Luotettavuuden kokonaiskuva

Ilkka Norros ja Urho Pulkkinen

Rakenne

1. Luotettavuusvaatimukset
2. Luotettavuuden mallintamisesta
3. Dependability Case –menetelmä
4. Johtopäätöksiä ja ehdotuksia

Luotettavuusvaatimukset

IP:n realisoima globaali datapakettien siirtopalvelu on uusi geneerinen media, joka on tullut jäädäkseen

Monien IP-sovellusten kehityskulku:

IP-yhteyden tarkoituksenmukaiset luotettavuusvaatimukset ovat erilaisia riippuen

- sovelluksen kriittisyydestä käyttäjälle
- vaihtoehtoisten yhteyksien tai palvelujen tarjolla olosta
- yhteyden hinnasta

Laatu ja luotettavuus

- IP-median luotettavuuskysymys on ensisijassa kvalitatiivinen: kulkevatko paketit A:sta B:hen vai eivät?
- Palvelunlaatu on saman asian kvantitatiivinen puoli: miten tiuhaan paketteja voi lähettää niin että ne menevät perille?
- Lähes kaikki sovellukset vaativat käytännössä jonkinlaista palvelunlaatua – käyttäjä toivoo voivansa luottaa myös tietynasteiseen laatuun
- Laadun ja luotettavuuden muodostama kokonaisuus on pidettävä käsitteellisesti selkeänä ja eriteltynä
- Loppukäyttäjälle tarjoutuvan huippulaadun ja huippuluotettavuuden yhdistäminen IP-tekniikalla on joka tapauksessa vaikea yhtälö

Luotettavuuden mallintaminen

- Globaali IP-infrastruktuuri on valtava heterogeeninen ja orgaanisesti kehittyvä kokonaisuus, jonka tarjoaman palvelun luotettavuutta ei voi tutkia eikä mallintaa puhtaasti ”annettuna” teknisenä systeeminä

- Analyysit ovat kuitenkin mahdollisia ja hyödyllisiä, kun ne

  - rajataan hyvin valittuihin osasysteemeihin, kuten esim.
    - topologinen redundanssi, varmistukset ja suojaukset
    - protokollien robustisuus, ohjelmistovirheet, tietoturva
    - operoivan henkilöstön toiminta

  - liitetään luotettavuuden kokonaiskuvaan:
    erilaatuiset välttämättömät osatekijät ovat ”sarjaan kytkettyjä”:
    luotettavuus on kokonaisuus, jossa heikoin lenkki dominoi!

- Perinteiset luotettavuusmallit soveltuvat verkon fyysisen rakenteen tarkasteluun
  - fyysisen rakenteen tarkastelu analogista minkä tahansa järjestelmän analyysin kanssa (esim. sähköverkot ja voimalaitokset)
  - komponenttien luotettavuustarkastelu mahdollista; luotettavuusdataa laitteistoista on saatavilla tai kerättävissä
  - access-verkot puumaisia → tarkastelu helppoa
  - core-verkot aitoja verkkoja → tarkastelu teknisesti vaikeampaa
  - core-verkkoja isommat kokonaisuudet hankalia tarkasti mallinnettaviksi
- Myös ohjelmistovirheiden ja inhimillisten virheiden analyysiin on olemassa muilla aloilla kehitettyjä lähestymistapoja työn lähtökohdaksi
- Toimivia dynaamisten ilmiöiden luotettavuusmallinnusmenetelmiä ei ole

Luotettavuusmallien käyttötarkoituksia

- Luotettavuusindeksien määrittely
- Verkon rakenteiden (luotettavuus)optimointi
- Verkon suunnittelun tukeminen
- Verkon kunnossapidon ja uusinnan suunnittelu
- Luotettavuuden mittaaminen ja arvioiminen eri näkökulmista:
  - käyttäjät
  - laitetoimittajat
  - suunnittelijat
  - operaattorit
  - viranomaiset
- Luotettavuuden parantamisen kustannusten arviointi

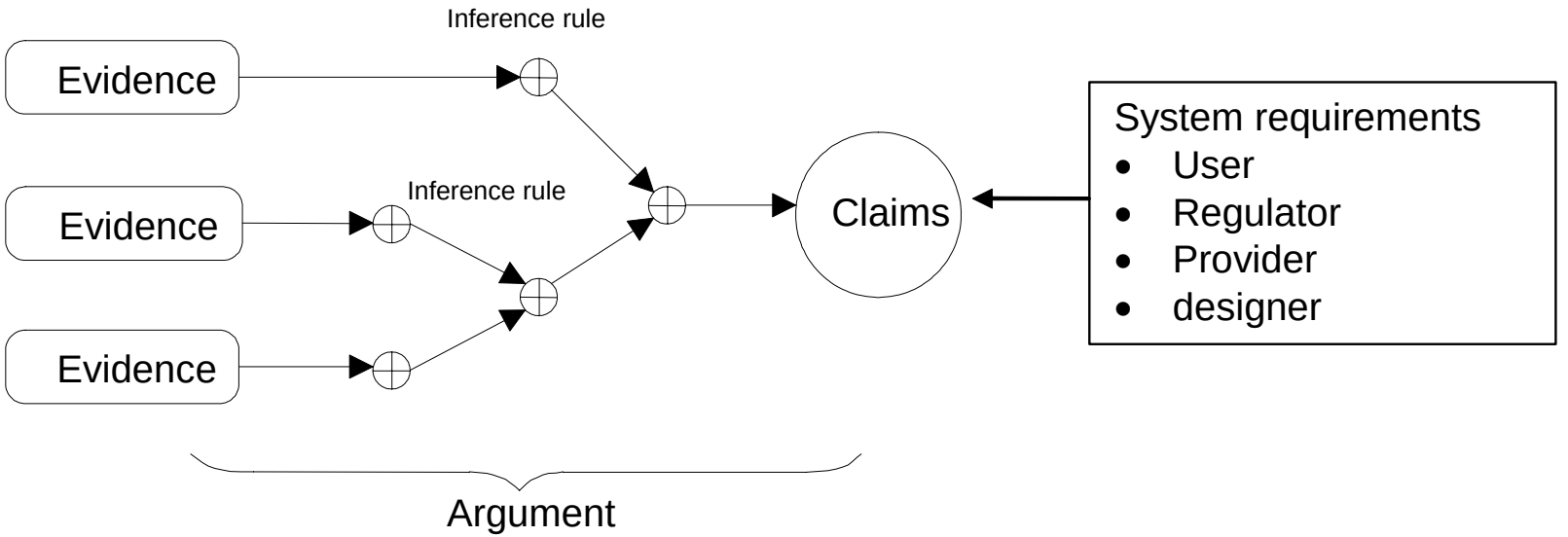
Dependability Case

- Lähestymistapa on lähtöisin turvallisuuskriittisten järjestelmien arvioinnista (Safety Case), ja sitä on sovellettu mm. ydinvoimalaitosten turvallisuustarkasteluissa

- Safety Case on määritelmänsä mukaan
  - *dokumentoitu evidenssikokonaisuus, jonka perusteella voidaan osoittaa (validisti), että tarkasteltava järjestelmä on riittävän turvallinen tarkasteltavaan tehtävään koko elinkaarensa ajan*

- Dependability Case olisi vastaavasti
  - *dokumentoitu evidenssikokonaisuus, jonka perusteella voidaan osoittaa (validisti), että tarkasteltava järjestelmä on riittävän luotettava tarkasteltavaan tehtävään koko elinkaarensa ajan*

Dependability Case'n rakenne



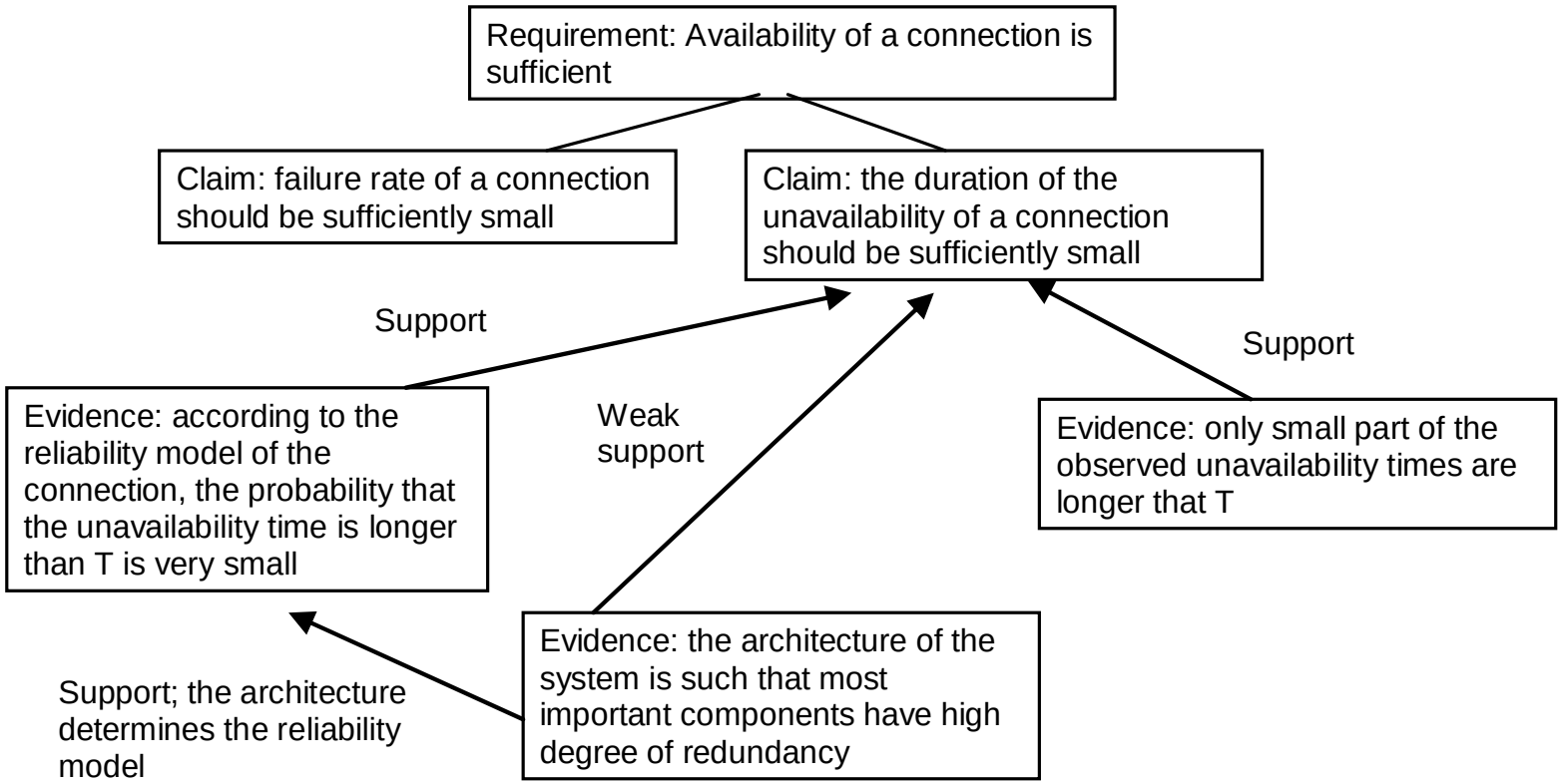
- Järjestelmän vaatimukset (käyttäjiltä, viranomaisilta jne…) määrittelevät, millaisia luotettavuusominaisuuksia järjestelmällä tulee olla
- Vaatimukset voidaan kääntää väittämiksi, jotka koskevat järjestelmän luotettavuutta (käytettävyys, rakenne, robustisuus, kustannukset jne)
- Toiminnalliset vs. ei toiminnalliset vaatimukset
- Suunnittelusta, analyyseista ja käyttökokemuksista saatua evidenssiä voidaan käyttää pääteltäessä luotettavuusväittämien voimassaoloa
- Inference rules ⇔ mallit, luotettavuusmallit, analyysit, kokemukset
- "Case" kokoaa asianmukaiset indikaattorit johdonmukaiseksi kokonaisuudeksi

Kellä on luotettavuusvaatimuksia minkin aspektin osalta:

	User	Operator	Manufacturer	Designer	Regulator
Availability	Operator	Operator 2			Operator
Reliability	Manufacturer (terminal)	self Manufacturer			Operator
Maintainability	Manufacturer (terminal)	self Manufacturer	Manufacturer 2		Operator
Robustness		Designer	Designer	self	
Controllability	Operator	Manufacturer	Designer	self	Operator
Invulnerability	Operator	User Operator Manufacturer Designer		self	Operator Manufacturer Designer

Dependability Case -esimerkki:

Vaatimus: Liittymän yhteydellä core-verkkoon on riittävä käytettävyys



Johtopäätöksiä ja ehdotuksia

”Luotettavuusprosessi”

- IP-infrastruktuurin luotettavuuden seuranta, parantaminen ja ylläpitäminen on prosessi, jolle muodostuu institutionaalisia muotoja ja käytäntöjä
- Luotettavuudesta huolehtiminen on kaikkien osapuolten yhteinen asia; myös käyttäjien tulisi vaatia asianmukaista luotettavuutta erilaisille verkoille ja palveluille
- Käytettävyyden (availability) monitoroinnin ja luotettavuusdatan keräämisen menetelmiä tulee kehittää kohti standardoituvia käytäntöjä; laadullisia käyttökokemuksia tulisi hyödyntää systemaattisesti
- “Luotettavuusprosessi” edistää hyvien käytäntöjen (best practices) vakiintumista eri yhteyksissä; nämä suojaavat ”luotettavuuskulttuuria” rapautumiselta myös taloudellisten paineiden alla

Tutkimuksen haasteita

- Olemassa olevia luotettavuuden mallinnus- ja analyysitekniikoita voidaan soveltaa IP-verkkoihin ennen kaikkea fyysisen rakenteen osalta
- Luotettavuuden aspektien kuvaamiseksi voidaan laskea erilaisia mielekkäitä indeksejä; luotettavuuden kokonaiskuvan luomiseen ja ylläpitämiseen tarvitaan kuitenkin myös Dependability Case –tyyppistä metodia
- Virheet verkkojen konfiguroinnissa ovat merkittävä vikojen lähde - verkkoja operoivan henkilöstön korkeaa ammattitaitoa vaativaa työtä olisi syytä tutkia kuten esim. turvallisuuskriittisiä työtehtäviä
- Tietoliikennepalvelujen kriittisyysluokitusta on kehitettävä
- Pitkällä tähtäyksellä verkkotekniikan tulisi kehittyä siihen suuntaan, että luotettavuus olisi yksi sisäänrakennetuista periaatteista; ”defense-in-depth” –ajattelulle perustuva verkonrakennus helpottaisi itse asiassa myös luotettavuuden mallinnusta ja arviointia