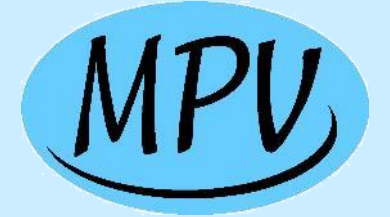


Humanoidirobottien laadunvarmistus

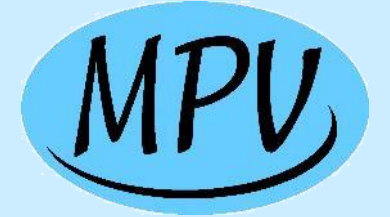


Matti Vuori www.mattivuori.net matti.vuori@mattivuori.net @Matti_Vuori



Sisällysluettelo 1/4

<u>Koko maailma robottihuumassa – taas</u>	<u>6</u>
<u>Oppimisen aika</u>	<u>7</u>
<u>...Muutenkin mielenkiintoinen aihe...</u>	<u>8</u>
<u>Robottityyppejä</u>	<u>9</u>
<u>Humanoidirobotit</u>	<u>10</u>
<u>Monenlaisia</u>	<u>11</u>
<u>Keskeisiä piirteitä</u>	<u>12</u>
<u>Toiminnan ohjaus</u>	<u>13</u>
<u>Laaja laatuavaruus</u>	<u>14</u>
<u>TEKOÄLYSTÄ</u>	<u>15</u>
<u>Suhteemme tekoälyyn</u>	<u>16</u>
<u>Edes FBI ei osaa: Kasvojentunnistus ei toimi</u>	<u>18</u>
<u>Ei arvo sinänsä, vaan eritasoista lisäarvoa</u>	<u>19</u>
<u>Uusi konsepti, uusi teknologiapaketti</u>	<u>20</u>
<u>Mitä uutta eri tasoilla?</u>	<u>21</u>
<u>Monenlaisia älysystemejä</u>	<u>22</u>
<u>Älyn määrä ja luonne vaihtelee</u>	<u>23</u>

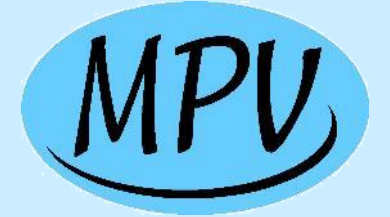


Sisällysluettelo 2/4

<u>Ja "älyn" kasvaessa kaikki muuttuu</u>	24
<u>Älysteemin arkkitehtuuri</u>	25
<u>LAADUN TASOJA</u>	26
<u>Robotti ja sen äly ovat aina kontekstissa</u>	27
<u>Käyttäjäkokemus kriittinen varmistettava</u>	28
<u>Mutta senkin päällä on kulttuurinen kokemus</u>	29
<u>Sosiaalisten vaikutusten arviointi</u>	30
<u>Käytettävyyden heuristisia periaatteita</u>	31
<u>Testausta eri tasoilla</u>	32
<u>Hajoita ja hallitse testauskohde teknisesti</u>	33
<u>Hajoita ja hallitse tyyli älyn osa-alueittain</u>	34
<u>Epädeterministinen monitoimijaympäristö</u>	36
<u>Älyn testaamisen haasteita</u>	38
<u>TEKOÄLYN TESTAAMISESTA</u>	39
<u>Älyn toimintalogiikan selvittäminen</u>	42
<u>Testauksen kohteena käyttäytyminen suhteessa odotuksiin</u>	43
<u>Onko äly sellaista kuin ihmisellä?</u>	44

Sisällysluettelo 3/4

<u>Äly psykologisena haasteena</u>	45
<u>Älyn testattavuus – lokitus tärkeää</u>	46
<u>Testidata suunniteltava huolella</u>	47
<u>Datan poikkeamatarkastelun tarkistuslista</u>	48
<u>TESTITYYPPEJÄ</u>	49
<u>Olennaisia testityyppejä lyhyesti</u>	50
<u>Tekoälysystemin käytettävyyden arviointi ja testaus</u>	54
<u>Inhimilliset virheet</u>	56
<u>Robottisysteemin korkean tason riskianalyysin kysymyksiä (sampler)</u>	58
<u>Älysystemin matalan tason riskianalyysin kysymyksiä (sampler)</u>	59
<u>Tietoturvatestaus</u>	60
<u>Turvallisuuskriittisyys</u>	61
<u>Arkkitehtuurin arviointi ja teknologioiden valinta</u>	62
<u>Turvallisuuskriittisten systemien arkkitehtuuri</u>	63
<u>Oppimisen testaus</u>	64
<u>Oppiminen testauksen ongelmana</u>	65
<u>Oppivan turvallisuuskriittisen systeemin kaksi ongelmaa</u>	66



Sisällysluettelo 4/4

<u>Tietoturvallisuus</u>	67
<u>"Etiikan" testaus</u>	68
<u>Robotin olosuhdetestaus</u>	69
<u>Tuotantotestaus</u>	70
<u>Kooste testauksen haasteita</u>	71
<u>Ylläpidettävyyden testaus</u>	76
<u>OSAAMISPALETIN MUUTOKSIA</u>	77
<u>Osaamishaasteita</u>	78
<u>Tarvittavissa kompetensseissa muutoksia</u>	79
<u>YHTEENVETO</u>	80
<u>Kymmenkunta nyrkkisääntöä</u>	81

Koko maailma robottihuumassa – taas

- Ensimmäistä kertaa roboteista kohistiin vuosikymmeniä sitten, kun niitä alettiin soveltaa valmistavassa teollisuudessa mm. kokoonpanotöissä, hitsauksessa ja maalauksessa. Tein itse noin 30-sivuisen paperin niiden turvallisuudesta 30 vuotta sitten.
- Nyt odotetaan uutta tuleamista:
 - Fyysiset robotit kirurgien apuna, vanhusten ja vammaisten tukena, ohjelmistorobotit automatisoimassa tietotyötä, kaikkien teollisuustöiden robotisointi...
 - Suomalaisten olisi fiksua tehdä alueella menestystuotteita!
- Tänäpä mietitään siksi ihmisenkaltaisten humanoidirobottien laadunvarmistusta eli testausta ja muuta niiden arviointia.

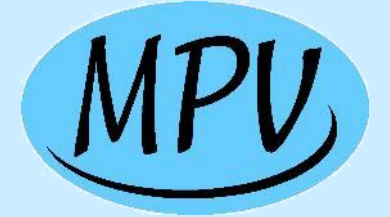
Oppimisen aika

- Nyt alkaa oppimisen aika.
- Robottien valmistajien on opittava tekemään hyviä robotteja – hyödyllisiä, helppoja, turvallisia.
- Robottien hyödyntäjien pitää oppia kehittämään palveluja ja työjärjestelmiä, joissa älykäs robotti on luonteva elementti – hyödyllinen, helppo, turvallinen osa, jonka avulla saadaan aikaan toimiva sosiotekninen kokonaisuus, hyvä työpaikkakokemus ja hyvä palvelukokemus.
- Kummassakin asetelmassa tarvitaan suunnittelutaitoja ja suunnitelmien ja niiden toteutuksen arvioinnin taitoja ja käytäntöjä.
 - Testausta, systeemin analysointia, riskianalyysiä jne...

...Muutenkin mielenkiintoinen aihe...

- Roboteissa on paljon mielenkiintoista yleisemminkin.
- Niissä äärimmäistyvät monen testauksen haasteet:
 - Uusi disruptiivinen konsepti.
 - Älykkyys ja oppivuus.
 - Monenlaista turvallisuuskriittisyyttä.
 - Erilainen psykologinen suhde testaajaan.
 - Jne...
- Niinpä niiden tarkastelu voi opettaa meille tärkeitä asioita!
- **Ok, humanoidirobotteja saadaan odottaa muuhun kuin sosiaaliseen käyttöön vielä vähän aikaa. Siihen asti ne toimivat uuden teknologian prototyyppeinä ja niiden miettiminen on siksi hyvin hyödyllistä.**

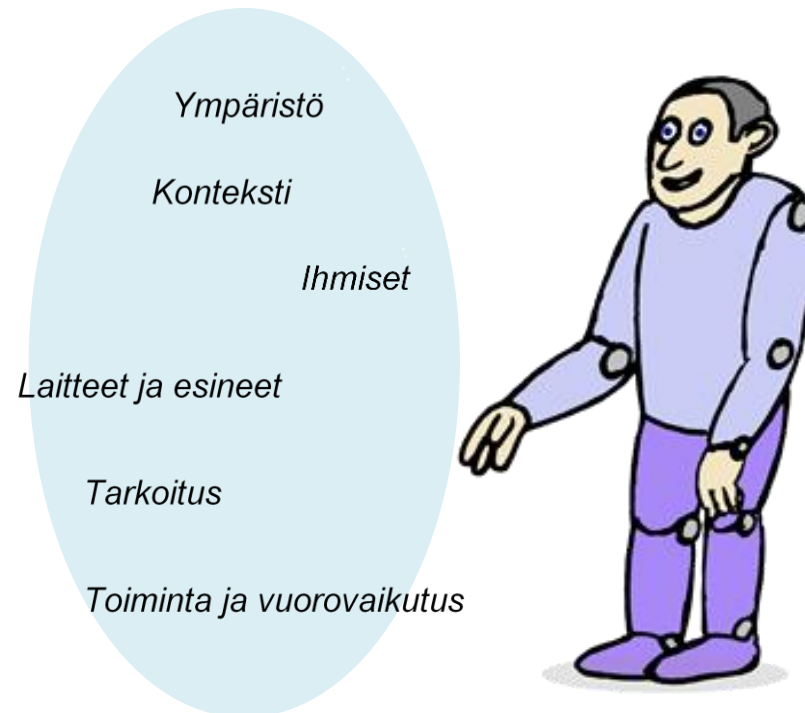
Robottityyppejä



	Vain ohjelmistopohjainen	Fyysinen
Yhteistoiminnallinen robotti	Ohjelmistoagentti Päätöksenteon tukijärjestelmä Virtuaalinen työpari	Ihmisenkaltainen humanoidirobotti Teollisuusrobotti Vanhusten ja vammaisten apulainen
Itsenäisesti toimiva robotti	Tekoälyjärjestelmä prosessissa, datan käsittelyssä	Eristetty teollisuusrobotti Ihmistä välttelevä apurobotti Robottiajoneuvo

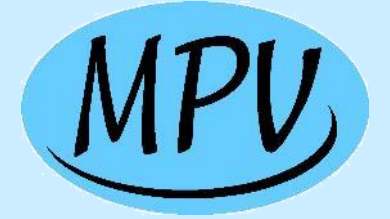
Humanoidirobotit

- Odotetaan tulevaisuudessa olevan tavallinen näky työpaikoilla, laitoksissa ja kotitalouksissa.
- Saa nähdä, miten pian...
- Edustavat uudenlaista kehittynyttä, älykästä automaatiota.



Monenlaisia

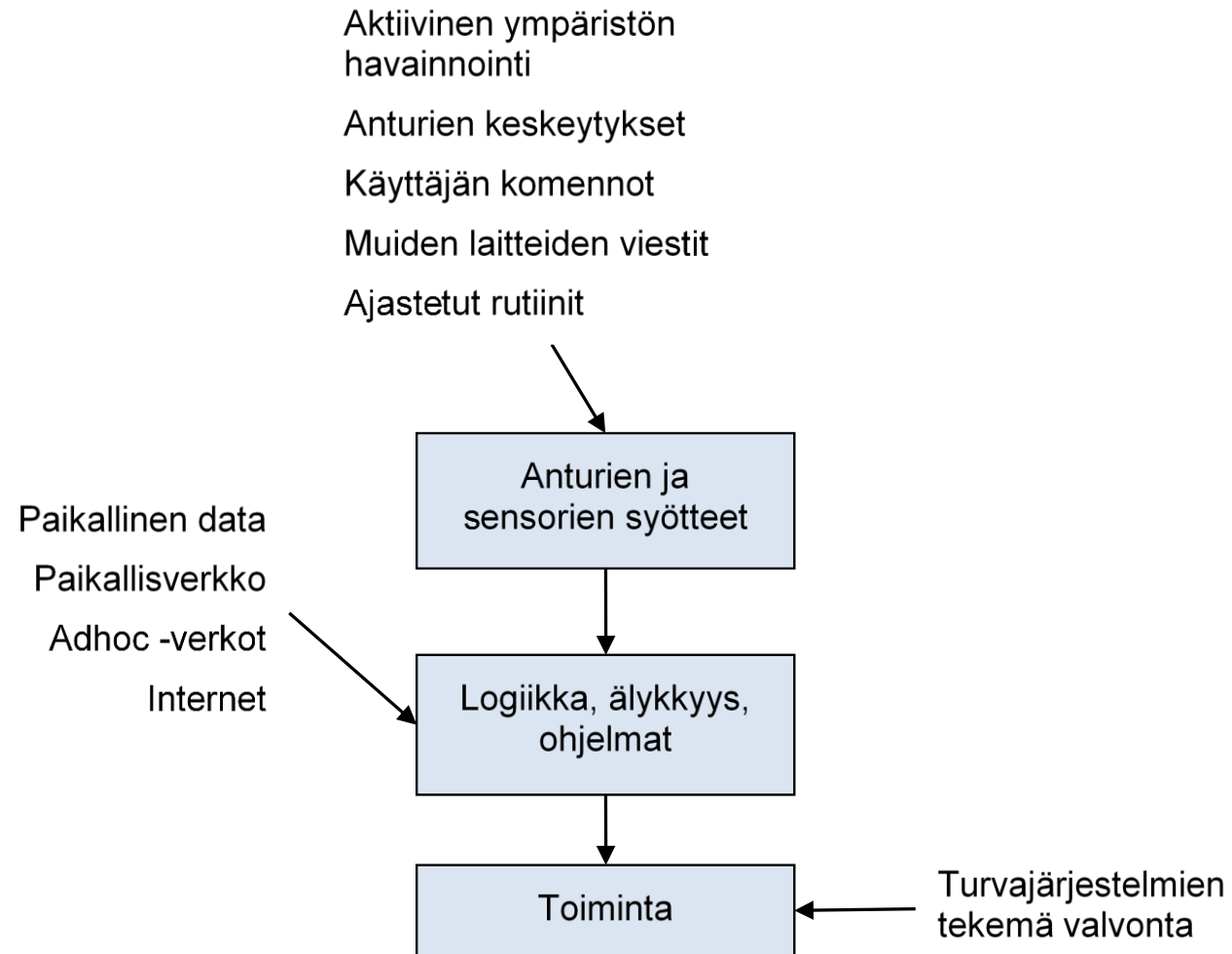
- Jotkut yksinkertaisia fyysisen työn apulaisia ja kykenevä tekemään yksinkertaisia tehtäviä – kuten nostoapulainen ikäihmisille, tai imuroijarobotti.
- Jotkut suuntautuneet viestintä- ja muistiavuksi käyttäjälle.
- Joidenkin idea on tarjota henkilökohtaista seuraa ja iloa
- Koko vaihtelee.
- Jotkut turvallisuuskriittisempiä enemmän kuin toiset.
- Autonomia vaihtelee
- Kyky oppia vaihtelee.



Keskeisiä piirteitä

- On uusi asia
- On ihmisenkaltainen
- On fyysinen, ja liikkuva
- Voi nostaa, siirtää asioita
- Sillä on kehittynyt aistijärjestelmä
- On älykäs
- On persoonallinen
- On oppiva
- On ohjelmistojärjestelmä
- On verkottunut paikallisesti ja maailman kanssa
- On ”tietovaarallinen”
- On teknisesti monimuotoinen ja monimutkainen

Toiminnan ohjaus



Laaja laatuavaruus

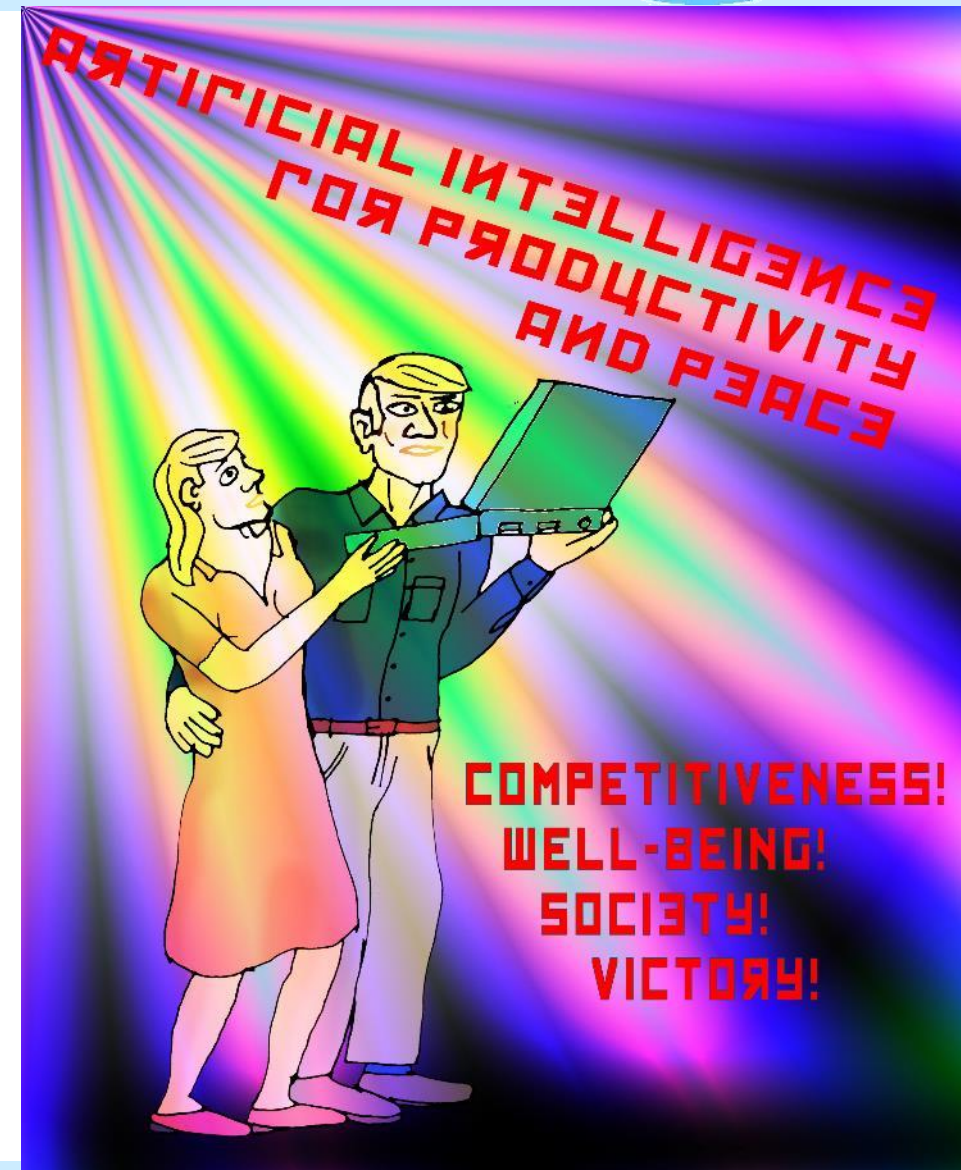
- Jo "tavallisen" automation laadulla paljon tekijöitä – hyödyllisyys, käytettävyys, luotettavuus, turvallisuus, ylläpidettävyys jne...
- Humanoidirobotin idea on olla jossain mielessä ihmisen kaltainen – samanlaista muotoa, samanlaista käyttäytymistä.
- Niinpä laadun maailma laajenee korostuneemmin "sosiaaliseen laatuun" – eli miten robotti on osa ihmisten joukkoa.
- Tämä laatu on keskeistä robotti-transformaatioissa ja työpaikkojen ja palvelujen laadussa.
- Siksi siihen pitää panostaa tietoisesti. Enää ei mitenkään riitä se, että tehdään robotin toiminnoille toiminnallista testausta – kuten on edelleen testauksen valtavirta monilla tuoteryhmillä.
- Haaste koskee yhtäläillä systeemin laatua kuin prosessin laatua – robottien hyödyntäjien suunnittelukäytäntö uusille työjärjestelmille on aivan kriittinen.

TEKOÄLYSTÄ



Suhteemme tekoälyyn 1/2

- Tekoälystä puhutaan paljon, se on lähes menestyksemme hopealuoti...
- Testauksen idea on luoda tolkkua (sensemaking) uusiin asioihin, nähdä selväjärkisesti hypen läpi ja auttaa uuteen teknologiaan liittyvässä päätöksenteossa.
- Testauksen (ml. epäempiiriset tuotteen arvioinnit) pitää unohtaa lyhenteet ja lupaukset ja lähestymistavoillaan paljastaa todellisuus.



Suhteemme tekoälyyn 2/2

- Tekoälypuhe on usein teknistä, detaljista, toimii teknologiaretoriikan ehdoilla.
- Jotta testaus tuo lisäarvoja ja ottaa paikkansa, sen pitää tuoda toinen näkökulma asioihin eikä antautua toisten kielipeliin.
- Tämä ei merkitse omaa kielipeliä, vaan selkeyden.
- **Ajatelkaamme siis omilla aivoillamme, toistamatta älykauppaiden retoriikkaa.**
- **Tämän esityksen idea onkin nostaa esille asioita, joissa on ajattelemisen aihetta.**

Edes FBI ei osaa: Kasvojentunnistus ei toimi

- <https://www.inverse.com/article/29470-facial-recognition-fbi>
- “third-party investigators said the entire system was reckless, unproven, and biased during a House Oversight Committee hearing”
- “FBI’s own tests show the system is only somewhat accurate. When the system was asked to pull the 50 closest-matching faces from a set of nearly 1 million, it got the right one only 86% of the time”
- “The Bureau has not tested the accuracy rate when pulling candidate lists of fewer than 50 potential matches”
- “hasn’t done any false positive testing to see how often non-matching faces are flagged as potential hits”
- **...Mitenkähän hyvin pienemmät toimijat ja innokkaat startupit tekevät testauksensa?...**



Ei arvo sinänsä, vaan eritasoista lisäarvoa

- Tekoäly ei ole arvo sinänsä. Sen käyttö on iso arvolupaus:
 - Voi poistaa tylsiä tai vaarallisia töitä.
 - Auttaa vaikeissa asioissa.
 - Korostaa sitä, mikä tekemisessä / asiassa on hienoa.
 - Vähentää työtä, kustannuksia, vähentää työvoimaa.
- Tekoälyä ei kannata ajatella binäärisesti – on tai ei, vaan miettiä, miten kuhunkin asiaan saisi etua lisäämällä ohjelmallista älykkyyttä, joka kenties hyödyntää kokemuksia ja kerättyä dataa.

Uusi konsepti, uusi teknologiapaketti

- Teollisessa kulttuurissa ihmiset ekstrapoloivat testauksensa lähestymistavan historiastaan ja edellisistä projekteista ”juuri riittävästi”.
- Kun testin alla oleva järjestelmä ottaa ison hyppäyksen haasteissa koko testausta pitäisi arvioida uudelleen.
- Olisi virhe ajatella tekoälyä vain yhtenä uutena ohjelmoitavana laitteena, ja automaation uutena tyyppinä.
- **Pitää esiymmärtää konseptitasolla millaista on hyvä tekoäly ja tekoälytuote, jotta osataan tuottaa tietoa sen hyvyydestä ja asettaa oikeita odotuksia.**
- Toistaalta testauksen pitää lähteä ymmärtämisestä, sensemaking: miten uusi asia toimii ja käyttäytyy.

Mitä uutta eri tasoilla?

Taso	Uutta ja huomioonottettavaa
Ihmisen suhde älyyn	Inhimillistäminen, ihmettely -> tietoisuus tästä ja vastatoimia
Tuote- ja järjestelmäkoneptit	Disruptiivisia? Uusia? Arvioitava konseptitasoa, testattava käyttäjäkokemusta
Objektiivisesti, metodisesti kohdattava asia	Työkaluja löytyy asian hallintaan (siis pitäisi löytyä ammattilaiselta)
Käyttäytyvä systeemi	Älyn luonne ja logiikka pitää kenties tunnistaa testaamalla "Toiminnon" sijaan tunnistus, päättely
Tekninen systeemi	Bittejä liikkuu, mutta testaustaktiikoita ja välineitä löytyy

Monenlaisia älysteemejä

- Eri tarkoituksia:
 - Diagnoosi.
 - Asiantuntijajärjestelmä.
 - Älykäs toiminnallisuus.
 - Ohjelmistorobotiikka.
 - Viestintä. Asiakaspalvelija.
 - Lisätty todellisuus.
 - Turvajärjestelmät ml. tietoturva.
 - Jne...
- Itsenäisiä teknisiä tai ihmisen apulaisia.
- Aika usein **lisäävät älyä systeemiin (Augmented Intelligence) tai tehostavat ihmisen älyä.**

Älyn määrä ja luonne vaihtelee

- Yksinkertainen sääntöpohjainen logiikka:
 - JOS jotain, niin SITTEN jotain.
- Oppivat systeemit.
 - Muotoilevat itse käyttäytymisensä opetutuksen ja oppiminen perusteella.
 - Epäeksaktia logiikkaa: todennäköisyydet, painokertoimet...
 - Data tärkeää – Big Data...
- Tietoiset järjestelmät. Ei vielä näköpiirissä...

Yksinkertainen
automaatti

Kompleksinen ja
vaikea persoona



Ja ”älyn” kasvaessa kaikki muuttuu

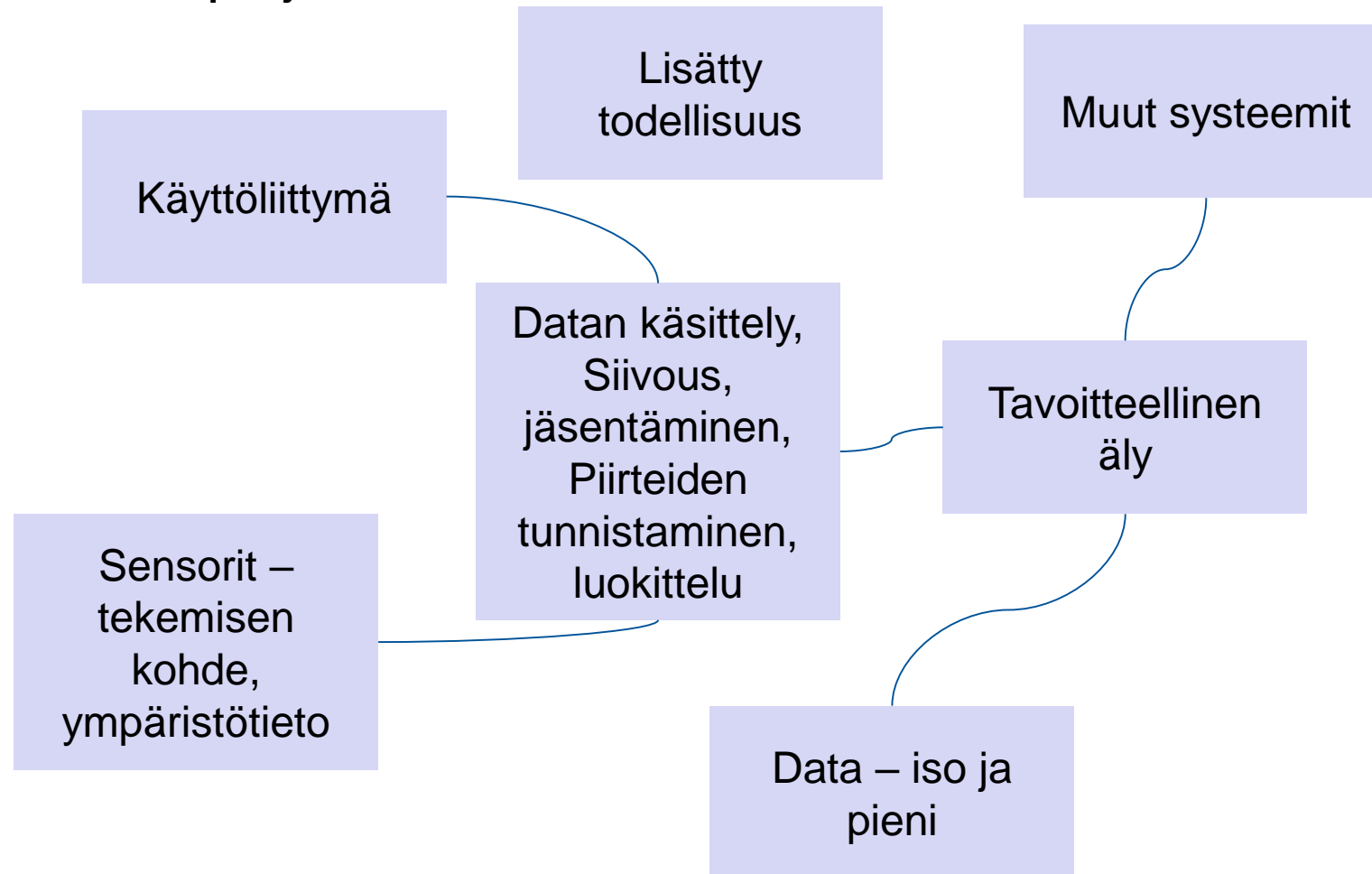
- Epätietoisuus systeemin luonteesta.
- Epävarmuus sen luotettavuudesta ja turvallisuudesta.
- Oma kontrolli kenties vähenee.
- Epäluuloisuus kasvaa...



**Tekoäly voi vaarantaa
tietosuojasi, fyysisen
turvallisuutesi tai elinkeinosi**

Älysystemin arkkitehtuuri

- Huom: Näitä on paljon erilaisia.



LAADUN TASOJA

Robotti ja sen äly ovat aina kontekstissa

- Robotti ei ole yksinään, se on aina jossain tuotteen tai järjestelmän kontekstissa:
 - Tarkoitus.
 - Toiminta.
 - Käyttäjät.
 - Edut.
 - Riskit.
 - Toimintaperiaatteet.
- **...Ja älystä saa tolkkua vain kontekstissa** ja sitä pitää testata kontekstin näkökulmasta.
 - Tietokantojenkin yhteydessä kiinnostaa kyky selvittää transaktioista, eikä toiminta kaikilla mahdollisilla SQL-kyselyillä.

Käyttäjäkokemus kriittinen varmistettava

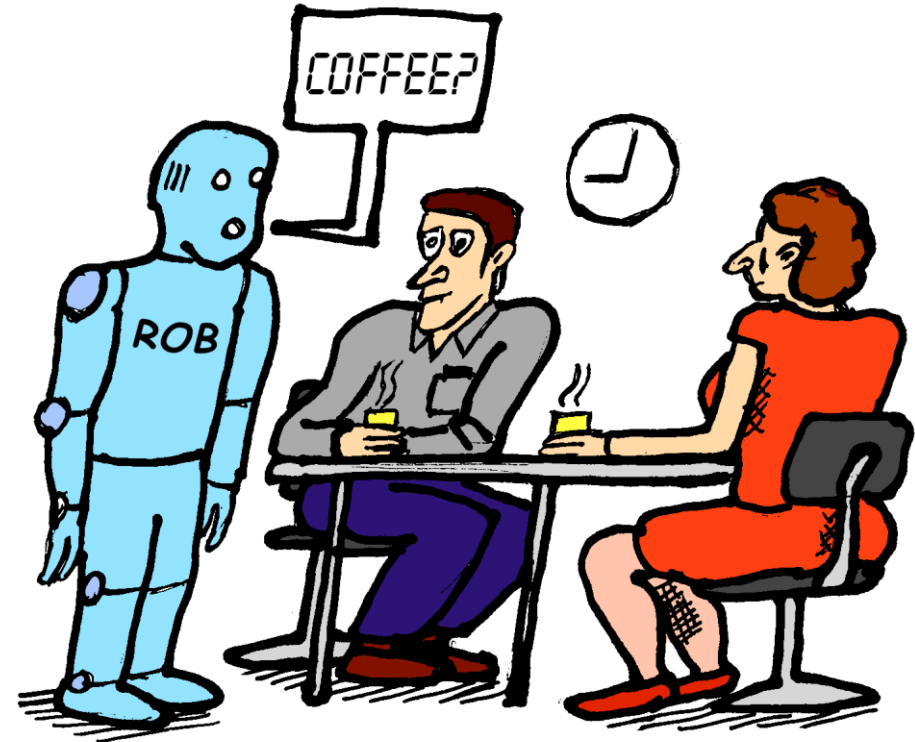
- Laadun yhdellä ylimmällä tasolla on käyttäjäkokemus.
- Se on kriittistä startupeille ja kaikille uuteen konseptiin perustuville tuotteille.
- Mutta teknologiayritykset usein siinä huonoja.
- **Siis tekoälytuotteissa huippuoleellista varmistaa.**
- Ymmärrystä eri aikoina:
 - 1990: Auton ajo-ominaisuudet ovat parhaimmillaan, kun niitä ei huomaa.
 - 2000: Käyttöliittymä on parhaimmillaan, kun sitä ei huomaa; kun sitä on mahdollisimman vähän.
 - 2017: Tekoäly on parhaimmillaan, kun sitä ei huomaa (ellei kyseessä ole lelu). Robotti on parhaimmillaan, kun se ei kiinnitä huomiota työpaikalla.
 - Tekoäly ei ole itseisarvo, vaan sen avulla parannetaan sitä, mikä tuotteessa on hienoa tai vähennetään sitä, mikä ei ole niin hienoa.

Mutta senkin päällä on kulttuurinen kokemus

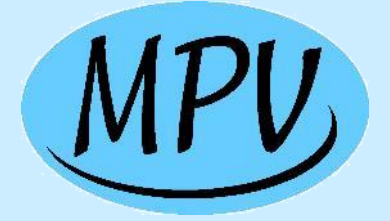
- Miten hyvin käyttäjät kokevat robotin sopivan heidän toiminnalliseen kontekstiinsa ja kulttuuriinsa?
- Vaatiiko robotti tarpeetonta valvontaa? Häiritseekö sen läsnäolo?
- Pelottaako se vaikkapa lapsia tai kotieläimiä?
- Jne...
- Kyse konseptitason analysoinnista ja testauksesta, missä pitää erottaa suunnittelun päälinjat pienistä detaljeista.
- Konseptin sopimattomuus kulttuuriin on iso riski ja siksi tärkeä analysoitava asia.
- Tämä tehdään aina robotin käyttökontekstissa.

Sosiaalisten vaikutusten arviointi

- Sosiaalisia vaikutuksia pitää arvioida uuden robottisysteemin suunnittelun yhteydessä.
- Aiheesta on oma kalvosetti "Yhteistoiminnallisen humanoidirobotin sosiaalisia vaikutuksia työpaikalla"



Käytettävyyden heuristisia periaatteita



- Ihmisen ja robotin työnjako on hyvä: kumpikin tekee hänelle paremmin sopivia asioita.
- Ihmisellä on viimeinen päätösvalta asioita.
- Robottiin pitää voida luottaa.
- On selvää, kummalla on kulloinkin kontrolli.
- Kontrollin vaihto on luotettava.
- Robotin käyttö yksinkertaistaa systeemiä käyttäjälle.
- Robotin toiminta sopii käyttäjän mentaalimalliin.
- Robotti viestii kuhunkin tilanteeseen ja olosuhteisiin sopivalla tavalla.
- Robotti ei vie ihmisen huomiota tehtävästä.
- Robotti toimii kaikissa olosuhteissa (vrt. automaattibussi, joka ei toimi, kun tiellä on lunta...)

Testausta eri tasoilla

- Ohjelmistojen osalta tyypillinen jäsenitys yksikkö-integrointi-järjestelmä-hyväksymistestaus-jako.
- Sensorit ja toimilaitteet – logiikka – käyttäytyminen.
- Yksi laite – laiteparit – laiteparvi.
- Tarkkuus, voima – nopeus, sujuvuus – kyvykkyys skenaarioissa ja käyttötapauksissa.
- Asian eristetty yksinkertainen testaus – yksinkertainen tilanne yhdistettynä muihin elementteihin tai toimijoihin – monimutkainen vuorovaikutustilanne.
- Paikallinen toiminta – paikallinen alue / konteksti / verkko – globaali tilanne.
- Ohjelmisto – ohjelmiston ja raudan yhteistoiminta (ml. käyttöliittymä) – kokonaistuote.

Hajoita ja hallitse testauskohde teknisesti

- Systemin eri elementit.
 - Sensorit – tunnistamisen rajat.
 - Datan luokittelija – oikeellisuus, luotettavuus...
 - Logiikka – päätteleekö äly oikein kaikissa tilanteissa.
 - Eri elementeille voi olla erilaisia lähestymistapoja. Päättelyn malleille validointi, sensoreille fuzzaus.
- Kokonaisjärjestelmä teknisesti ja datan kannalta.
 - End to end skenaariot, käyttötapaukset.
- Ihminen-tekniikka -järjestelmän analysointi ja testaus.
 - Työn analyysi.
 - Käytettävyys- ja käyttökokemus.
 - Riskianalyysi.

Hajoita ja hallitse tyyli älyn osa-alueittain 1/2

Osa-alue	Testattavia asioita
Logiikka ja kognitio	Tietojen käsittelyn oikeellisuus
Käyttäytyminen	Tilanteiden hallinta – normaalit tilanteet, poikkeustilanteet, vaaratilanteet Toiminta eettisiä valintoja edellyttävissä tilanteissa
Toiminta työssä	Tavoitteen ymmärtäminen ja säilyttäminen Työnkulun kokonaisuuden hallinta
Kommunikointi	Syötteiden ymmärtäminen Viestintä ulospäin Dialogin hallinta
Aistit	Sensorien tunnistuskyky, tarkkuus, robustius datalle ja olosuhteille

Hajoita ja hallitse tyyli älyn osa-alueittain 2/2

Osa-alue	Testattavia asioita
Luonne	Vuorovaikutustyylin sopivuus ihmiselle, kontekstiin, kulttuuriin
Roolin ottaminen	Sopiva rooli tehtävässä – apulainen, vastuullinen, tietotuki
Oppiminen	Opitun oikeellisuus Opetettavuus
Reflektointikyky	Tekemisen selittäminen, perustelu
Tietopohja (katselmointi)	Mitä tietoja hyödyntää – tietokannat, tiedonkeruu, asiantuntijoilta kerätyt säännöt
Ratkaisujen metataso (katselmointi)	Perusteet älytason ja muun konseptin valinnalle

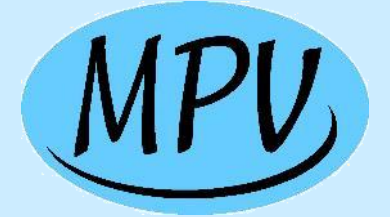
Epädeterministinen monitoimijaympäristö 1/2

- Kun robotti toimii ympäristönsä tekniikan kanssa, asiat tapahtuvat samanaikaisesti, epädeterministisellä tavalla.
- Järjestelmä on tuntematon ja muuttuu – uusia laitteita, ihmisiä ja robotteja.
- Osanottajat kommunikoivat monilla erilaisilla tavoilla ja niillä saattaa olla eri rooleja eri toiminnoissa.
- Jotkut saattavat olla vihamielisiä ja niiden luotettavuus on tuntematon.
- "Vainoharhaisia" turvallisuus- ja luotettavuusstrategioita järjestelmien suunnittelussa ja testauksessa

Epädeterministinen monitoimijaympäristö 2/2

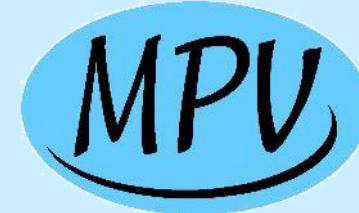
- Mietittävä kokonaissysteemin skenaarioita – miten eri toimijat toimivat, miten muut reagoivat niiden toimintaan, miten robotti hallitsee erilaiset kokonaisuuden poikkeamat.
 - Tehtävä poikkeamatarkasteluja ja luotettavuusanalyysijä.
 - Testauksen lähtökohta on älykäs skenaarioiden manuaalinen tutkiva testaus.
- Testiautomaatio edellyttää kokonaisjärjestelmän mallia, jonka avulla voidaan kokonaisuutta ”pommittaa” erilaisilla vuorovaikutuksilla
- Yksinkertaisemmassa muodossa ja käsitteistössä tämä on yhdessätoimivuus- ja yhteensopivuustestausta.

Älyn testaamisen haasteita 1/3



- Mitä älykkäämpi systeemi on, sitä mielenkiintoisia ilmiöitä ja ongelmia sillä on.
- Testauksessa pitää ajatella inhimillisiä virheitä – miten tekoäly voi tehdä niitä.
- Jos ja kun äly on ihmisen tukena, sen pitää löytää sopiva auttajan rooli. Äly on parhaimmillaan silloin, kun sitä ei huomaa!
- Älyn odotetaan osaavan perustella tekemisensä. Jos se ei onnistu, logiikan selvittämisessä on työtä.

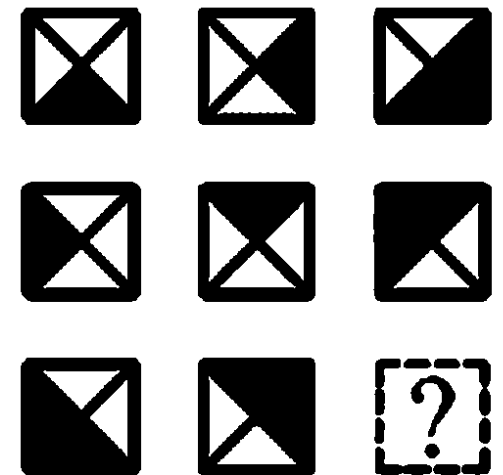
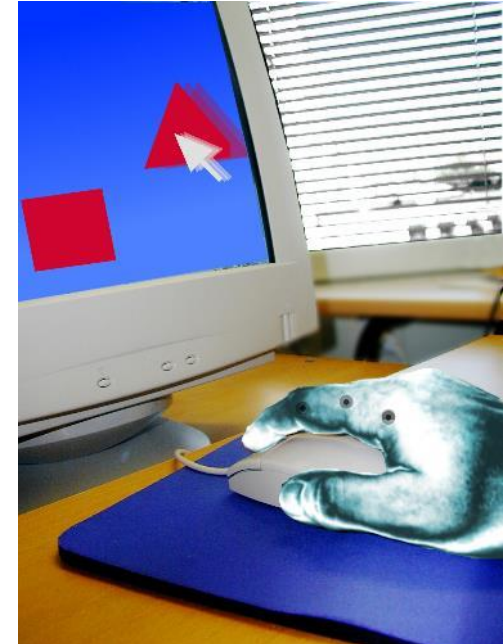
```
AssertEquals(AI.Ask("What is the meaning of life?"), "42");
```



TEKOÄLYN TESTAAMISESTA

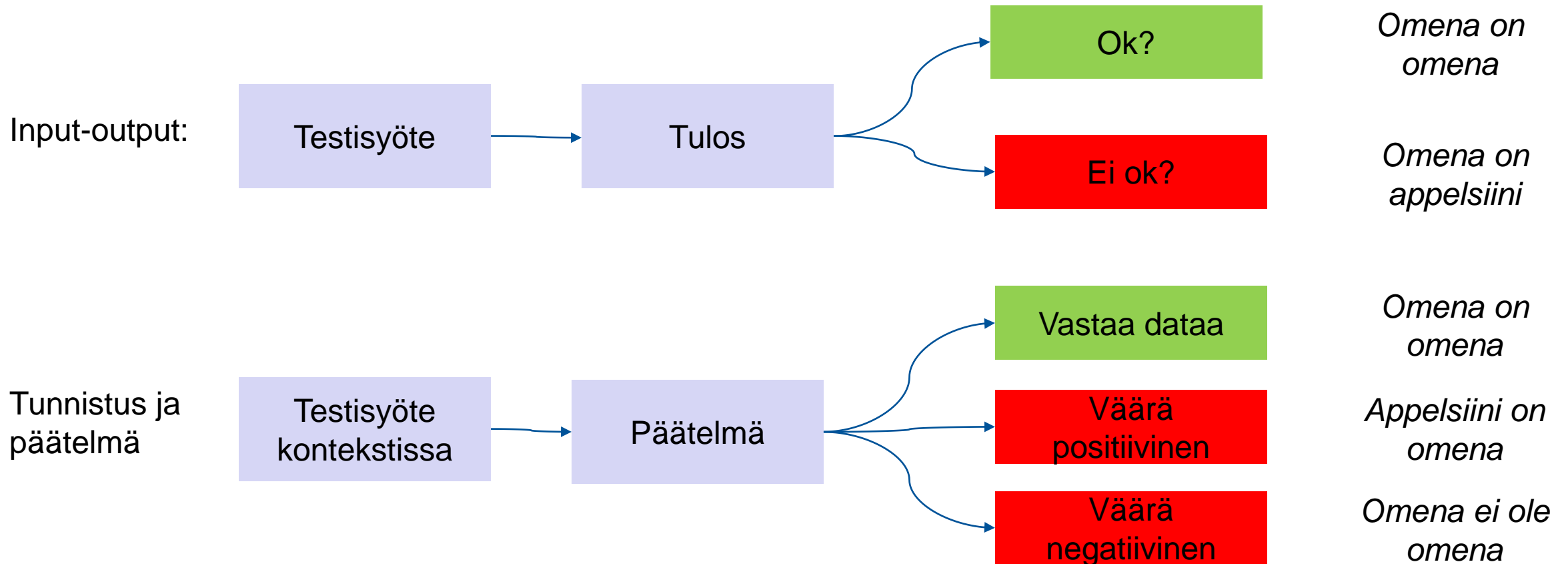
Älyn testaamisen haasteita 2/3

- Perinteisille systeemeille kerrotaan käytössä ja testauksessa asiat eksaktisti.
- Älykkäille asiat näytetään ja asiat eivät ole eksakteja, vaan kaikella on todennäköisyys.
 - Tunnistettiinko potilas oikein, onko nyt kodissa ”pimeä”.
- Normaalien systeemien logiikka voi täydentyä ja sitä voidaan tietoisesti muuttaa, mutta älykkään oppivan systeemin käyttäytyminen muuttuu huomaamatta opettamisen/oppimisen myötä.



Älyn testaamisen haasteita 3/3

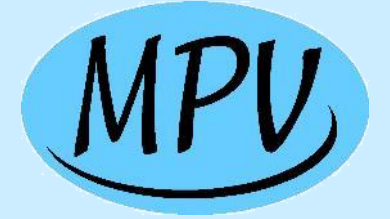
- Tieteellisempään havaintojen tulkintaan



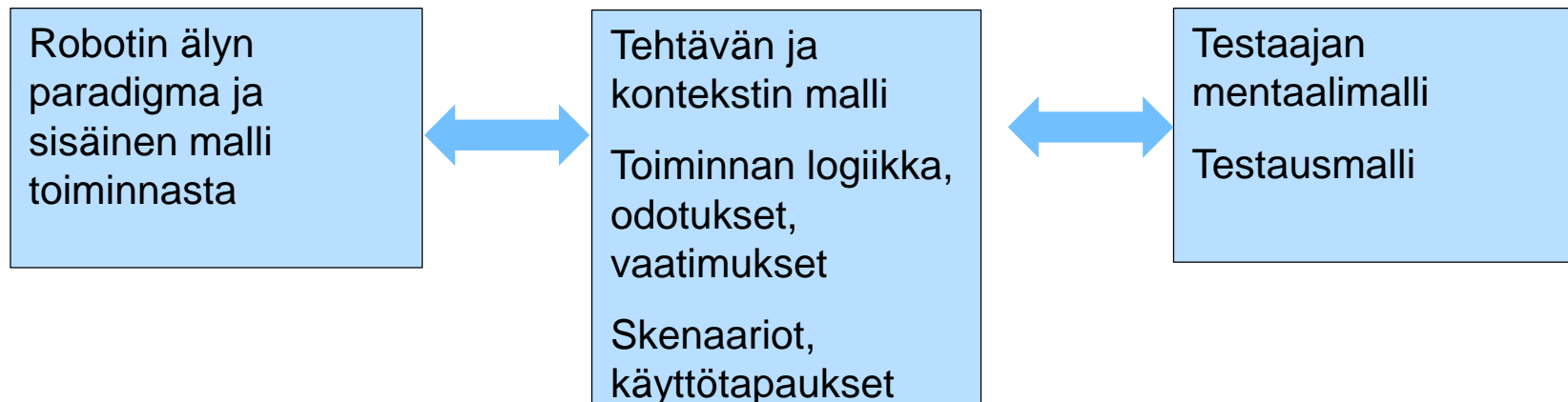
Älyn toimintalogiikan selvittäminen

- Ensimmäinen haaste on selvittää tutkivalla testauksella se logiikka, jolla systeemin äly toimii oikeasti.
- Mahdollisimman avoimia testiskenaarioita, jotta älyllä on liikkumavaraa.
- Älykästä järjestelmää ei saa kunnioittaa, vaan se pitää laittaa koville, ongelmiin ja umpikujiin. Tarvitaan lähes psykologin ajattelua.
- Olosuhteita, syötteitä ja muuta vaihtelemalla selviää, miten systeemi toimii.
- Perinteiset testaustekniikat, kuten päätöspuut, ekvivalenttiositus, raja-arvoanalyysi yms. ovat tärkeitä.

Testauksen kohteena käyttäytyminen suhteessa odotuksiin



- Testaajan ei järjestelmätasolla tarvitse tietää älykkyyden mekanismeista. Testauksen kohteena ei olekaan "robotti" tai "äly", vaan käyttäytyminen.
- Ei tarvitse tuntea robotin sisäistä logiikkaa, vaan löytää hyviä testimalleja.
- Järjestelmätestaus ratkaisee. Se on systeemin validoinnin taso.

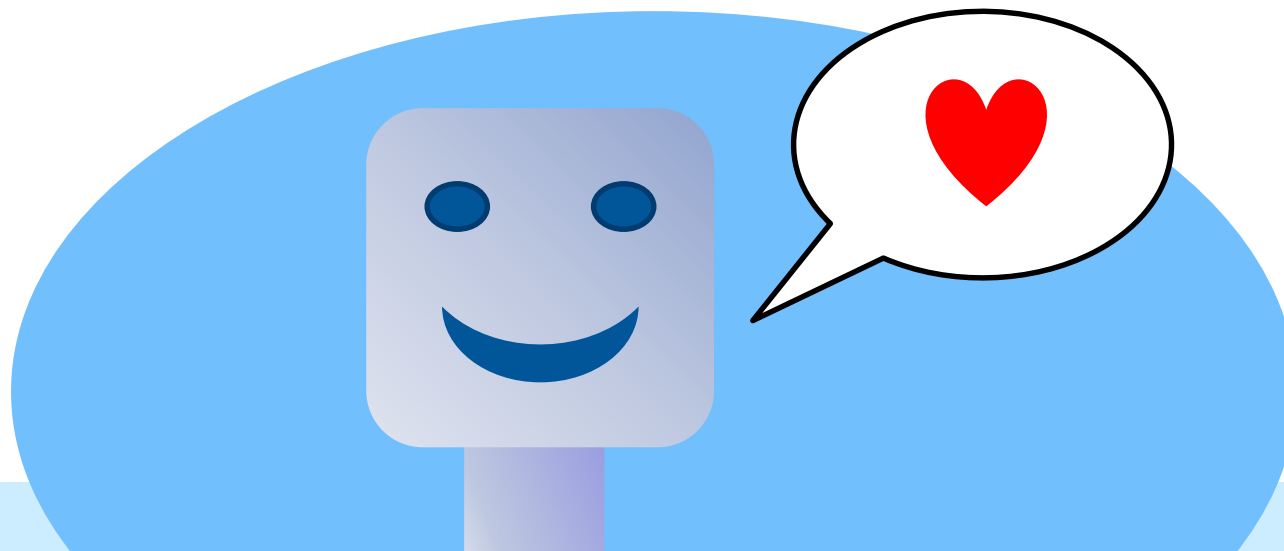


Onko äly sellaista kuin ihmisellä?

- Neuromorphisten tietokoneiden kehittäjät pyrkivät kehittämään ”koneaivoja”, jotka matkivat ihmisiä ja samalla edellytyksiä samankaltaiselle älylle.
- Miksei äly voi olla jotain ihan muunlaista?
- ...Sitä se tulee olemaankin...
- Testauksessa ei ainakaan pidä tehdä oletuksia.

Äly psykologisena haasteena

- Testaajat ovat ihmisiä – psykologia.
- Vaarana ihmetys, kunnioitus, huolenpito – hyvän testauksen vihollisia.
- Hyvän testauksen pitäisi tähdätä ohjelmiston rikkomiseen Ei saa välittää sen hyvinvoinnista.
- Mitä älykkäämpi systeemi on ja mitä enemmän se vaikuttaa inhimilliseltä, sitä enemmän sitä pitää tietoisesti koetella testauksessa.

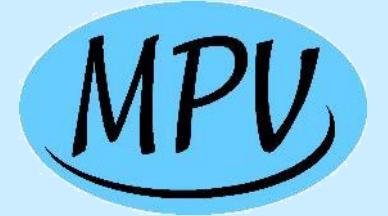


Älyn testattavuus – lokitus tärkeää

- Testattavuus on ikuinen ongelma...
- Koska on järkevää testata eri elementtejä erikseen, on huolehdittava testattavuudesta.
 - Esimerkiksi sensorien ja datan luokittelijoiden testaus erikseen ja yhdessä: tunnistetaanko kuvassa olevat asiat oikein? Muuten ei älyssä ole mitään tolkkua...
- Lokitusmahdollisuus on osa testattavuutta.
 - Koska tekoäly kaipaa paljon dataa on luonnollista, että dataa käyttäväkin systeemi tuottaa sitä ja tarjoaa sitä ulospäin.
 - Toimenpiteiden perustelu selväkielisesti on huipputärkeää lokitusta – sellaisesta lokista voi selvittää, miten äly tunnistasi ja tulkitse tilanteen ja miten toimenpiteet syntyivät.

Testidata suunniteltava huolella

- Opetusdata vs. testidata.
 - Jos testataan opetusdatalla, mitä se kertoo?
 - Regressiotestauksessa relevanttia.
 - ...Oppiessa suhde aiemmin kohdattuun dataan muuttuu...
- Datan merkitys korostuu:
 - Realismi.
 - Rikkinäinen, puuttuvan datan hallinta.
 - Toiminnon estävä data.
 - Robustius datan siivoukselle.
- => Datapohjainen testaus, fuzz-testaus oleellista.



- Äly tarvitsee dataa. Mitä tapahtuu jos:
 - Datalähde menee rikki ja dataa ei tule.
 - Data on väärää, faktuaalisesti virheellistä.
 - Datasta puuttuu asioita.
 - Dataformaatti on rikki.
 - Dataa on liian vähän.
 - Dataa on valtavasti.
 - Data on vinoutunut.
 - Data on väärästä lähteestä.
 - Datan lokalisointi on väärä.

TESTITYYPPEJÄ

Olennaisia testityyppejä lyhyesti 1/4

- Robottikonseptin arviointi.
 - Hyvien konseptien löytäminen on vaikeaa. Konseptin kriittinen arviointi on tärkeää.
 - Mihin uudesta ideasta on? Vertailu vastaaviin ja nykyiseen tilanteeseen. Onko se vaivan ja kustannusten arvoinen?
 - Kenelle, mihin kontekstiin? Vastaako tarvetta (toiminta, käyttäjät, markkinat)? Haluttavuus? Toimivuus käytännössä? Riskit? Teknologia? Eettisyys? Jne...
 - Sopivuus kulttuuriin.
 - Kokeilut apuna. Analyysi. Tarkistuslistat.

Olennaisia testityyppejä lyhyesti 2/4

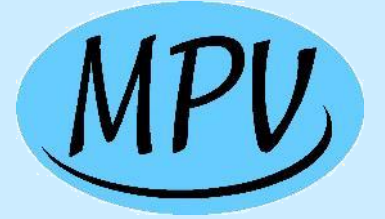
- Käytettävyys- ja käyttäjäkokemuksen testaus.
 - Ihminen-tekoäly-kokonaisuuden arviointi ja testaus.
 - Tarvitaan osaavia ammattilaisia. Toiminnallisen testauksen perinne ei riitä.
 - Eri kehitysvaiheissa: alussa ideoita, myöhemmin niiden validointia.
 - Käyttäjäkokemus ja käytettävyys.
 - Työanalyysi osa laadun arviointia.
 - Analyttiset arvioinnit. Tarkistuslistat.

Olennaisia testityyppejä lyhyesti 3/4

- Riski- ja luotettavuusanalyysit.
 - Riskianalyysi oleellinen disruptiivisille tuotteille. ”Mikä voisi mennä pieleen...”.
 - Kohteena työjärjestelmä, kokonaistuote, arkkitehtuuri, logiikka, data... Siis kaikilla tasoilla.
 - Luotettavuusanalyysi tarpeen, koska kokonaissysteemin teknologia monimutkaista.
 - => Tietoa kokeelliseen testaukseen.
- Tietoturvatestaus.
 - Lähtökohtana tietoriskianalyysi.
 - Mitä tietoa älysteemi käyttää, tuottaa; mitä on varjeltava.
 - Kokonaisuus ja sen eri elementit ja näkökulmat.

Olennaisia testityyppejä lyhyesti 4/4

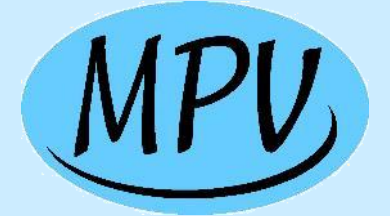
- Robottijärjestelmän toiminnallisuustestaus.
 - Järjestelmän eri elementeille, eri abstraktiotasoisille.
 - Tutkiva testaus, datatestaus.
 - **Hyvä uutinen: Järjestelmätasolla / ulkoisen käyttäytymisen tasolla ei edelleenkään tarvitse tuntea tekoälykomponenttien sisäisiä detaljeja (miten se hermoverkko toimii) – sen ymmärtäminen voi jäädä hermoverkkopalikan kehittäjälle.**



- Kun äly on ihmisen auttaja, on testauksen kohteena äly-ihminen -systemi ja ihmisen ja älyn suhde.
- Perinteinen arviointitapa on kaksiosainen:
 - 1) Analyysi:
 - Heuristinen arviointi.
 - Työn analyysi – tehtävän / skenaarion analysointi vaiheittain.
 - Tarkistuslistojen käyttö – konseptitasolta detaljeihin.
 - 2) Käytettävyytestaus.

- Käytettävyytestaus:
 - Ohjattu skenaario, jota koehenkilö toteuttaa.
 - Seurataan koehenkilöä ja tehdään havaintoja.
 - Koehenkilö ääneenajattelee tunteuksiaan. Muut ovat hiljaa.
- Aluksi ja lopuksi haastattelu.
- Sitten havaintojen analysointi.

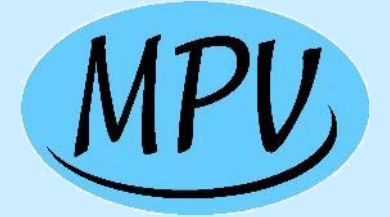
- Ks. Käyttöliittymien kehittämisen työkalupakki
- <http://www.mattivuori.net/julkaisuluettelo/liitteet/tk-doit.pdf>



- Jens Rasmussenin jako:
 - Lipsahdukset: Taitopohjaiset virheet – tekoäly painaa vahingossa väärää nappia. Sensorivirheitä yms...
 - Sääntöpohjaiset virheet: Tuttujen tilanteiden sääntöihin liittyvät. Väärän säännön valinta, virheet säännöissä, vanhentunut sääntö jne... Olennaisia, kun systeemi perustuu staattisiin sääntöihin.
 - Tietopohjaiset virheet. Kun tekoäly joutuu ei-rutiinitilanteessa päättelemään, esim. hakee big datan perusteella potentiaalisimman vaihtoehdon toimenpiteelleen. Olennainen virhetyyppi. Oppiminen muuttaa toimintaa.

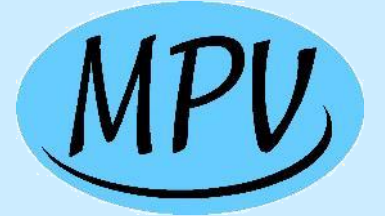
Inhimilliset virheet 2/2

- ”Toimintovirheet”, jotka liittyvät älyn tulkintavirheisiin ja ajoitukseen – älykäs voi olla hidas. Olennaisia roboteille:
 - Tehdään väärälle kohteelle (väärä tunnistus).
 - Jätetään jokin asia tekemättä.
 - Tehdään jotain ylimääräistä.
 - Tehdään kaksi kertaa.
 - Tehdään liian aikaisin.
 - Tehdään liian myöhään.
 - Yritetään tehdä, mutta epäonnistutaan.
- Tällaisia pitää testata sopivilla testeillä.



- Työtiimin konseptin tarkastelu
 - Työtiimin konsepti - toimintajärjestelmän kolmiomalli: tekijät, välineet, kohde, normit, yhteistyö, työnjako
 - Uuden toimijan vaikutukset
 - Robotin sosiaaliset vaikutukset jml.tekniikan inhimillistäminen
- Riskilajit
 - Työturvallisuus
 - Keskeytysriskit
 - Tietoriskit
 - Sosiaaliset riskit

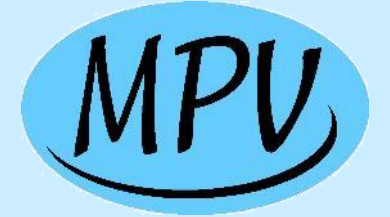
Älysteemien matalan tason riskianalyysin kysymyksiä (sampler)



- Toimii väärin?
 - Kokonaisjärjestelmän tasolla mietittävä.
- Muutokset:
 - Älylähde vaihdetaan toiseen?
 - Datalähde vaihdetaan toiseen?
- Väärinkäyttö:
 - Älyn käyttö väärään tarkoitukseen?
 - Älyn väärinopettaminen?
- Tilanteet:
 - Älyn toiminta poikkeustilanteissa?
 - Älyn käyttö eri kontekstissa?
 - Muutokset kontekstissa – toimijat, olosuhteet, välineet...
- Sabotaasi

Tietoturvatestausta

Taso	Älykkään systeemin erityispiirteitä
Yleistä	Ei ole "AI OWASP"ia → pitää itse soveltaa ja tunnistaa systeemin mahdollisia haavoittuvuuksia.
Data	Tietosuoja ja data omistajuus vaikuttavat testattaviin asioihin.
Käyttäytyminen ja	Implisiittinen käyttäjän tunnistaminen (käyttäjän "tapa olla ja tehdä") eksplisiittisen sijaan. Ei saa tulla virheitä -> testattava sen robustius. Testattava pääsy opetustilaan ja opetusdatan lataus.
Arkkitehtuuri	Lisää uhkapinta-alaa uusista komponenteista ja datasta.
Matalan tason design, toteutus	Erilainen koodi: C++-koodia voidaan tarkastaa, katselmoida, mutta opetetulle hermoverkolle se on vaikeaa. Kehittäjät tekevät uudenlaisia ongelmia...



- Turvallisuuskriittisen laitteen ”turvallisuuselinkaari” vaarojen ja mahdollisten ongelmien tunnistamisesta suunnittelun kautta kokonaisjärjestelmän validointiin.
- Erotetaan robotin toiminnallinen järjestelmä ja turvajärjestelmät.
- Turvallisuusstandardit antavat hyviä ohjeita turvallisuuden suunnitteluun ja testaukseen: riskien tunnistaminen, luotettavuusanalyysit, teknisen alustan robustius, kokonaisuuden turvallisuus validoidaan kattavilla testeillä.
- Tahallinen väärinkäyttö oleellista! Huomioon otto, estäminen.
Humanoidirobotit laitetaan väistämättä tekemään kaikenlaista omistuiista.

Arkkitehtuurin arviointi ja teknologioiden valinta

- Arkkitehtuurin arviointi on tärkeää, kun on vaihtoehtoja, kun systeemi on uudenlainen, kun on tiedossa muutoksia...
 - Älysystemit ovat juuri tällaisia.
- Arvioinnin ei tarvitse olla raskas. Nopea skenaarioiden arviointi:
 - Älyn toteutuksen vaihto.
 - Datalähteen vaihtaminen.
 - Uutta dataa.
 - Jne...
 - ... Kaikki perinteiset järjestelmien muutos-skenaariot.
- Arviointi tukee systeemin komponenttien valintaa – ml. oikeanlaisen älymoottorin valinta


Turvallisuuskriittisten systeemien arkkitehtuuri

- Haasteista johtuen oppiva äly on hyvä pitää operatiivisessa järjestelmässä ja sen arkkitehtuurissa.
 - Käsitteellisesti, rakenteellisesti ja toiminnallisesti.
- Varsinaisia virallisia turvatoimia hoitaa tyhmä, muuttumaton järjestelmä.
- Äly voi tietysti tehdä operatiivisessa systeemissä ennakoivaa turvallisuustyötä.
- Tämä helpottaa systeemin validointia ja sertifiointia.
- Selkeä sääntöpohjainen äly, joka voidaan vaikka katselmoida, on helpoimpi tapaus.

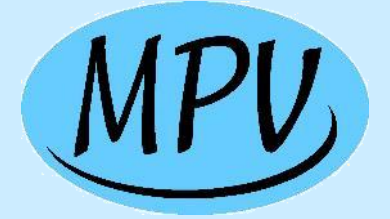
Oppimisen testaus

- Osa älyä voi olla oppimiskyky. Testauksella pitää selvittää, että senkin mekanismit toimivat. Että äly:
 - Oppii oikeita asioita.
 - Oppii ne oikein.
 - Ei opi vaarallisia asioita.
 - Varmistaa oppimisensa käyttäjältä tarpeen mukaan.
 - Omasta älystään huolimatta tottelee käyttäjää.

Oppiminen testauksen ongelmana

- Oppiva systeemi oppii testatessakin! 
- Jos testataan live-systeemiä, vaikutus ei ole hallittu eikä toivottu.
 - Varsinkin, jos tehdään tiheästi automaattitestausta.
- Systeemi pitää siis joko kopioida testaukseen tai estää sen oppiminen testauksen ajaksi.

Oppivan turvallisuuskriittisen systeemin kaksi ongelmaa



- Laitteet ovat vaarallisimmillaan poikkeus- ja häiriötilanteissa. Ne pitää testatakin kunnolla.
 - Käyttäytyminen sellaisissa voidaan ohjelmoida, mutta entä jos käyttäytyminen syntyy opettamalla? Jaksetaanko niiden opettamiseen panostaa?
 - Turvajärjestelmän merkitys korostuu, mutta tilanne ei ole helppo.
- Tietty konfiguraatio validoidaan testaamalla, mutta mikä merkitys on tietyn oppimistason validointitesteillä, kun robotin oppiminen muuttaa käyttäytymistä?

Tietoturvallisuus

- Erilaisia verkkoja.
- Dynaaminen laitteiden verkko.
- Tietoturvallisuuden arviointi ja testaus ei sinänsä eroa juurikaan muiden ”mobiilien” järjestelmien vastaavasta.
- Älykäs robotti on kuitenkin aktiivinen ja informaatiointensiivinen ja voi älykkyytensä vuoksi tehdä kaikkea ”mielenkiintoista”.
- Älylaite voi aina vakoilla ihmisiä ja ympäristöä.
- Sille annetut oikeudet ja niiden noudattaminen.
- OWASP Mobile Project on hyödyllistä tutustuttavaa
- https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

”Etiikan” testaus

- Viime aikoina on ollut esillä tekoälyn etiikka.
 - Autonomisen robotin suhde ihmiseen: voidaanko se esimerkiksi opettaa vahingoittamaan ihmistä? Ja milloin? Mitä kaikkea robotti saa tehdä pelastaakseen ihmisen?
 - Jos autolla on valittavana törmäys lapsiin tai vanhuksiin, kumman se tekee?
- Tällaisenkin käyttäytymisen testaus tulee jossain vaiheessa vastaan.
 - Pitää pystyä simuloimaan kaikkia tilanteita
- (Tietynlaista sääntöpohjaista tehtävään sidottua käyttäytymistä ei vielä voida pitää etiikkana, siksi lainausmerkit.)
- Etiikassa on usein kyse robottisysteemin valmistajan etiikasta tai sen hyödyntäjän etiikasta.

Robotin olosuhdetestaus

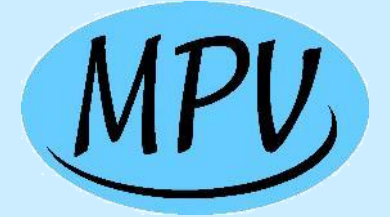
- Toimivuus vaikkapa niiden eri aistien kannalta haastavissa olosuhteissa: heikko valaistus, vastavallo, melu, erilaiset lattiaratkaisut jne...
- Ja tietysti kaikkien niiden vaihtelu.
- Esimerkiksi hahmontunnistus on ongelmallinen, jos se ei toimi luotettavasti hämärässä, vaan tuottaa vääriä tulkintoja tai taustamelu haittaa äänikomentoja.

Tuotantotestaus

- Älykkyyden kulttuuriin sopii se, että käytössä kaikki tapahtumat logitetaan ja:
 - Logeista tunnistetaan ongelmia ja viestitään tuotekehitykselle korjaustarpeet.
 - Logeista opitaan käyttöprofiileja, joita käytetään suunnittelussa ja testauksessa.
- Ongelmien tunnistus:
 - Poikkeus testimallista.
 - Poikkeus datassa jo olevista profiileista.
 - Asserttien laukeaminen, poikkeusten heitto.
 - Prosessorin kuormitus, toiminnon nopeus.
 - Jne...

Kooste testauksen haasteita 1/5

Element	Test types (most essential)	Special challenges
Overall system (robot in action, in environment, in collaboration, as part of systems).	Concept testing (analysis, simulation, mock-ups).	Validating that the robot concept is best one for the context, goals. Validating that the robot has a cultural fit to where it will operate.
	Functional testing.	For automated testing: Environment simulation, programmatically created user gestures, voice commands... For MBT: Modelling of environment (elements and behaviour) – including devices and humans. Use cases / stories for both humans and the robot. Exploratory testing important due to complexity. Testing the operating logic in a simulated environment vs. testing the physical robot in the real world. Changing environment setup. Need a paranoid approach to how other system elements behave.

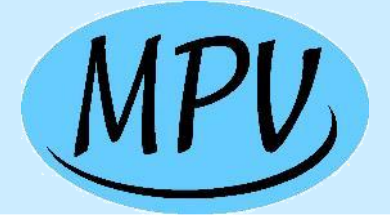


Kooste testauksen haasteita 2/5

Element	Test types (most essential)	Special challenges
	Safety testing.	Need a thorough risk / safety analysis for basis. Testing requirements from safety standards – advocate advanced techniques, such as MBT. Safety is related to security too – dangerous remote control...
	Security testing.	Low level of trust in any system elements.
	(Regulatory) validation testing.	Uncertainty of the regulations and their interpretation, uncertainty of what standards are applicable.
	Performance / capability testing.	–
	Compatibility, co-existence testing.	Testing of the diverse technologies and variations in the collaborating environment.
	User experience testing.	Need to assess overall relation between human & robot – is as planned?

Kooste testauksen haasteita 3/5

Element	Test types (most essential)	Special challenges
	Localization testing.	Whole behaviour, meaning of control gestures, behavioural rules – it can really be cultural testing of cultural fit (by no means checking of translations...).
	Upgradeability.	Testing of updating software or hardware.
Control system	Functional testing.	Testing of movement in practical spaces.
	Reliability testing.	Reliability analysis as basis.
Intelligence systems	Testing of logic, decisions.	All deviations, non-determinism, context data.
Sensory system (perception system)	Functional testing.	(Depends on sensor). Variation on input – gestures, sound, ambience...
	Reliability testing – defective sensor etc...	–



Kooste testauksen haasteita 4/5

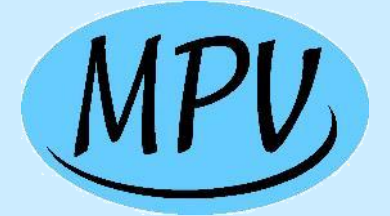
Element	Test types (most essential)	Special challenges
Safety system	Functional safety testing.	Testing requirements from safety standards (such as SFS-EN 61508 series) – can be very demanding! Needs safety / reliability analysis for basis.
Communications system (technical)	Functional testing.	–
	Reliability testing.	–
	Performance testing.	Including load, stress testing.
	Security testing.	–
Human interface (user)	Usability testing, analysis.	The new ways of interaction can be difficult to validate.
	Analysis and testing of human errors.	Must test for human errors thoroughly (voice, gesture commands).
	Obedience testing.	Who is in control, when many humans are present (or TV is on).
	Functional testing.	Exploratory testing is critical – need to have almost a “psychological” approach.

Kooste testauksen haasteita 5/5

Element	Test types (most essential)	Special challenges
Human interface (programming & configuration)	(As for user interface).	
	Security testing.	Who can program / configure? Consider remote control.

Ylläpidettävyyden testaus

- Menneen ajan jäykkien sääntöpohjaisten järjestelmien iso ongelma oli ylläpidettävyys. Kun sääntöjä, dataa pitää muuttaa, se ei ole helppoa.
- Uusillekin järjestelmille voi olla, että ”Siperia opettaa...”.
- Ylläpidettävyyttä perinteisesti vain arvioidaan ja katselmoidaan, mutta sitä kannattaa testata:
 - Miten helppoa on opettaa systeemille uutta logiikkaa ja opettaa se pois vanhasta? Pitääkö opittu pyyhkiä kokonaan pois?
- Ylläpidettävyyteen liittyy myös siirrettävyys ja vaikka komponenttien vaihdettavuus, kun sopivampia (tai halvempia) tulee tarjolle.



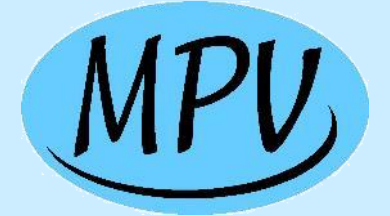
OSAAMISPALETIN MUUTOKSIA

Osaamishaasteita

Testausalue	Osaamisalue
Fyysinen toiminta, toimilaitteet ja sensorit	Teollisuusautomaatio
Turvallisuus	
Tuotekonseptit	Teollinen muotoilu
Kulttuurinen sopivuus	Käyttökokemussuunnittelu
Käyttötavat	
Käyttöliittymät	
Käyttäjäkokemus	
Ohjelmistotekniikka	Tietotekniikka
Datan käsittely	
Tietoverkot	
Tietoturvallisuus	Tietoturvallisuus
Äly	Tekoäly

Tarvittavissa kompetensseissa muutoksia

- Uudenlaisia testaajakompetensseja:
 - Koesuunnittelu – monipuolisia, päteviä koeasetelmia.
 - Datatiedemiehen osaaminen.
 - Sensoriosaaminen.
 - Luotettavuustekninen osaaminen.
 - Jne...



YHTEENVETO

Kymmenkunta nyrkkisääntöä 1/3

- Humanoidirobotti on uudenlainen elementti työjärjestelmässä ja siksi sen arviointi pitää olla poikkeuksellisen kattavaa.
 - Kaikki teknologian elementit.
 - Työjärjestelmän piirteet.
 - Sosiaalisen systeemin arviointi.
- “Laadunvarmistus” liittyy robottiin sinänsä ja sen toimintaan työpaikan kontekstissa. Niinpä hyödyntäjillä on iso vastuu tekemistensä arvioinnissa osana työjärjestelmän suunnittelua ja hankintoja.
- Konseptin arviointi – miten se sopii toimintaympäristöönsä – ja käyttökokemuksen testaus ovat elintärkeitä.

Kymmenkunta nyrkkisääntöä 2/3

- Robotin älyä ja ihmismäisiä piirteitä ei saa kunnioittaa testauksessa. Robotti pitää laittaa koville ja sen ohjelmisto ”rikkoa”. (Fyysistä robottia ei kannata kovin rikkoa kovin usein.)
- Robottijärjestelmä on monimutkainen, mutta testaajan logiikka pitää testauksen ymmärrettävänä ja riittävän yksinkertaisena.
- Testaustilanteesta riippuen voidaan löytää erilaisia testaustasoja, joiden soveltaminen pitää testauksen hallittuna ja auttaa luomaan robustin alustan robotin älylle.
- Ensin pitää testauksen avulla ymmärtää, mitä ollaan testaamassa. Tutkiva testaus voi edellyttää lähes psykologin otetta selvittäessään robotin käyttäytymistä.
- On ymmärrettävä robotin turvallisuustaso ja sovitettava testaus tasoa vastaaviin vaatimuksiin.

Kymmenkunta nyrkkisääntöä 3/3

- Turvallisuus- ja luotettavuusanalyysit ovat tärkeitä, koska uusia konsepteja ei aina ymmärretä. Tahallisen väärinkäytön mahdollisuudet on tunnistettava ja niiden estomekanismit testattava.
- Tietoturvallisuutta ei saa unohtaa robottituotteissakaan.
- Ihmisenkaltaisissa roboteissa on poikkeuksellisen paljon testaushaasteita ja niiden ratkomiseen tarvitaan monipuolista osaamista ja erilaisia osaajia.
- Jokaiseen robottituotekehitystilanteeseen pitää suhtautua ajatuksella, että ensin pitää unohtaa tekniikan detaljit ja selvittää mistä asiassa on kyse kokonaisuuden kannalta.