

Tosi aikajärjestelmät – Luento 6: Luotettavuus ja turvallisuus

Tiina Niklander

Burns & Wellings luku 5 tai
Krishna & Shin luvut 7 ja 8

Luotettavuus ja vikasietoisuus

- n Yleistä:
 - n Vika, virhe, häiriö
 - n Vikatyyppejä
 - n Mitä voidaan tehdä: estää, havaita, sietää, korjata
 - n Vian havaitseminen
 - n Vian sieto
- n Monentaminen ja toisintaminen
- n Turvallisuus ja luotettavuus
- n Riippuvuus (dependability)
- n Esimerkkejä

Vika, virhe, häiriö

- n Virhe (error, bug, mistake)
 - n Ohjelmiston poikkeaminen määrittelystä
- n Vika (fault)
 - n Virheellisen ohjelmakohdan suoritus
- n Häiriö (failure)
 - n Viasta aiheutuva ulkoisesti havaittava poikkeama määrittelystä
 - n Kaikki virheet ja viat eivät välttämättä johda häiriöön

Mistä häiriöt syntyvät?

- n Määrittely- tai suunnitteluvirheet
 - n Puutteellinen määritelmä
 - n *Suunnitelmassa (tai toteutuksessa) virheitä*
- n Komponenttiviaat
 - n Vanheneminen, huono valmistuserä, tms.
- n Ympäristön vaikutus
 - n Elektromagneettinen häiriö
 - n Liikaa lämpöä, kiihtyvyyttä, värinää, yms.

Vikatyyppejä

- n Pysyvä vika (permanent)
 - n Poistuu järjestelmästä vasta korjauksen jälkeen
- n Tilapäinen vika (transient)
 - n Ilmenee hetken ja häviää
 - n Syynä esimerkiksi elektromagneettinen säteily
 - n Muita nimiä: soft error
- n Toistuva vika (intermittent)
 - n Ilmaantuu satunnaisesti aika-ajoin
 - n Irtonainen johto, lämpöherkkä komponentti

Häiriökäyttäytyminen (failure mode)

- n Fail-silent
 - n Aina oikea tulos, tai ei vastausta lainkaan
 - n Helppo malli teoreettisissa tarkasteluissa
- n Fail-consistent, value-error
 - n Laskennan tulos voi olla väärä, mutta sama tieto kaikille kommunikointiin osallistuville
- n Byzantine, arbitrary, malicious
 - n Laskennan tulos voi olla erilainen eri vastaanottajille.

Mitä voidaan tehdä?

- n Pysyvä vika
 - n Varataan laitteistoon ylimääräistä kapasiteettia, jotta toiminta voi jatkua
 - n Korjataan myöhemmin
- n Tilapäinen (tai satunnainen) vika
 - n Toivutaan viasta, laitteisto on yleensä edelleen ehjä
 - n Havaitaan ja tehdään vain laskenta uudelleen
- n Tyypillisesti tutkimuksissa on valittu vikaantumisen malliksi joko
 - n Pysyvä vika + fail silent tai
 - n Tilapäinen vika + fail consistent tai byzantine

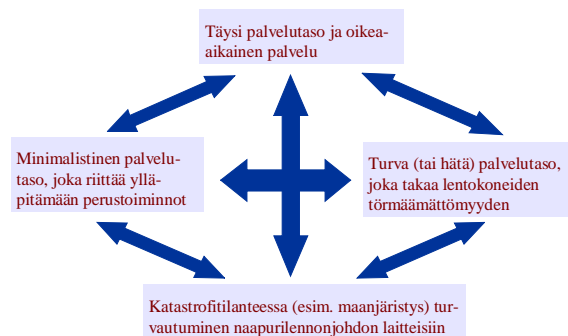
Vian havaitseminen

- n Vian havaitseminen edellyttää sekä tietoa nykyisestä tilasta että suunnitellusta tilasta
- n Suunnitellun tilan tieto voidaan saada
 - n Joko etukäteen pääteltyä (a priori)
 - n Tai vertailutietona rinnakkaisista järjestelmistä
- n Prosessorin häiriökäyttäytyminen voidaan yrittää havaita
 - n Laittomasta toiminnasta: esim. suorituskäskyn nouto data-alueelta, virheellinen opkoodi, liian pitkään kestänyt suoritus

Vikaantumisen sieto

- n Perustuu aina monentamiseen (redundancy)
- n Useita vaihtoehtoisia palvelutasoja
 - n Täysi vikasetoisuus: järjestelmä tarjoaa vioista riippumatta saman pysyvän palvelutason
 - n Alentunut palvelutaso: järjestelmä tarjoaa edelleen palvelua, mutta sen suorituskyky on alentunut vikojen seurauksena
 - n Turvallinen pysähtyminen (fail safe): Järjestelmä ei enää tarjoa palvelua, mutta varmistaa, että 'pysähtyminen' tapahtuu turvallisesti

Esimerkki: lennonvalvonta



Vikasietoisuus

- n Järjestelmä on *k*-vikasietoinen, jos se toimii määritelmänsä mukaan vielä, kun korkeintaan *k* komponenttia on vikaantunut
- n Hierarkkinen rakenne (järjestelmä voi olla komponentti ylemmän tason järjestelmälle)

Luotettavuus ja vikasetoisuus

- n Yleistä
- n **Monentaminen ja toisintaminen**
 - n *k*-vikasietoisuus, *n*-versiointi
 - n Laitteisto, ohjelmisto vai aika
 - n Äänestys, konsensus, toipuminen
- n Turvallisuus ja luotettavuus
- n Riippuvuus (dependability)
- n Esimerkkejä

Monentaminen on vanha keksintö

- n *"The most certain and effectual check upon errors which arise in the process of computation is to cause the same computations to be made by separate and independent computers; and this check is rendered still more decisive if their computations are carried out by different methods."* D. Lardner, Edinburg Review, 1825

Laitteisto

- n Lisätään järjestelmään laitteistoa, jota ei tarvittaisi, jos mikään ei koskaan vikaantuisi
- n Lyhytaikainen käyttötapa
 - n Häiriön havaitsemiseen
 - n Kaikki komponentit suorittavat samat operaatiot ja tuloksesta äänestetään
- n Pitkäaikainen käyttötapa
 - n Korvataan vikaantunut järjestelmän osa vastaavalla toimivalla varaosalla

Laitteisto

- n Monentaminen on kallista, koska tarvitaan ns. 'turhia' osia valmiiksi järjestelmään
- n Avaruusluotaimiin on pakko asentaa valmiiksi riittävä määrä varaosia, joita voidaan ottaa käyttöön tarvittaessa
- n Huollettavammissa järjestelmissä (esim. auto, lentokone) voidaan käyttää äänestysmenettelyä ja vikaantuneet osat korjataan, kun niitä havaitaan

Kuinka monta toisintoa tarvitaan?

- n Kun halutaan sietää k eri virhettä, tarvitaan
 - n $k+1$ toisintoa, jos virhe pysäyttää toiminnan (fail-silent tai fail-stop)
 - n $2k+1$ toisintoa, jos johdonmukainen vikaantuminen eli virhe on sama kaikille (fail-consistent)
 - n $3k+1$ toisintoa, jos Bysanttilainen vikaantuminen eli 'pahantahtoinen' toiminnallisuus, vikaantunut komponentti tuottaa satunnaisia tuloksia (malicious, arbitrary)

Äänestys ja konsensus

- n Vähintään kolme samanlaista voi äänestää ja käyttää enemmistöpäätöstä
- n Kaksi voi havaita vian, mutta ei päättää oikeaa tulosta (fail silent mahdollinen)
- n Miten lähellä tulosten pitää olla toisiaan? (Pyörityserot eri laitteistoilla)
Onko 1.400978 sama kuin 1.400984 ?
- n Likimääräinen samuus sallittava, jos syötteillekin sallitaan pientä vaihtelua

Äänestystapoja

- n Enemmistöpäätös (majority vote)
 - n $x, y \in P_i$, joss $d(x, y) \leq \epsilon$, valitaan $\max(P_i)$
 - n Valitaan yksi arvoista $x \in P_i$
- n k -enemmistöinen päätös (k -plurality vote)
 - n Valitaan joku P_i , jossa vähintään k jäsentä
- n Keskiwertopäätös (median vote)
 - n Valitaan vastauksista arvoltaan keskimmäinen

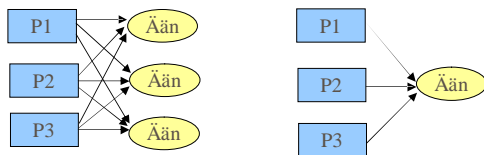
Arkkitehtuurivaihtoehdot

- n Kaksi synkronoitua prosessoria (lock-step dual processor)
 - n Verrataan tuloksia, jos eroja -> fail-silent
 - n Havaitsee kaikki viat
- n Kaksi erillistä prosessoria (loosely-synchronized dual processor)
 - n Havaitsee virheellinen tuloksen,
 - n Tarvitsee erillisen vian etsinnän
- n Kolme prosessoria (TMR - triple modular redundant)
 - n Äänestyksen jälkeen havaitaan virhe ja tiedetään viallinen komponentti
- n Uusi idea (2003): Dual Lock-Step
 - n Oikeasti siis neljä prosessoria

n-modulaarinen monennus (NMR)

- n Tyypillinen laitteistotason ratkaisu
- n N prosessoria ja äänestetään tulos
- n N yleensä pariton
- n Tarvitaan $2m+1$ prosessoria, jotta selvittää m:sta vikaantumisesta
- n TMR - triple modular redundant

NMR kaavakuvia



PLC (ohjelmoitava logiikkakontrolleri)

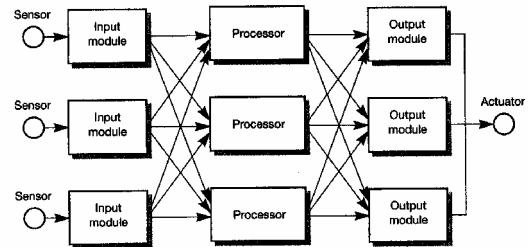


Figure 6.21 A typical arrangement for a high-reliability PLC.

Storey: Safety-critical computer systems

Dual Lock Step

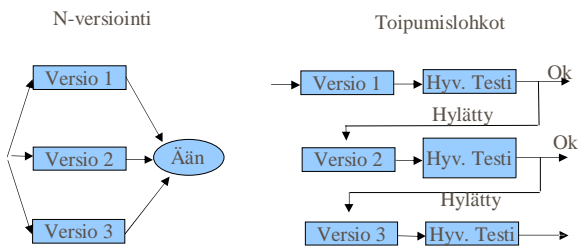
- n Tähän tuo kaavakuva artikkelista
- n (tai koko asia pois)

Baleani et al: Fault-Tolerant Platforms for Automotive Safety-Critical Applications. CASES'03, s. 170-177, ACM.

Ohjelmisto

- n Laitteistotason monentaminen mallina
- n N-versiointi
 - n Tehdään N eri toteutusta samasta ohjelmasta
 - n Tavoitteena eri virheet eri ohjelmissa
- n Toipumislohkot (recovery block)
 - n Toistettavissa oleva ohjelman suorituksen osa
 - n Toistossa voidaan käyttää samaa ohjelmakomponenttia tai jotain toista versiota
 - n Toistetaan vain, jos ens. suoritus virheellinen

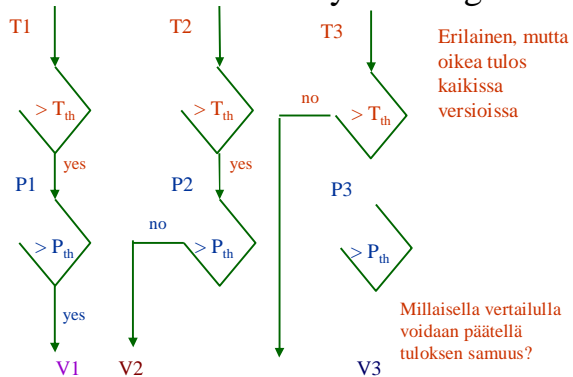
Ohjelmiston monentaminen



N-versiointi

- n Kallista
- n Riippumattomat työryhmät, ei yhteistoimintaa
- n Vaikuttavia tekijöitä:
 - n Vaatimusten spesifiointi (entä jos tässä virhe)
 - n Ohjelmointikieli ja Algoritmi
 - n Työkalut, koulutus ja ohjelmointitaito

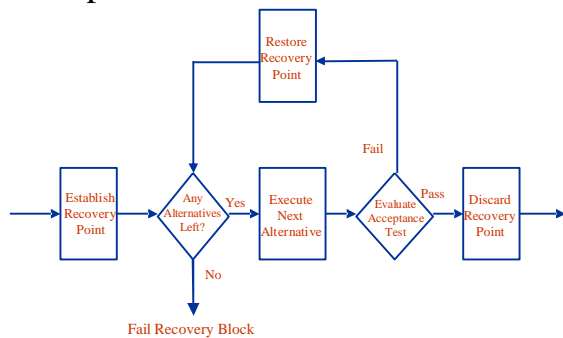
Vertailun tai äänestyksen ongelma



Toipumislohko

- n Lisätään ohjelmaan toipumispisteitä (recovery point)
 - n Tällainen voi olla esim. checkpoint, jossa ohjelman koko tila tallennetaan
- n Vikatilanteessa suoritus voidaan peruuttaa edelliseen pisteeseen ja jatkaa siitä uudelleen
- n Toipumispisteestä seuraavaan voidaan käyttää jotain vaihtoehtoista menetelmää tai versiota

Toipumislohko

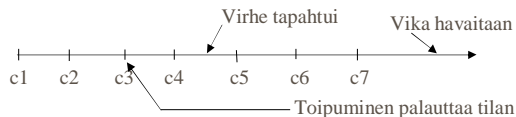


Vertailu: N-versio / toipumislohko

	N-versio	Toipumislohko
Toimintamalli	Staattinen	Dynaaminen
Kehityskustannus	Versiot + ohjaus	Moduulit + hyv-testi
Suorituskustannus	N resurssia	Toipumispisteet
Virheen hav.	Äänestys, joustava kommunikointi ohjaimen kautta	Hyväksymisestä Taaksepäin toipuva, vähäinen yleiskuorma
Atomisuus		

Aika

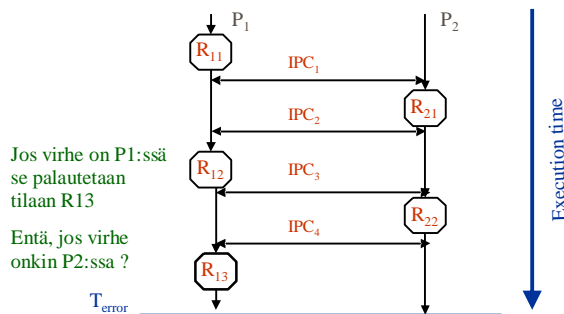
- n Ajan toisintaminen -> laskennan toistaminen myöhemmin
- n Edellytys: aikarajat sallivat kaksinkertaisen suorituksen ainakin vikatilanteissa
- n Toipumislohkojen käyttö perustuu tähän



Kaksi tapaa toipua ajassa

- n Toipuminen eteenpäin
 - n Siirretään järjestelmän tilaa eteenpäin turvalliseen tilaan
 - n Tilat määrättävä jokaiselle järjestelmälle erikseen
- n Toipuminen taaksepäin
 - n Palautetaan turvallinen aiemmin suoritettu tila
 - n Yleisempi lähestymistapa

Dominoefekti kommunikoiivat prosessit



Informaatio

- n Koodataan lisätietoa, jolla voidaan havaita ja jopa korjata virheitä
 - n Tallennetaan sama tieto kahteen kertaan
 - n Pariteettibitti
 - n Tarkistussumma
- n Hamming etäisyys
 - n Käytetään arvioimaan bittijonojen samuutta

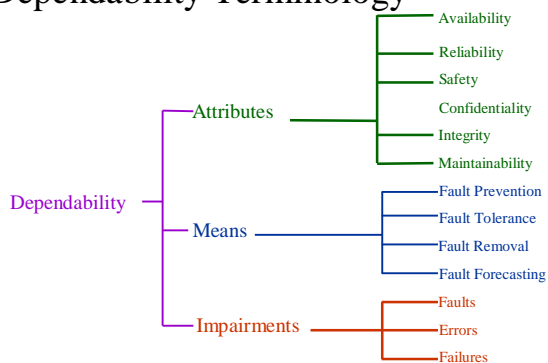
Luotettavuus ja vikasetoisuus

- n Yleistä:
- n Monentaminen ja toisintaminen
- n **Turvallisuus ja luotettavuus**
- n **Riippuvuus (dependability)**
- n Esimerkkejä

Turvallisuus ja luotettavuus

- n **Turvallisuus:** Järjestelmä ei aiheuta hengenmenoja, loukkaantumisia, sairauksia, omaisuuden tai ympäristön vaurioitumista.
- n **Luotettavuus:** mittari, joka kertoo kuinka hyvin järjestelmä vastaa toiminnankuvausta.
- n **Turvallisuus** on siis todennäköisyys, että järjestelmän toiminta ei johda vahinkoon toimiva järjestelmä suunnitelmansa mukaan tai ei.

Dependability Terminology



Virheen käsittely

- n Virheen havaitseminen
 - n äänestys, hyväksymisestä
- n Virheen (tai vahingon) eristäminen
- n Virheestä toipuminen
 - n Konsensus, toipumislohko
- n Virheen korjaus
 - n Korjauksen jälkeen palautetaan taas toimintaan

Luotettavuus ja vikasetoisuus

- n Yleistä:
 - n Monentaminen ja toisintaminen
 - n Turvallisuus ja luotettavuus
 - n Riippuvuus (dependability)
- n **Esimerkkejä**
 - n Avaruussukkulan tietokonejärjestelmä
 - n Prosessin ylösnousemus (process resurrection)

Avaruussukkula

- n Viisi tietokonetta, joista neljä samassa ryhmässä
- n Viidennessä koneessa on muista täysin riippumaton ohjelmistototeutus lähinnä varalla
- n Kaikki koneet kytketty yhteen viidellä rinnakkaisella väylällä

Avaruussukkula

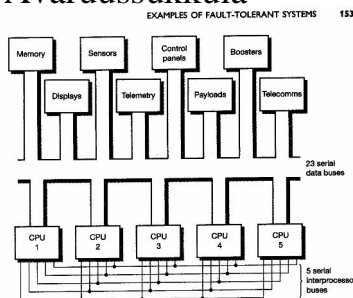


Figure 6.20 Architecture of the space shuttle's computer systems.

Kuva 6.20 teoksesta: N. Storey Safety-critical computer systems. Prentice Hall 1996

Prosessin ylösnousemus

- n Artikkelit
 - n Kihwal Lee ja Lui Sha: Process Resurrection: A Fast Recovery Mechanism for Real-Time Embedded Systems. Proc of RTAS'05, IEEE.
- n Idea:
 - n Tehdään uudelleenkäynnistys niin nopeaksi, että uudelleenkäynnistetty prosessi ehtii valmistua alkuperäisen aikarajan sisällä!

Prosessin ylösnousemus

- n Ratkaisuidea:

Artikkelin kuva 2

Yhteenveto

- n Virheiden ja vikojen luokat ja mallit
- n Toisinnetaan
 - n Laitteisto: N-modulaarinen, äänestys
 - n Ohjelmisto: N-versiointi, toipumislohko
 - n Aika: Toivutaan eteen- tai taaksepäin
 - n Informaatio: tuplaus, lisäkoodaus, tarkistussumma
- n Prosessi: virheen havaitseminen, eristäminen, toipuminen, korjaaminen