Kolmas päivä, 31.8

- ap, 9.00-12.00
  - harjoitustehtävän palaute
  - viranomaisvalvonta

    valtuutukset, viranomaisen tehtävät, valvonnan lähtökohdat ja strategiat, ohjeiden seuraaminen, viranomaiselle asetettavat vaatimukset, turvallisuuden byrokratisointi
  - turvallisuuden osoittaminen

    turvallisuusseloste, uusien systeemien turvallisuus, turvallisuuden byrokratisointi
  - turvallisuuskriittisten systeemien suunnittelu,

    vaatimukset, suunnitteluprosessi, automaation turvallisuus, ihminen – kone liitäntä, tietokonetuetut työkalut
- ip, 13.00-16.00
  - esimerkkinä ydinvoima

    historia, välttämättömät ja riittävät vaatimukset, teknologiakehityksen elinkaari, johtamisjärjestelmän komponentit, onnettomuusmalli PRA-analyysiin, yhteisviat
  - turvallisuusjohtamisen haasteet

    mitä riittää, turvallisuus versus muut tavoitteet, balanssien varmistaminen, konservatiivinen päätöksenteko, lisää monimutkaisuutta, parempia työkaluja?
  - katse tulevaisuuteen

    yhteiskunnan asettamat vaatimukset, uudet uhat, security
  - harjoitustehtävä 3

Toinen harjoitustehtävä

Oleta, että olet äskettäin palkattu keskisuuren organisaation turvallisuusjohtajaksi, olet käynnyt ensimmäisen kuukauden haastattelemassa ihmisiä ja olet huomannut että ruutiineja puuttuu 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?

Palaute, harjoitustyö 2 (1/3)

1. Varmista, että ylin johto on sitoutunut turvallisuuden parantamiseen, ja että organisaatio tietää sen. Kulttuurin muutos tapahtuu pääasiassa alemmilla tasoilla, mutta sen pitää lähteä liikkeelle ylhäältä.
2. Palkkaa tai mieluummin ylennä olemassa olevan henkilöstön keskuudesta riskivastaavat kaikkiin toiminnallisiin yksiköihin tai jopa useampia yksiköiden koosta riippuen. Heidän tehtävänään on vastata ja raportoida eteenpäin yksiköiden riskitilanteesta. Riskivastaavat tarvitsevat myös lisäkoulutusta.
3. Suorita kattava riskikartoitus yksikkötasolla painottaen erityisesti työntekijöiden kokemuksia riskeistä, mutta pyri ottamaan huomioon myös riskit, joita työntekijät eivät edes itse tunnista. Huomioi ainakin
    - työtehtävät
    - infrastruktuuri
    - laitteisto
    - aktiviteetit

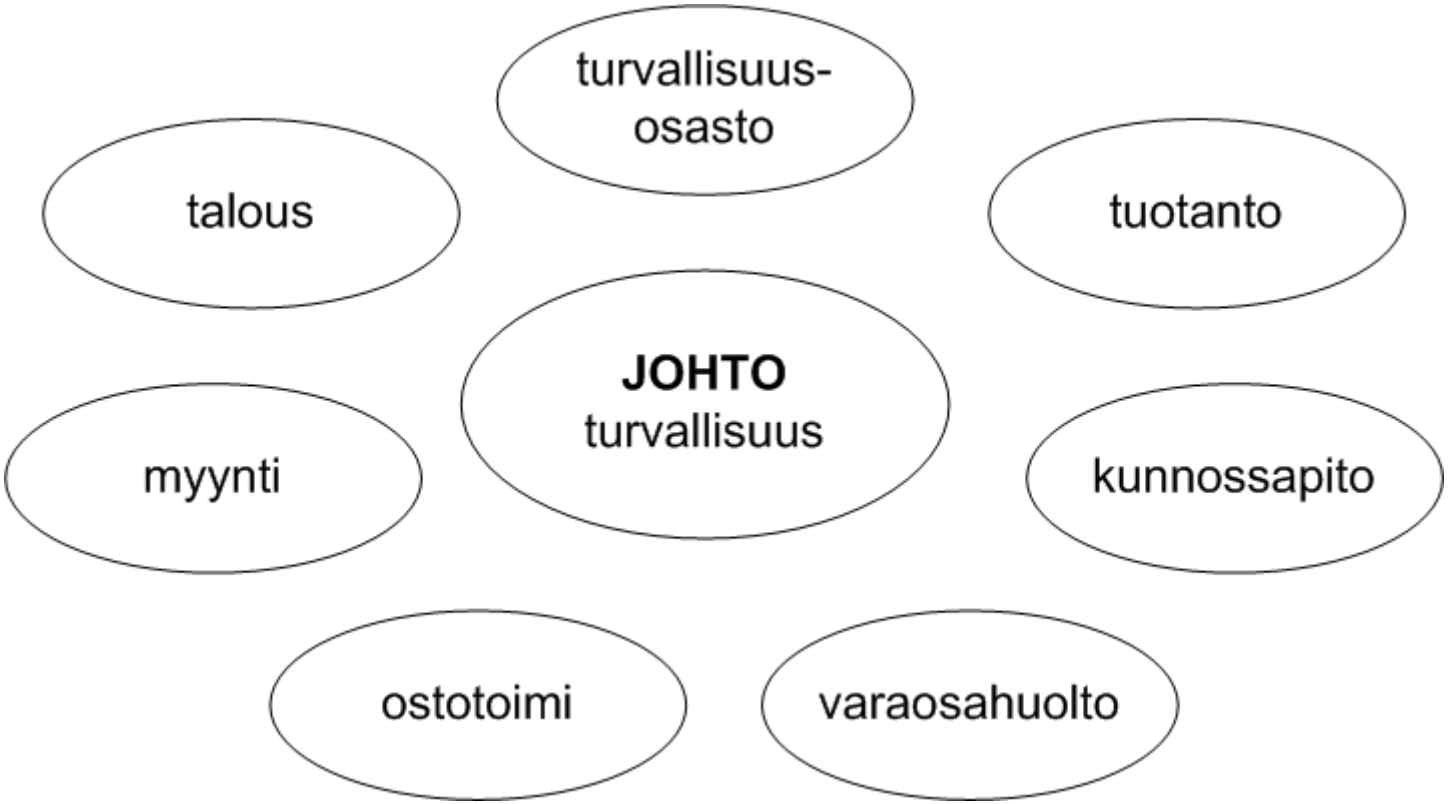
Palaute, harjoitustyö 2 (2/3)

4. Ota käyttöön riskien arviointi kaikkien uusien projektien ja merkittävien laite ym. hankintojen yhteydessä. Projektin toteuttajien ja/tai laitteen käyttäjien on syytä olla mukana tässä arvioinnissa.
5. Mikäli riskikartoituksessa on havaittu puutteita henkilöstön osaamisessa, täydentävät koulutukset on syytä aloittaa välittömästi asiaankuuluvan henkilöstön osalta. Samalla on syytä valistaa koko henkilöstöä uusista riskienhallintatoimenpiteistä ja riskivastaavista, ja mikäli nähdään hyödylliseksi, myös järjestää koulutusta onnettomuuksien tai muiden vaarallisten tilanteiden varalle. Perusvalmiudet sairaskohtaukseen reagoimiseen ovat tarpeelliset kaikissa organisaatioyksiköissä.
6. Käynnistä systemaattinen riskitilanteiden seuranta. Seurannan on syytä kattaa ainakin laitteiston poikkeustilanteet sekä henkilöstölle aiheutuneet vaara- ja läheltä piti –tilanteet. Riskivastaavat ovat vastuussa tiedon keräämisestä, ja se tarkastellaan ja säilötään kootusti organisaatiotasolla.
7. Seuraa laitteiston toimintaa ja henkilöstön hyvinvointia myös normaalitilanteessa, jotta riskejä voidaan välttää ennalta. Esimerkiksi laitteiston toiminnan muutokset tai työntekijöiden lisääntynyt kuormitus voivat ennakoida riskien kasvua. Jos poikkeuksia havaitaan, puutu niihin!

Palaute, harjoitustyö 2 (3/3)

8. Kehitä ohjeistus vakavien sisäisten tai ulkoisten onnettomuuksien varalle, ja pidä huolta, että henkilöstö tuntee ohjeistuksen ja se on helposti saatavilla.
9. Aloita tarvittavat projektit työympäristöön ja työvälineisiin liittyvien riskien hallitsemiseksi aloittaen vakavimmista käyttäen haluamaasi riskimittaa. Normaalin työn keskeyttäminen voi jopa osoittautua tarpeelliseksi tässä vaiheessa. Huomioi ainakin seuraavat
    - lisää erityisen riskialttiisiin toimintoihin tai aktiviteetteihin kontrollit riskien minimoimiseksi
    - korjaa puutteet työympäristössä
    - korjaa puutteet työvälineissä
10. Pidä huolta, että riskienhallintasuunnitelmaa tarkastetaan vuosittain, tai jopa useammin, mikäli työn luonne sen vaatii. Suunnitelma on syytä myös tarkastaa merkittävimpien projektien yhteydessä.
11. Järjestä riskienhallintajärjestelmän auditoinnit kuntoon.
12. Varmista, että turvallisuusnäkökohdat tulevat myös osaksi johdon katselmuksia.

Turvallisuus kuuluu kaikille



Viranomaisvalvonta

Viranomainen on julkisyhteisö, kuten kunnan, kirkon tai valtion pysyvä toimielin, jolle on säädöksillä annettu toimivalta ja velvollisuus tiettyjen tehtävien hoitamiseen omalla toimialallaan.

Suomalaisia turvallisuusviranomaisia

- Poliisi
- Puolustusvoimat
- Rajavaritiolaitos
- Pelastuslaitos
- Työsuojeluhallinto
- TUKES
- STUK
- Valvira
- Evira
- Fimea
- jne.

Viranomaisen tehtävät

- Omalla toimialuellaan määritellä hyväksyttävälle toiminnalle asetettavat vaatimukset (säännöstöt)
- Valvoa että säännöstöjen vaatimukset täyttyvät
  - pyynnöstä myöntää toimilupia organisaatioille, jotka toimivat määritellyillä alueilla
  - tarkastuksilla varmistua siitä, että vaatimukset täyttyvät ja peruuttaa annettuja toimilupia elleivät niitä enää täyty

Qualification, validation and verification

- Kelpoistus

  Kelpoistuksella (qualification) tarkoitetaan prosessia, jonka perusteella osoitetaan kyky täyttää määritellyt vaatimukset (vastaa ISO 9000:n pätevöintiprosessia).

- Kelpuutus

  Kelpuutuksella (validation) tarkoitetaan objektiiviseen näyttöön perustuvaa varmistumista siitä, että tiettyä käyttöä tai soveltamista koskevat vaatimukset on täytetty.

- Todentaminen

  Todentamisella (verification) tarkoitetaan objektiiviseen näyttöön perustuvaa varmistumista siitä, että määritellyt vaatimukset on täytetty.

Valvonnan strategiat

- general – detailed (a dimension characterising the level of detail of the requirements in the regulatory system),
- case – rule based (a dimension characterising if the safety argumentation is built as a single case or in compliance with a certain set of generic rules),
- deterministic – probabilistic (a dimension characterising the relative weight, which is laid either on deterministic or probabilistic safety arguments),
- performance – process based (a dimension characterising the relative weight, which is laid either on assessing the output of used work processes or their internal structure and control),
- level of involvement (a dimension characterising the relative weight, which the regulator is placing on own oversight as compared with oversight of self-regulative functions of the licensees).

B. Wahlström (2007). Reflections on regulatory oversight of nuclear power plants, Int. J. Nuclear Law, 1, pp.344–377.

WENRAn turvallisuusvaatimukset (Issues)

A: Safety Policy
B: Operating Organisation
C: Management System
D: Training and Authorization of NPP Staff (Jobs with Safety Importance)
E: Design Basis Envelope for Existing Reactors
F: Design Extension of Existing Reactors
G: Safety Classification of Structures, Systems and Components
H: Operational Limits and Conditions (OLCs)
I: Ageing Management
J: System for Investigation of Events and Operational Experience Feedback
K: Maintenance, In Service Inspection and Functional Testing
LM; Emergency Operating Procedures and Severe Accident Management Guidelines
N: Contents and Updating of Safety Analysis Report (SAR)
O: Probabilistic Safety Analysis (PSA)
P: Periodic Safety Review (PSR)
Q: Plant Modifications
R: On-site Emergency Preparedness
S: Protection against Internal Fires
T: Natural Hazards

http://www.wenra.org/media/filer_public/2016/07/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf

Esimerkkejä WENRA dokumentin vaatimuksista

A: 1.3 The safety policy shall include a commitment to continuously develop safety.

B: 1.3 Responsibilities, authorities, and lines of communication shall be clearly defined and documented for all staff with duties important to safety.

C: 3.2 The licensee shall ensure that it is clear when, how and by whom decisions are to be made within the management system.

D: 2.3 Appropriate training records and records of assessments against competence requirements shall be established and maintained for each individual with tasks important to safety.

G: 3.2 The failure of a SSC in one safety class shall not cause the failure of other SSCs in a higher safety class. Auxiliary systems supporting equipment important to safety shall be classified accordingly.

H: 5.1 Adequate margins shall be ensured between operational limits and the established safety systems settings, to avoid undesirably frequent actuation of safety systems.

J: 1.4 Staff responsible for evaluation of operational experience and investigation into events shall receive adequate training, resources, and support from the line management.

Q: 2.1 The licensee shall establish a process to ensure that all permanent and temporary modifications are properly designed, reviewed, controlled, and implemented, and that all relevant safety requirements are met.

Lyhennetty vaatimuslista

- Yleiset vaatimukset
  - sitoutuminen turvallisuuden jatkuvaan parantamiseen
  - johto, henkilökunta, alihankkijat ja urakoitsijat ymmärtävät laitoksen ja ovat sitoutuneita ja motivoituneita
  - työtä tehdään systemaattisesti (suunnittelu, suoritukset, kerätään palautteita, arvioidaan, selitetään, dokumentoidaan)
  - resursseja on riittävästi (osaamista, aikaa, rahaa, tilaa)
  - käytetään tarkoituksenmukaisia menetelmiä ja työkaluja
- Erityisiä vaatimuksia
  - mukautettu suhtautuminen turvallisuuteen, luokitusjärjestelmä
  - syväpuolustus, riskianalyysi, redundanssi, diversiteetti, turvallisuustekniset käyttöehdot
  - käyttökokemusten hyödyntäminen, muutosten hallintaa, tarkastuksia
  - viranomaisvalvontaa (lupakäsittely, raportointi, ilmoitukset)

Huono käyttöohje?

Working to rule, or working safely?

Ohjeita ei aina seurata!

- ohje mahdollisesti ei sovi tilanteeseen, mutta ennalta mietityt toimenpiteet ovat tavallisesti parempia kuin pelkkä improvisointi
- ohjetyypit
  - tavoitteet on määritelty
  - prosessi on määritelty
  - toimenpiteet on määritelty (if ... then ...)
- yleinen suhtautuminen ohjeisiin
  - jos tehdään ohjeiden mukaan homma ei tule tehtyä
  - ohjeita pitää aina noudattaa
  - jos ohjeita noudattaa, ei tule haukkuja

Andrew Hale, David Borys (2013). Working to rule, or working safely? Part 1: A state of art review, Safety Science, Vol.55, p.207–221.
Andrew Hale, David Borys (2013). Working to rule, or working safely? Part 2: The management of safety rules, Safety Science, Vol.55, p.222–231.

Käyttöohjeet

Käyttöohjeet pitää suunnitella yhtä huolellisesti kuin valvomotkin

- TMI onnettomuudessa käyttöohjeiden toteutus oli keskeinen syy tapahtumien kulkuun
- tapahtuma- ja oirepohjaiset käyttöohjeet
- ennakolta mietitty toimintastrategia aina on parempi kuin tilanteessa kehitetty toimintatapa edellyttäen että tilannetta diagnostisoidaan oikein
- käyttöohjeesta poikkeaminen pitää olla sallittua, mutta jos poiketaan, tilannetta pitää analysoida kunnolla ja käyttöohjetta pitää päivittää analyysin mukaisesti
- käyttöohjeita voidaan suunnitella kahdella tavalla, ylhäältä alas tai alhaalta ylös

Rules to Achieve Safety

- Some questions as guidelines for an evaluation of safety rules

  Are the future users and working conditions known? What are the justifcations for the rule? Are there other possible means (technical, ergonomical, etc.) for achieving the same result? Is the new rule coherent with the other different existing systems of rules? Are there possibilities for conficts and ways of solving them? Is the new rule adaptable to changes in conditions?

- Acceptability

  Is the (physical, mental, etc.) cost of implementation not too high? Is the rule suited to the real activity (and not only to the prescribed one)? Is the rule suited to the user's competence; to different levels of his future experience? Can possible difficulties of implementation be discussed with the users? Are possible adaptations of the rule foreseen?

- Accessibility

  How is the rule made known? Is the support of the rule easily accessible? Are the means of rule implementation foreseen and available? Are the conditions of rule implementation sufficiently explicit? Is the rule content accessible to the users (readability, linguistic, logical intelligibility)? Is the rule cognitively justifed for the users?

J. Leplat: About implementation of safety rules, Safety Science 29 (1998) 189-204

Viranomaiselle asetettavat vaatimukset

- selkeä rooli, joka heijastuu käytäntöihin
- yhteiskunnan ja sidosryhmien luottamus
- integriteetti ja riippumattomuus
- päätökset ovat perusteltavissa ja lainsäädännön mukaisia
- valtaa käytetään tarvittaessa
- sekä virallisia että epävirallisia kommunikointikanavia käytetään
- laaja ja syvällinen osaaminen
- riittävät resurssit
- selkeät ja peittävät vaatimukset eri alueilla ja tasoilla
- systemaattinen käyttökokemusten hyödyntäminen
- itseluottamus
- toimivat kansainväliset kontaktit

Turvallisuuden osoittaminen

- Vaatimusten täyttäminen
  - suunnitteluprosessin hyvyys
  - tuotteiden ja osatuotteiden laatu
- Väittämät
  - deterministinen vaatimus ***i*** on täytetty
  - probabilistinen vaatimus ***j*** on täytetty
- Todisteet
  - rakenteelliset (määrättyjä suunnitteluvirheitä 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

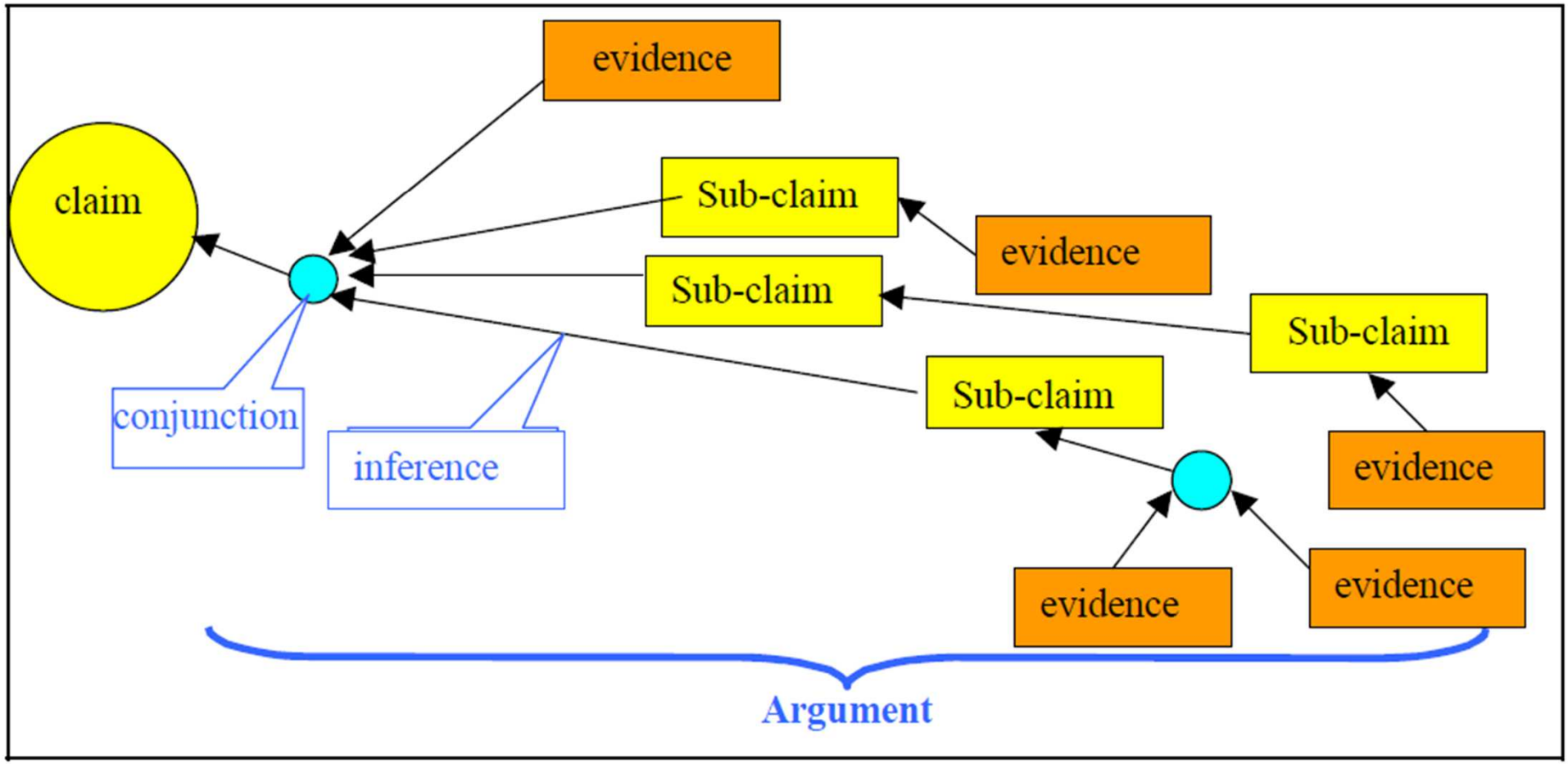
- tunnistetut turvallisuusuhat
- tunnistetut systeemien, rakenteiden ja komponenttien mahdolliset vikaantumismekanismit
- käytetyt turvallisuusperiaatteet ja miten niitä on huomioitu laitoksen suunnittelussa ja käytössä
- miten normaalit käyttöolosuhteet ja mahdolliset virhetilanteet on analysoitu ja 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

Turvallisuuden byrokratisointi

"Businesses are in the stranglehold of health and safety red tape. . . We are waging war against this excessive health and safety culture that has become an albatross around the neck of businesses". David Cameron, UK Prime Minister

Onko vaatimukset viety liian pitkälle?

- hierarkiat organisaatioissa
- erikoistuminen kapeisiin alueisiin
- iso määrä formaalisia vaatimuksia ja sääntöjä
- osa toiminnasta on siirtynyt asiantuntijoilta byrokraateille

Miten vaatimusten eroavaisuudet eri maissa ja eri toimialueiden välissä vaikuttavat?

S.W.A. Dekker (2014). The bureaucratization of safety, Safety Science, 70, 348–357.
K. Vedal Størkersen (2015). Survival versus safety at sea. Regulators' portrayal of paralysis in safety regulation development, Safety Science, 75, 90–99.

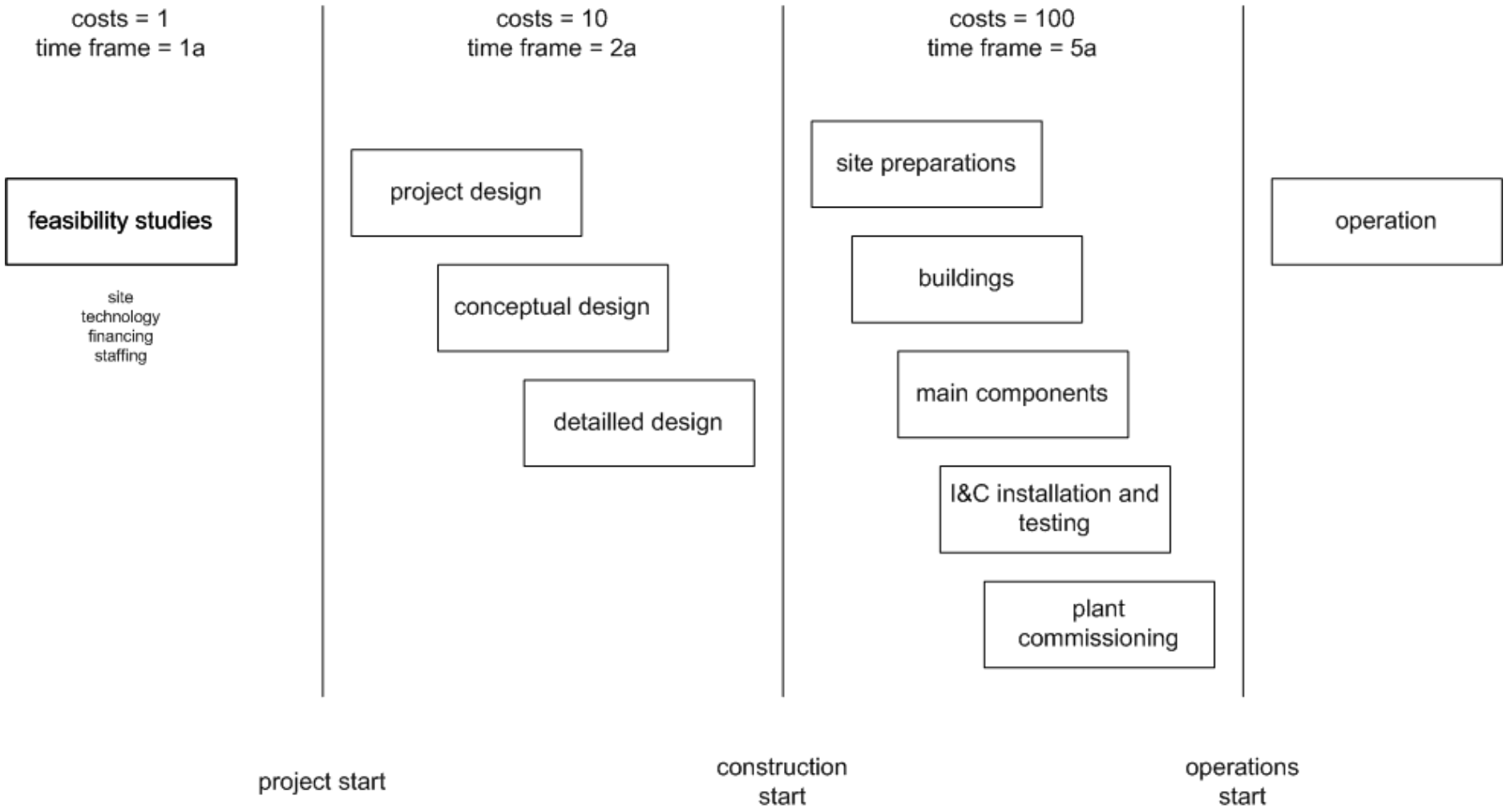
Turvallisuuskriittisen systeemin suunnittelu

Design a safe car – drive a car safely

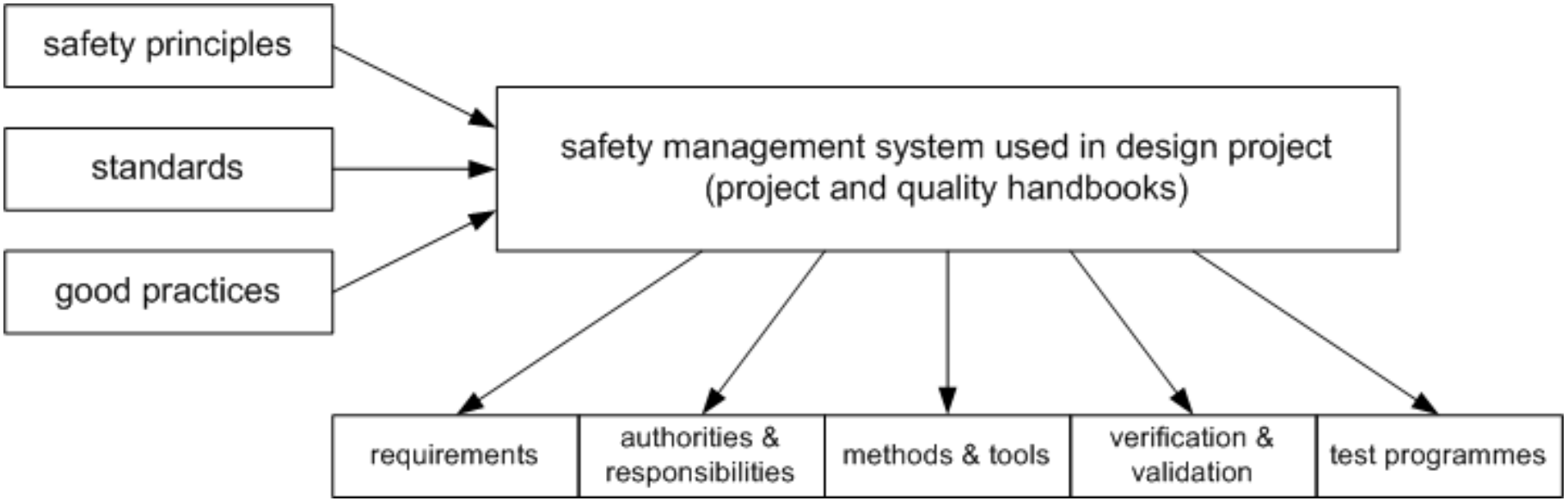
- Systeemille asetettavat vaatimukset?
- Turvallisuusperiaatteiden käyttäminen
- Systeemin jakaaminen osasysteemeihin ja edelleen komponenteihin
- Osasysteemien suunnittelu ja komponenttien valinta
- Asteittainen komponenttien ja osasysteemien integrointi ja testaus (V&V)
- Kelpoistamissuunnitelman laatiminen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

Hyvä suunnitteluprosessi ja riittävä laadunvarmistus!

Uuden laitoksen rakentaminen



Suunnitteluprojektin johtamisjärjestelmä



Safety principles

- Safety reserves

  robustness, resilience, defence in depth, safety barriers, safety margins, fail-safe, single failure criterion

- Information and control

  experience feedback, human factors engineering, operating procedures, system usability, operational interfaces, safety automation, risk communication, precaution

- Demonstrability

  inherently safe, proven design, simplicity, quality assurance and control, inspections and reviews, verification and validation, safety case, inspectability and maintainability

- Optimisation

  continuous improvements, safety quantification, rest risks, human reliability, cost and benefit analysis, ALARA, BAT, substitution principle, risk informed regulation, safety integrity levels, risk homeostasis

- Organisational principles

  standards, guidelines, emergency plans, crisis management, safety management, safety culture, management of the unexpected

J. H. Saleh, K. B. Marais, F. M. Favaró (2014). System safety principles: A multidisciplinary engineering perspective, J.Loss Prevention in the Process Industries, 29, pp.283-294.

N. Möller, S. O. Hansson, J.-E. Holmberg, C. Rollenhagen (eds.), 2017 (tulossa): Handbook of Safety Principles, John Wiley & Sons, Inc.

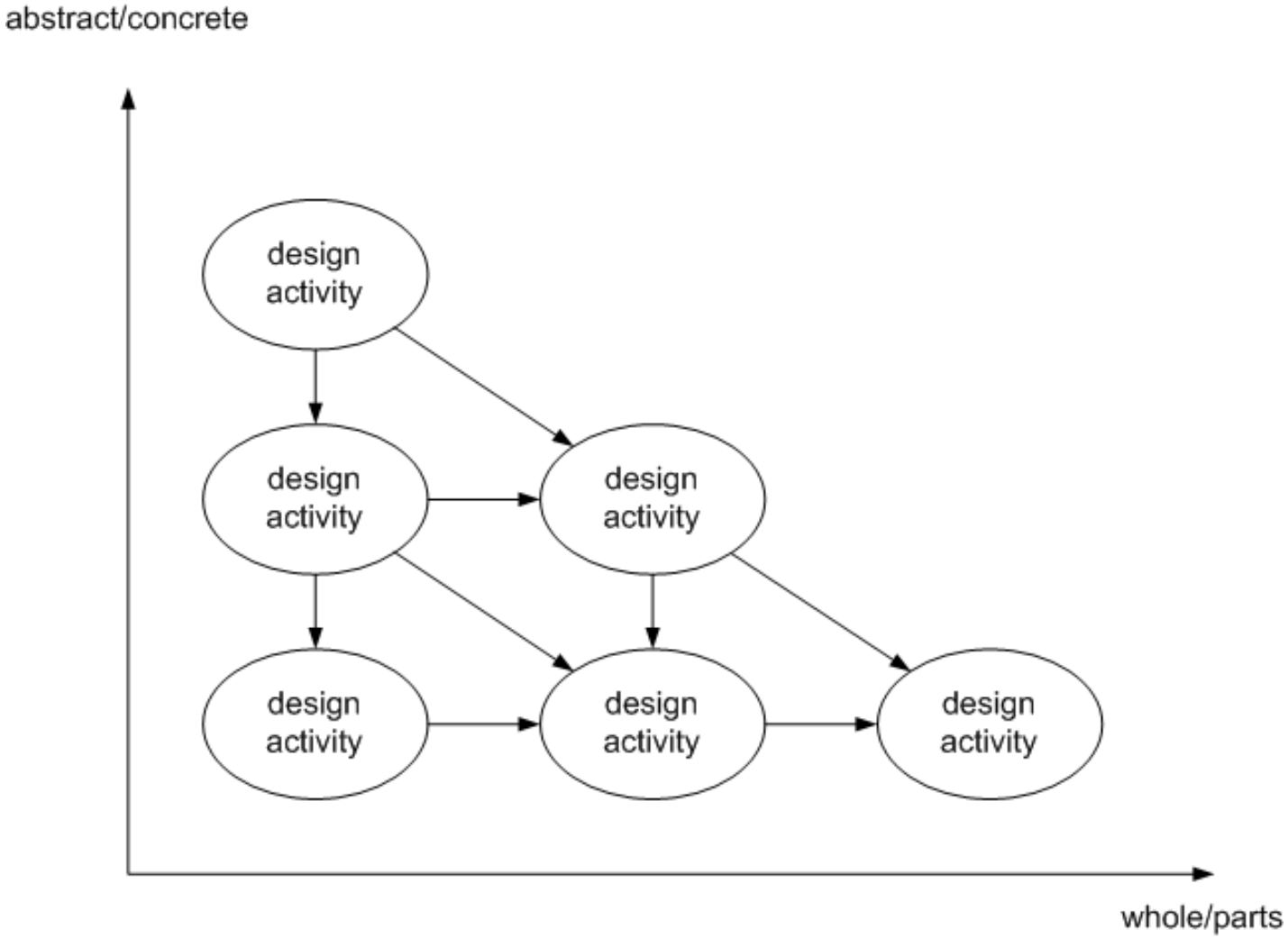
Systeemille asetettavat vaatimukset

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

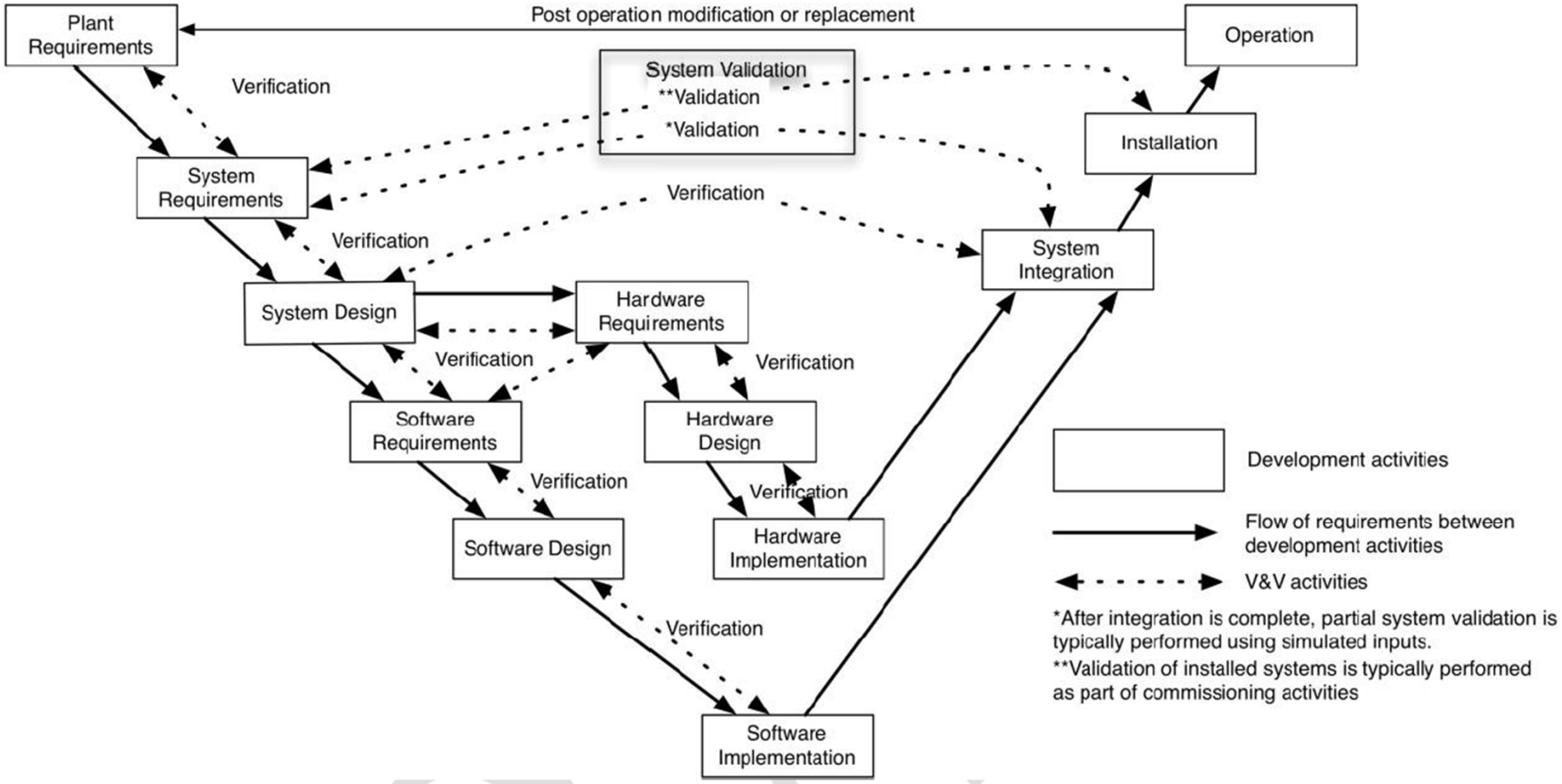
Vaatimusten hallinta

- 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

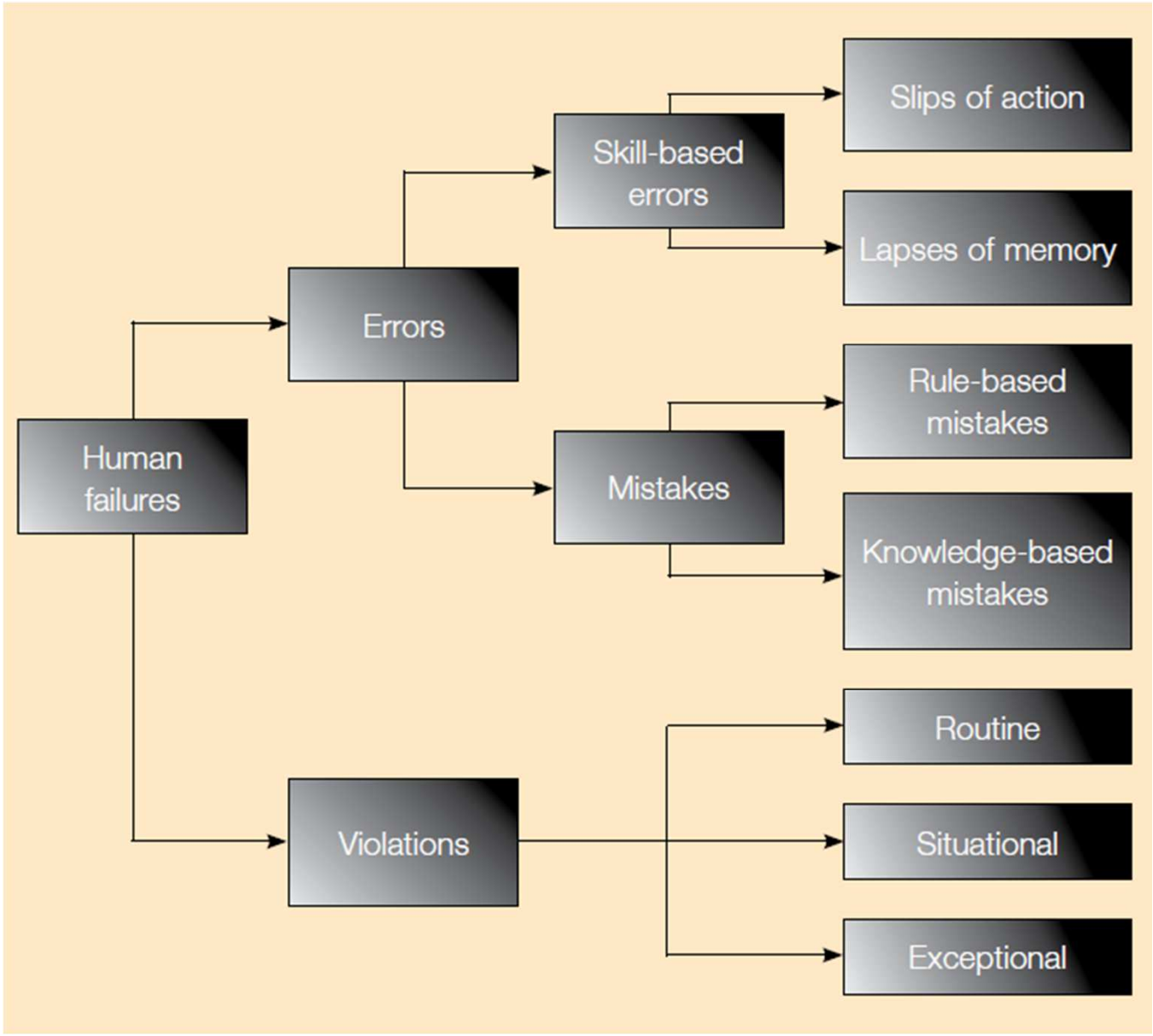
- aktiiviset virheet
- piilevät virheet

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

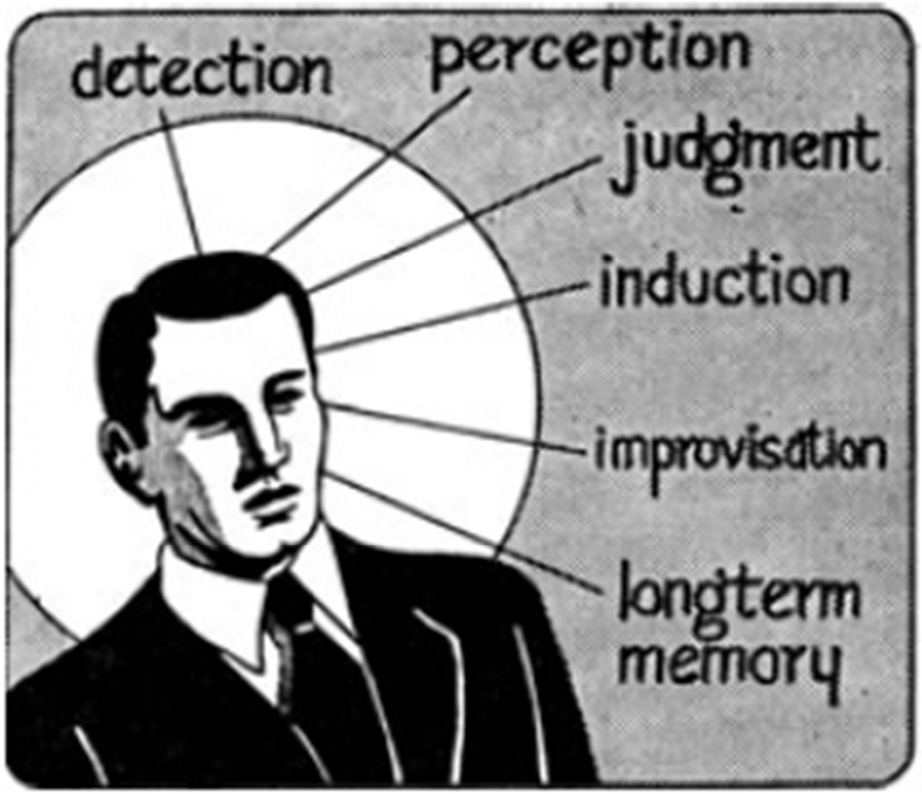


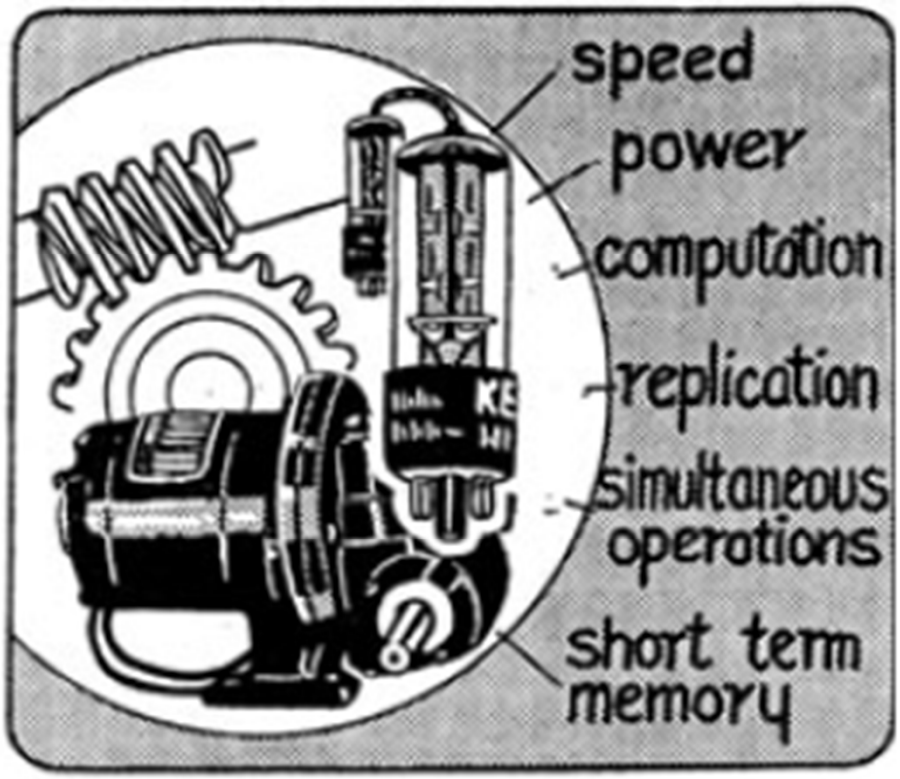
Systeemien sovittaminen ihmisiin

- Toimintojen allokointi ihmisten ja automaation välillä
- Ihmisen ja koneen välisen rajapinnan suunnittelu ja kelpoistaminen
  - valvomon suunnittelu
  - tehtävien suunnittelu
  - näyttöjen suunnittelu
  - käyttöohjeiden suunnittelu
  - konseptien 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





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

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	

Human factors assessment in periodic safty reviews

a) staffing levels, rules and restrictions on absences
b) availability of qualified staff
c) staff selection criteria and methods
d) competence requirements and verification
e) training programs
f) policy to maintain the know-how of the plant staff
g) training of safety culture
h) programmes for the feedback of operating and event experience to prevent human errors
i) fitness for duty programmes and controls
j) human–machine interfaces
k) style, clarity and completeness of procedures

JK Vaurio (2009). Human factors , human reliability and rsk assessment in license renewal of a nuclear power plant, Reliability Engineering and System Safety, 94, 1818–1826.

Automaation turvallisuus

- Hyvä suunnitteluprosessi
  - suunnitteluprosessin johtamisjärjestelmä
  - suunnitteluprosessin aikana käytettyjä turvallisuusperiaatteita
  - 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 automaatio

- suorittaa kaikki vaaditut toiminnot
- ei suorita mitään ylimääräistä toimintoa

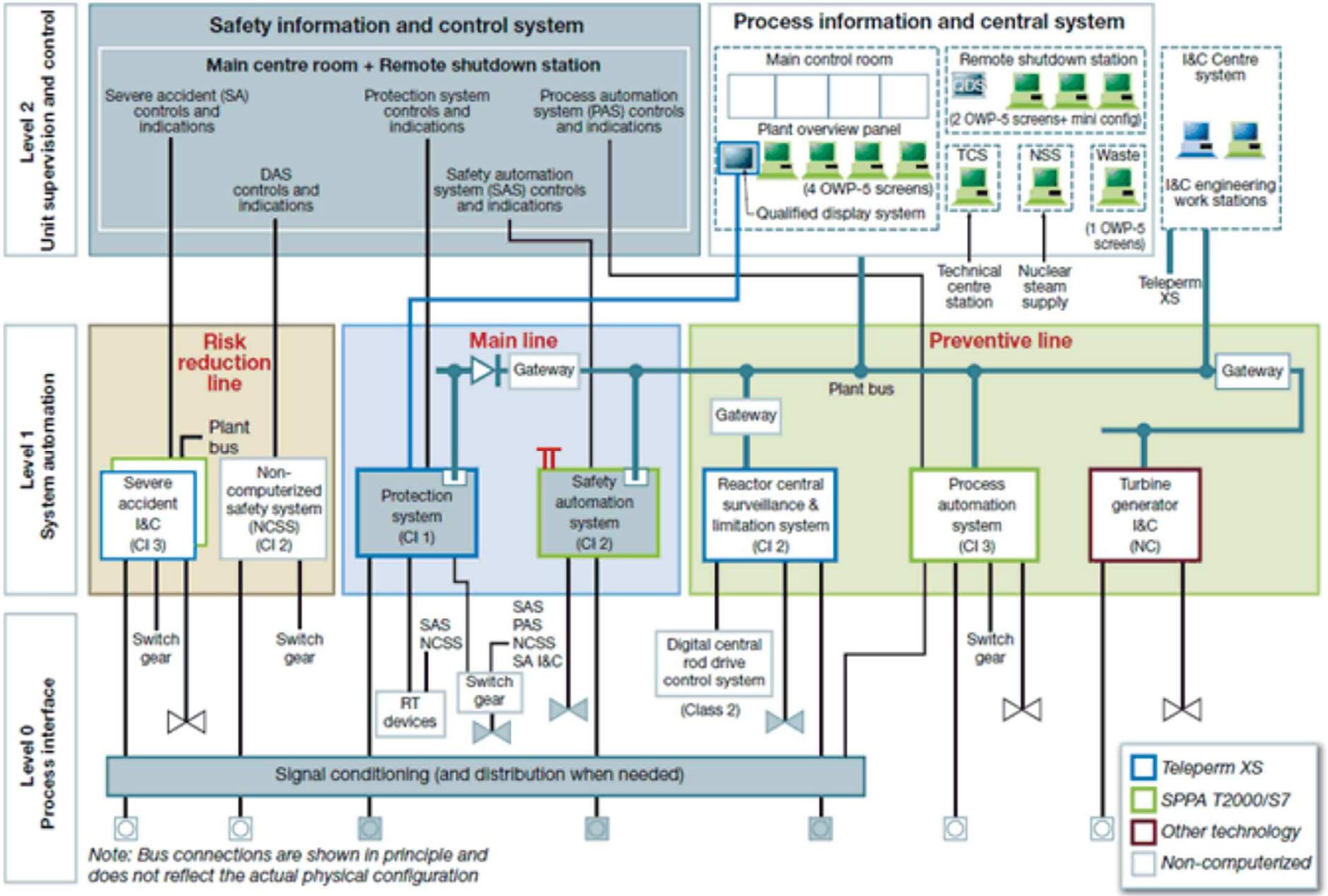
Ongelman lähteet

- 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

Digitaaliset automaatiojärjestelmät

- Ohjelmistojen vaatimusmäärittelyissä saattaa olla virheitä ja/tai ristiriitaisuuksia
- Täydellistä testausta ei ole mahdollista
- Ohjelmistossa saattaa olla piileviä virheitä
- Ohjelmistojen kehitystyökaluissa saattaa olla virheitä
- Kuinka erilaiset ohjelmistojen on oltava, jotta voidaan väittää ettei yhteisvikoja ole mahdollisia?
- Miten voidaan olla varmoja siitä, että yhden virheen korjaaminen ei ole tuonut uusia virheitä?
- Miten voidaan arvioida ohjelmiston luotettavuutta?
- Ohjelmistosuunnittelijat rakentavat usein takaportteja ohjelmistoihin
- Ohjelmistot ovat alttiita kyberhyökkäyksiin



Tyypillinen automaation arkitehtuuri ydinvoimalaitoksella

Tietokonetuetut työkalut

Kompleksisuuden hallintaan tarvitaan työkaluja

- systeemien, osasysteemien ja komponenttien suuri lukumäärä
- eri osasysteemien kytkentöjen suuri lukumäärä ja niiden mahdollinen epälineaarisuus
- tavoite- ja vaatimushierarkioiden sisäiset ja ulkoiset relaatiot
- integroituneisuus (matala, korkea)
- takaisin- ja myötäkytkennät
- ihmisten ja organisaatioiden vaikutukset
- päätösten vaikutukset vaikeasti ennustettavissa

Muutamia esimerkkejä

- Erilaiset simulointiohjelmat
- HAZOPin tukijärjestelmät
- Probabilistisen riskianalyysin tukijärjestelmät
- Vaatimusten hallintajärjestelmät
- Konfiguraation tukijärjestelmät
- Dokumentaatiojärjestelmät
- CAD ja CAM järjestelmät
- Virtualinen todellisuus
- Sosiaalisten järjestelmien simulointi
- Yhteistyön tukeminen

Esimerkkinä ydinvoimaa

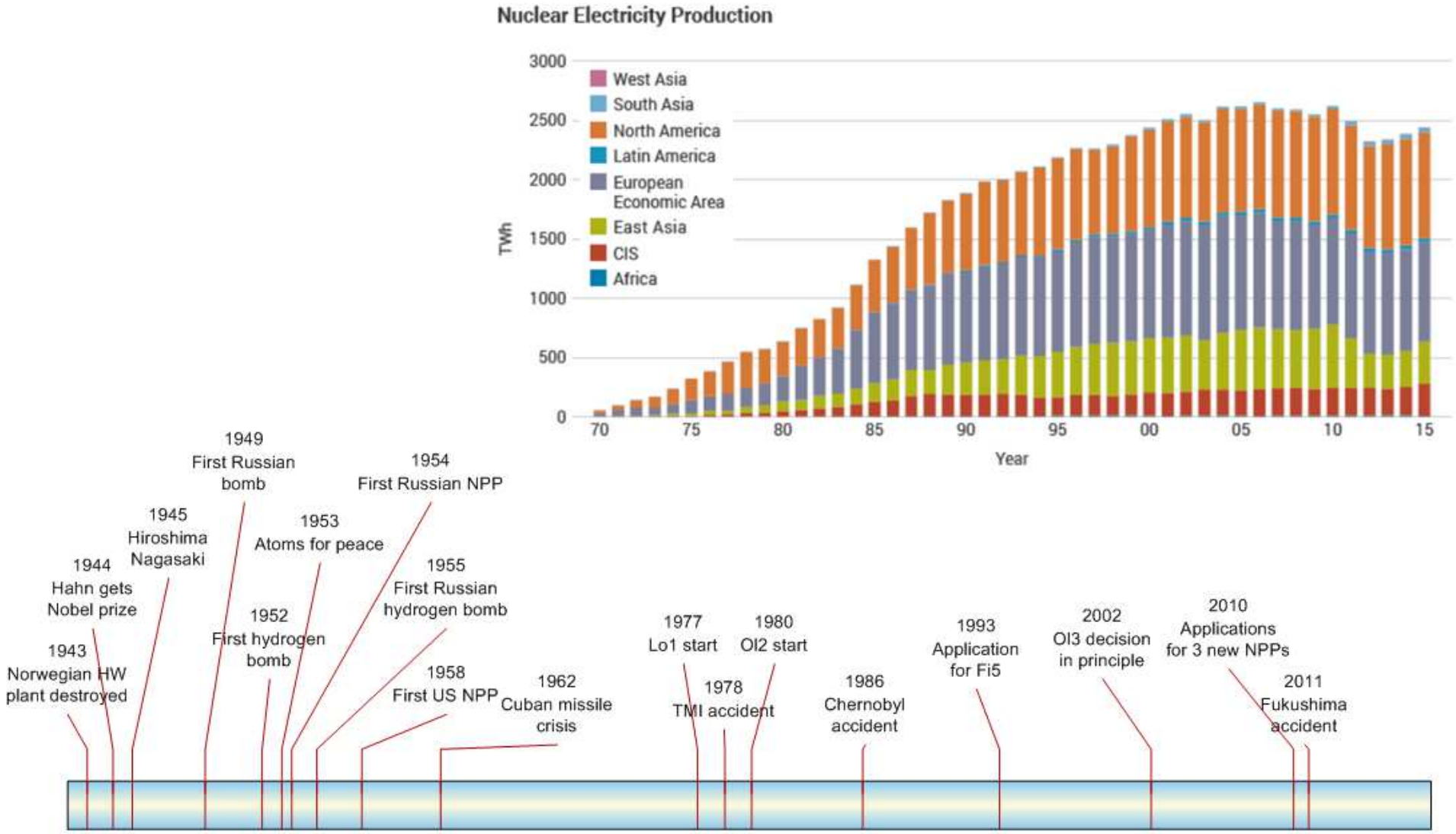
Onko mahdollista rakentaa ja käyttää turvallisesti?

- Historia
  - kilpavarustelu
  - nopea rakentaminen
  - kolme onnettomuutta
  - uusi tuleminen?
  - ongelmalliset projektit
- Turvallisuusajattelu
  - riittävät ja välttämättömät ehdot
  - laitosten elinkaari (suunnittelu, käyttö, purkaminen)
  - syväpuolustus ja turvallisuusluokittelu
  - turvallisuusseloste
  - viranomaisvalvonta

Turvallisuusvaatimukset (keskustelua)

- Välttämättömät ehdot
  - kattava riskianalyysi
  - anteeksi antava valvomo
  - kattava testausohjelma
  - dokumentointi (systeemikuvaukset, käyttöohjeet)
  - sitoutuminen turvallisuuden jatkuvaan kehittämiseen
- Riittävät ehdot
  - paras tietämys ja osaaminen on käytetty
  - uhat ja käyttötilanteet on käsitelty
  - uskottavat tarkastukset ja testaukset
  - henkilöstö on saanut koulutusta
  - huomautuksiin on vastattu uskottavasti

Synty, kehitys ja muutamia ajankohtia



Ydinvoima varteenotettava teknologia?

Kyllä

- ei CO_2 päästöjä
- riittävät polttoainevarannot (nopeat reaktorit, torium)
- olemassa oleva säännöstö (periaatteet tunnetaan)
- kansainvälinen yhteistyö

Ei

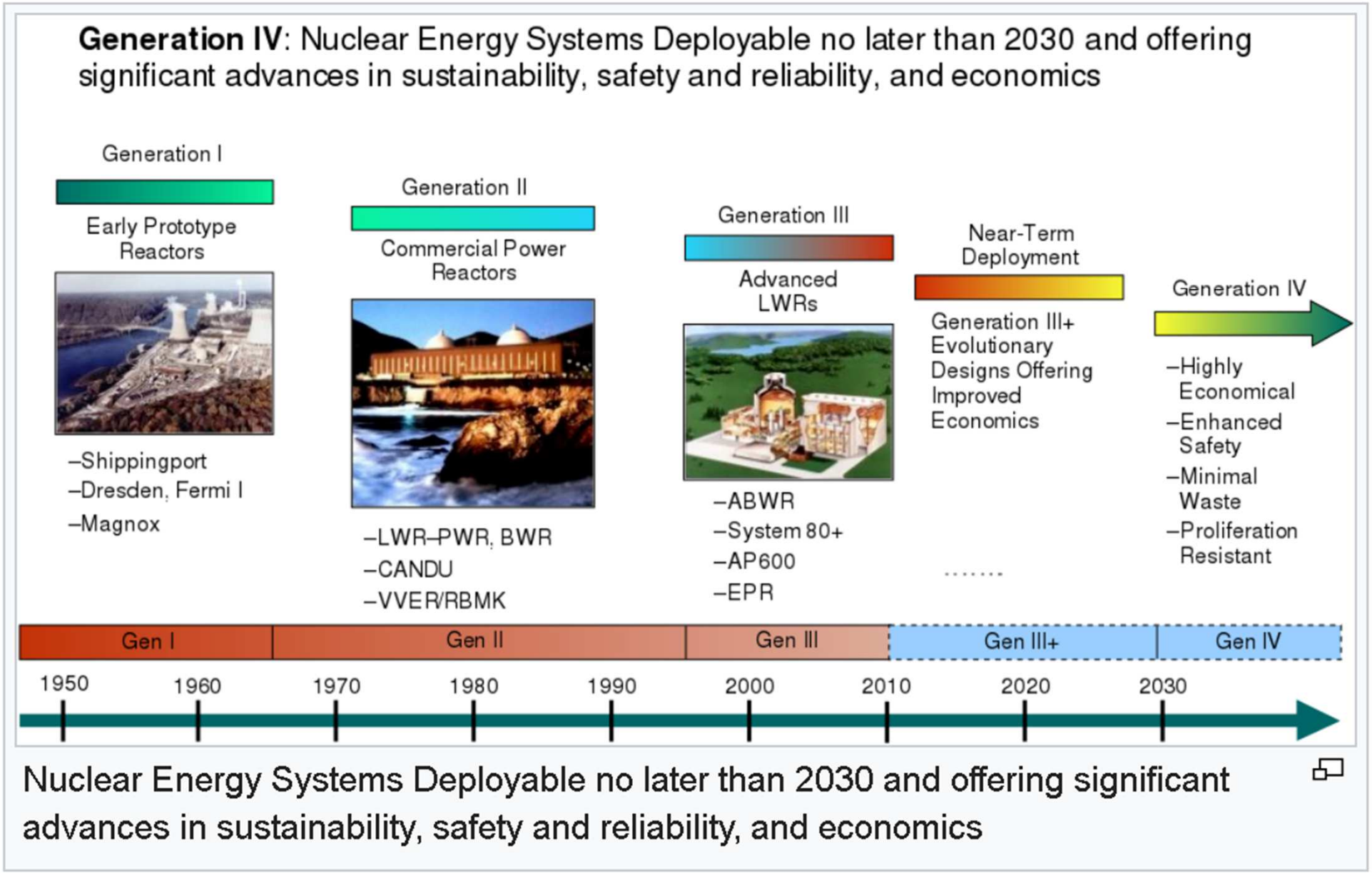
- poliittinen vastustus
- monimutkaisuus
- rahoitusvaikeudet

Plans For New Reactors Worldwide*

- Nuclear power capacity worldwide is increasing steadily, with over 60 reactors under construction in 15 countries.
- Most reactors on order or planned are in the Asian region, though there are major plans for new units in Russia.
- Significant further capacity is being created by plant upgrading.
- Plant life extension programs are maintaining capacity, in USA particularly.

* Tilanne helmikuussa 2017

An international task force (Generation IV International Forum) is developing six nuclear reactor technologies for deployment between 2020 and 2030. Four are fast neutron reactors.



Nuclear Energy Systems Deployable no later than 2030 and offering significant advances in sustainability, safety and reliability, and economics

Ydinvoiman eettiset näkökohdat

- Faustialainen sopimus?
- Moraaliteoriat
  - Seurausetiikka (kustannus – hyöty analyysi)
  - Teleologinen etiikka eli hyve-etiikka
  - Velvollisuusetiikka
  - Sopimusetiikka
- Vastustajien argumentit
  - Onnettomuudet
  - Jätekysymys
  - Terrorismi
- Ydinvoiman käyttö*
  - hyvää tekevä
  - vastuunalainen
  - kestävä

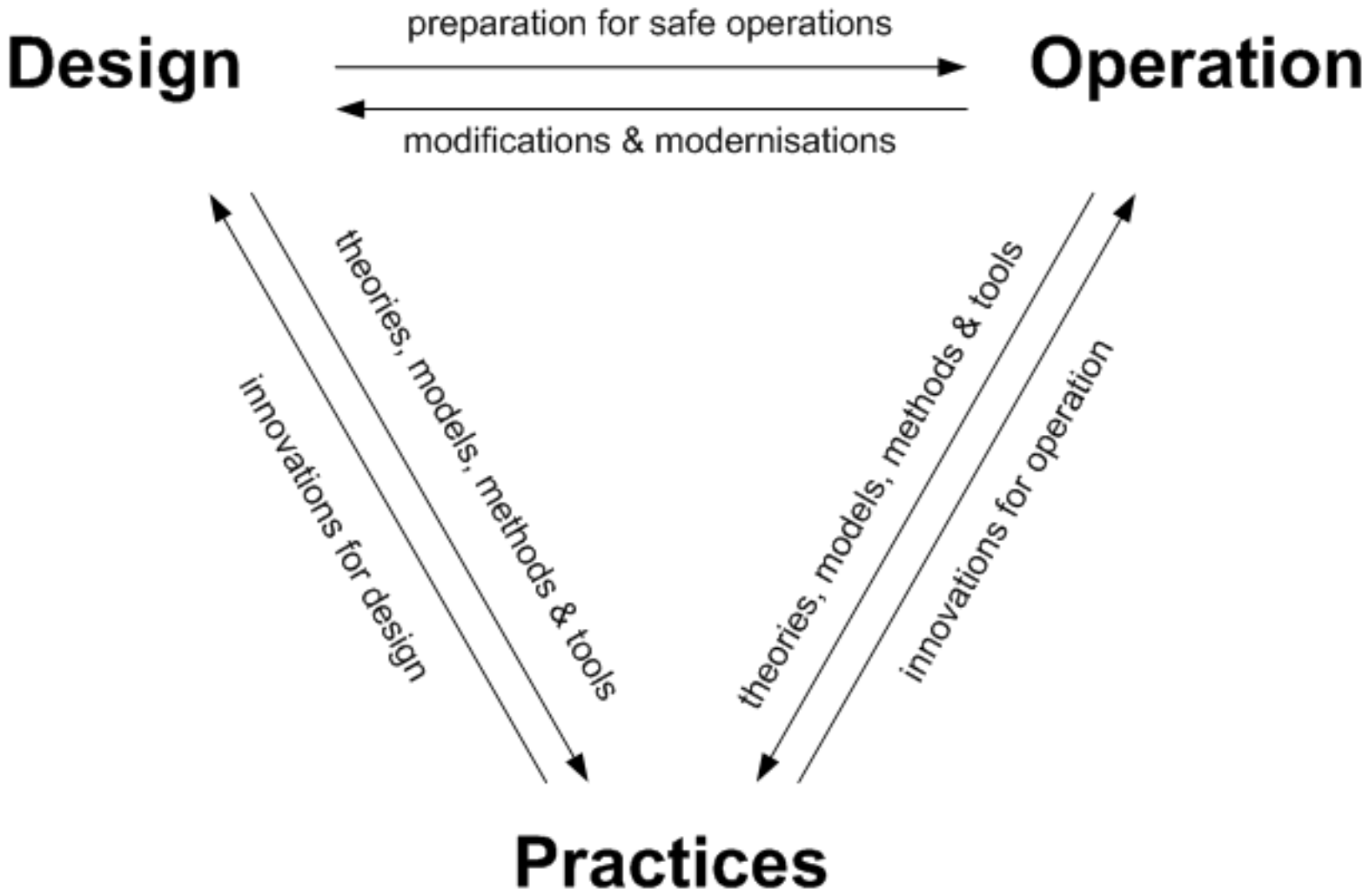
* A. Andrianov , V. Kanke, I. Kuptsov, V. Murogov (2015) . Reexamining the Ethics of Nuclear Technology, Sci Eng Ethics ,21:999–1018

Uudet reaktorikonstruktiot?

Evolutionary – revolutionary

- tuttujen konseptien raameissa OK
- isoja muutoksia teknologiaan johtanevat tarpeeseen uusia suuria osioita vaatimusjärjestelmissä
- konkreettinen suunnitteluprosessi todennäköisesti toisi paljon uutta miettimistä
- torium polttoainekierto on mahdollinen , mutta edellyttäisi paljon uutta tutkittavaa
- ennenkuin Suomeen tuodaan uutta teknologia pitäisi löytyä kunnollinen referenssi jossakin

Teknologiakehityksen elinkaari



YVL-valvonnan lähtökohdat Suomessa*

- Luvituskäytäntö

  periaatepäätös, rakentamislupa, käyttölupa, määräaikainen turvallisuusarviointi

- Vaatimukset

  kvantitatiiviset riskiarviot, suunnittelua ohjaavat tilanteet, turvallisuustekniset käyttöehdot, varautuminen vakaviin onnettomuuksiin, turvallisuusseloste

- Turvallisuusperiaatteiden soveltaminen

  syvyyssuuntainen puolustus, turvallisuusluokittelu, moninkertaisuus-, erottelu- ja erilaisuusperiaatteet, respiittiaika, yksittäisvikakriteeri

*Ydinturvallisuusohjeet (YVL-ohjeet), http://www.stuk.fi/saannosto/stukin-viranomaisohjeet/ydinturvallisuusohjeet

YVL_E7_prosessi

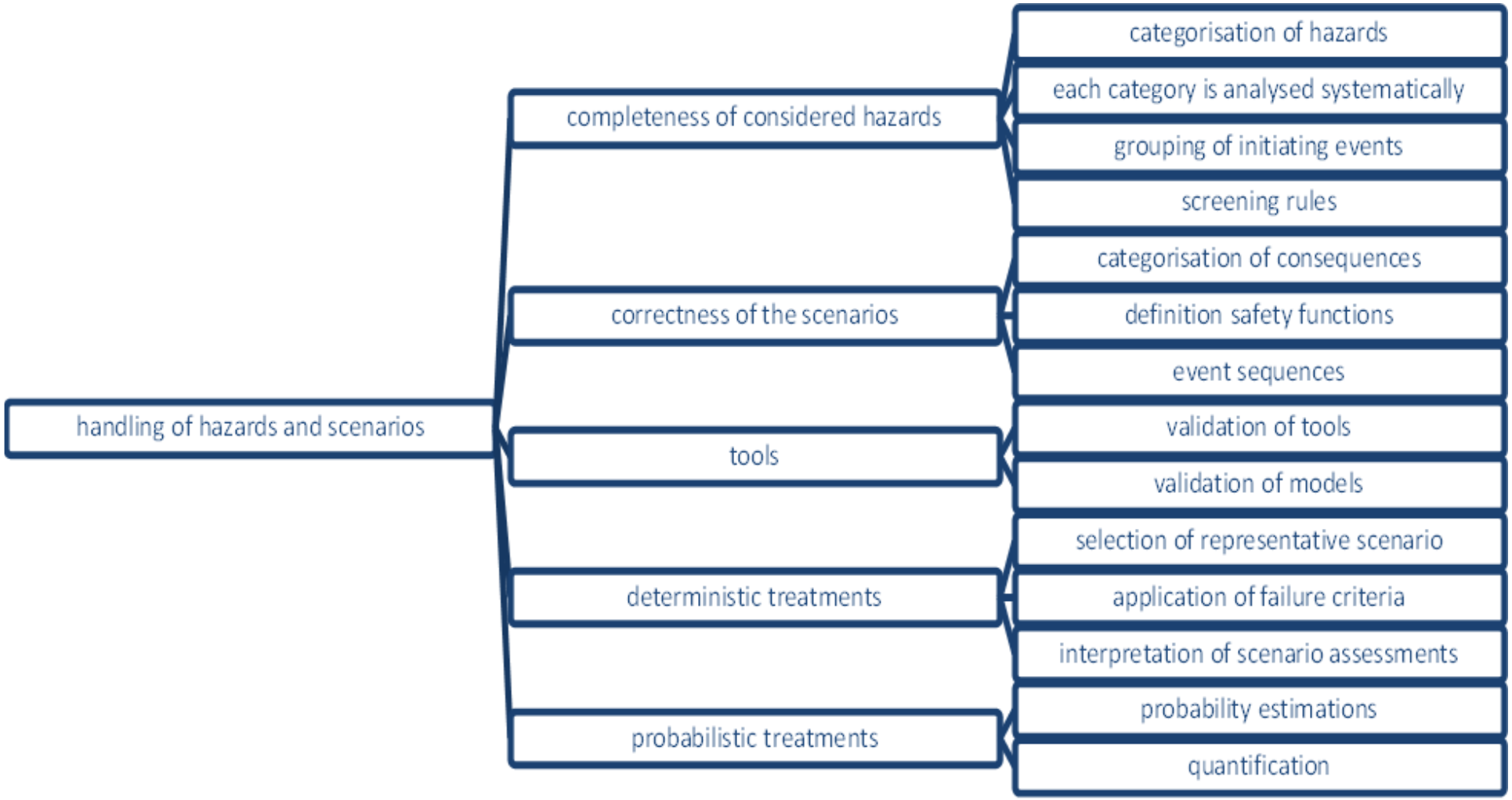
Johtamisjärjestelmän komponentit

- Räätälöity uuden suunnittelua varten tai olemassa olevan käyttöä varten
- Käytettävät tukijärjestelmät
- Suoritteiden jatkuvaa valvontaa
- Organisaatoorinen oppiminen
- Henkilöstön valinta ja kouluttaminen
- Johtaminen käytännössä
- Sidosorganisaatioiden huomioonottaminen

Onnettomuusmalli PRA-analyysiin

- uhat (set of hazards $H=\{h_1, \ldots , h_m\}$)
- alkutapahtuma (postulated initiating event)
- vaikeuttavat tilanteet kuten piilevät viat, turvallisuusautomaation tila, tms. (set of aggravating conditions $A_i= \{a_{i1}, \ldots , a_{in}\}$)
- muodostetaan skenariojoukko (set of scenarios $S=\{s_{ij}=(h_i,a_{ij}) \mid i=1, \ldots , m, j=1, \ldots , n\}$
- arvioidaan ja/tai lasketaan skenarioiden s_{ij} todennäköisyydet $p_{ij} = P(s_{ij})$
- skenario s_{ij} dominoi skenariota s_{ik} jos $p_{ij}>p_{ik}$
- tarkastellaan ei-dominoituja skenarioita

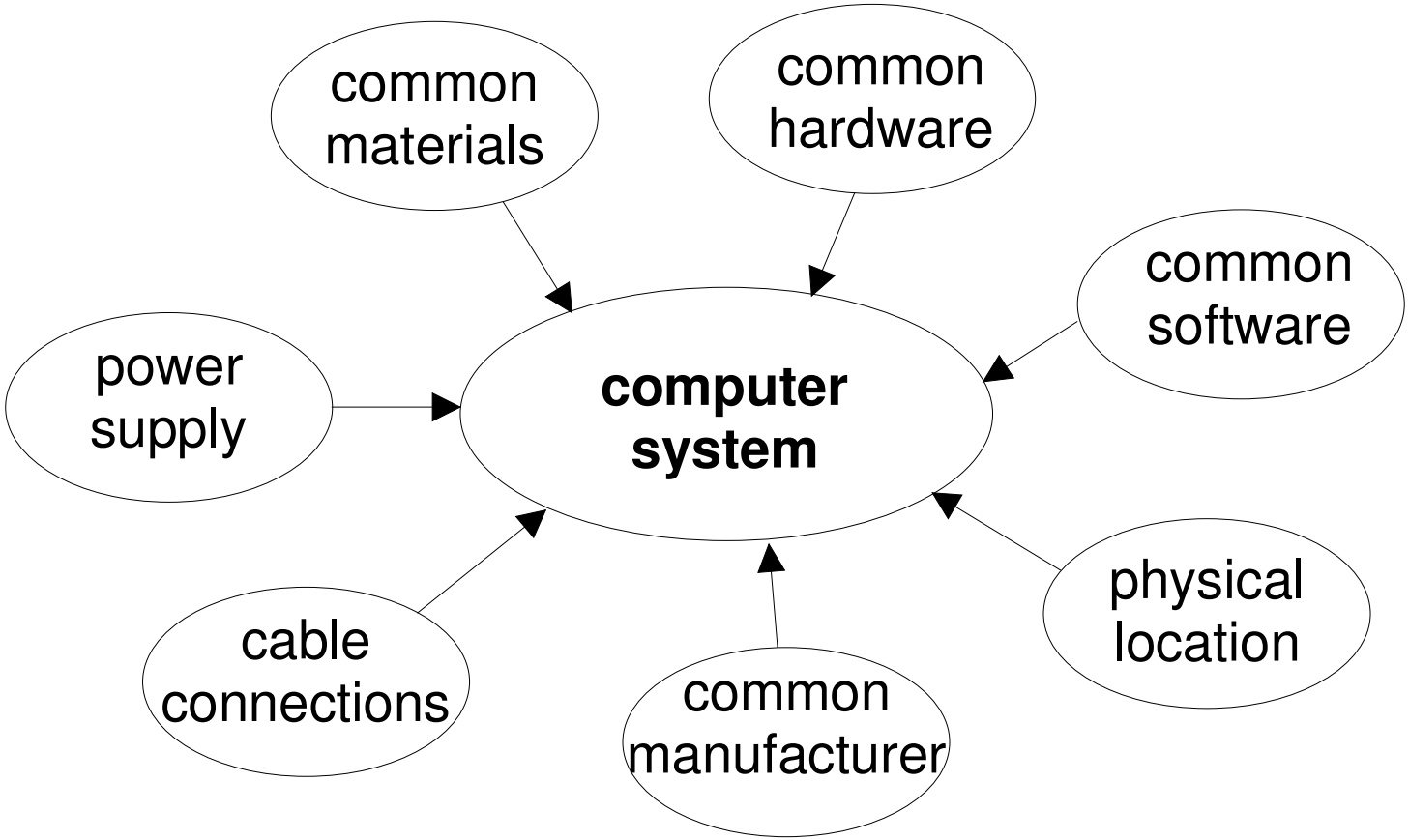
Onnettomuudet turvallisuusselosteessa



Turvallisuusselosteen rakentaminen

- Väitteet (täyttää vaatimusta $v_i \in V=\{v_i \mid i=1, \ldots, N\}$)
- Todisteet
  - rakenteelliset (suunnitteluprosessita kerätyt todisteet)
  - empiiriset (testauksesta kerätyt todisteet)
- Eteneminen
  - periaatepäätös (yhteiskunnan kokonaisetu)
  - rakentamislupa (näin on suunniteltu)
  - käynnistyslupa (näin on rakennettu)
- Todisteiden yhdistäminen uskottavaan loppuväitteeseen (laitosta voidaan käynnistää)

Possibilities for CCFs in systems



Turvallisuusjohtamisen haasteet

- Mikä turvallisuus?
- Mitä riittää?
- Muut tavoitteet?
- Mitä pitää tehdä?
- Pienet todennäköisyydet ja isot kustannukset (konservatiivisuus päätöksissä)?
- Turvallisuus kontra tuottavuus?
- Mitä tiedetään ettei tiedetä?
- Mitä ei tiedetä ettei tiedetä?
- Uskoa että XYZ on turvallinen, mutta kuitenkin jaksaa kyseenalaistaa sitä

Konservatiivinen päätöksenteko

	todellisuus: p	todellisuus: 1-p
päätös	c_{11}	c_{12}
	c_{21}	c_{22}

$$k_1 = pc_{11} + (1-p)c_{12}$$

$$k_2 = pc_{21} + (1-p)c_{22}$$

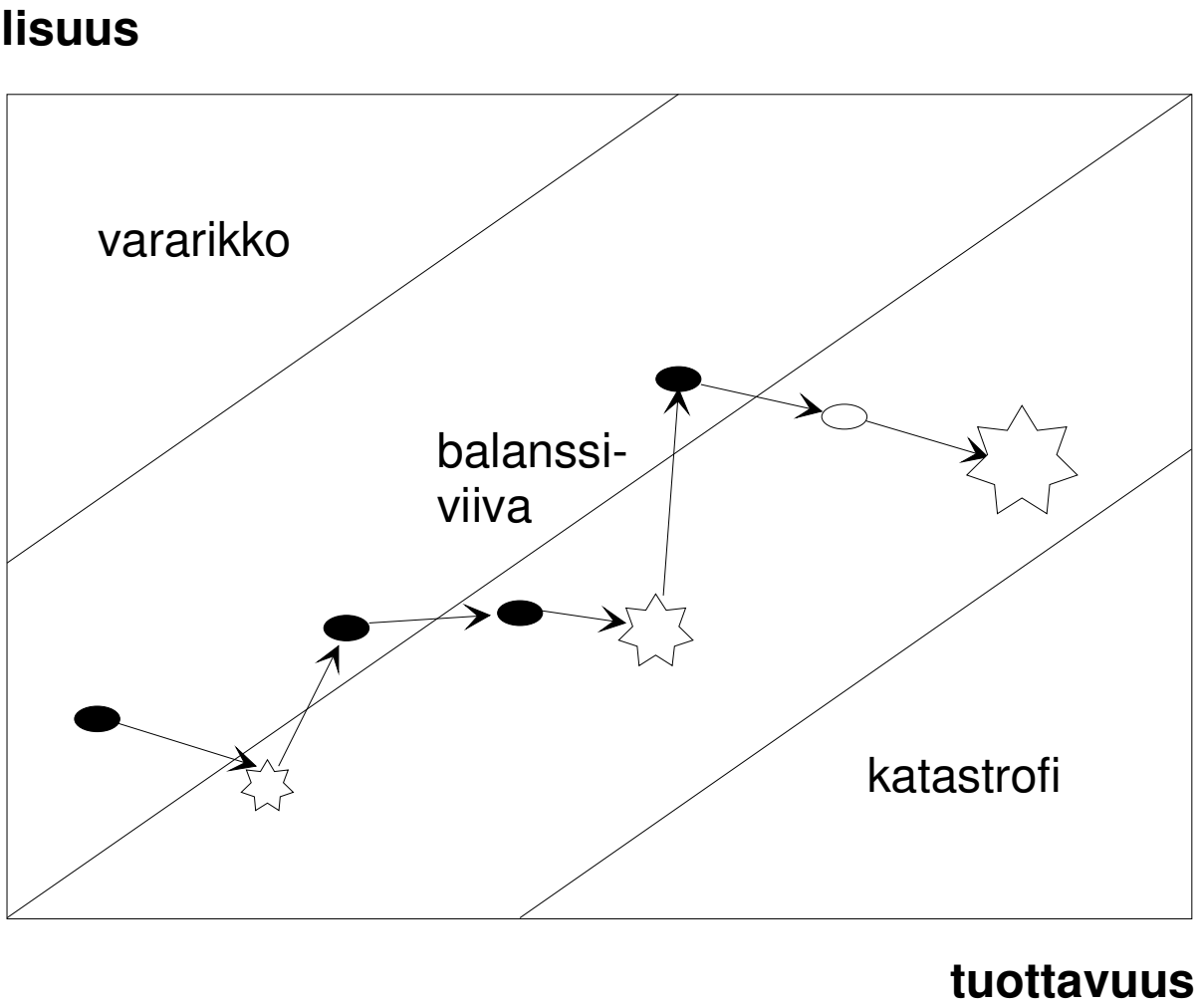
	tarpeellinen pysähdys		turha pysähdys			
pysäyttää	c_11	0	c_12	3	k_1	1,5
jatkaa	c_21	90	c_22	0	k_2	45,0
	p	0,5			p_bal	0,03226

Turvallisuus ja muut tavoitteet

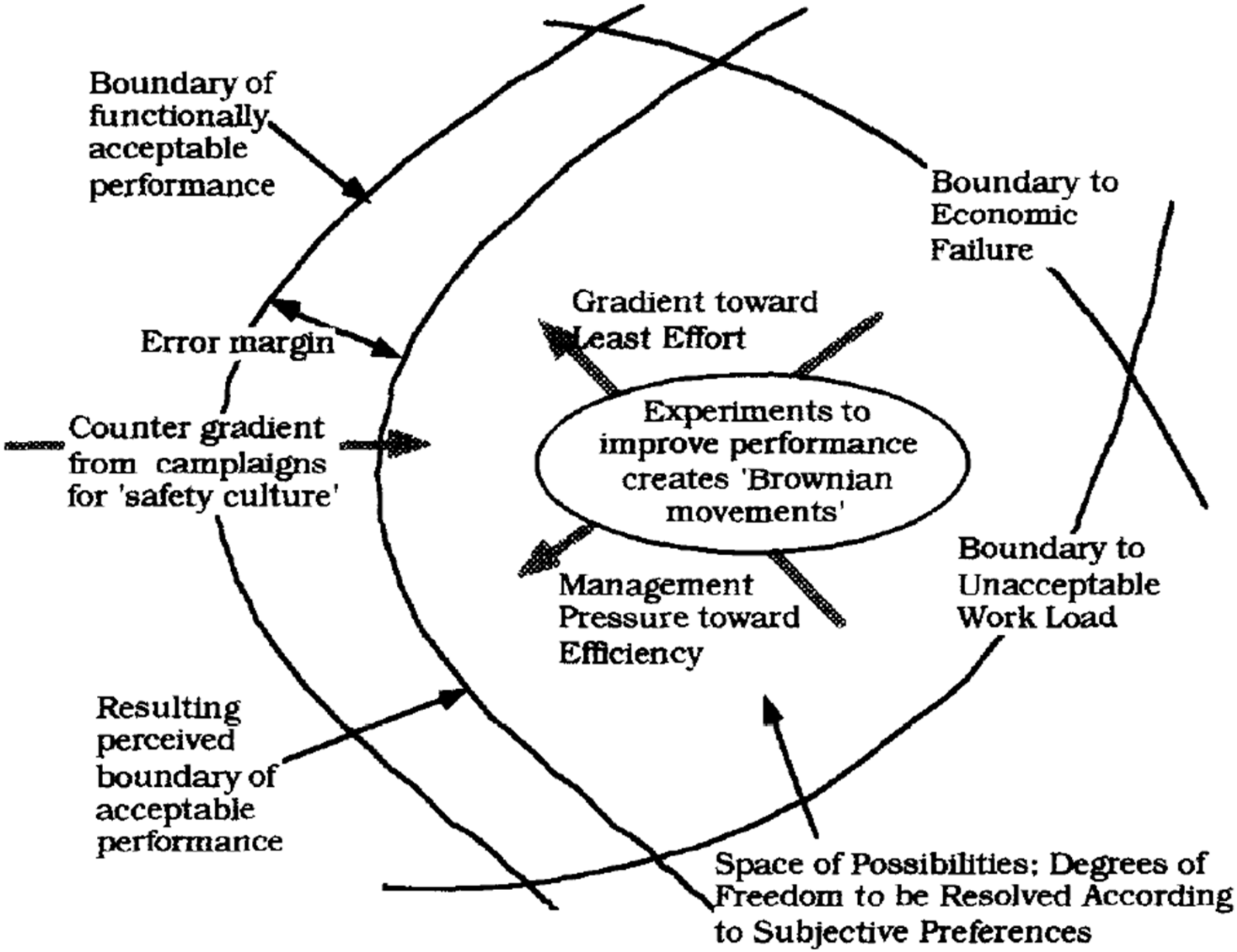
- Turvallisuus on yksi tavoite muiden joukossa
  - eri turvallisuudet

    suuronnettomuudet, päästöt ympäristöön, työturvallisuus, tulevat sukupolvet, aseellinen selkkaus, jne.
  - tuottavuus
  - tehokkuus
  - yhteiskunnan edut
- Monta tavoitetta päätöksenteossa
  - tila-avaruuden kielletyt alueet
  - painotettu summa
  - portfolioanalyysi

Tuottavuuden ja turvallisuuden tasapaino



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



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

Huomioonotettavia balansseja

- kokonaisuus – yksityiskohdat
- traditiot – uusitutuminen
- väliaikainen – kestävä
- prosessi – tuote
- samanlaisuus – moninaisuus
- kilpailu – yhteistyö
- valvonta – luottamus
- huolellisuus – tehokkuus
- suunnitella etukäteen – toimia tilanteen ehdoilla

Katse tulevaisuuteen

- Systeemit kasvavat ja tulevat entistä monimutkaisemmiksi
- SoS systeemien ymmärtämiseksi tarvitaan koko ajan laajenevaa tietotaitoa
- Yhteiskunnan riskien sietokyky pienenee
- Ilmastomuutos tuonee mukanaan uusia uhkia, kuten väestöryhmien ja maiden väliset jännitteet
- Riskihallinnan työkalut (mallit, tietokannat) paranevat

Uudet riskit ja niiden hallitseminen

- Sources of risk

  Natural sources; Human sources; Causal interactions between different sources

- Drivers of risk

  Knowledge of emerging risks; System complexity; Social and cultural dynamics; Degree of development, poverty and inequality; Natural resources and the environment; Competing interests, ideologies, values and religions; Variability in susceptibility to risk

- Governance issues

  Tackling complexity; Dealing with tractable and deep uncertainty; Governance of change and adapting institutions; Organisation and authority; Better agenda-setting; Resolving conflicts

IRGC (2010): Emerging risks Sources, drivers and governance issues, http://www.irgc.org/IMG/pdf/IRGC_Revised_Emerging_Risks_Concept_Note_March2010.pdf

Security (gates, guards, guns, geeks)

- Pääsy laitokseen
- Materiaalien ja esineiden vieminen laitokselle
- Vaarallisten aineiden käsittely laitoksella
- Erilaisten aseiden lisäystä (ydinvoima, kemia, biologia, tietojärjestelmien uhat)
- Cyber security
  - informaation varastaminen (piirrustuksia, systeemikuvauksia, turvallisuusseloste)
  - häirintä (henkilötietokannat, valvontajärjestelmät, automaatiojärjestelmät)
  - kiristystä (uhkavaatimuksia)
  - sabotaasit (turvallisuusjärjestelmät)

Cyber security

- Oma alueensa, vaikkakin samantapaisia menettelytapoja voidaan käyttää
- Muutama esimerkki
  - Stuxnet (kohteena Iranin sentrifuugilaitos)
  - Industroyer (kohteena Ukrainan sähköverkko)
  - WannaCry (kiristyssovellus, perustuu koodiin, joka oli varastettu US National Security Agencylta)
- Suojausten kehittämisessä pitää olettaa että hyökkääjät toimivat rationaalisesti
  - mitkä ovat hyökkääjäkategoriat ja niiden tavoitteet?

Human factors in security

- Neccessity to improve security culture
- Gender matters
- Age builds culture
- Industries Differ
- Security Awareness Training is not effective
- Seven dimensions of security culture
    - quality of communication
    - compliance
    - knowledge
    - secure behaviour
    - positive attitudes
    - norms
    - responsibilities

CLTRe North America, Inc. (2017): Indepth insights into the human factor; the 2017 Security Culture Report https://get.clt.re/report/

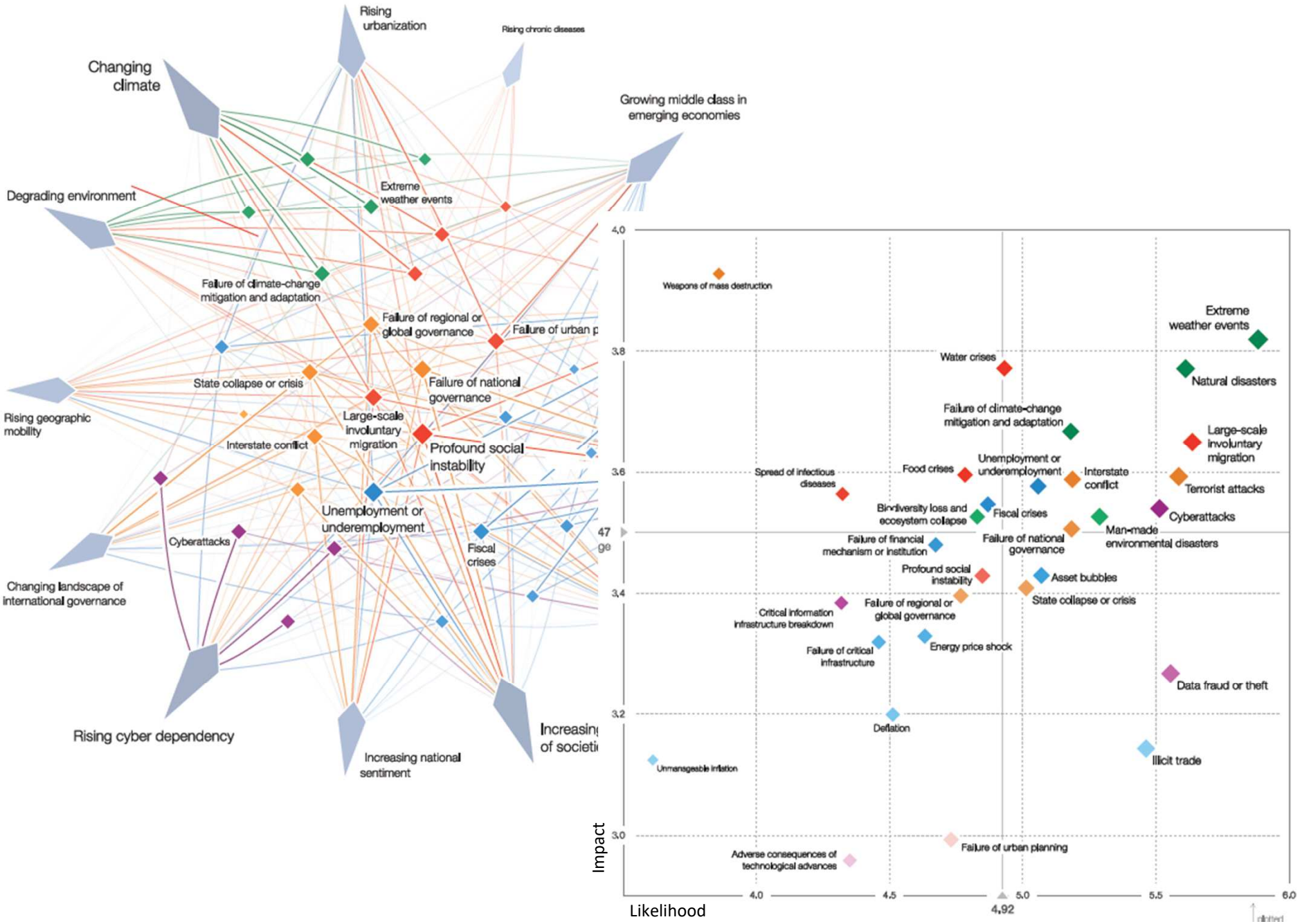
Terrorismin uhat

- Hyökkääjän tavoitteet?
- Ennen, aikana ja jälkeen
  - lainsäädännön puitteet, kansainvälinen yhteistyö, pelotus, suojausten rakentaminen, signaalien monitorointi, koulutus
  - hyökkäyksen tunnistaminen, hälyttäminen, vastatoimenpiteet, tilanteen seuranta, vaikutusten lieventäminen
  - tilanteen normalisointi, tapahtuman analysointi, syyllisten etsiminen, syysteemien muutokset

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

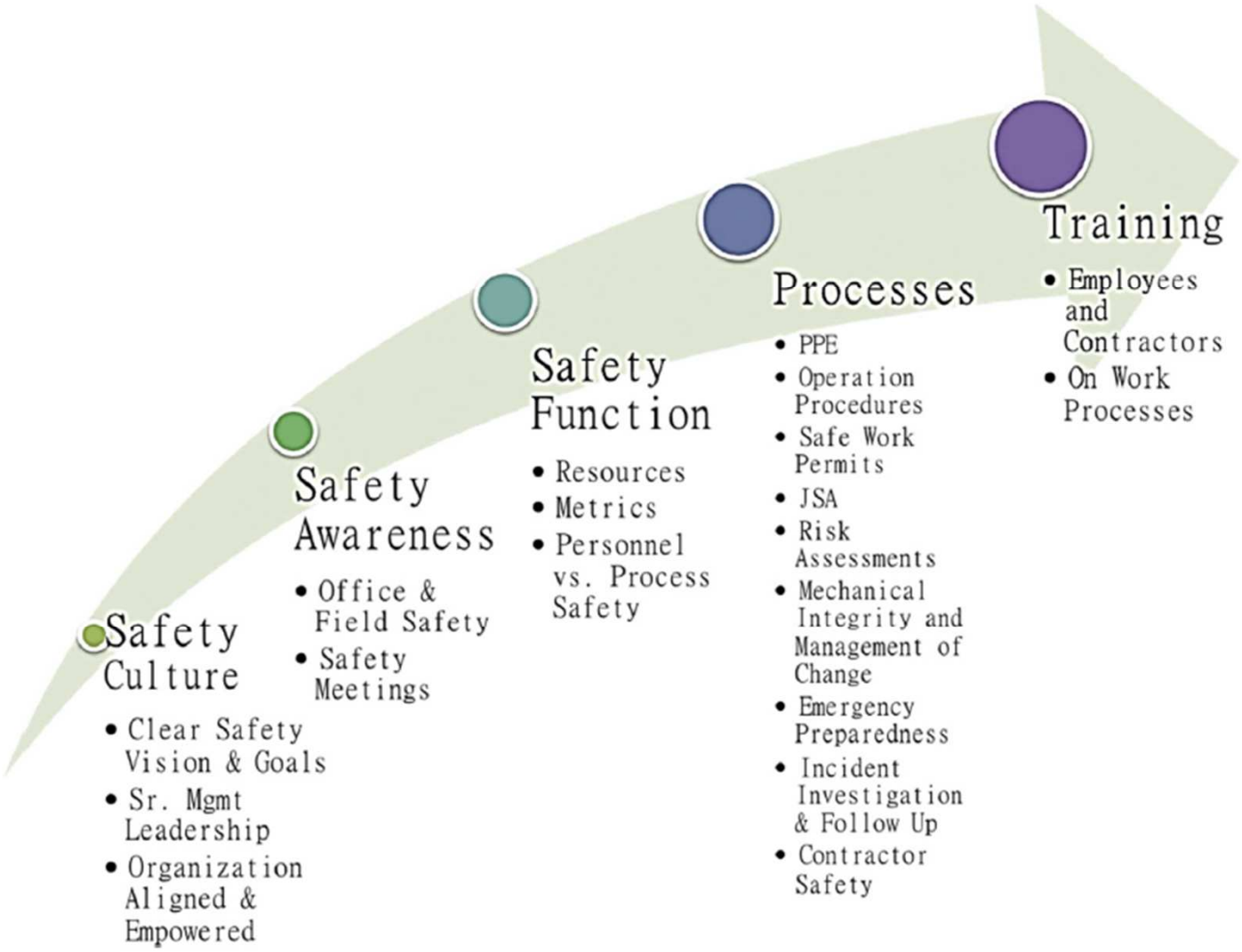
1. Introduction
2. Nuclear and radiological threats
3. Human and agricultural health systems
4. Toxic chemicals and explosive materials
5. Information technology
6. Energy systems
7. Transportation systems
8. Cities and fixed infrastructure
9. The response of people to terrorism
10. Complex and interdependent systems
11. The significance of crosscutting challenges and technologies
12. Equipping the federal government to counter terrorism
13. Essential partners in a national strategy: states and cities, industry, and universities

The National Academies Press (2002): Committee on Science and Technology for Countering Terrorism, National Research Council, http://nap.edu/10415



World Economic Forum (2017). The Global Risks Report 2017, 12th Edition, http://www3.weforum.org/docs/GRR17_Report_web.pdf

What does ‘safe’ look and feel like?



Ray A. Mentzer, Jiaqi Zhang, Wei Xu, M. Sam Mannan (2014). What does ‘safe’ look and feel like? Journal of Loss Prevention in the Process Industries 32 265-275.

Harjoitustehtävä 3

Aihe valinnan mukaan (kuvaus, analyysi, tulokset, suositukset, johtopäätökset)

- valitun systeemin riskianalyysi
- erään onnettomuuden tapahtuma-analyysi
- turvallisuusselosteen yksi osakokonaisuus
- artikelin, raportin tai keskustelun referointi

Aikataulu

- alustavan esseen kirjoittaminen 30.9 mennessä
- toisen kirjoittaman analyysin kommentointi noin kahden viikon sisällä
- lopullisen analyysin kirjoittaminen 31.10 mennessä

Kysymyksiä?