Business from technology

Inhimilliset tekijät haasteena automaatiosuunnittelulle

Leena Norros

ATS:n syysseminaari 21.11.2014
Helsinki

Monimutkaisen turvallisuuskriittisen työn keskeinen jännite

- Ydinvoimalaitoksen turvallisuussuunnittelu perustuu syvyyssuuntaiseen puolustusperiaatteeseen
- Valvomossa esim. automaattiset turvajärjestelmät, hätätilanne- ja muut ohjeet, turvallisuutta korostavat käytännöt, turvallisuuskulttuuri
- Tavoitteena on hallita järjestelmän vaihtelua ja vähentää epävarmuuksia

MUTTA

- Onko turvallisuuden lisääminen kasvattamalla systeemin stabiiliutta (proseduralisoimalla) menossa jo liian pitkälle: Lisäpanokset ovat joko tehottomia tai jopa haitallista turvallisuuden kannalta (Bieder & Bourrier 2013, Amalberti 2006, Rosness 2013)

=> Tarvitaan sekä stabiiliutta että joustavuutta, ja on osattava täyttää nämä vastakkaisilta näyttävät vaatimukset yhtä aikaa (Grote 2013)

- Prosessin, automaation, organisaation ja ohjeiston suunnittelussa (Papin 2003)
- Prosessin ohjaajien työssä; heidän on ratkaistava dilemma tilanteessa

Esitelmän juoni

- Tutkimusesimerkki hätätilanneohjeiden käytöstä
  - Hätätilanneohjeet ja niiden käyttö on osa automaatiota
  - Kokemuksemme mukaan ohjeiden käyttö korostuu (digitaalisen) automaation kehittyessä
- Kaksi tärkeää tehtävää joista inhimillisten tekijöiden tutkimuksen tulisi huolehtia automaatiosuunnittelussa
- Menetelmästä, jonka avulla voidaan arvioida ja kehittää automaatio- ja valvomoratkaisuja

The research problem

- Can balancing between stability and flexibility be considered as an inherent feature of appropriate behaviour in procedure usage

Collected data: Observing behaviour

Study 1: Orientation to procedures

- Operators
  - NPP 1 : 12 crews, N=44
  - NPP 2 : 6 crews (half of the operating crews) N=18
- Procedure designers
  - Power company R&D: 5 designers

- Interview questions posed to all subjects:
  - What is the role of procedures in process control?
  - Do such situations exist to which no dedicated procedures exist?
  - Do the procedures determine the course of actions totally in some situations?
  - Are alarms the primary starting point for action?
  - How would you characterise a good operator?

Study 2: Habits of action

- Operators
  - NPP1: 12 crews, N= 44)
- Simulated Loss of Coolant Accident with additional failure in plant protection signal
- Flow-chart type emergency operating procedures in use

- Data collection in simulator runs:
  - Orientation interview
  - Simulated scenario, observation
  - Expert evaluation of performance
  - Process tracing group interview
  - Nasa TLX
  - Usability questionnaire

Episodes in a simulated loss of coolant accident

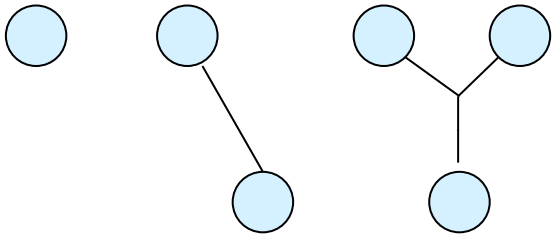
- Three procedure relevant episodes were identified in the scenario
  - Initial detection of emergency situation and scram
  - Taking accident identification procedure (A0) into use
  - Taking accident management procedure (A1) into use
- All 12 crews used the procedures as required; nevertheless variation within procedure following was identified in:
  - Information usage
  - Identification of situation
  - Dealing with automation
  - Decision making
  - Communication
  - Leadership
- We asked what do these differences mean?
- Do they reveal patterns of behaviour of the crews?

Episode 1: Habits of information usage

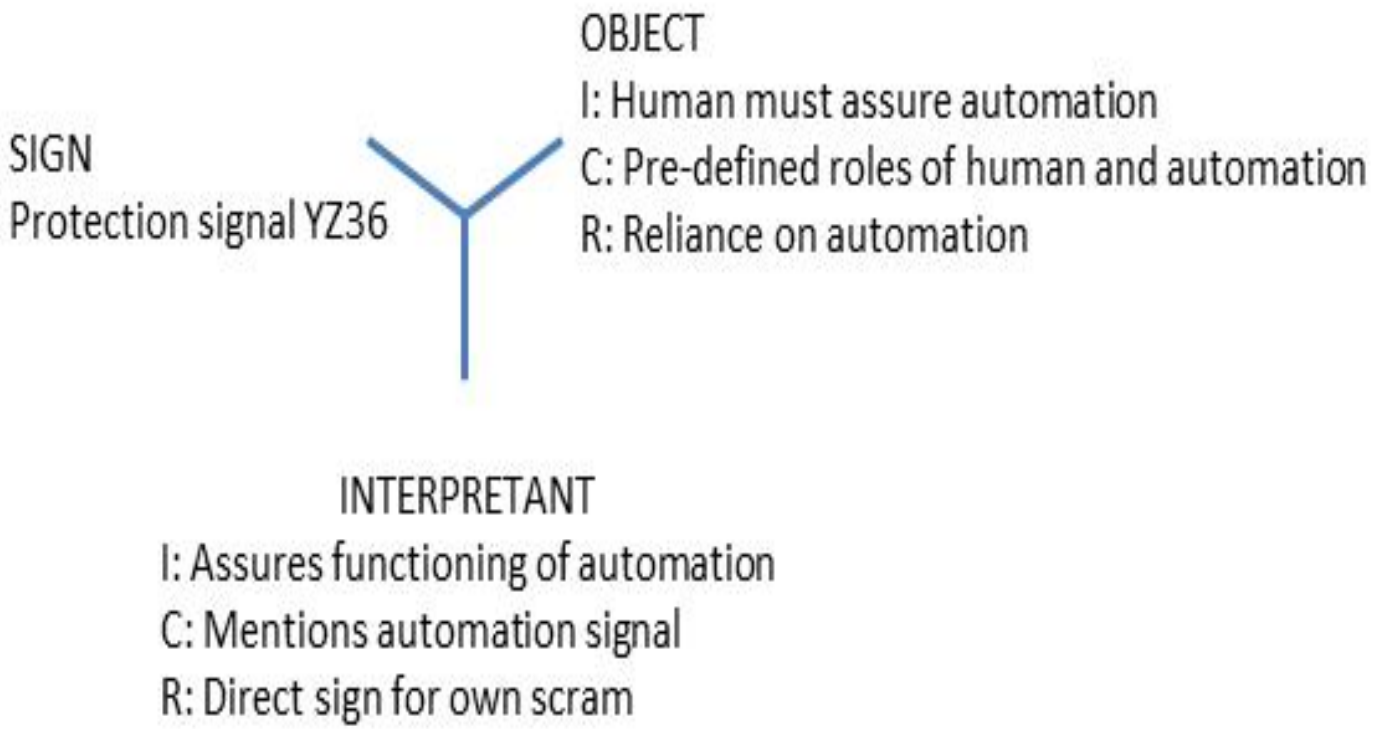
SIGN
I: Redundant & diverse information
C: Redundant information
R: Singular information

OBJECT
I: Validate phenomena by assuring information
C: Double-checking as a rule
R: Single signs are reliable

INTERPRETANT
Conducting the scram



Episode 1: Habits of dealing with automation



Crew I in episode 1	Crew B in episode 1	Crew A in episode 1
First, all three operators are looking at the process monitoring system **SS: "The doors of the ice condenser" [reads aloud the alarm text] "Do we have a small leak in the primary circuit, maybe a big one?"** **SS looks at trends on process monitoring system and plant protection signals. RO looks at display support system which displays a command to take I0 into use.** **RO looks at plant protection signals** **RO:"YZ 36 [name of the protection signal], I0"** **TO:"The pressurizer level crashed"** **SS:"Primary circuit pressure is 120 bars"** **TO turns to face SS, who listens actively.** **TO:"Now there is a big leak going on"** **SS [in reply to TO]:"Ice condenser doors are open there. Shall we scram the reactor? Yes, do it."** **RO:"Yes"**	First, all three operators are looking at the process monitoring system TO:"Ice condenser doors [reading from the alarm list]." RO:"The pressuriser level and circuit pressure are dropping" RO looks to the plant protection signals. SS:"Yes, we have some kind of a leak." TO:"Seems like a leak in a primary circuit" SS:"Conduct the scrams"	All operators are sitting at their respective desks SS:" Now came moisture alarm [reading from the alarm list]." TO:" Ice condenser doors [reading from the alarm list]. R looks at display support system displaying command to take I0 into use. R is silent. TO:" YZ36 [name of the protection signal]. SS:"Drop in pressurizer level". SS looks to the protection signal panel SS:"YZ36" TO:"Scram?" SS:"Yes".
Analysis: crew utilises different kinds and types of information and both RO and SS check the plant protection signal status. Information usage is also dialogical ➔ interpretative habit	**Analysis: Crew utilises both alarm and parameter information but draws the conclusion to conduct the scram without considering the plant protection signal status. ➔ reflects a confirmative habit**	**Analysis: Crew makes hasty observations based on alarm information mainly. The information provided by different systems is only read aloud. No one seems to be listening what the other person is saying. ➔ reactive habit**

We could identify corresponding differences in crews' ways of dealing with other tasks of the Episode 1

Crew	Habit of information usage	Habit of situation identification	Habit of dealing with automation	Habit of decision making
A	plant protection, pressurizer level	Disturbance	Cue to perform scram	SS
B	emergency cooling, pressurizer level, primary circuit pressure, plant protection	Leakage	Cue to perform scram	SS
C	containment isolation, plant protection coolant flows, pressurizer level, pressurizer level gradient	Mass balance	Realise isolation	SS
D	plant protection, pressurizer level, primary circuit pressure, several trends in PMS	Leakage	Cue to perform scram	procedure
E	alarms, plant protection, pressurizer level	Leakage	Realise isolation	SS
F	pressurizer level, plant protection, emergency cooling, pressurizer level	Leakage	Realise isolation	procedure
G	emergency cooling, plant protection	Leakage	Realise isolation	procedure
H	emergency cooling, primary circuit pressure, containment isolation, plant protection	Disturbance	Ensure isolation actively	procedure
I	emergency cooling, pressurizer level, primary circuit pressure	Mass balance	Cue to perform scram	SS
J	emergency cooling, plant protection	Disturbance	Cue to perform scram	procedure
K	plant protection, alarm info	Leakage	Cue to perform scram	procedure
L	alarms, plant protection signals, primary circuit pressure	Disturbance	Cue to perform scram	SS

Characterisation of all habits of dealing with the proceduralised process control tasks over all episodes

	Information usage (episodes 1 & 2)	Interpretation of process situation	Dealing with automation	Decision making	Communication	Leadership
Interpretative 32,1%	Variety of sources, redundancy and diversity in information sources, dialogue in interpretation of information	Interpretation by considering functional meaning of process events	Human assures the automatic functions. Shared responsibility of human and automation.	SS makes decision to scram the process. Human as an active, present agent in decision making.	Dialogue concerning process status in the situation. Diverse and redundant information communicated. Reflects creation of joint awareness.	Active engagement of each operator in all the decision points. Transparency in contemplation enables to spot false conceptions.
Confirmative 40,5%	Multiple source but taken for granted	Identify the process events based on an existing typology of possible events e.g. a leak.	Automation functioning is observed but not taken action on. Reliance on the pre-defined roles of human and automation	Scram is conducted paced by the procedure. Actions are controlled by the procedure	Statements made aloud concerning process parameters. Reflects confirmation of own interpretations.	The end result of the decision making process is stated and confirmed by all the operators
Reactive 27,4%	Variation in information sources not sufficient	Identify that something is going on but now strive to understand or label the situation	Automation information is taken for granted, reflects total reliance on automation	Not identified in the data	Process state is not explicitly mentioned. Transfer of support system information.	No real collaboration. SS announces the next steps.

=>Balancing between stability and flexibility is characteristic for this habit

Mitä lisäarvoa inhimillisten tekijöiden analyysi tuo suunnittelulle?

- NUREG 0711, YVL B5 esitetään 12 tehtävää - OK
- Oman kokemuksemme perusteella keskeistä on ollut vastata kahteen kysymykseen:
- Mikä on hyvä valvomo?

  =>Tarvitaan yleisen tason käsitteellinen referenssi
- Miten tehdä objektiivinen mutta suunnittelun kannalta informatiiviinen arviointi?

  =>Tarvitaan käsitteellinen referenssi ja arviointimetodi jonka avulla välineen käyttäjät tuottavat uutta tietoa ratkaisusta käytössä, sen tarkoituksenmukaisesta käyttötavasta ja käytön oppimisesta

Hyvä valvomo?

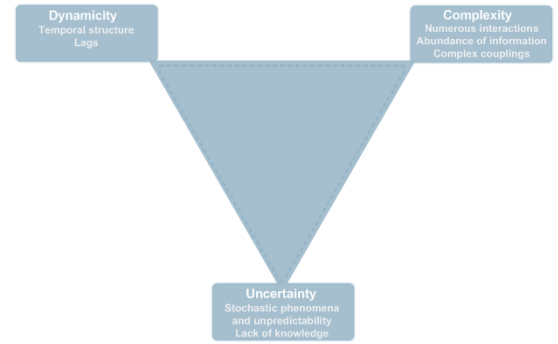
VALOKUVA

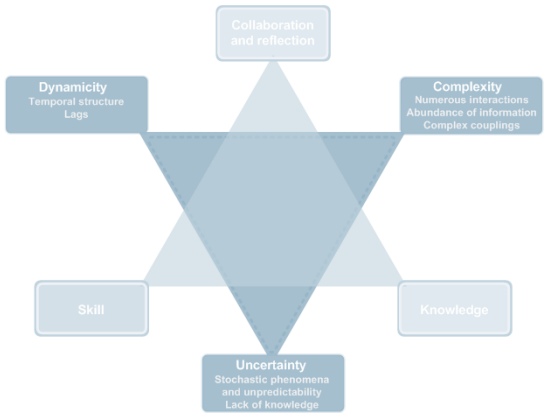
Systeemikäytettävyys ratkaisun ”hyvänä”

Systeemikäytettävyys:

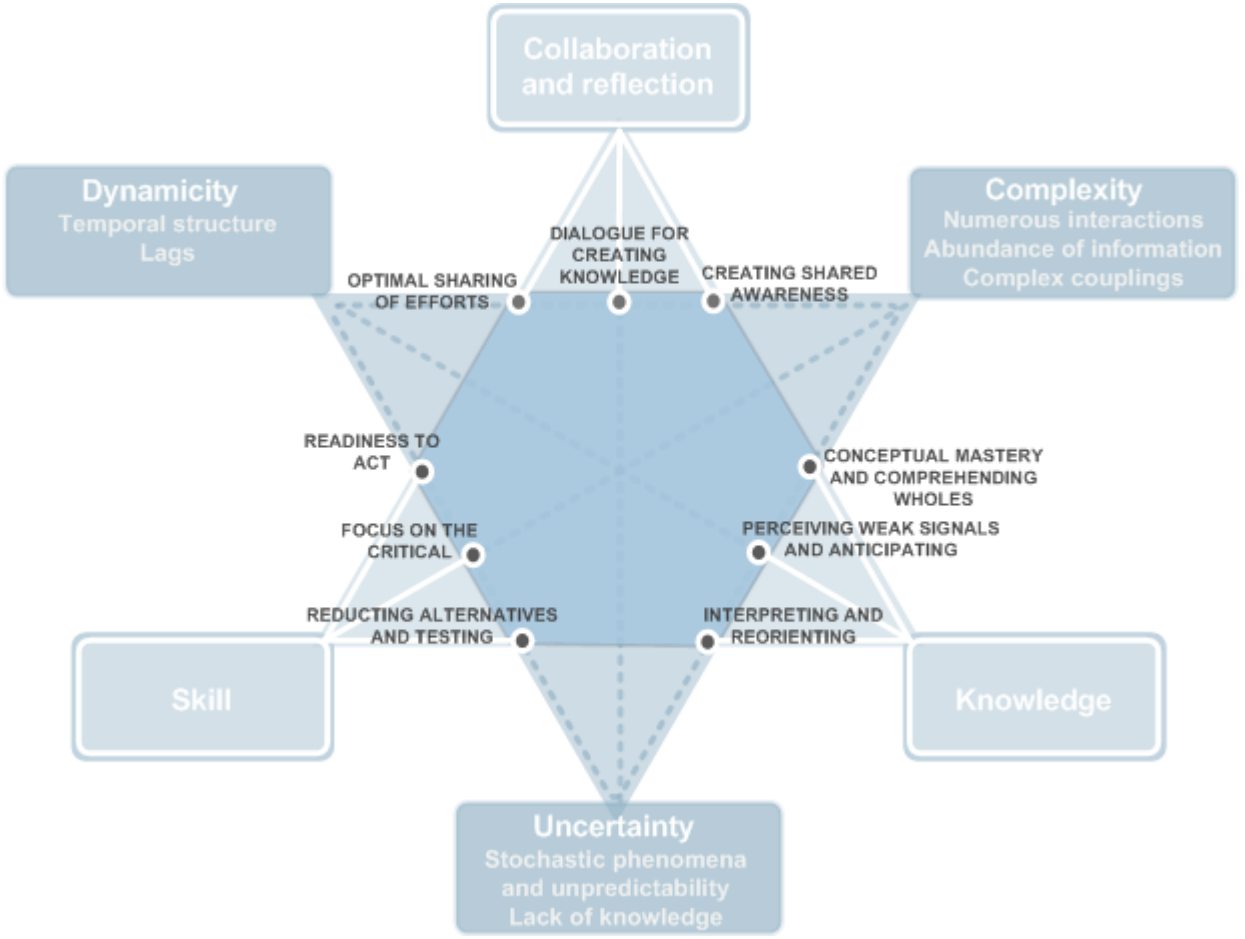
- Teknologian kyky toimia kaikissa käytettävyyteen vaikuttavissa välinerooleissa
- tukien tietyn perustehtävän täyttymistä niin, että toimintajärjestelmän päämäärät saavutetaan.
- Ilmenee teknologian käytössä toiminnan tuloksen, toimintatavan ja käyttäjäkokemuksen muodossa.

VALOKUVA

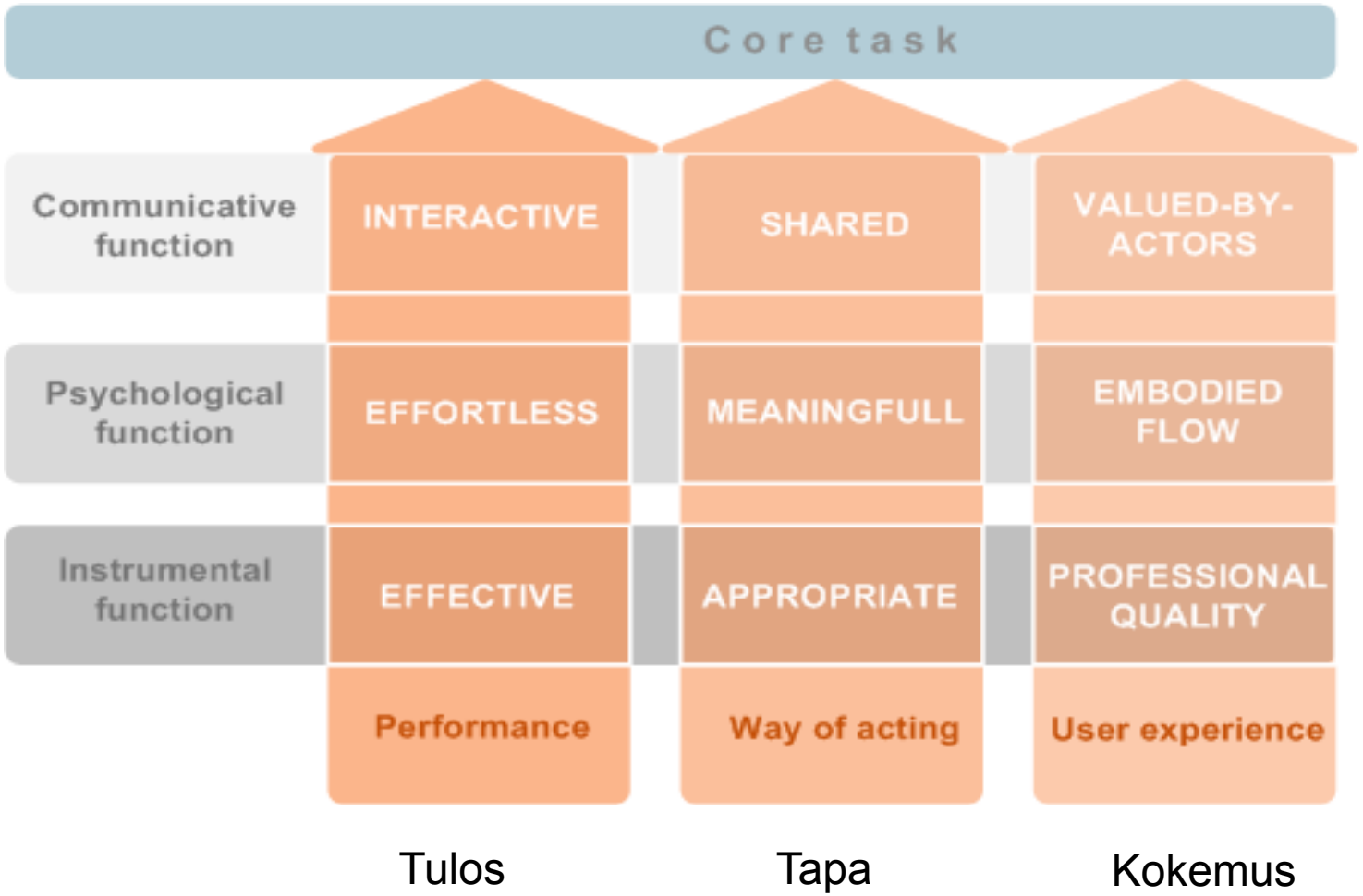




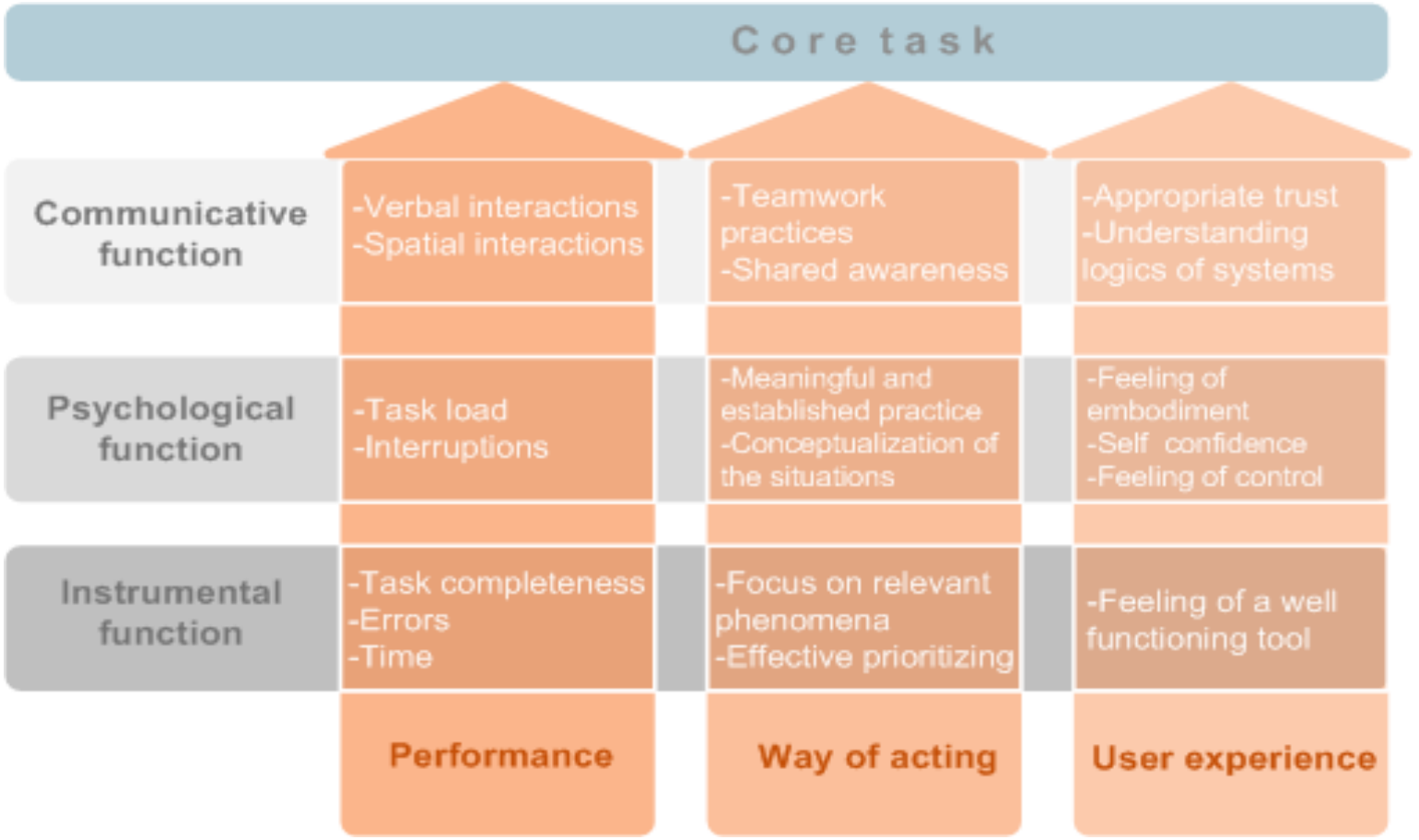
Core-task functions of highly automated work



Systeemikäytettävyyden arviointikehikko



Systeemikäytettävyyden mittareita eri indikaattoreille

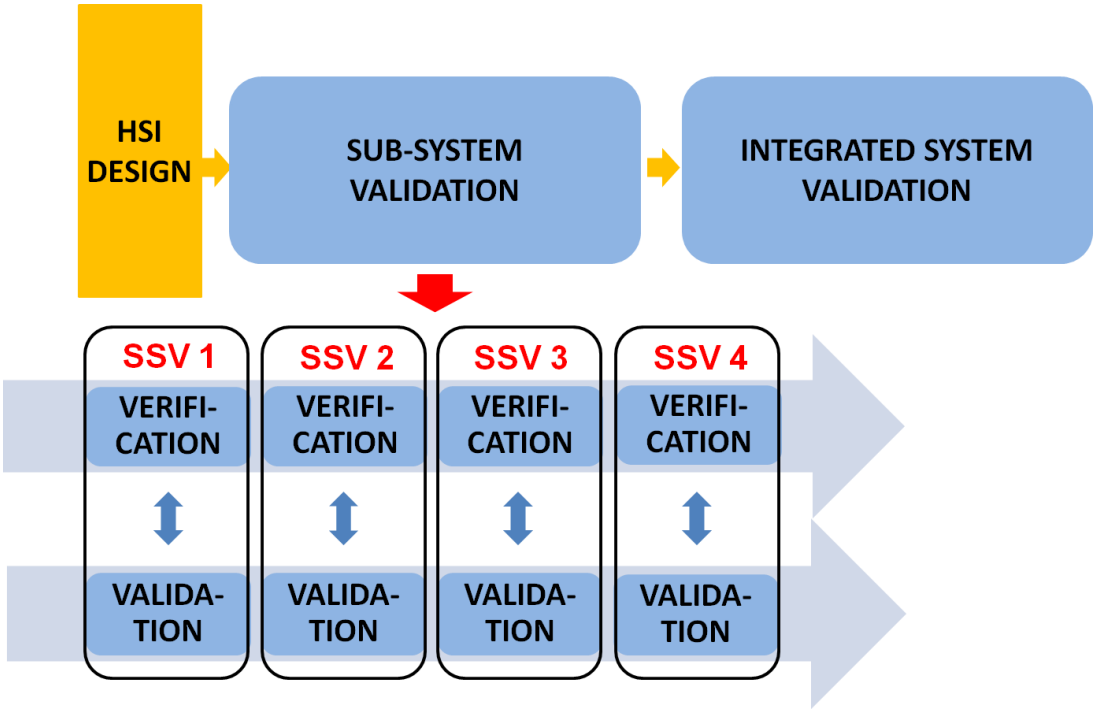


Arviointimetodi

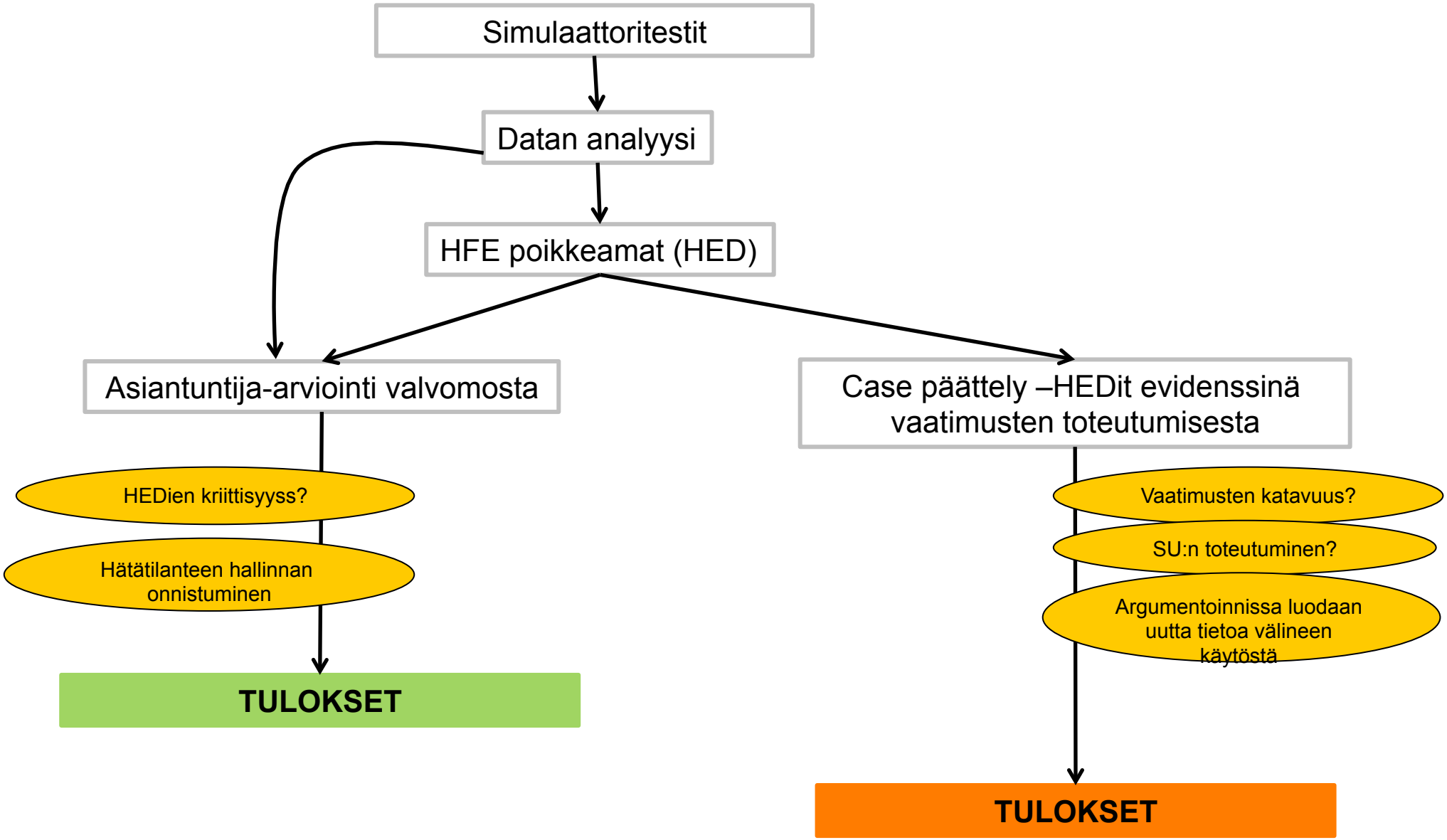
VALOKUVA

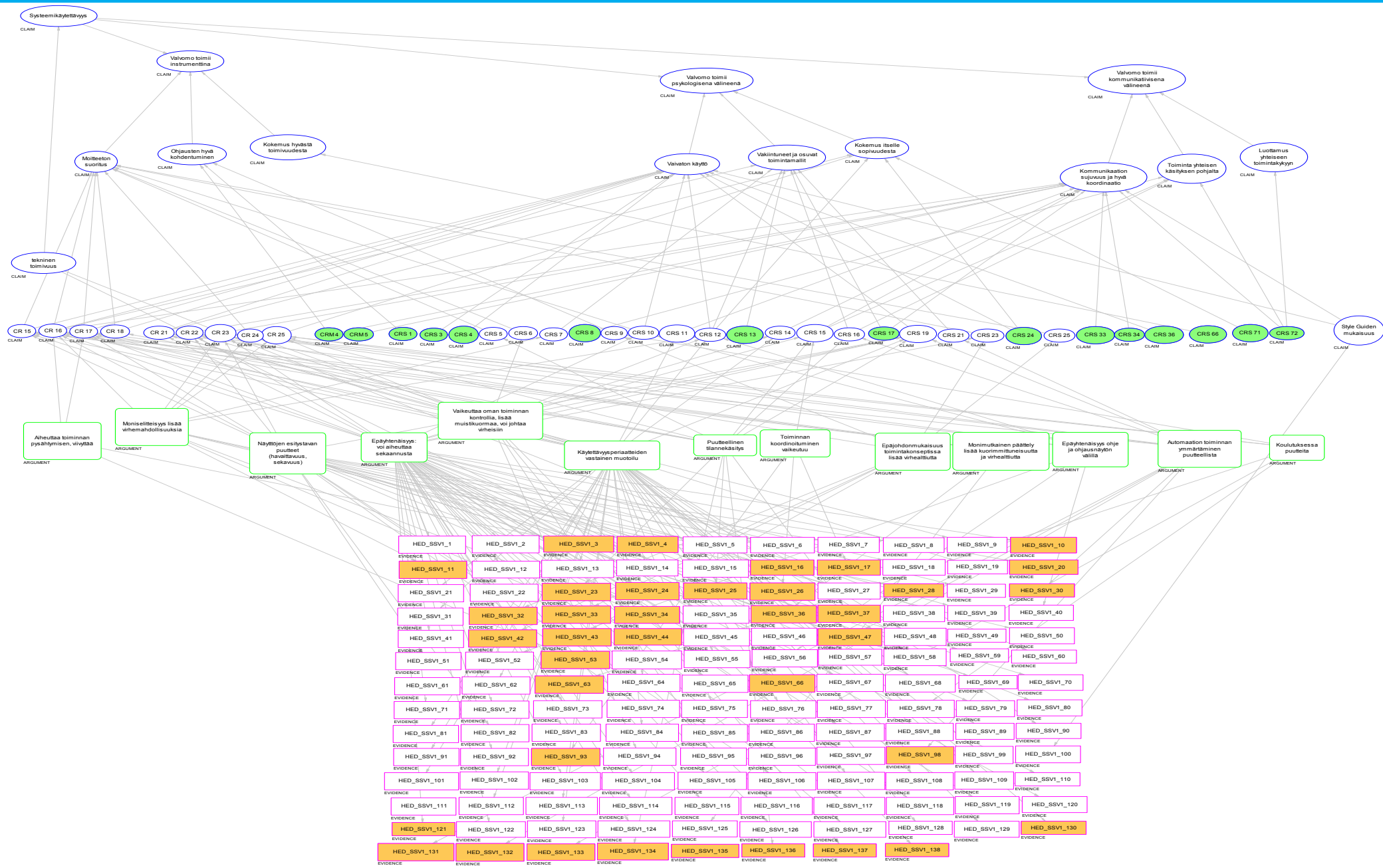
Osajärjestelmävalidoinnin (SSV) ja integroidun validoinnin (ISV) muodostama arviointiprosessi

- Standardit tuntevat vain ISV:n
- SSV sisältää testisarjan, jossa arviointituloksia kumuloidaan
- SSV:llä on erityisiä tiedon luomiseen pyrkiviä laatuvaatimuksia
- Formaalit laatuvaatimukset täytetään kuten ISV:ssä.
- Arviointiprosessi varmistaa systeemin eri tasoilla että laitoksen turvallista operointia tuetaan tarkoituksenmukaisella tavalla



Asiantuntija- ja vaatimuspohjainen arviointi




Systeemikäytettävyys
Valvomo toimii instrumenttina
Valvomo toimii psykologisena välineenä
Valvomo toimii kommunikatiivisena välineenä
Moitteeton suoritus
Ohjausten hyvä kohdentuminen
Kokemus hyvästä toimivuudesta
Vaivaton käyttö
Vaikiintuneet ja osuvat toimintamallit
Kokemus itselle sopivuudesta
Kommunikaation sujuvuus ja hyvä koordinaatio
Toiminta yhteisen käsityksen pohjalta
Luottamus yhteiseen toimintakykyyn
tekninen toimivuus
Style Guiden mukaisuus
CR 15
CR 16
CR 17
CR 18
CR 21
CR 22
CR 23
CR 24
CR 25
CRM4
CRM5
CRS 1
CRS 3
CRS 4
CRS 5
CRS 6
CRS 7
CRS 8
CRS 9
CRS 10
CRS 11
CRS 12
CRS 13
CRS 14
CRS 15
CRS 16
CRS 17
CRS 19
CRS 21
CRS 23
CRS 24
CRS 25
CRS 33
CRS 34
CRS 36
CRS 66
CRS 71
CRS 72
Aiheuttaa toiminnan pysähtymisen, viivyttää
Moniselitteisyys lisää virhemahdollisuuksia
Näyttöjen esitystavan puutteet (havaittavuus, sekavuus)
Epäyhtenäisyys: voi aiheuttaa sekaannusta
Vaikeuttaa oman toiminnan kontrollia, lisää muistikuormaa, voi johtaa virheisiin
Käytettävyysperiaatteiden vastainen muotoilu
Puutteellinen tilannekäsitys
Toiminnan koordinoituminen vaikeutuu
Epäjohdonmukaisuus toimintakonseptissa lisää virhealttiutta
Monimutkainen päättely lisää kuormittuneisuutta ja virhealttiutta
Epäyhtenäisyys ohje ja ohjausnäytön välillä
Automaation toiminnan ymmärtäminen puutteellista
Koulutuksessa puutteita
HED_SSV1_1
HED_SSV1_2
HED_SSV1_3
HED_SSV1_4
HED_SSV1_5
HED_SSV1_6
HED_SSV1_7
HED_SSV1_8
HED_SSV1_9
HED_SSV1_10
HED_SSV1_11
HED_SSV1_12
HED_SSV1_13
HED_SSV1_14
HED_SSV1_15
HED_SSV1_16
HED_SSV1_17
HED_SSV1_18
HED_SSV1_19
HED_SSV1_20
HED_SSV1_21
HED_SSV1_22
HED_SSV1_23
HED_SSV1_24
HED_SSV1_25
HED_SSV1_26
HED_SSV1_27
HED_SSV1_28
HED_SSV1_29
HED_SSV1_30
HED_SSV1_31
HED_SSV1_32
HED_SSV1_33
HED_SSV1_34
HED_SSV1_35
HED_SSV1_36
HED_SSV1_37
HED_SSV1_38
HED_SSV1_39
HED_SSV1_40
HED_SSV1_41
HED_SSV1_42
HED_SSV1_43
HED_SSV1_44
HED_SSV1_45
HED_SSV1_46
HED_SSV1_47
HED_SSV1_48
HED_SSV1_49
HED_SSV1_50
HED_SSV1_51
HED_SSV1_52
HED_SSV1_53
HED_SSV1_54
HED_SSV1_55
HED_SSV1_56
HED_SSV1_57
HED_SSV1_58
HED_SSV1_59
HED_SSV1_60
HED_SSV1_61
HED_SSV1_62
HED_SSV1_63
HED_SSV1_64
HED_SSV1_65
HED_SSV1_66
HED_SSV1_67
HED_SSV1_68
HED_SSV1_69
HED_SSV1_70
HED_SSV1_71
HED_SSV1_72
HED_SSV1_73
HED_SSV1_74
HED_SSV1_75
HED_SSV1_76
HED_SSV1_77
HED_SSV1_78
HED_SSV1_79
HED_SSV1_80
HED_SSV1_81
HED_SSV1_82
HED_SSV1_83
HED_SSV1_84
HED_SSV1_85
HED_SSV1_86
HED_SSV1_87
HED_SSV1_88
HED_SSV1_89
HED_SSV1_90
HED_SSV1_91
HED_SSV1_92
HED_SSV1_93
HED_SSV1_94
HED_SSV1_95
HED_SSV1_96
HED_SSV1_97
HED_SSV1_98
HED_SSV1_99
HED_SSV1_100
HED_SSV1_101
HED_SSV1_102
HED_SSV1_103
HED_SSV1_104
HED_SSV1_105
HED_SSV1_106
HED_SSV1_107
HED_SSV1_108
HED_SSV1_109
HED_SSV1_110
HED_SSV1_111
HED_SSV1_112
HED_SSV1_113
HED_SSV1_114
HED_SSV1_115
HED_SSV1_116
HED_SSV1_117
HED_SSV1_118
HED_SSV1_119
HED_SSV1_120
HED_SSV1_121
HED_SSV1_122
HED_SSV1_123
HED_SSV1_124
HED_SSV1_125
HED_SSV1_126
HED_SSV1_127
HED_SSV1_128
HED_SSV1_129
HED_SSV1_130
HED_SSV1_131
HED_SSV1_132
HED_SSV1_133
HED_SSV1_134
HED_SSV1_135
HED_SSV1_136
HED_SSV1_137
HED_SSV1_138

Arvioinnissa opittua

- Argumentit antoivat tietoa seuraavista asioista:
  - Operointikonsepti: työnjako, johtaminen, automaatiotietoisuus
  - Toimintatavat: yhteistyö, tarkkaavaisuus ja havaitseminen, varmistukset, toimintarutiinit
  - Virheistä: käyttöliittymäratkaisut

- Välineen hallinnan kehittäminen on osa suunnittelua
- Automaatiosuunnittelun kannalta ihmisen toiminnan luotettavuudessa on kaksi toisiaan täydentävää näkökulma
  - Resilienssilähtöinen => systeemikäytettävyyden ja välineen hallinnan kehittäminen
  - Virhelähtöinen => nojataan HRA-analyyseihin

Johtopäätöksiä

- On toimintatapoja joissa yhdistyvät järjestelmän vakiointipyrkimys ja tilanteiden vaatima joustavuus
- Järjestelmää arvioitaessa ohjaajien huomiot operointikonseptin suhteen osoittavat samaa
- Automaatioratkaisujen suunnittelun, arvioinnin ja automaatioon liittyvän koulutuksen yhteydessä on suunnitelmallisesti tuettava tällaisia toimintatapoja

KIITOS!