Turvallisuusjohtaminen – systeemitekninen sovellus

14.5.2013

Björn Wahlström

bjorn@bewas.fi

Tsernobyl, 1986

onnettomuuden syitä

- reaktorin konstruktio
- henkilökunnan osaaminen
- organisaation puutteita

seuraukset

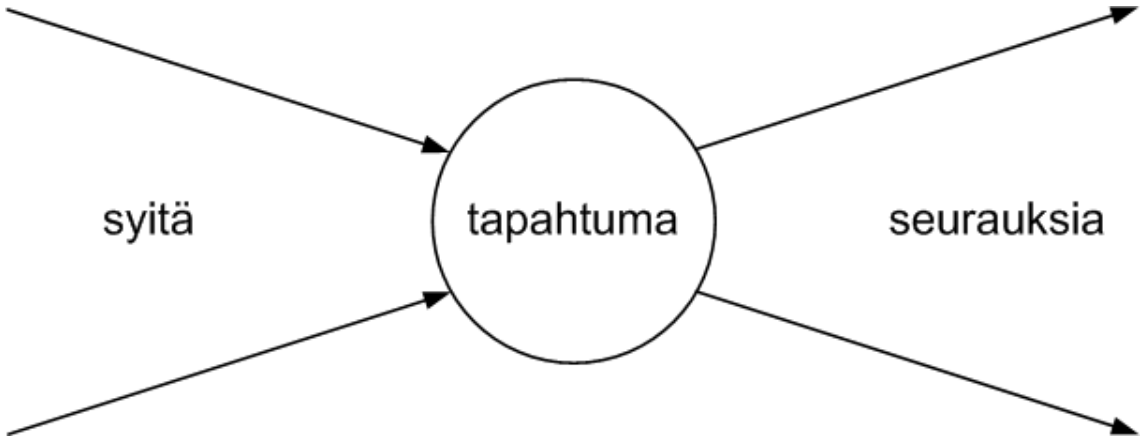
- 28 kuollutta 30 päivä sisällä
- >1800 kilpirauhasen syöpää
- suuria maa-alueita käyttö-kelvottomia pitkiä aikoja


Сибирь


COSTA CONCORDIA
© Reuters

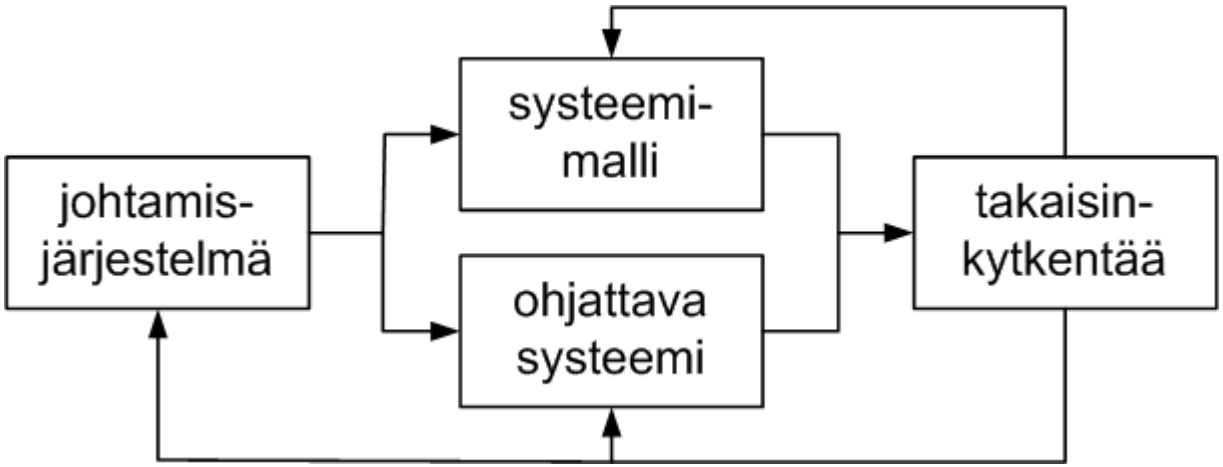
Miksi onnettomuuksia tapahtuu?

- Teknisen järjestelmän puutteita
  - huono konstruktio
  - puutteita kunnossapidossa
- Inhimmillisiä virheitä
- Organisatoorisia puutteita
- Tahallista tuhoamista (sabotaasi, terrorismi)



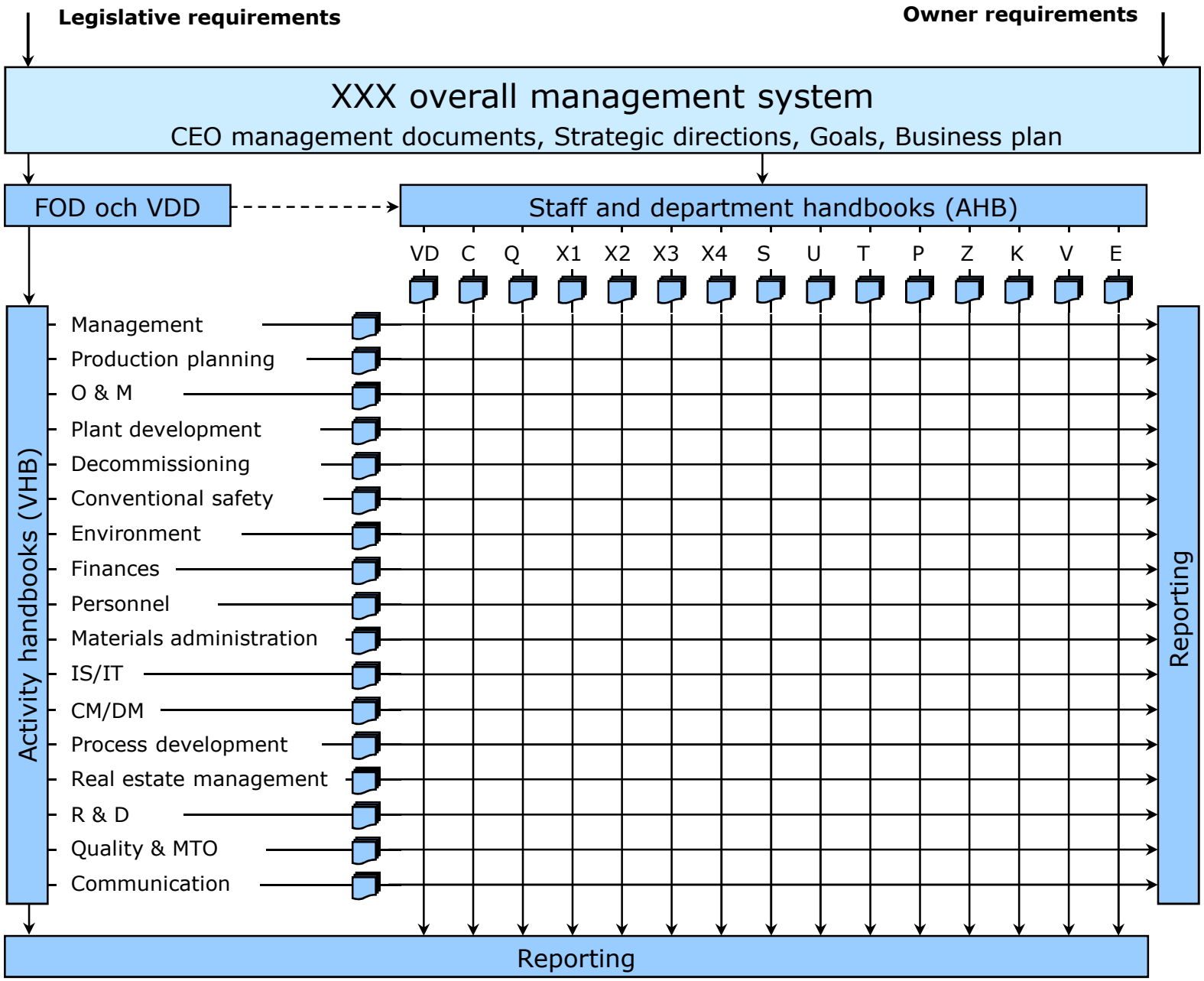
Turvallisuusjohtaminen

- Riskianalysi / turvallisuustekniikka (tunnistaa, poistaa, estää, lieventää)
- Käyttökokemusten hyödyntäminen
- Muutosten hallintaa

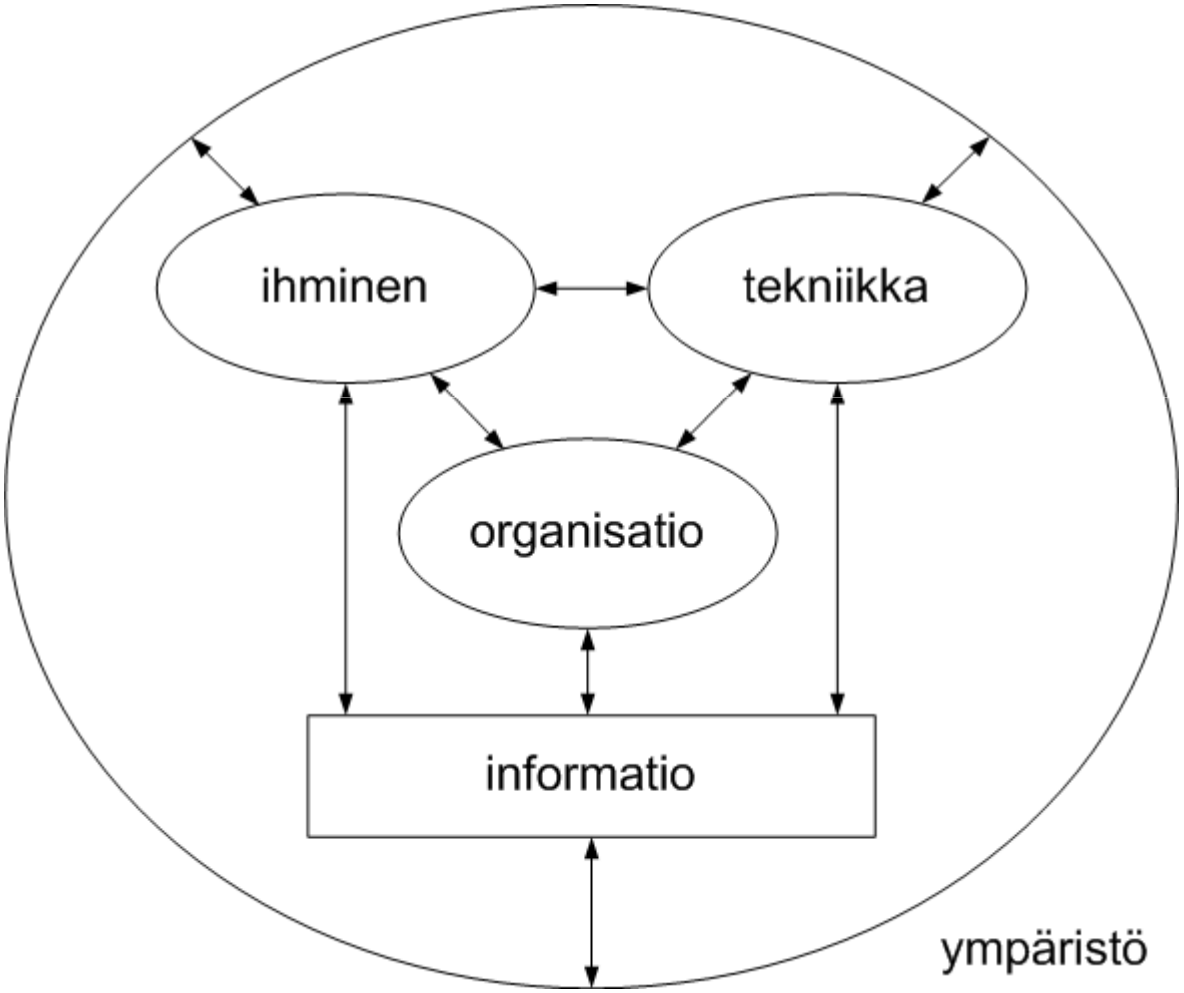


Johtamisjärjestelmä

- Missio, arvot, visio
- Organisaation rakenne
- Vastuut, toimivaltuudet, roolit
- Vaatimukset
- Kuvauksia millä tavalla vaatimukset voidaan täyttää (prosessit, aktiviteetit, tehtävät, menetelmät, työkalut)
- Käyttöohjeet
- Tarkastuksia ja auditointeja
- Itsearviointeja
- Järjestelmän päivittäminen ja ylläpito


Legislative requirements
Owner requirements
XXX overall management system
CEO management documents, Strategic directions, Goals, Business plan
FOD och VDD
Staff and department handbooks (AHB)
VD
C
Q
X1
X2
X3
X4
S
U
T
P
Z
K
V
E
Activity handbooks (VHB)
Management
Production planning
O & M
Plant development
Decommissioning
Conventional safety
Environment
Finances
Personnel
Materials administration
IS/IT
CM/DM
Process development
Real estate management
R & D
Quality & MTO
Communication
Reporting
Reporting

Systeemimalli

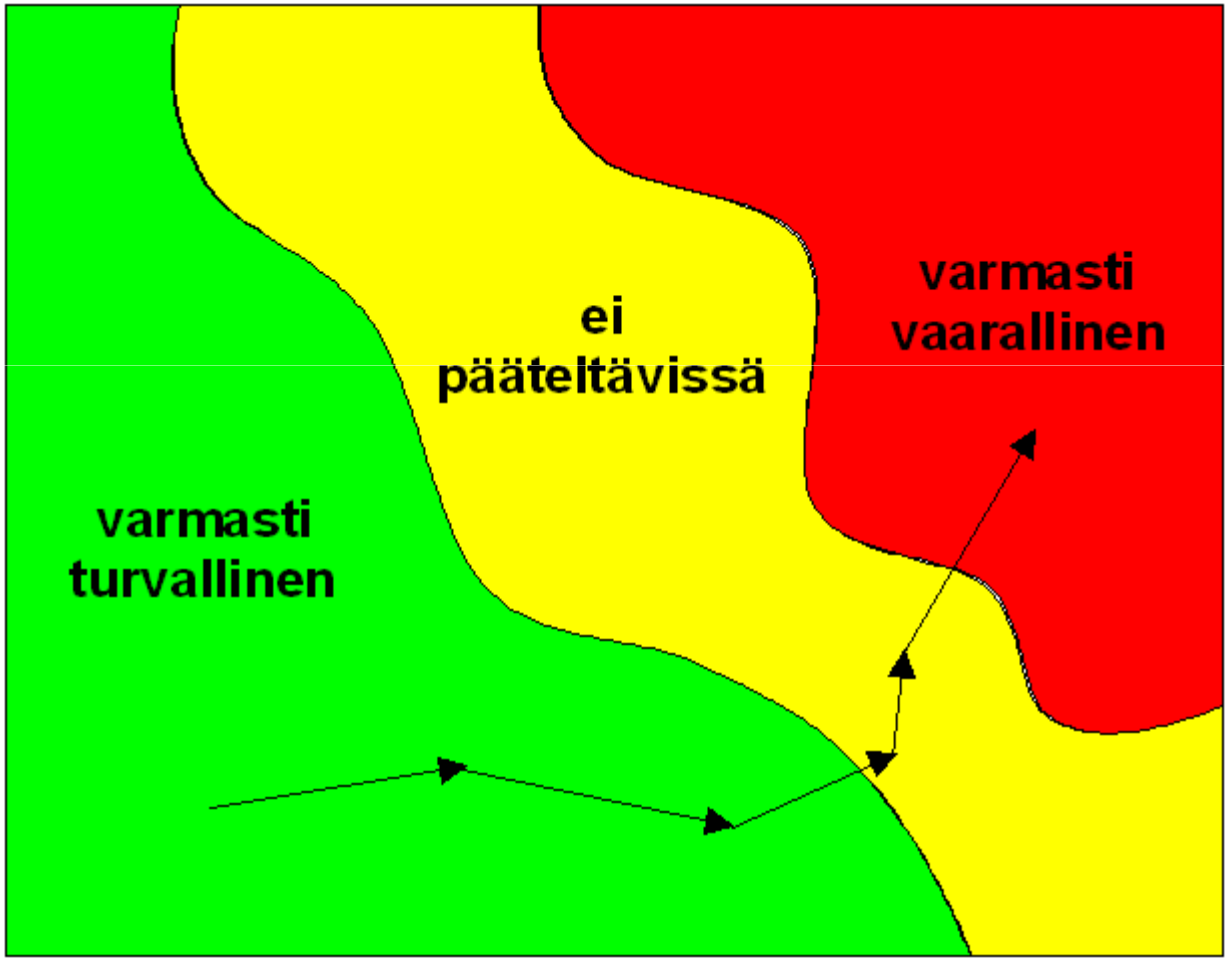


Systeemitekniikan kolme ongelmaa

Ohjausongelman neljä välttämätöntä ehtoa

- on olemassa päämäärä
- on olemassa malli
- systeemi on tarkkailtavissa
- systeemi on ohjattavissa

Systeemin tila

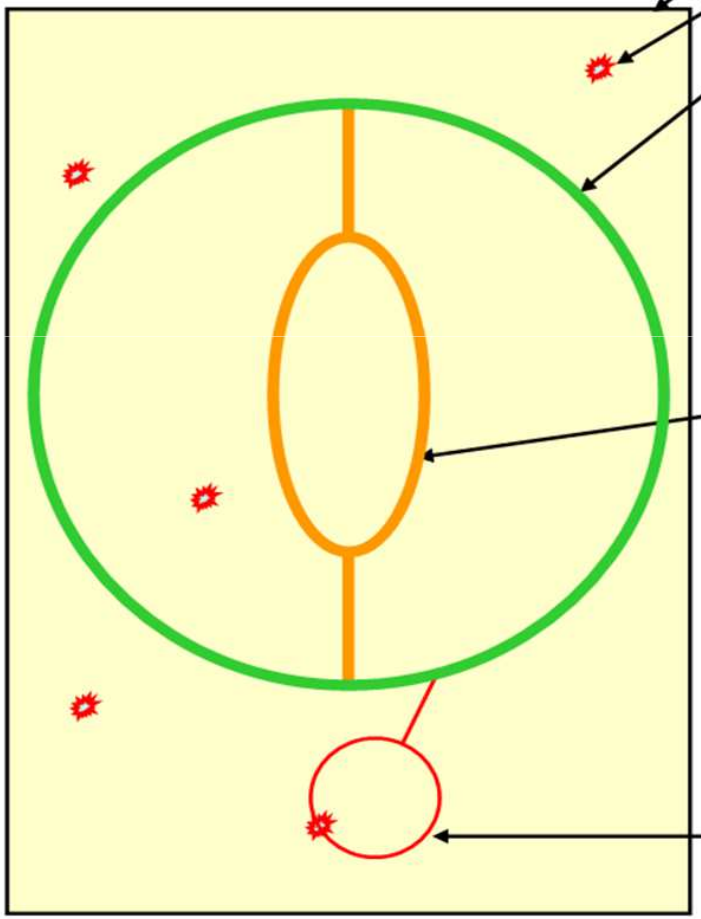


Onnettomuuden kaksi syytä

- Systeemi **on** vaarallisessa tilassa
  - vaarallinen tila on piilevä ja edellyttää laukaisevaa tapahtumaa
  - kerättävät mittaukset eivät pysty ilmaisemaan vaarallista tilaa
- Sopimaton ohjaus jossakin tilassa **vie** järjestelmää vaaralliseen tilaan
  - satunnainen tapahtuma (tekninen vikaantuminen)
  - virheellinen ohjaus (inhimmillinen virhe)
    - ohjausjärjestelmän suunnitteluvirhe
    - virheelliset ohjeet
    - puutteita osaamisessa

Example of Defensive Measures: the Minefield Metaphor - 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

Miten onnettomuuksia voidaan välttää?

- Ennustaa satunnaisia tapahtumia
  - riskianalysin kattavuus ja syvyys
- Välttää piileviä puutteita
  - tarkastuksia suunnitteluprojekteissa (V&V)
- Parantaa järjestelmän tilan valvontaa
  - vaarallisten tilanteiden indikaattorit
- Suunnittelussa huomioda odotetut vaihtelut
  - luoda järjestelmään luontaista toipumista

Osajärjestelmien tilakomponentit

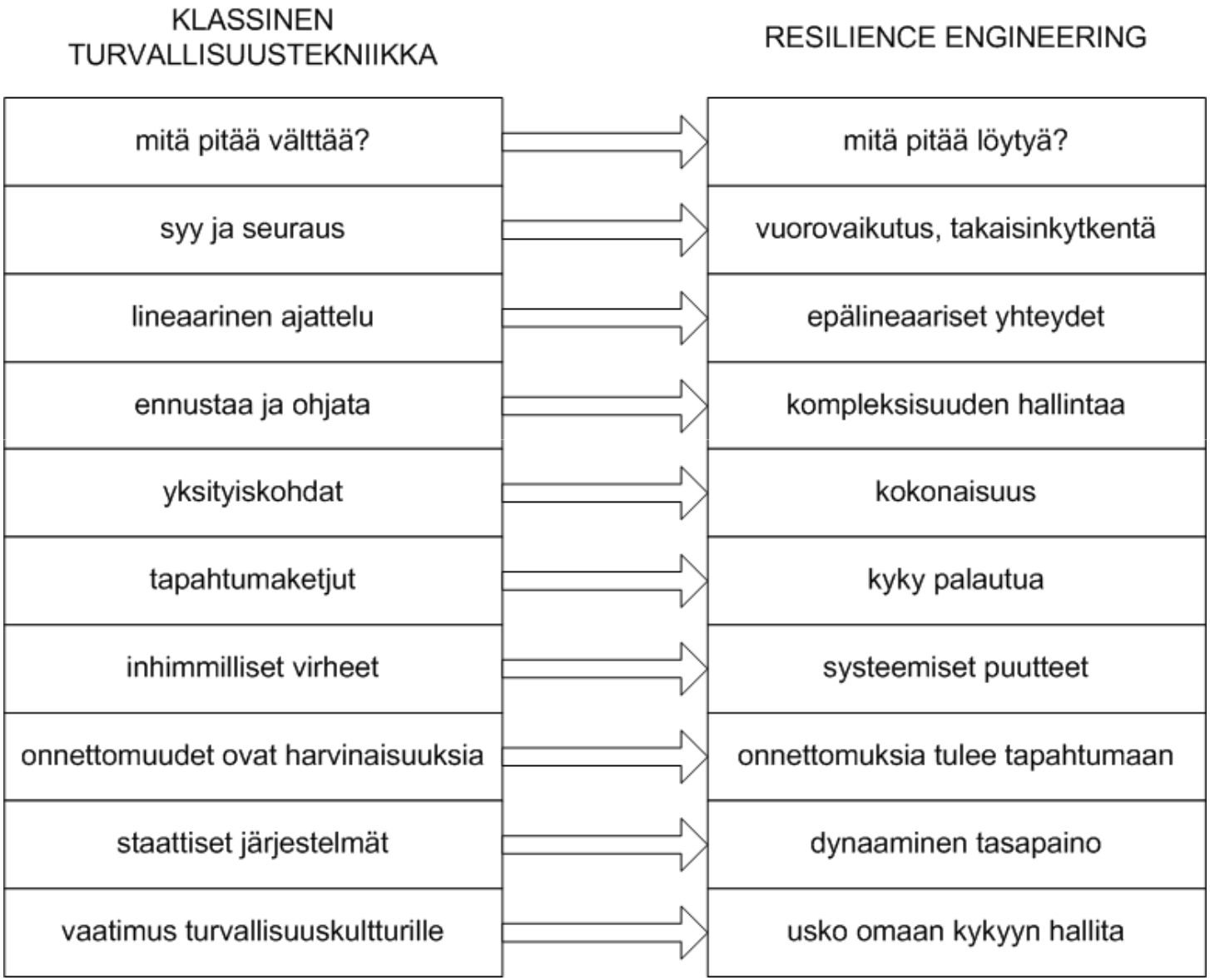
- Tekniikka
  - asema, nopeus, paine, lämpötila, pinnankorkeus, varaus, jne.
- Ihminen
  - terveydentila, peronaalisuuspiirteet, osaamista, taitoja, arvoja, arvostuksia, motivatio, jne.
- Organisatio
  - kultuuri, ilmasto, tietämys, johtamisjärjestelmä, käytännöt, jne.
- Informatio
  - tietokannat, etsintäalgoritmit, dokumentit, jne.

Mitä tiedetään ettei tiedetä

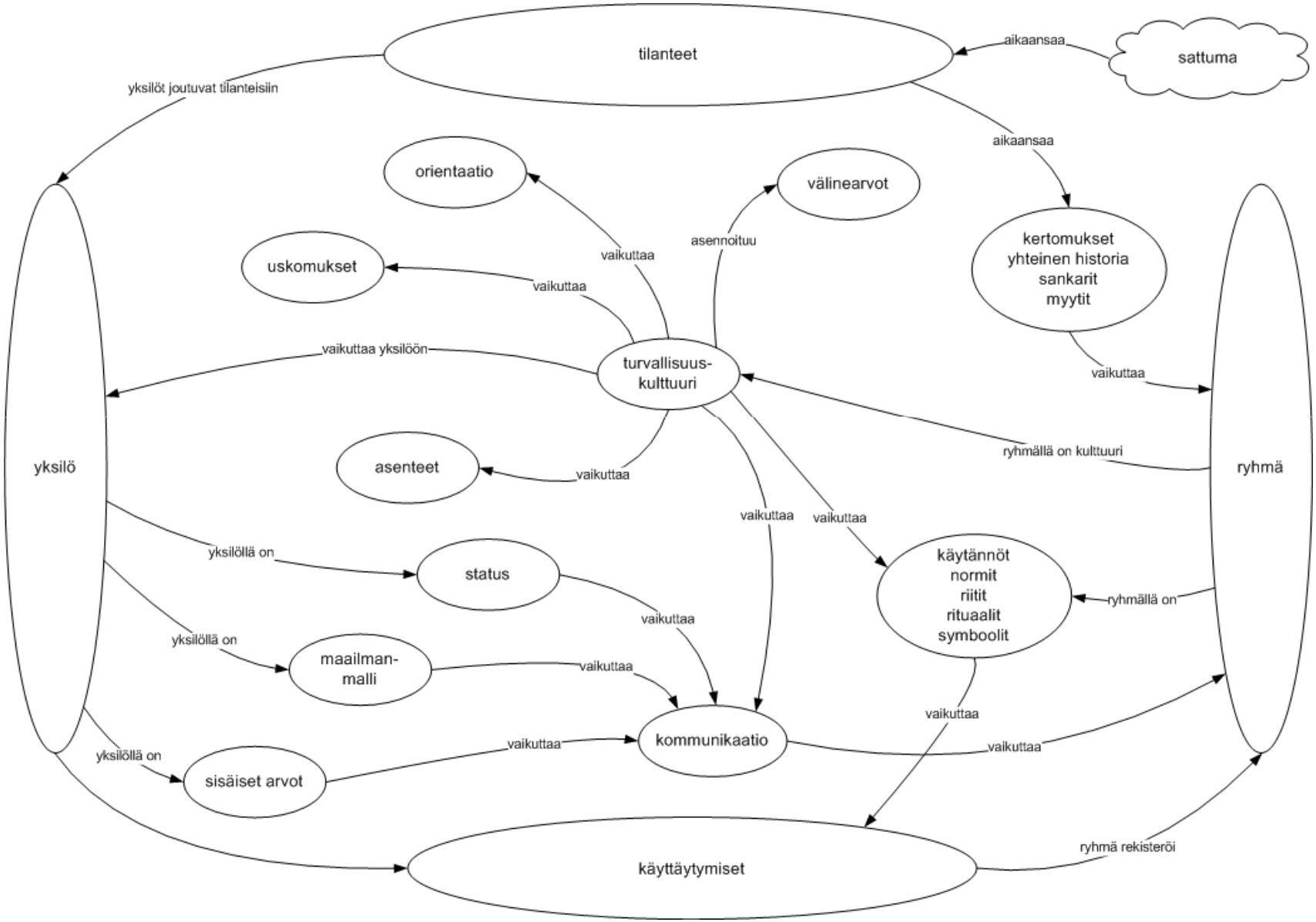
- Pienen maailman rajoitukset (malli)
- Ohjeisto ei koskaan voi olla täydellinen (Gödel)
- Perustavaa laatua oleva mahdottomuus ennustaa (Turing)
- Myös deterministiset järjestelmät voivat olla yllätyksellisiä (kaoottiset systeemit)
- Miten todennäköisyysjakaumat voidaan mallintaa?

Mitä ei tiedetä ettei tiedetä?

Paradigman muutos



Turvallisuuskultturi?



Voiko turvallisuuskultturia ohjata?

- Mitä käsitteellä tarkoitetaan?

  asenteet, käyttäytymiset, sankarit, normit, rituaalit, symboolit

- Kenen turvallisuuskultturi? Onko organisaatiolla yksi turvallisuuskulttuuri?

  johtamiskultuuri, käyttökulttuuri, kunnossapitokulttuuri, tekniikkakulttuuri?

- Voidaanko kultturia ohjata?
  - malli?
  - tavoitefunktio?
  - tarkkailtavuus ja ohjattavuus?

Johtopäätökset

- Ohjausmetafoora on hyödyllinen oivalluksen väline
- Systeemit ihminen ja organisaatio on mallinnettavissa yksinomaan kvalitatiivisesti
- Meillä tulee aina olemaan puutteita ympäristömme ymmärtämisessä
- Mallien antimien ennustuksiin uskotaan usein liikaa
- Turvallisuutta voidaa usein rakentaa järjestelmiin tukemalla niiden toipumiseen häiriöistä