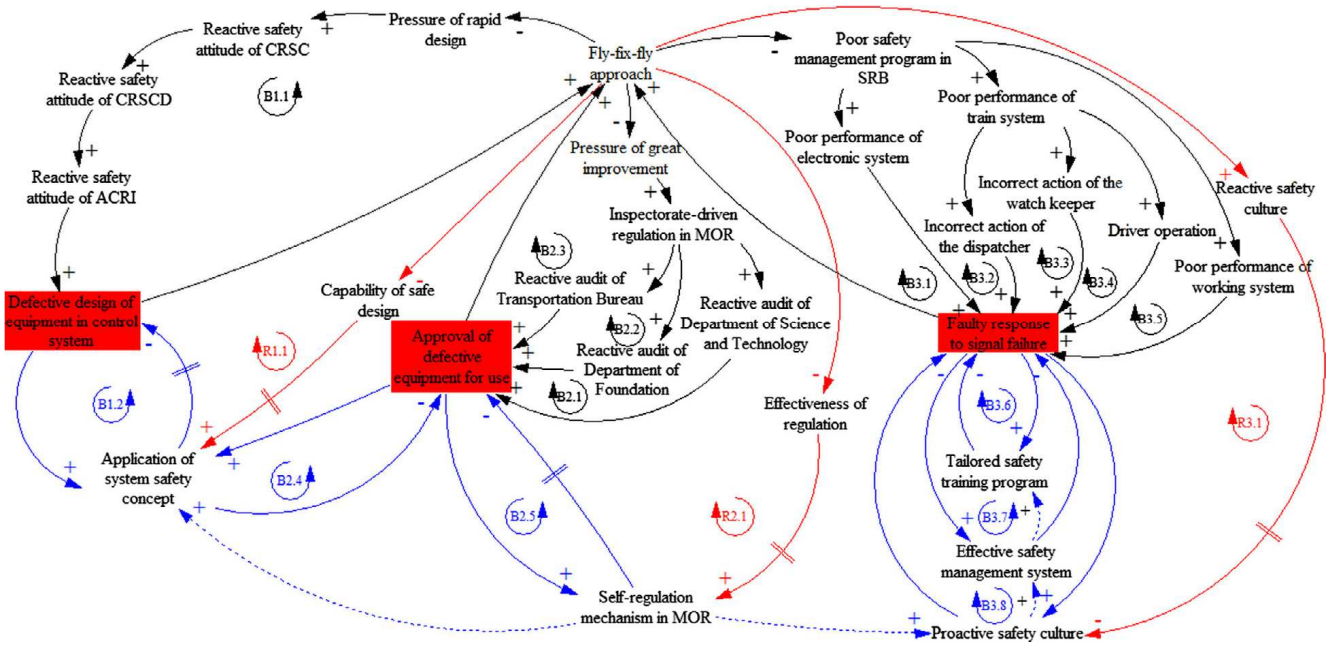
http://www.eimicrosites.org/heartsandminds/

Comparison Between Culture Survey Results and the Findings of the Incident Investigation and Causal Analysis

Safety culture survey before to the incident	Incident investigation and causal analysis
Safety highly prioritized	Safety subordinate to a dominating cultural value of 'meeting production targets'
Risk assessments carried out before and during work operations	Lack of risk assessments, poor understanding of risk assessment
High degree of compliance to rules and procedures, breaches sanctioned by management	Severe breaches of procedures, culture of non-compliance
Good climate for communicating safety-relevant information	Weaknesses in communication climate
Incidents and near misses reported, measures taken to prevent recurrence	Not all incidents and near misses reported, limited use of the organization's and others' safety experience
Insufficient managerial involvement	Insufficient managerial involvement

Stian Antonsen: Safety Culture Assessment: A Mission Impossible? Journal of Contingencies and Crisis Management, 17:4, 2009

Causal loop diagram for the 7.23 accident



Y. Fan, Z. Li, J. Pei, H. Li, J. Sun: Applying systems thinking approach to accident analysis in China: Case study of ''7.23'' Yong-Tai-Wen High-Speed train accident, Safety Science 76 (2015) 190–201

Myths about safety

- Human error is the largest single cause of accidents and incidents
- Systems will be safe if people comply with the procedures they have been given
- Safety can be improved by barriers and protection; increasing the layers of protection leads to higher safety
- Root cause analysis can identify why mishaps happen in complex socio-technical systems
- Accident investigation is the logical and rational identification of causes based on facts
- Safety always has the highest priority and will never be compromised

D. Besnard, E. Hollnagel: I want to believe: some myths about the management of industrial safety, Cogn Tech Work (2014) 16:13–23
J. Lundberg, C. Rollenhagen, E. Hollnagel: What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals, Safety Science 47 (2009) 1297–1311

Human and organizational biases

Beliefs about human behaviour

How do humans behave? What motivates people? Why do people make errors / mistakes? How reliable are people in general? How do humans behave in groups / teams? How does the presence of others influence the individual?

Beliefs about organizations

How can people be influenced / led? What is the most effective way to organize work? How do organizations learn / change? What kind of phenomenon is organizational culture? Is an organization just an aggregate of its individual members

Information and uncertainty

How can safety be measured? What is considered valid information? How can information be gathered? What are the uncertainties associated with information? What are “risks” and “probabilities”?

Safety models

How do accidents happen? What is safety? Is it possible to predict accidents? What is the role of humans in accidents or safety? How do organizations contribute to safety? What is safety culture? How does occupational safety differ from e.g. process safety?

T. Reiman, C. Rollenhagen: Human and organizational biases affecting the management of safety, Reliability Engineering and System Safety 96 (2011) 1263–1274

Organisaation puutteet

- Puutteelliset mallit
- Sopimattomat tavoittet
- Puutteellinen tilanteen seuranta
- Puutteelliset ohjaukset
- Eri ohjausten puutteellinen koordinointi
- Ohjausalgoritmien puutteellinen sovittaminen muuttuneeseen tilanteeseen
- Puutteita strategisessa suunnittelussa

T. Kontogiannis : Modeling patterns of breakdown (or archetypes) of human and organizational processes in accidents using system dynamics, Safety Science 50 (2012) 931–944.

Results from 18 empirical and 4 review studies

- Economic pressures
  - Lack of a shared sense of responsibility for safety-related issues
  - Safety/production trade-offs
- Disorganization
  - Confusion in roles and responsibilities
  - Breakdown in communication and information flow
  - Complex safety management systems
- Dilution of competence
  - Employees unfamiliar with local work
  - Lack of industry-specific knowledge and
- Organizational differences
  - Fragmented decision-making processes
  - Distrust and conflicts between organizations

V. Milch, K. Laumann: Interorganizational complexity and organizational accident risk: A literature review, Safety Science 82 (2016) 9–17

Organisational Integrity Dimensions

- Critical tasks
  - Equipment design
  - System design
  - Task environment
- Leadership
  - Supervision
  - Job design
- Process and procedures
- Ensuring competence
  - Recruitment
  - Training
  - Appraisal
- Workload management
  - Manpower levels
  - Fatigue control
- Communications
  - 2-Way communications
  - Trust
- Learning and improving
  - Incident investigation
  - Governance processes
- Change management

G. Moon, W. I. Hamilton: Developing an Organisational Integrity framework, for nuclear safety, Cogn Tech Work (2013) 15:39–45

Organisational errors

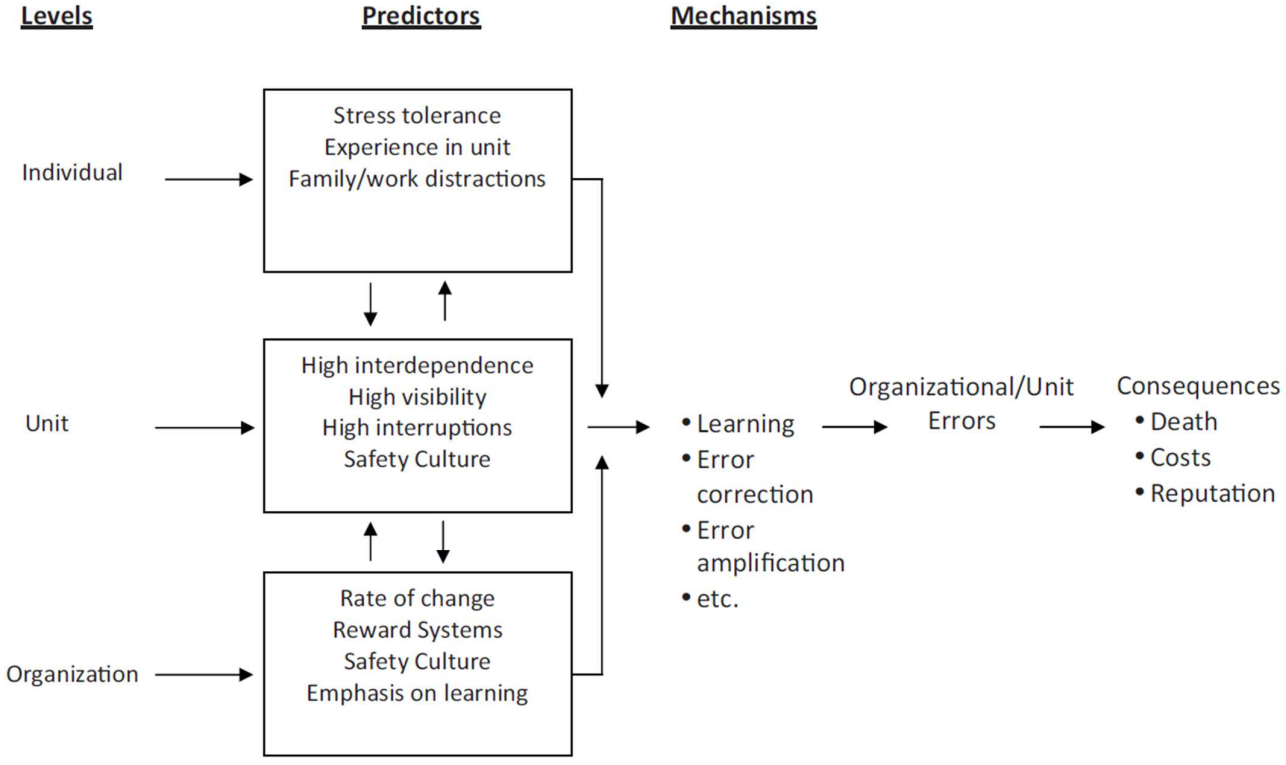


Fig. 1. Multiple-level predictors and mediating mechanisms.

P.S. Goodman, R. Ramanujam, J.S. Carroll, A. C. Edmondson, D.A. Hofmann, K.M. Sutcliffe: Organizational errors: Directions for future research, Research in Organizational Behavior 31 (2011) 151–176

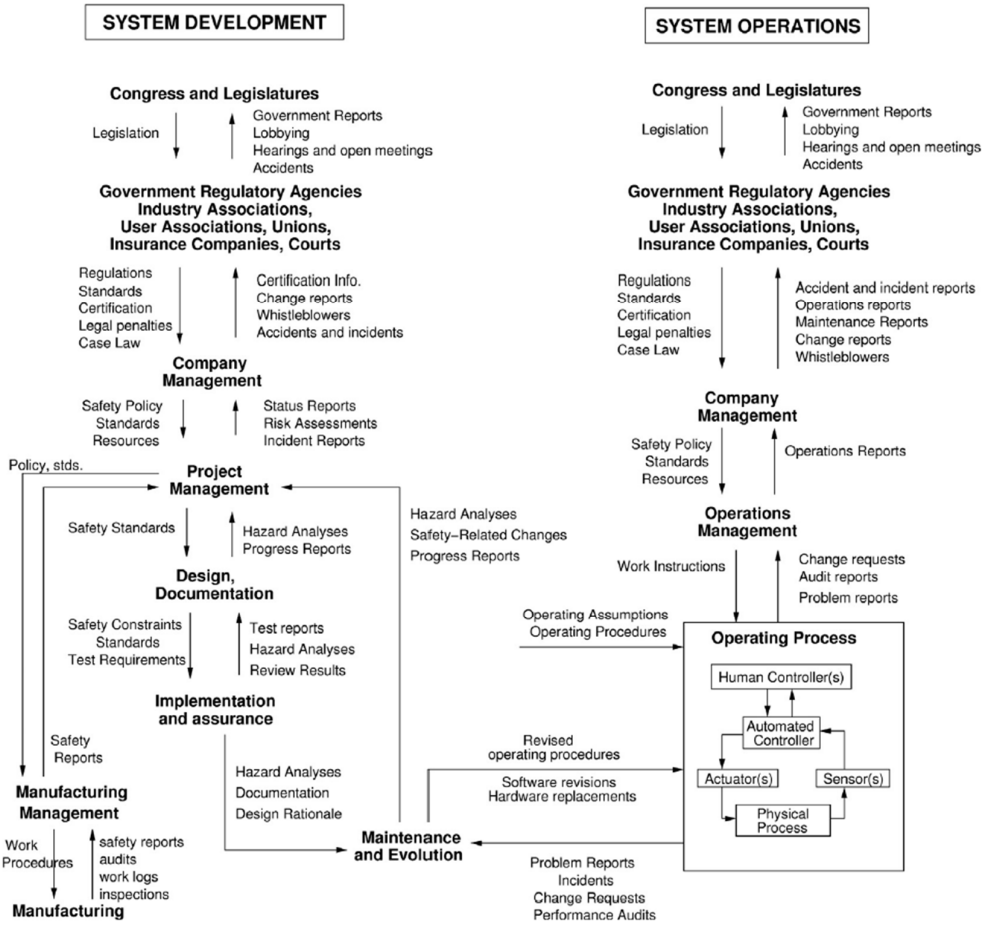
Organisatooristen puutteiden syyt

- Leadership
- Operational attitudes and behaviours
- Impact of the business environment
- Competence and training
- Risk assessment and risk management
- Oversight and scrutinity
- Organisational learning
- Communication

R.H. Taylor, L.G.A. van Wijk, J.H.M. May, N.J. Carhart: A study of the precursors leading to‘organisational’ accidents in complex industrial settings, Process Safety and Environmental Protection, 93 (2015) 50–67

Organisaatioiden mallintaminen

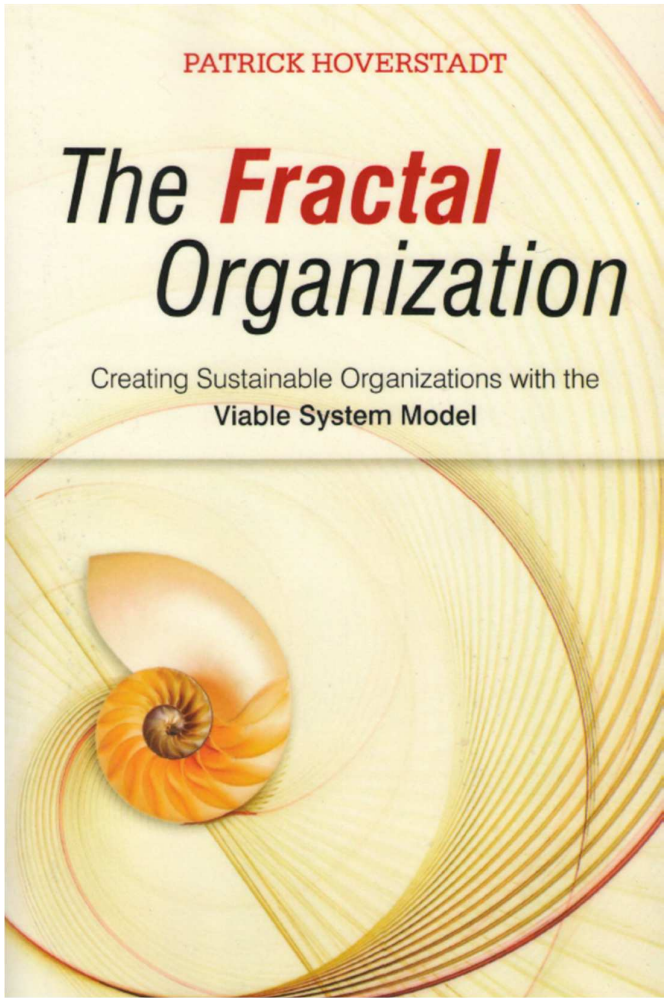
- Esiintyviä turvallisuusongelmia voidaan ainakin periaatteessa selittää organisaation puutteilla
- Haasteena on valita organisaation malli, joka nostaa esille turvallisuuden kannalta tärkeät asiat
  - mallin rajoittaminen
  - mallin sisäiset osat (tilasuureet) ja niiden väliset vaikutusmekanismit
  - mallin validointi
- Mallin pitää olla kvalitatiivinen ja yleisellä tasolla
  - onko löydettävissä mallien kehys, johon yksityiskohtaisempia malleja voidaan sijoittaa?



Leveson, N.G., 2004. A new accident model for engineering safer systems. Safety Science 42, 237–270.

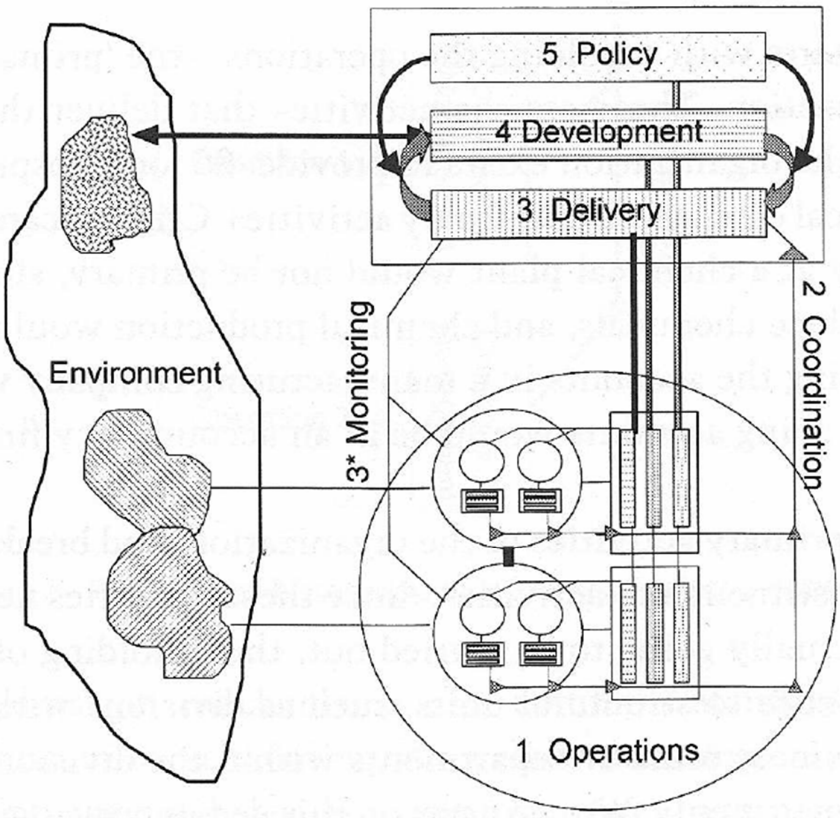
Fraktaalinen organisaatio

- Based on the Viable System model
- The same functional structure is used at each hierarchical level in the organisation
- From the book
  - you can't solve the problem with the same reasoning that caused the problem
  - all management disciplines tend to have their own areas of interest and their own language
  - 21 pathological archetypes
  - requirements on monitoring
    - sporadic
    - unannounced
    - skip one management level
    - in depth

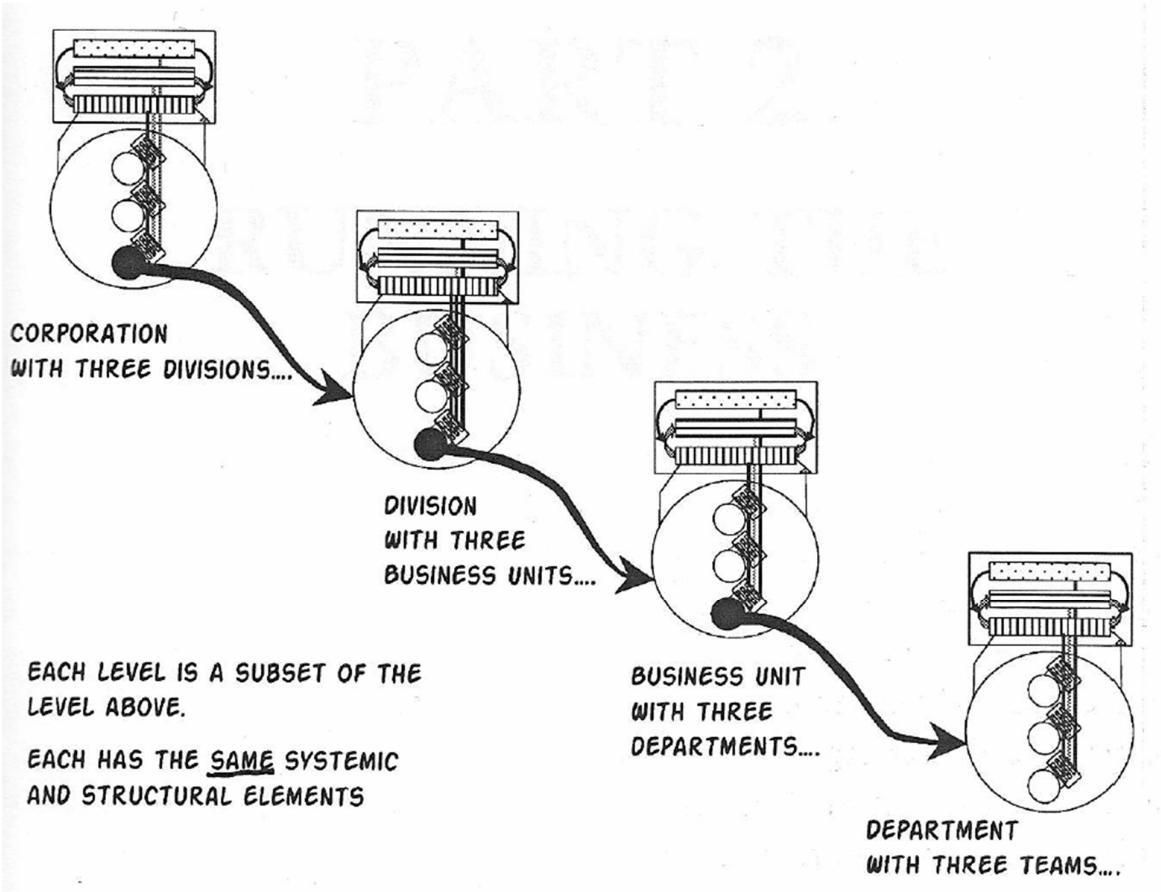


Hoverstadt, P. (2008). The Fractal organisation, Wiley.

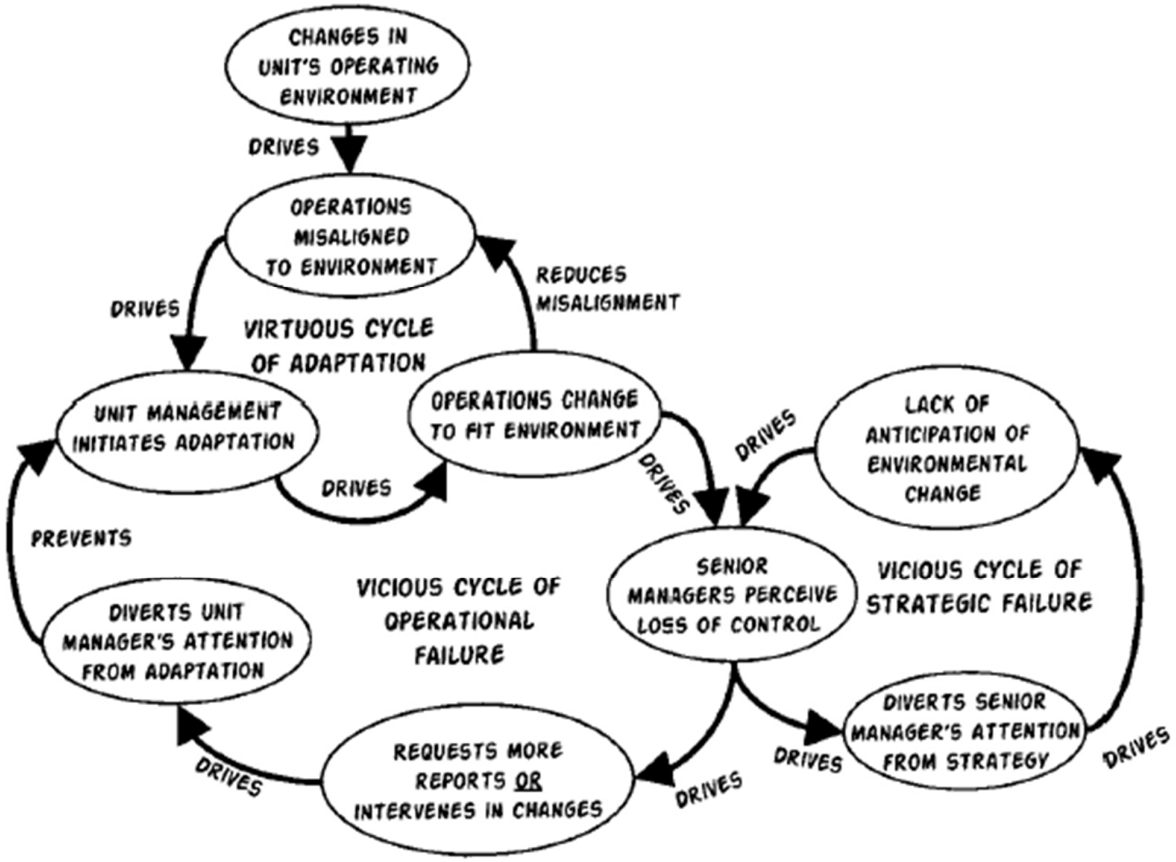
Viable systems model



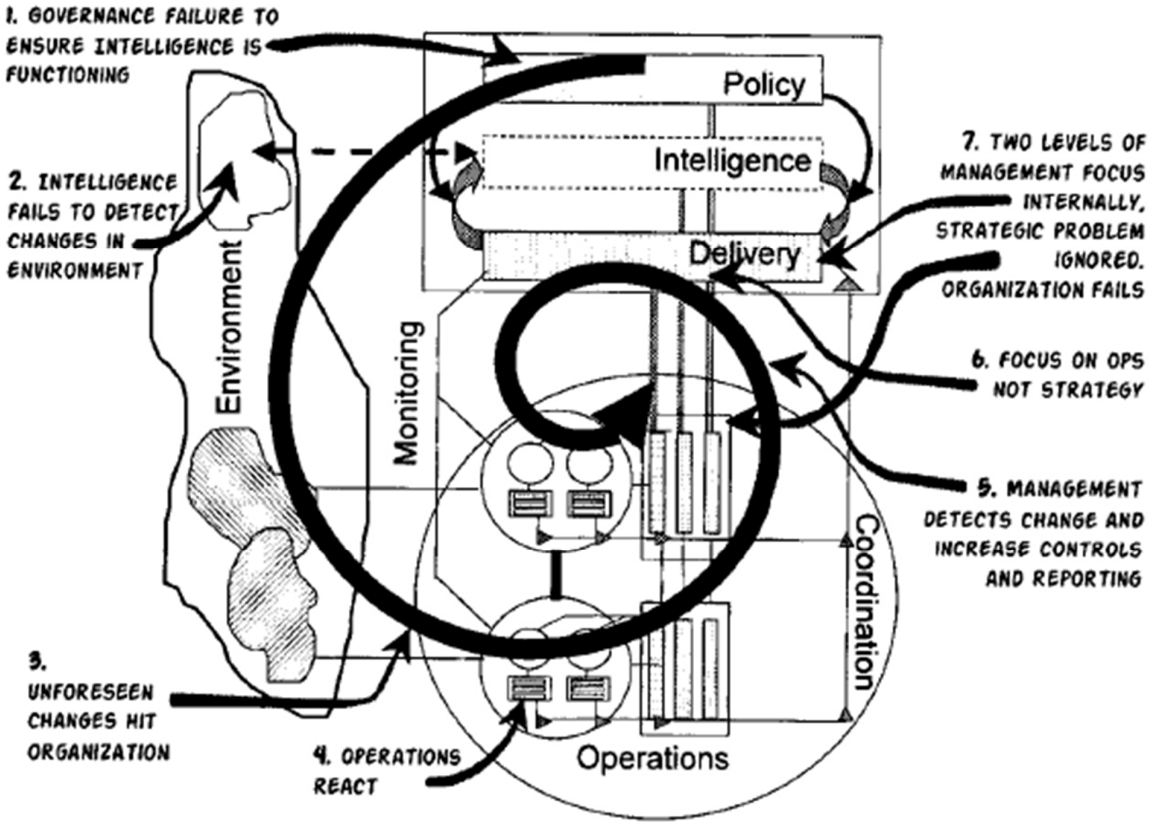
A fractal structure

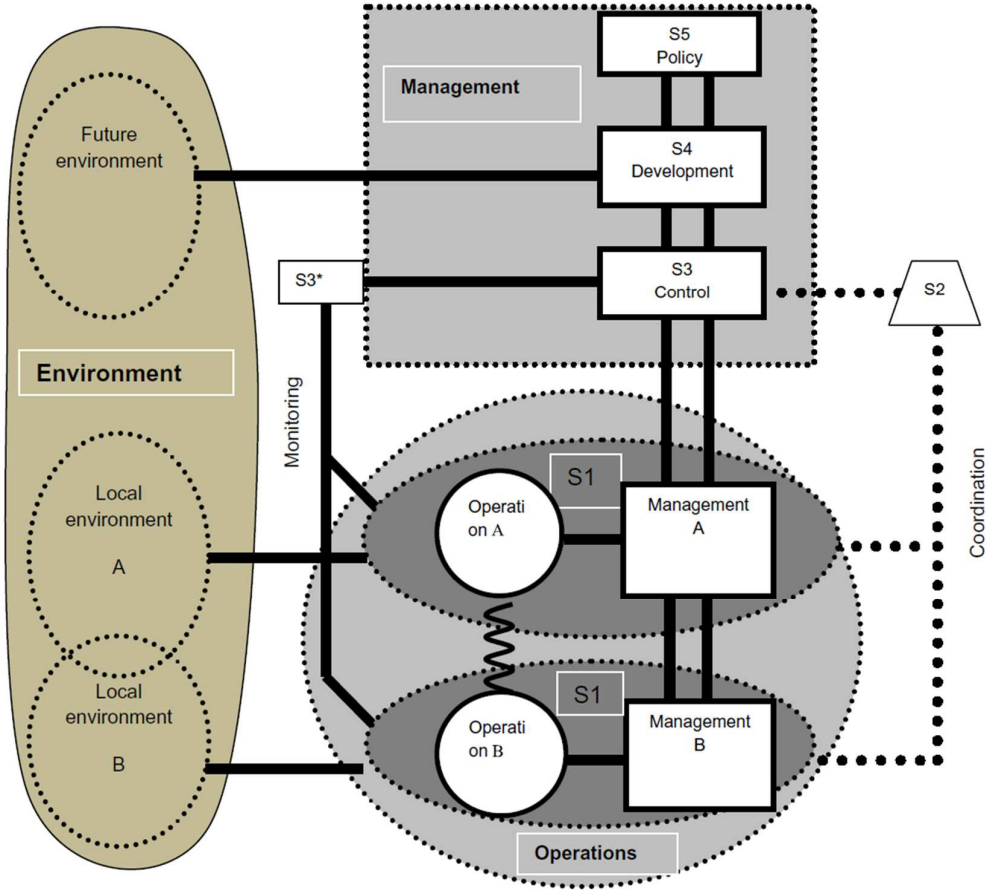


Dynamics of the control dilemma



The death spiral





K. Kazaras, T. Kontogiannis, K. Kirytopoulos (2014). Proactive assessment of breaches of safety constraints and causal organizational breakdowns in complex systems: A joint STAMP–VSM framework for safety assessment, Safety Science 62, 233–247.

A classification of organizational control flaws.

1. Inadequate formulation of safety policy and goals (Inadequate System 5)
   a) Ambiguous safety policy or lack of safety policy
   b) Imbalance between exploitation and exploration
   c) Trapped in the often unnoticed loop between formulating goals and monitoring
   d) Eroding safety goals
2. Inadequate adaptation to changes (Inadequate System 4)
   a) Open loop
   b) Lack of double loop learning
3. Inadequate assignment of control authority and responsibilities (Inadequate System 3)
   a) Imbalance between autonomy versus centralized control
   b) Gaps and overlaps of responsibilities
   c) Responsibility assigned is not suited to personnel
4. Inadequate design and ineffective implementation of safety plans (Inadequate mapping of System 5 to Systems 1 and 2)
   a) Mismatch between the safety plans and the strategy of managing uncertainty
   b) Lack of coordination
   c) Inconsistency between plans and routines in practice
   d) Plans not following changes in the system, stagnant plans
   e) Lack of resources
   f) Ineffective training procedures
5. Inadequate modeling of the state of the safety performance (Inadequate mapping of System 4 to Systems 1 and 2)
   a) Inadequate feedback control
      - Inadequate safety audits
      - Inadequate learning from events process
      - Improperly designed reporting schemes
   b) Inadequate feed-forward control
      - Lack of management of changes, inadequate risk analysis
      - Lack of leading safety indicators

Manager or Leader?

Management = a function

- Planning/Budgeting
- Organizing/Staffing
- Task Distribution/Follow-up
- Controlling/Problem Solving

Leadership = a relationship

- Create a shared understanding
- Establishing Direction
- Aligning People
- Motivating and Inspiring

To manage means to accomplish activities and master routines, while to lead means to influence other and create shared understanding as a driver for change

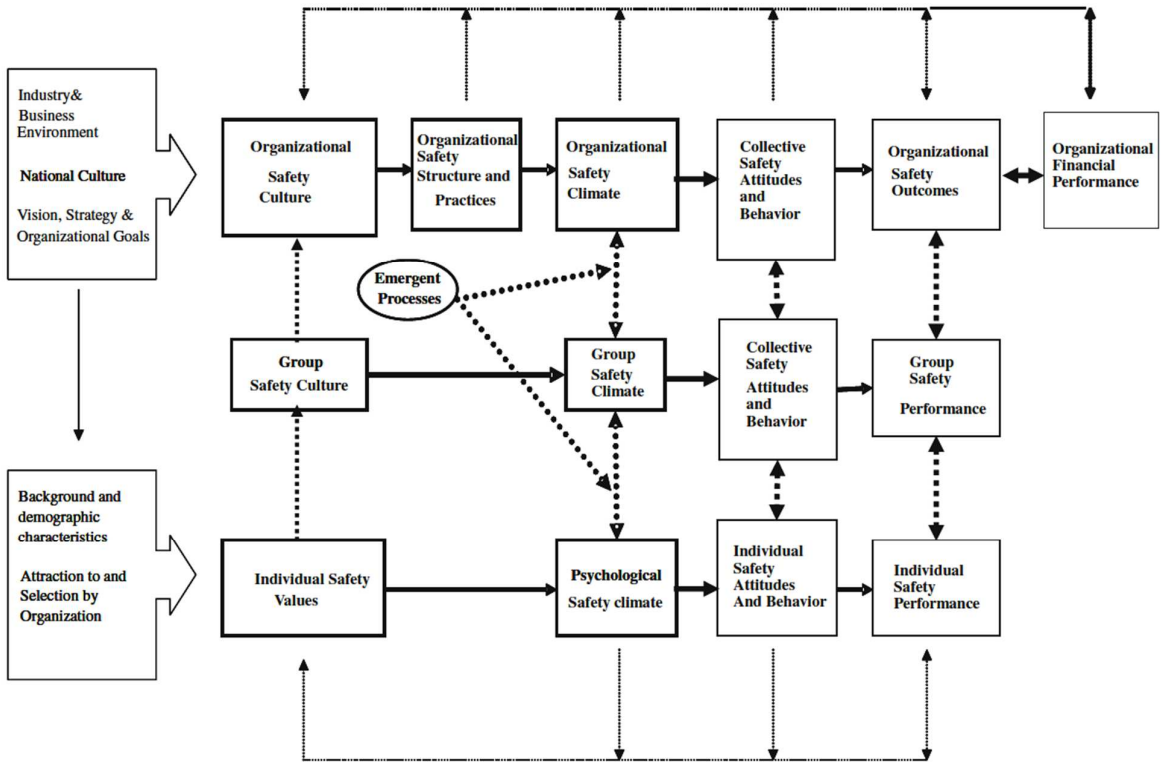


Fig. 9. Adapting an organizational performance model for safety purpose.

Zahra Mohaghegh, Ali Mosleh (2009). Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations, Safety Science 47 (2009) 1139–1158.

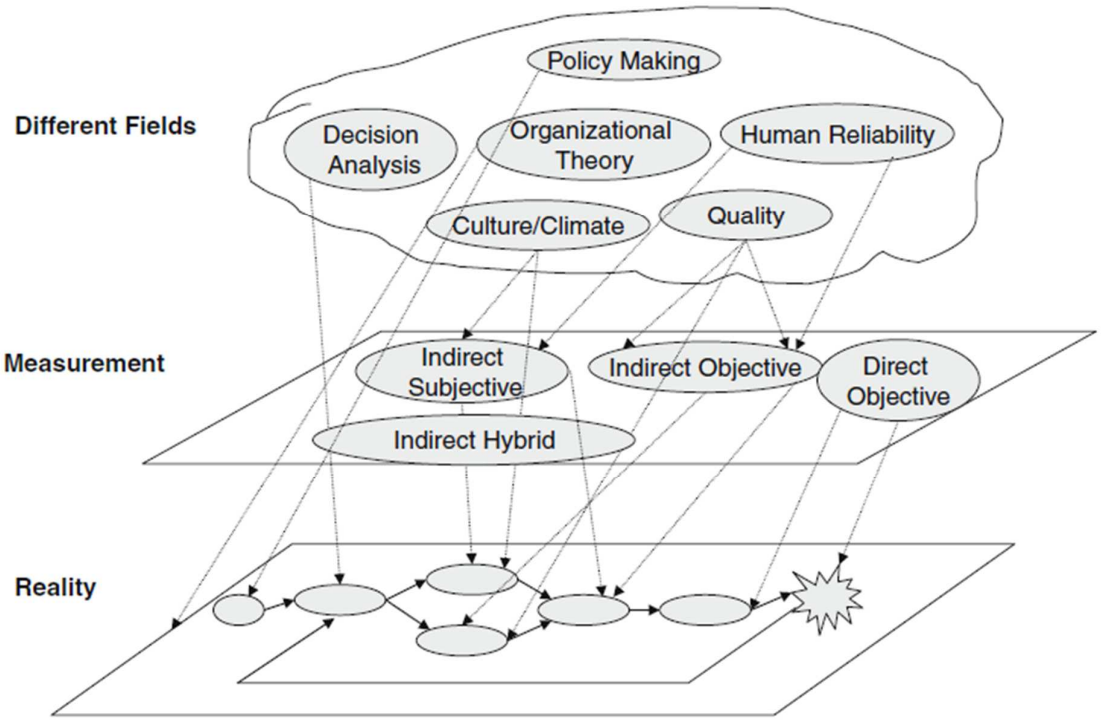


Fig. 1. Conceptual relation between supporting fields and theories, measurement, and reality in organizational safety causal modeling.

Zahra Mohaghegh, Ali Mosleh (2009). Measurement techniques for organizational safety causal models: Characterization and suggestions for enhancements, Safety Science 47 (2009) 1398–1409.

Turvallisuuskriittisen systeemin suunnittelu

Design a safe car – drive a car safely

- Systeemille asetettavat vaatimukset?
- Turvallisuusperiaatteiden käyttäminen
- Systeemin jakaaminen osasysteemeihin ja edelleen komponenteihin
- Osasysteemien suunnittelu ja komponenttien valinta
- Asteittainen komponenttien ja osasysteemien integrointi ja testaus (V&V)
- Kelpoistamissuunnitelman laatiminen ja käyttäminen

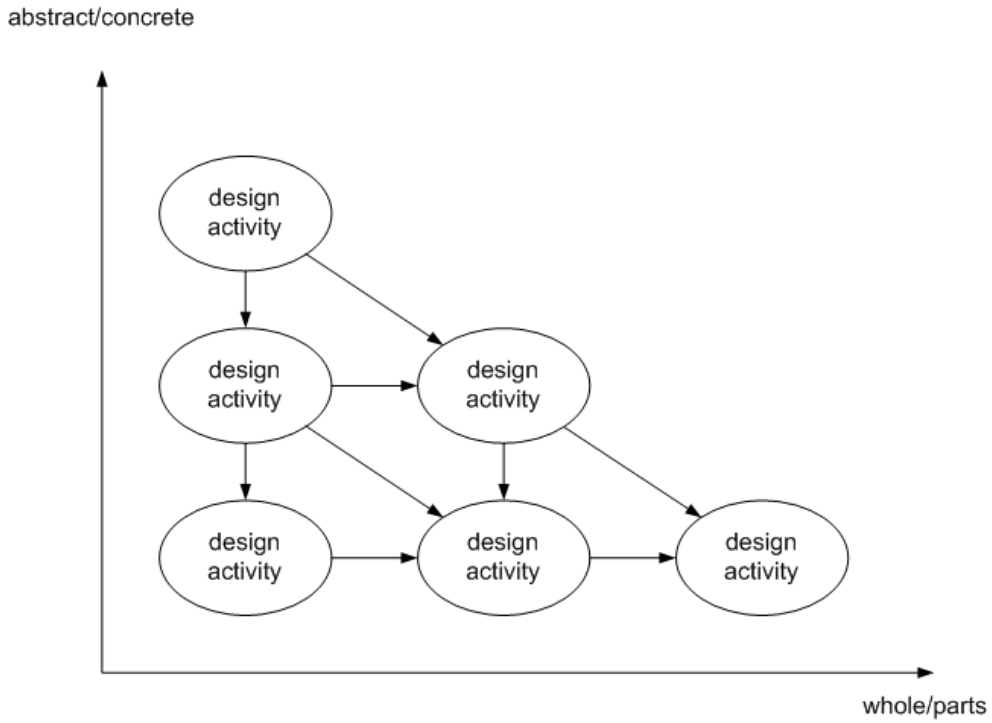
Systeemille asetettavat vaatimukset

- Suunnitteluperustan luominen
  - mitkä tapahtumaketjut laitoksen pitää hallita (suunnittelua ohjaavat tilanteet)
    - alkutapahtumat
    - vältettävät onnettomuudet
    - mahdolliset päästörajoitukset
    - rajoittavat altistumiset
  - turvallisuusjärjestelmille asetettavat vaatimukset
  - ihminen-koneliitännälle asetettavat vaatimukset
  - valmiussuunnitelmalle asetettavat vaatimukset
- Osasysteemit ja niiden liitännät
- Komponenteille asetettavat vaatimukset

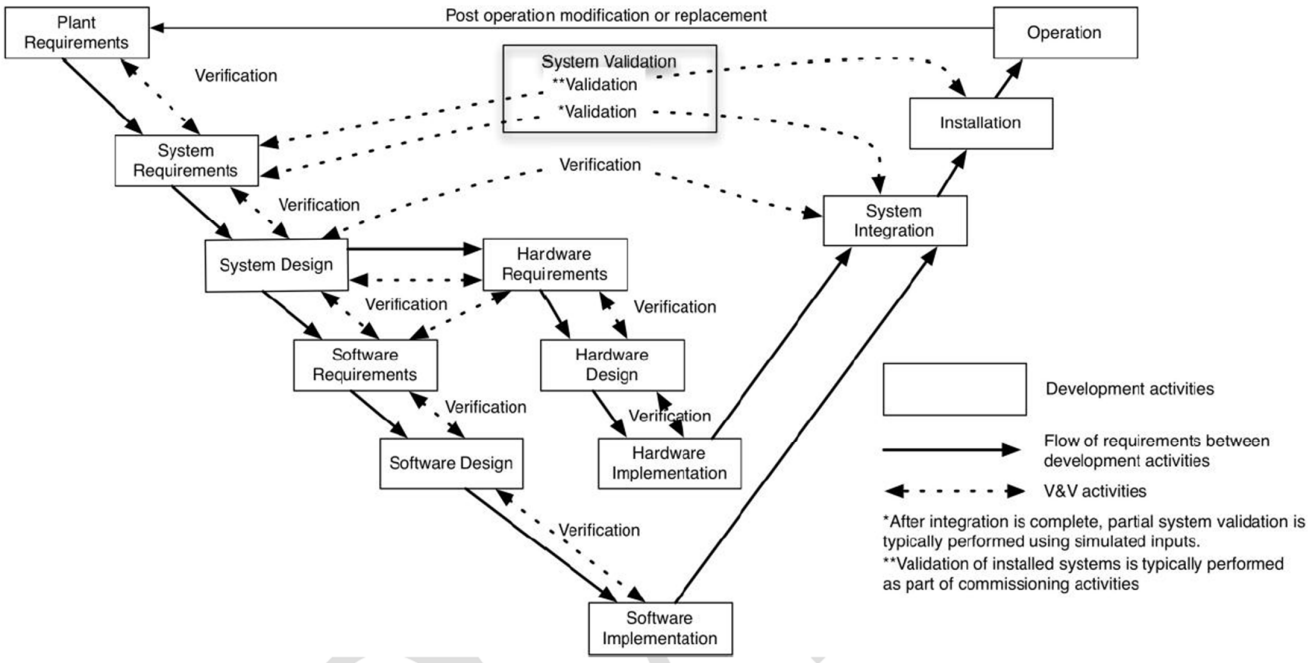
Vaatimusten hallinta

- Hierarkiat
  - abstrakti – konkreettinen
  - systeemi – osasysteemit – komponentit
- Toiminnalliset vaatimukset
- Ei-toiminnalliset vaatimukset
- Hallinnan tukijärjestelmät
  - tietokanta (nimikkeet, attribuutit, kytkennät, ...)
  - täydellisyys, johdonmukaisuus, oikeellisuus
  - vaatimusten toiminnallisuuden tarkastaminen
  - automatisoitu koodin generointi
  - dokumentoinnin generointi

Suunnittelun eteneminen



Modularisointi ja integrointi



Ihmisten huomioonottaminen

Inhimilliset virheet onnettomuuksien aiheuttajina

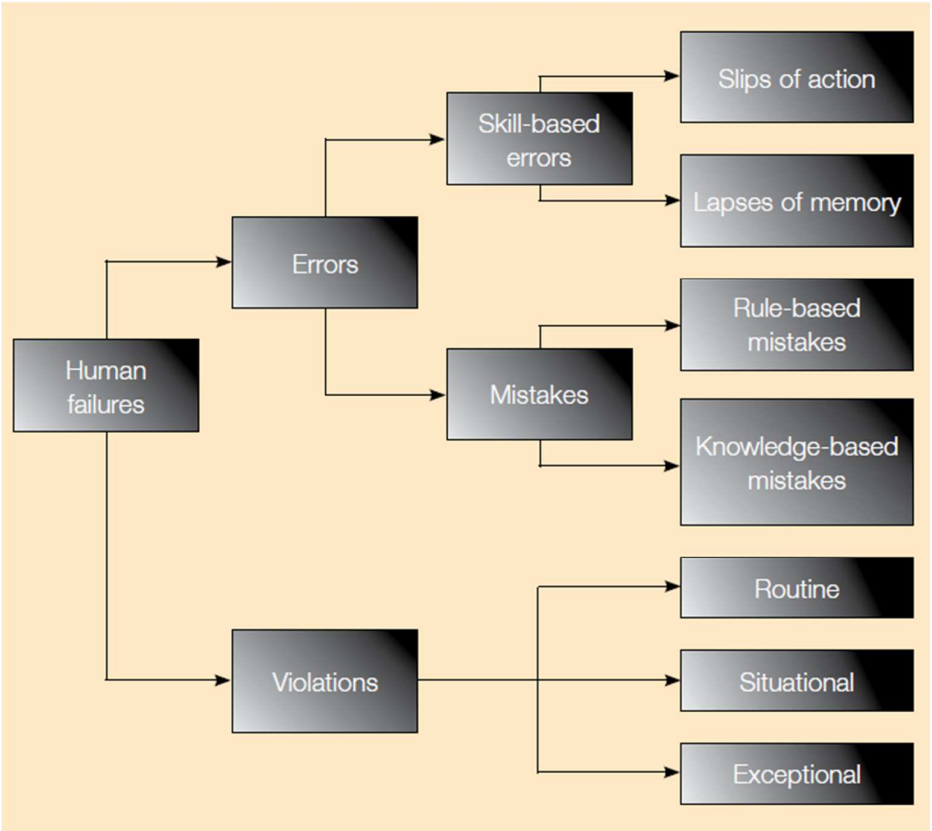
- aktiiviset virheet
- piilevät virheet

Virheiden syyt

- huonoa suunnittelua
- puutteellista koulutusta
- puutteellinen valvonta
- tehoton kommunikointi
- epätietoisuutta rooleista ja vastuista

HSE (2009). Reducing error and influencing behaviour, http://www.hse.gov.uk/pubns/books/hsg48.htm

Inhimmilliset virheet

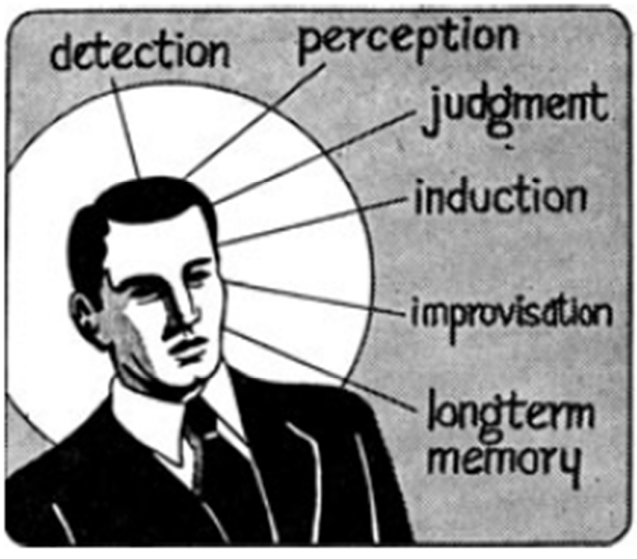


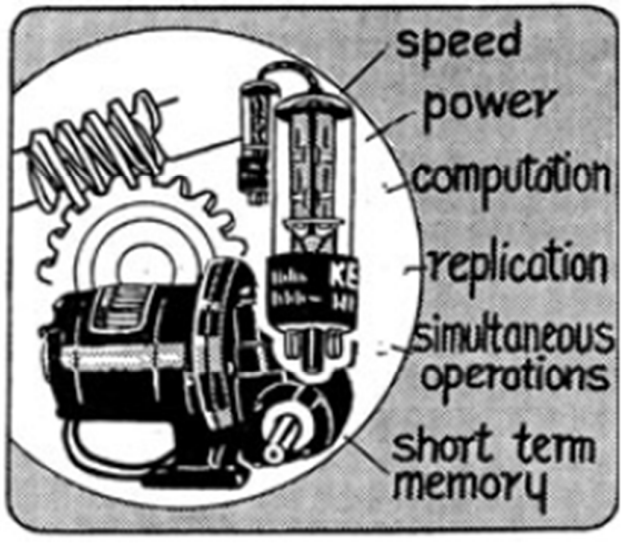
Systeemien sovittaminen ihmisiin

- Toimintojen allokointi ihmisten ja automaation välillä
- Ihmisen ja koneen välisen liitäntäpinnan suunnittelu ja kelpoistaminen
  - valvomon suunnittelu
  - tehtävien suunnittelu
  - näyttöjen suunnittelu
  - konseptin testaus simulaattorilla
  - turvallisuusselosteen kirjoittaminen

Bainbridge, L. (1983). "Ironies of Automation." Automatica, 19: 775-779
NUREG-0700 (rev.2): Human-System Interface Design Review Guidelines, US Nuclear Regulatory Commission, 2002

The original Fitts list from 1951





Työjako ihmisen ja koneen välillä

Humans appear to surpass present-day machines in respect to the following:	Present-day machines appear to surpass humans in respect to the following:
Ability to detect a small amount of visual or acoustic energy	Ability to respond quickly to control signals and to apply great force smoothly and precisely
Ability to perceive patterns of light or sound	Ability to perform repetitive, routine tasks
Ability to improvise and use flexible procedures	Ability to store information briefly and then to erase it completely
Ability to store very large amounts of information for long periods and to recall relevant facts at the appropriate time	Ability to reason deductively, including computational ability
Ability to reason inductively	Ability to handle highly complex operations, i.e. to do many different things at once.
Ability to exercise judgment	

J. C. F. de Winter, D. Dodou: Why the Fitts list has persisted throughout the history of function allocation, Cogn Tech Work (2014) 16:1–11

Turvallisuuden osoittaminen

- Vaatimusten täyttäminen
  - suunnitteluprosessin hyvyys
  - tuotteiden ja osatuotteiden laatu
- Väittämät
  - deterministinen vaatimus ***i*** on täytetty
  - probabilistinen vaatimus ***j*** on täytetty
- Todisteet
  - rakenteelliset (määrättyjä suunnitteluvirheita on vältetty)
  - empiiriset (osajärjestelmän ja/tai komponentin testaus)
- Päätöksenteko
  - hyväksytty (siirrytään seuraavaan väittämään)
  - ei hyväksytty (argumentit siitä, miksi ei hyväksytty)

Turvallisuusseloste (safety case)

Turvallisuusseloste on mukautettu elinkaaren vaiheeseen ja kuvaa erityisesti

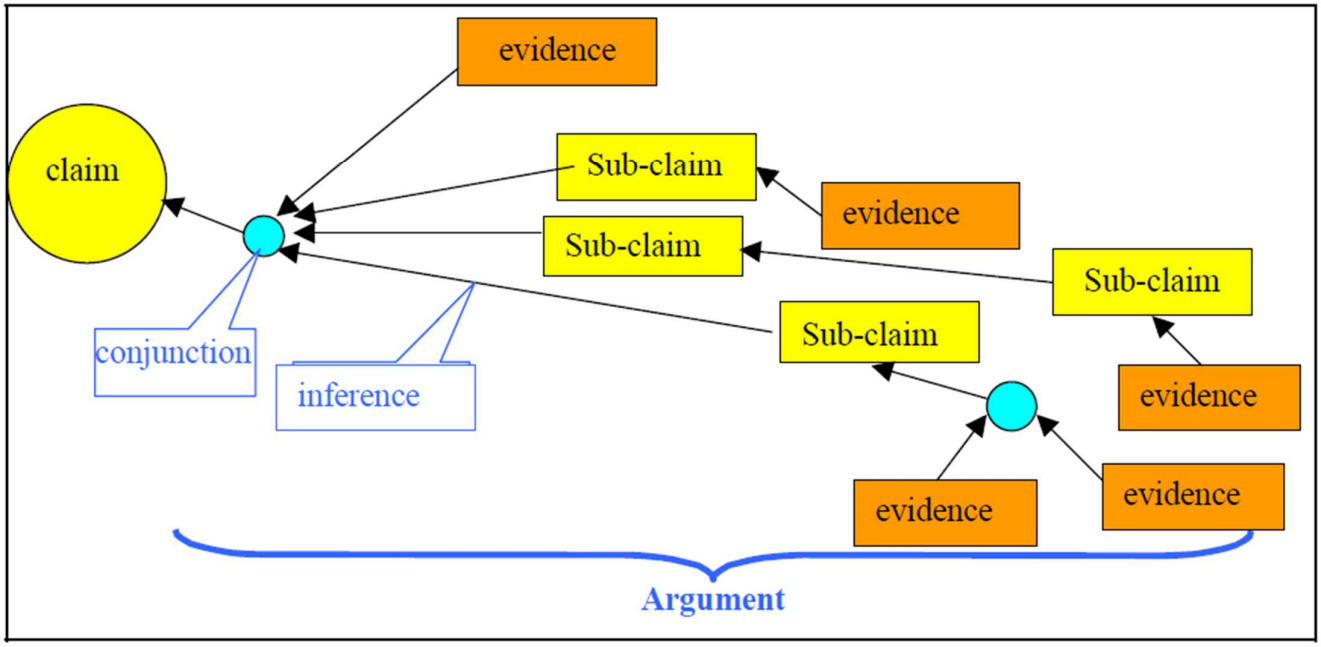
- tunnistetut turvallisuusuhat
- tunnistetut systeemien, rakenteiden ja komponenttien mahdolliset vikaantumismekanismit
- käytetyt turvallisuusperiaatteet ja miten niitä on huomioitu laitoksen suunnittelussa ja käytössä
- miten normaalit käyttöolosuhteet ja mahdolliset virhetilanteet on analysoitu ja huomioonotettu
- miten päästöt ja jätteet on hoidettu
- turvallisuushallinnan perusteet esim. miehitys, käyttö- ja kunnossapidon ehdot sekä valmiusjärjestelyt

HSE, Office for Nuclear Regulation (2013). The purpose, scope, and content of safety cases, NS-TAST-GD-051 Revision 3
http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf

Turvallisuusselosteelle asetettavat vaatimukset

- ymmärrettävä
  laitos sekä sen suunnitteluperusteet, käyttö ja ylläpito
- pätevä
  kaikki käyttötilanteet ja mahdolliset muutokset on kuvattu
- täydellinen
  riskit on käsitelty ALARP periaatteen mukaisesti
- osoitettavissa todisteilla
  vaatimukset ja oletukset on dokumentoitu ja voimassa
- robustinen
  syvyyspuolustus ja riittävät marginaalit ovat voimassa
- integroitu
  liitynnät ulkoisiin tapahtumiin on identifioitu ja käsitelty
- tasapainoinen
  tietämystä on käytetty ja epävarmuudet on käsitelty
- tulevaisuuteen katsova
  arvioidaan uuden tietämyksen saapuessa ja pidetään päivitettynä

Figure 1: Claim, arguments and evidence structure



BEL V, BfS, CSN, ISTec, ONR, SSM, STUK (2013). Licensing of safety critical software for nuclear reactors – Common position of seven European nuclear regulators and authorised technical support organisations, http://www.onr.org.uk/software.pdf

Uusien systeemien turvallisuus

Evolutionary – revolutionary

- tuttujen konseptien raameissa OK
- isoja muutoksia johtanevat tarpeeseen uusia suuria vaatimusten osioita
- suunnitteluprosessin arviointi todennäköisesti toisi paljon uutta miettimistä
- ydinvoimapuolella thorium polttoainekierto on mahdollinen , mutta edellyttäisi paljon uutta tutkittavaa
- ennenkuin Suomeen tuodaan täysin uutta teknologia pitäisi saada kunnollinen referenssi jossakin

Automaation turvallisuus

- Hyvä suunnitteluprosessi
  - suunnitteluprosessin johtamisjärjestelmä
  - suunnitteluprosessin aikana käytettyjä turvallisuusperiaatteita
  - joukko suunnitteluvirheitä on pystytty välttämään
- Perinpohjainen testaus
  - modulirakenne, jossa moduulit on testattu erikseen ja yhdessä
  - realiaikaisuusvaatimusten täyttyminen
  - varakapasiteettivaatimusten täyttyminen

Mikä on riittävä todiste automaation kelpoisuudesta?

Automaation ongelmat

Osoitettava että

- suorittaa kaikki vaaditut toiminnot
- ei suorita mitään ylimääräistä toimintoa

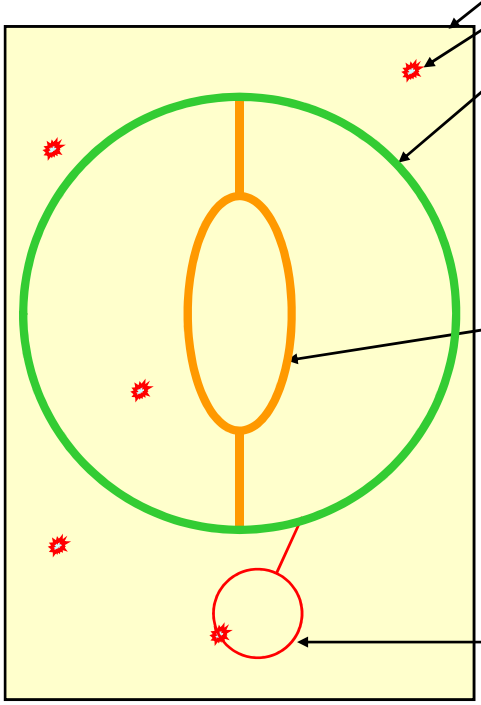
Ongelman lähteet

- Turingin teoreema (tietokoneen ohjelman käyttäytymistä ei voida ennustaa ajamatta sitä)
- Gödelin teoreema (vaatimukset eivät voi olla samanaikaisesti ristiriidattomia ja täydellisiä)
- Ashbyn periaate (ohjausjärjestelmän on oltava yhtä komplexinen kuin ohjattava järjestelmä)

B. Wahlström: Differences between analog and digital I&C, NPIC & HMIT 2015, Charlotte, NC, February 22-26, 2015
B. Wahlström: Safety principles and I&C design, NPIC & HMIT 2015, Charlotte, NC, February 22-26, 2015

Example of Defensive Measures: Cyclic Behavior with Well-Identified Influence Factors

Influence Factors: whatever affects software trajectory



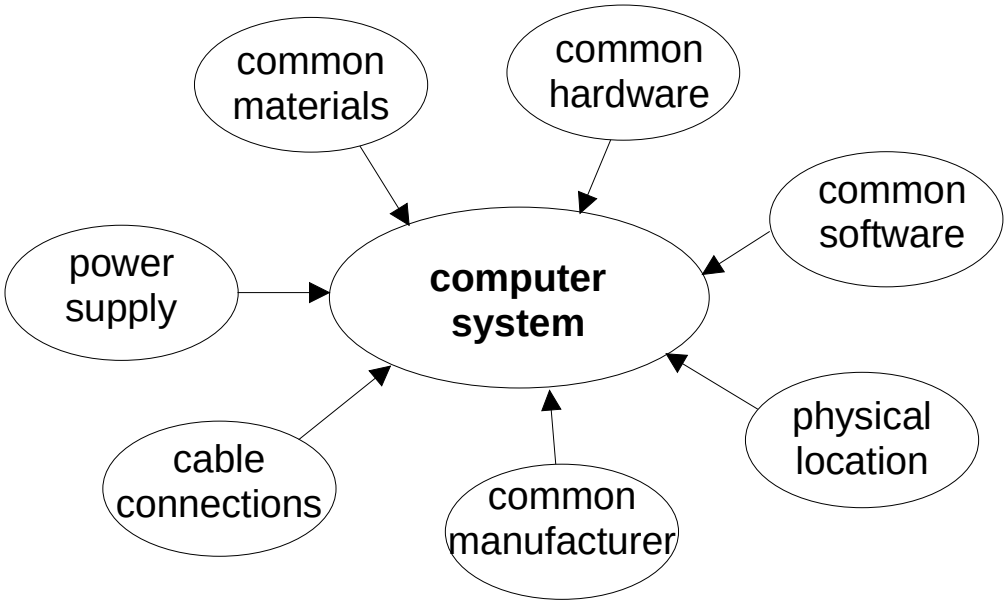
Complete domain of behavior
May contain residual digital faults

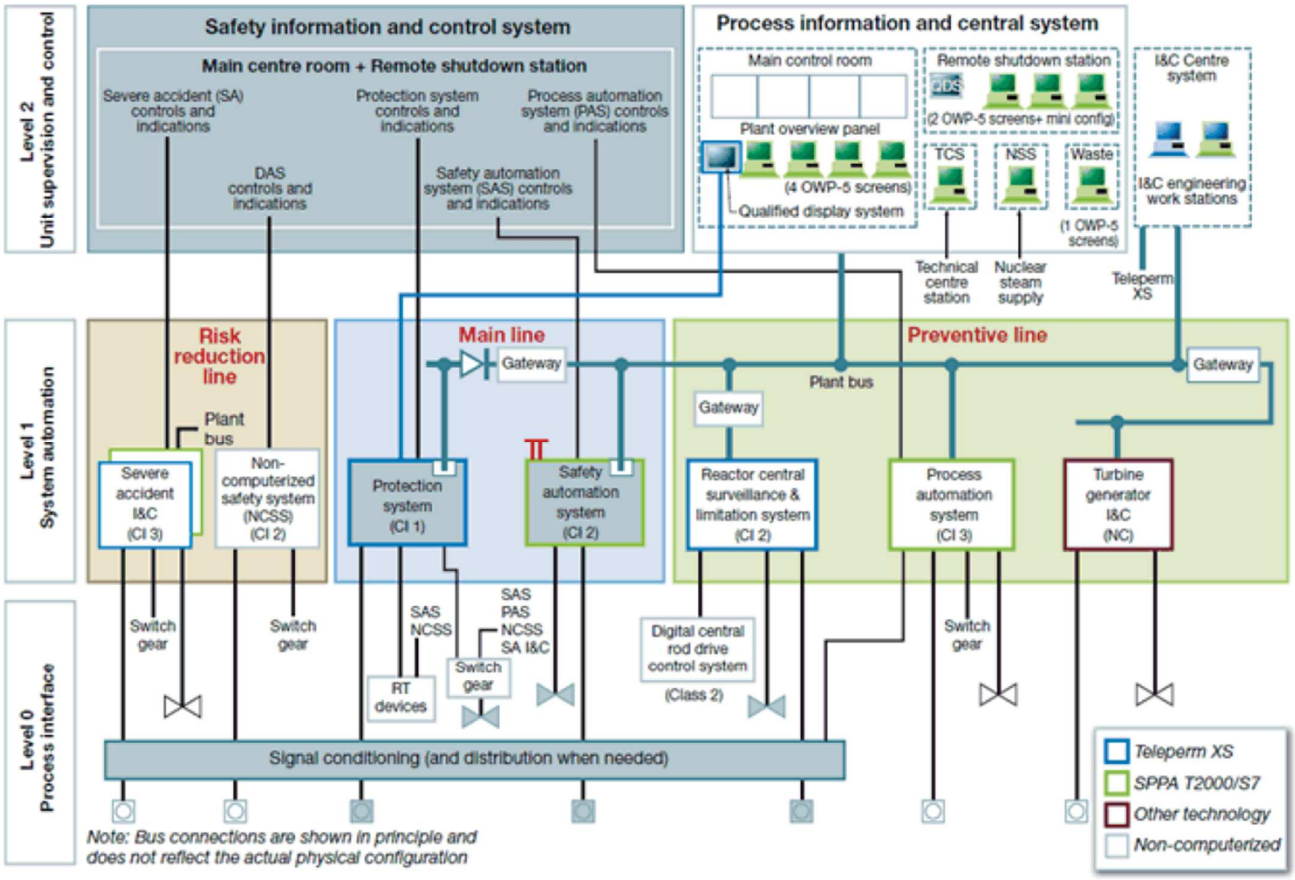
Path exercised continuously in normal situations
Influence factors during continuous operation:
- normal process inputs (validated before use)
- short-term memory (as little as possible)
- clock interrupts (thorough verification)
- *(process-related interrupts: none)*
- *(resource management: static)*

Path exercised in occasional but tested situations
Infrequent factors that could disrupt cyclic behavior:
- initialization (only once)
- operator requests (single channel)
- hardware failures (single channel)
- exceptions (very simple)
- *(particular dates & times: avoided)*
- plant transients: affect all channels

Path exercised in unanticipated or untested situations

Possibilities for CCFs in systems





Automaation arkitehtuuri suunnitteella olevalla laitoksella

Toinen harjoitustehtävä

Oleta että olet äskettäin palkattu keskisuuren organisaation turvallisuusjohtajaksi, olet käynnyt ensimmäisen kuukauden haastattelemassa ihmisiä ja olet huomannut että ruutiineja puuttu eikä kukaan näytä olevan vastuussa turvallisuudesta. Sait käteen OHSAS 18001 normiston, joka koskee teitä. Laadi hahmotelma siitä, miten edetään.

- toiminnalliset yksiköt?
- yksiköiden tehtävät?
- mahdolliset tehokkuusindikaattorit?
- normaali raportointi?
- erityistilanteiden tunnistaminen ja raportointi?
- koulutussuunnitelma?