# *Vikasietoisuus ja luotettavuus*

**Luotettavuussuureet**
**Keskuksen vikasietoisuus**
**Mallinnusmenetelmät**



## *Vikasietoisuuden peruskäsitteitä ovat*

- ✔ ***Vikaantuminen*** **(failure, malfunction) - poikkeama tarkoitetusta/määritellystä oikeasta toiminnasta**
- ✔ ***Vika*** **(fault) - sellainen laitteen tai ohjelman tila, joka voi johtaa vikaantumiseen**
- ✔ ***Virhe*** **(error) - laitteen tai ohjelman (moduulin) tuottama väärä vaste. Virhe indikoi että moduulissa on vika, moduuli on saanut virheellisen syötteen tai sitä on käytetty väärin. Johtaa vikaantumiseen, ellei systeemi siedä kyseistä vikaa. Vika voi olla olemassa ilman, että virheitä sattuu.**

## *Mitä on vikasietoisuus?*

- ✔ ***Järjestelmän kyky jatkaa tarkoitettua oikeaa toimintaa, vaikka siinä on vika.***
- ✔ ***Puhelinkeskus on esimerkki vikasietoisesta järjestelmästä.***
- ✔ ***Vikasietoisuus edellyttää*** **redundanssia (varmennusta).**



## *Viat jaetaan*

- ✔ **Kestonsa perusteella:**
  - ***pysyviin*** **(permanent, tai stuck-at)**
  - ***häilyviin*** **(intermittent), joka ei poistu korjaamatta mutta jonka vaikutus ei tunnu aina**
  - ***hetkellisiin*** **(transient), joka voi vaikuttaa hetken ja sitten hävitä ilman korjaustoimenpiteitä.**
- ✔ **Näkyviin ja näkymättömiin (latent).**
- ✔ **Vaikutuksensa perusteella.**
- ✔ **Yleisemmin puhutaan *vikamalleista*.**

## *Graceful degradation on*

- ✔ ***järjestelmän kyky jatkaa toimintaa yhden tai usean peräkkäisen vian sattuessa normaalia alhaisemmalla suorituskyvyn tasolla.***
- ✔ **Esim. useissa RAID (redundant arrays of inexpensive disks) konfiguraatioissa kirjoitusten nopeus laskee levyvian sattuessa, mutta toiminta voi kuitenkin jatkua.**



## *Luotettavuus ja käytettävyys*

- ✔ ***Luotettavuus (reliability)*** $R(t)$ **= Todennäköisyys, että järjestelmä ei vikaannu ajan** $t$ **kuluessa ehdolla, että se toimi virheettömästi ajan hetkellä** $t = 0$**.**
- ✔ ***Käytettävyys (availability)*** $A(t)$ **= Todennäköisyys sille, että järjestelmä toimii virheettömästi ajan hetkellä** $t = 0$**.**

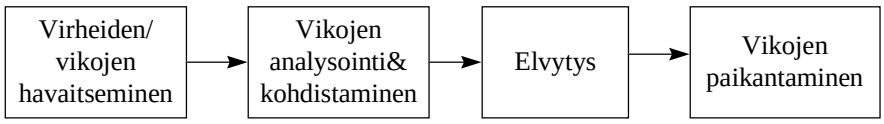
- ***Kunnossapidettävyys (maintainability) M*(*t*) = todennäköisyys sille, että järjestelmä palaa virheettömään toimintaan ajan *t* kuluessa, ehdolla että se oli vialla ajan hetkellä *t* = 0.**



## *MTTF, MTTR, MTBF*

- **MTTF = Mean-Time-To-Failure = vikaantumisajan odotusarvo**
- **MTTR = Mean-Time-To-Repair = korjausajan odotusarvo**
- **MTBF = Mean-Time-Between-Failure = kahden peräkkäisen vikaantumisen välin odotusarvo**

## *Puhelinkeskus pyrkii luotettavuuteen*



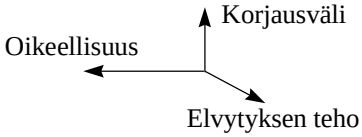

*Hyödyntää:*
- *redundanssia*
- *uudelleen käynnistyksiä*
  - *yksittäinen ohjelma*
  - *oheisprosessori*
  - *yksi pääprosessori*
  - *koko järjestelmä*



## *Redundanssin päätyypit ovat*

- *Laitteistoredundanssi*, esim kahdennus (1+1), r/n -periaate kahdennus vaatii periaatteessa *self-checking* - viat itse tunnistavat puolikkaat.
- *Ohjelmistoredundanssi* (tarvitaan aina).
- *Tietoredundanssi* (esim. pariteettibitti).
- *Ajallinen redundanssi* (esim. viivästetty uudelleensuoritus).

## *Vikasietoisuuden tavoitteet vaihtelevat sovelluksen mukaan*




- Yhteinen tavoite on *käytettävyyden* parantaminen.
- Muita tavoitteita painotetaan sovelluksen mukaan:
  - *Oikeellisuus* ( computational integrity) - tärkeää esim. laskutuksen osalta.
  - *Korjausväli* (long life systems) - esim avaruus-luotaimet
  - *Elvytyksen tehokkuus* (fault coverage) - kuinka hyvin vikasietoisuusmekanismit suoriutuvat tehtävästään.
  - *Lisäksi painaa järjestelmän suorituskyky ja hinta.*

- Kriittiset sovellukset (life-critical), pitkäikäiset järjestelmät, kaupalliset.



## *Puhelinkeskuksen keskeiset luotettavuusvaatimukset ovat*

Q.543: Premature release:
Puhelun ennenaikaisen purkautumisen todennäköisyys minkä tahansa 1 min aikana keskuksen viasta johtuen

$$P \leq 2 \times 10^{-5}$$

Keskimääräinen sisäisestä syystä johtuva Down-time: 2 min/vuosi.

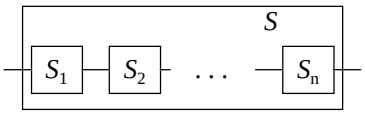
*Jos järjestelmälle keskimääräinen seisokki on esim 20 min*

$\Rightarrow$ *MTTF (seisokkien väli) = 10 vuotta.*

# *R, F, Λ, MTTF*



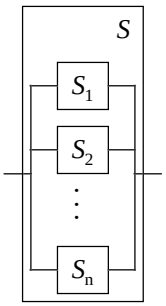
# *Luotettavuuden kombinatoriikka*




Sarjajärjestelmä $S$ toimii, jos kaikki sen osat $S_i$ toimivat

$$R_s = \prod_{i=1}^{n} R_i$$

Lohkojen vikaantumiset ovat riippumattomia




Rinnakkaisjärjestelmä vikaantuu, jos kaikki sen lohkot vikaantuvat:

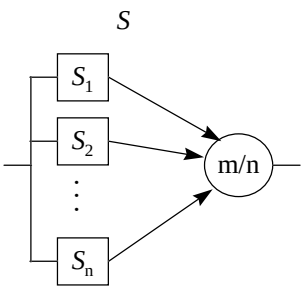
$$F_s = \prod_{i=1}^{n} (1 - R_i)$$

$$R_s = 1 - F_s = 1 - \prod_{i=1}^{n} (1 - R_i)$$

Esim. Kahdennettu järjestelmä:

$$R_s = 1 - (1 - R)^2$$

# *Luotettavuuden kombinatoriikka jatk.*




Kuormanjakojärjestelmä toimii, jos *m* kaikkiaan *n*:stä osajärjestelmästä toimii

(Bernoullin kokeille pätee binomijakauma)

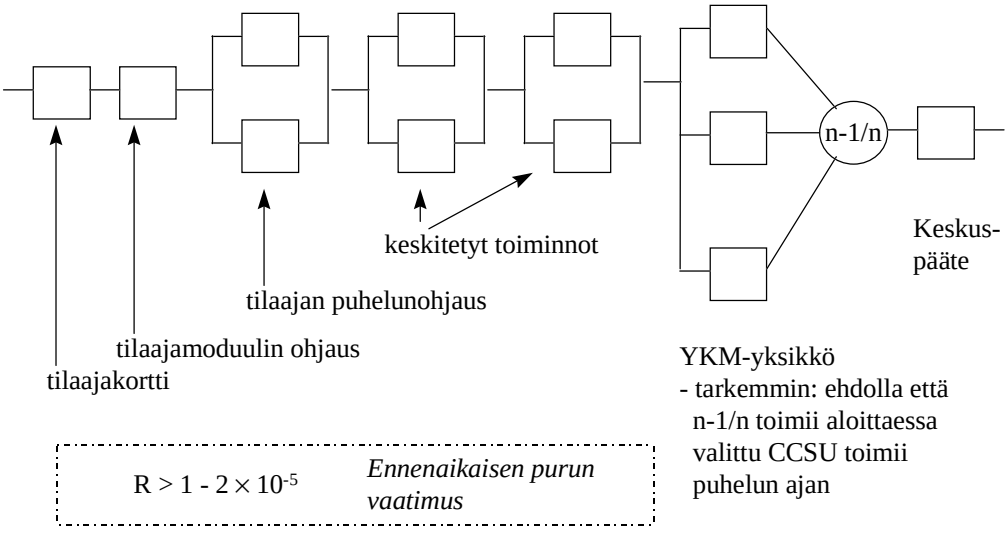
$$R_{m/n} = \sum_{k=0}^{m-1} \binom{n}{k} R^{n-k} (1 - R)^k$$

Esim. $R_{2/3} = R^3 + 3R^2$

Otetaan esim. $R$=0.9 $\Rightarrow R_{2/3} = 0.972$



# *Keskuksen luotettavuus tilaajan kannalta*




YKM-yksikkö
- tarkemmin: ehdolla että n-1/n toimii aloittaessa valittu CCSU toimii puhelun ajan

$R > 1 - 2 \times 10^{-5}$ *Ennenaikaisen purun vaatimus*

# $\lambda$:n yksikkö

[$\lambda$] = fit = vikojen lukumäärä/$10^9$h

Pistoyksikköjen vikaantumistiheydet ovat luokkaa 0.1 - 10 kfit.

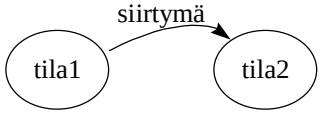
Esim. keskuksen tilaajakortin vikatiheys on 2 kfit. Paljonko on MTTF?

$$\text{MTTF} = 1/\lambda = \frac{10^9\text{h}}{2000} = \frac{1000\,000}{2 \times 24 \times 360} = 580 \text{ vuotta.}$$



# *Markovin ketjuihin perustuva luotettavuuden mallinnus*

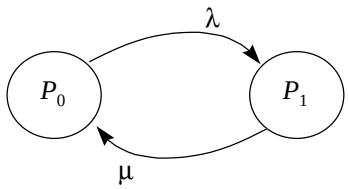
*Järjestelmä mallinnetaan tiloina, jotka joiden ehtojen voimassa oloa ja siirtyminä, jotka kuvaavat tapahtumia, joiden tuloksena järjestelmä siirtyy tilasta toiseen.*




*Menetelmällä voidaan ratkaista luotettavuuksia, joiden välillä on monimutkaisia riippuvuuksia.*

# *Markovin ketjuihin perustuva mallinnus*

(discrete event, continuous time)




λ = vikaantumistiheys
μ = korjaamistiheys
(korjaamisaika on exponentiaalisesti jakautunut)

$P_i$ = tilan *i* todennäköisyys

esim. $P_0 = R(t)$, $P_1 = F(t)$

Järjestelmä mallinnetaan tiloina, jotka joiden ehtojen voimassa oloa ja siirtyminä, jotka kuvaavat tapahtumia, joiden tuloksena järjestelmä siirtyy tilasta toiseen.