Satunnaisvikaantumisten hallinta ja laskenta

Juha Korhonen, ÅF-Consult Oy

7.11.2011

Innovation by experience

Vikaantumisen mekaniikkaa

- Mitä vikaantuminen on?
  - Järjestelmä/yksikkö/moduuli/komponentti ei toteuta oikein sille tarkoitettua tehtävää
- Laite tai järjestelmä voi vikaantua eri tavoilla
  - Systemaattinen vikaantuminen
  - Satunnaisvikaantuminen
- Luotettavuusteoria
  - Järjestelmän eliniän arviointi
    - Arviointisuureita (esim. MTTF, MTBF, MTTR)
  - Fyysinen vikaantuminen on satunnaistapahtuma
    - Vikaantuminen noudattaa kuitenkin tilastollisia malleja

Vikaantumisen mekaniikkaa

- Vaaralliset vikaantumiset ja turvalliset vikaantumiset
  - Jaottelu perustuu järjestelmän tilan tarkkailuun vikaantumisen jälkeen
  - Turvallisessa vikaantumisessa järjestelmän ohjattavat laitteet toimivat yhä halutulla tavalla osana turvallisuuteen liittyvää järjestelmää, eli saattavat prosessin turvalliseen tilaan
  - Vaarallisella vikaantumisella tarkoitetaan tilannetta, jossa turvallisuuteen liittyvä järjestelmä on estynyt reagoimasta potentiaalisesti vaaralliseen tilanteeseen
  - Lepovirtaperiaate vs. työvirtaperiaate

Vikaantumisen mekaniikkaa

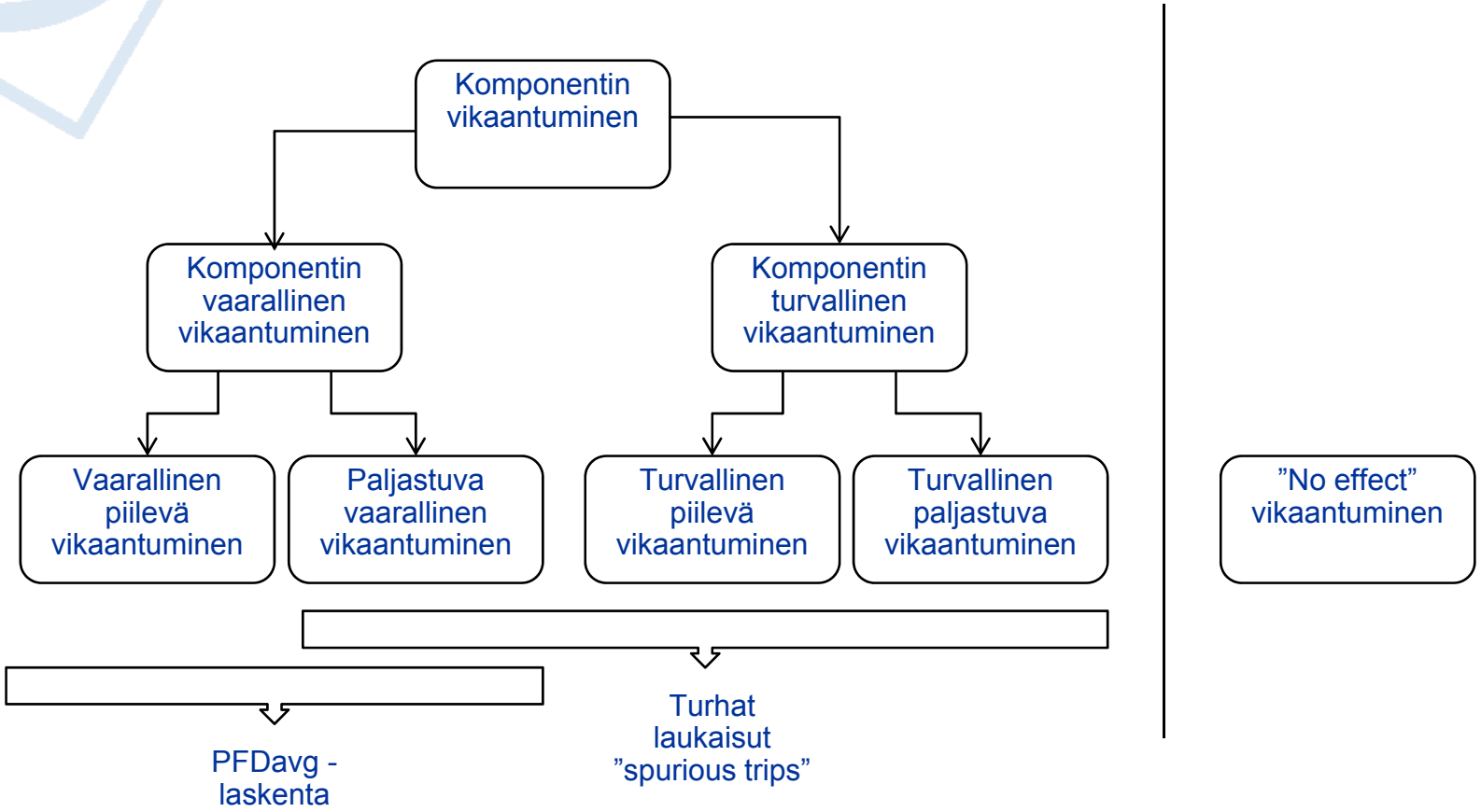
- Turvallisessa vikaantumisessa järjestelmä tulkitsee prosessin olevan virheellisesti vaarallisessa tilassa ja suorittaa usein näin ollen virheellisen järjestelmän alasajon eli turhan laukaisun

- Vaarallisessa vikaantumisessa järjestelmän toiminta on vikaantumisen vuoksi estynyt, jolloin vaadetilanteessa järjestelmä ei pysty suorittamaan laukaisua

Vikaantumisen mekaniikkaa

- Paljastuvat vikaantumiset ja piilevät vikaantumiset
  - Paljastuva vika on vikaantuminen, joka havaitaan järjestelmän sisäisellä diagnostiikalla tai normaalin operoinnin yhteydessä, esimerkiksi valvomosta käsin
  - Piilevällä vikaantumisella vastaavasti tarkoitetaan tilannetta, jossa järjestelmä vikaantuu, mutta vikaantumista ei havaita lainkaan
  - Esim. analogiamittauksen 4-20 mA –mittausalueen tarkkailu

Vikaantumisen mekaniikkaa



Innovation by experience

Vikaantumisen mekaniikkaa

- Määritellään termi vikatiheys (λ), jolla kuvataan komponentin kaikkea satunnaista vikaantumista tietyllä aikavälillä.
  - λ_S Turvallinen vikaantuminen
  - λ_{SD} Turvallinen, paljastuva vikaantuminen
  - λ_{SU} Turvallinen, piilevä vikaantuminen
  - λ_D Vaarallinen vikaantuminen
  - λ_{DD} Vaarallinen paljastuva vikaantuminen
  - λ_{DU} Vaarallinen piilevä vikaantuminen
- $\lambda = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$

Vikaantumisen mekaniikkaa

- Turvallisten vikaantumisten suhde, SFF (safe failure fraction)
  - Termillä tarkoitetaan sitä määrää kaikista satunnaisista virheistä, jotka johtuvat joko turvallisista vioista tai diagnosoiduista vaarallisista vioista
  - Vaikutus lähinnä arkkitehtuuristen vaatimusten varmistamisessa

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D}$$

Vikaantumisen mekaniikkaa

- Diagnostiikan kattavuus, DC (diagnostics coverage)
  - Termi määritellään havaittujen vikaantumisten suhteeksi kaikista vikaantumisista
  - Määriteltävä erikseen vaarallisille vikaantumisille ja turvallisille vikaantumisille
  - PFDavg –laskennassa mielenkiinto kohdistuu vaarallisten vikaantumisten diagnostiikan kattavuuteen

$$DC_D = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$$

Vikaantumisen mekaniikkaa

- Referenssidiagnostiikka
  - Referenssidiagnostiikassa (reference diagnostics) voidaan mitata yksittäisen virtapiirin toimintaa, jolloin mittaus perustuu tietyn turvallisuuteen liittyvän järjestelmän suureen tarkkailuun
  - Arvoja yleensä 0 ja 0.9 välillä
- Vertailudiagnostiikka
  - Vertailudiagnostiikassa (comparison diagnostics) vertaillaan kahden tai useamman turvallisuuteen liittyvän järjestelmän yksikön informaatiosisältöä. Jos tutkittavan järjestelmän virtapiirissä, prosessorissa tai muistiyksikössä tapahtuu vikaantuminen, se havaitaan erona vertailtavaan yksikköön nähden.
  - Arvoja yleensä 0.9 ja 0.999 välillä

Vikaantumisen mekaniikkaa

- Yhteisvikaantuminen (common-cause failure)
  - Yhteisvikaantumisella tarkoitetaan tilannetta, jossa yksittäinen vikaantumistilanne aiheuttaa usean eri komponentin vikaantumisen
  - Redundanssi
    - Hyvällä suunnittelulla voidaan välttää osa yhteisvikaantumistilanteista
  - Kuinka määrittää yhteisvikaantumisen todennäköisyys?
    - IEC 61508 esitteli niin kutsutun β –tekijään perustuvan mallin
    - Kvalitatiivinen lähestymistapa

Vikaantumisen mekaniikkaa

- Määräaikaiskoestusväli, TI (test interval)
  - Piilevät vikaantumiset havaitaan yleensä vasta määräaikaistestauksen yhteydessä
  - Paljastuvat vikaantumiset korjataan ennalta määritellyn korjausajan puitteissa, MTTR (mean time to repair)
  - Onko määräaikaiskoestus täydellinen, eli löytyvätkö kaikki piilevät vikaantumiset testauksen yhteydessä?
    - Testausohjelman suunnittelu tärkeässä roolissa
  - Määräaikaistestauksen yhteydessä oletetaan laitteet korjattavaksi ”uutta vastaavaan kuntoon”, onko todellisuutta?

Järjestelmäkonfiguraatiot - turvallisuus ja luotettavuus

- 1oo1 –konfiguraatio
  - Ei redundanssia
  - Turvallisuusmielessä suhteellisen heikko valinta
  - Luotettavuusmielessä suhteellisen heikko valinta
  - TET 1 –tason ratkaisu

Järjestelmäkonfiguraatiot - turvallisuus ja luotettavuus

- 1oo2 –konfiguraatio
  - Vikaantuu vaarallisesti, kun konfiguraation molemmat laitteet vikaantuvat vaarallisesti
  - Turvallisuusmielessä huomattavasti parempi kuin 1oo1 –konfiguraatio
  - Luotettavuusmielessä jopa heikompi valinta kuin 1oo1 –konfiguraatio
  - TET 2 –tason ratkaisu

Järjestelmäkonfiguraatiot - turvallisuus ja luotettavuus

- 2oo2 –konfiguraatio
  - Vikaantuu vaarallisesti, kun kumpi tahansa konfiguraation laitteista vikaantuu vaarallisesti, näin ollen turvallisuusmielessä konfiguraatio on hyvin haavoittuvainen
  - Luotettavuusmielessä konfiguraatio on erittäin hyvä ratkaisu. Turha laukaisu tapahtuu vasta, kun molemmat konfiguraation laitteet vikaantuvat turvallisesti
  - TET 1 –tason ratkaisu

Järjestelmäkonfiguraatiot - turvallisuus ja luotettavuus

- 2oo3 –konfiguraatio
  - Äänestysmenettely, konfiguraation ulostulo määräytyy vähintään kahden konfugraation laitteen päätyessä samaan tulokseen
  - Yhdistää 2oo2- ja 1oo2- konfiguraatioiden hyvät puolet, hyvät ominaisuuden niin luotettavuus- kuin turvallisuusmielessä
  - Kalliimpi toteuttaa kuin edellä mainitut konfiguraatiot

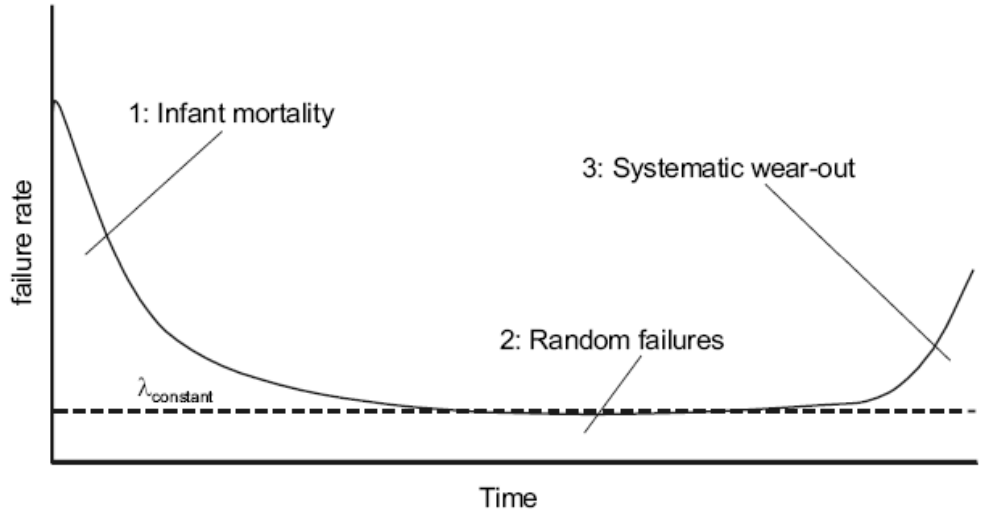
Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Vikatiheys
  - Tärkein mittasuure vikaantumistodennäköisyyden laskennassa
  - Kuvaa sitä, kuinka usein komponentti vikaantuu tietyllä aikavälillä
  - Matemaattinen määritelmä (Oreda 1997):
    - Vikatiheys lausutaan todennäköisyytenä sille, että komponentin todellinen elinikä (T) pysyy välillä [t, t+δt]. Näin ollen vikatiheys on keskimääräinen todennäköisyys sille, että vikaantuminen tapahtuu mainitulla aikavälillä.

$$\lambda(t) \cdot \Delta t \approx \Pr(t < T \leq t + \Delta t \,|\, T > t)$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Ammekäyrä
  - Varhaisvikaantumisvaihe
  - Vakiovikaantumisvaihe
  - Vanhenemisvikaantumisvaihe



Innovation by experience

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Toimintavarmuus (reliability)
  - Matemaattisesti toimintavarmuuden määritelmä voidaan esittää todennäköisyytenä sille, että järjestelmä toimii halutulla tavalla aikavälillä nollasta t:hen, T edustaa vikaantumisen ajanhetkeä, joka on satunnaismuuttuja:

$$R(t) = P(T > t)$$

  - Kääntäen toimintavarmuuden puute (unreliability) voidaan määritellä:

$$F(t) = 1 - R(t)$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Komponentin vikaantumisen mahdollisuutta tietyllä toimintavälillä voidaan kuvata todennäköisyyden tiheysfunktiolla (probability density function)
- Tiheysfunktio jakautunut jonkin jakaumamallin mukaisesti

$$f(t) = \frac{dF(t)}{dt}$$

- Vikatiheys ajan suhteen voidaan lausua todennäköisyyden tiheysfunktion ja toimintavarmuuden kautta

$$\lambda(t) = \frac{f(t)}{R(t)}$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Esimerkki: vikatiheys jakaantunut eksponentiaalisesti
  - Näin ollen tiheysfunktio voidaan määritellä

$$f(t) = \lambda e^{-\lambda t}$$

  - Ja edelleen toimintavarmuus

$$R(t) = e^{-\lambda t}$$

  - Ja vikatiheys

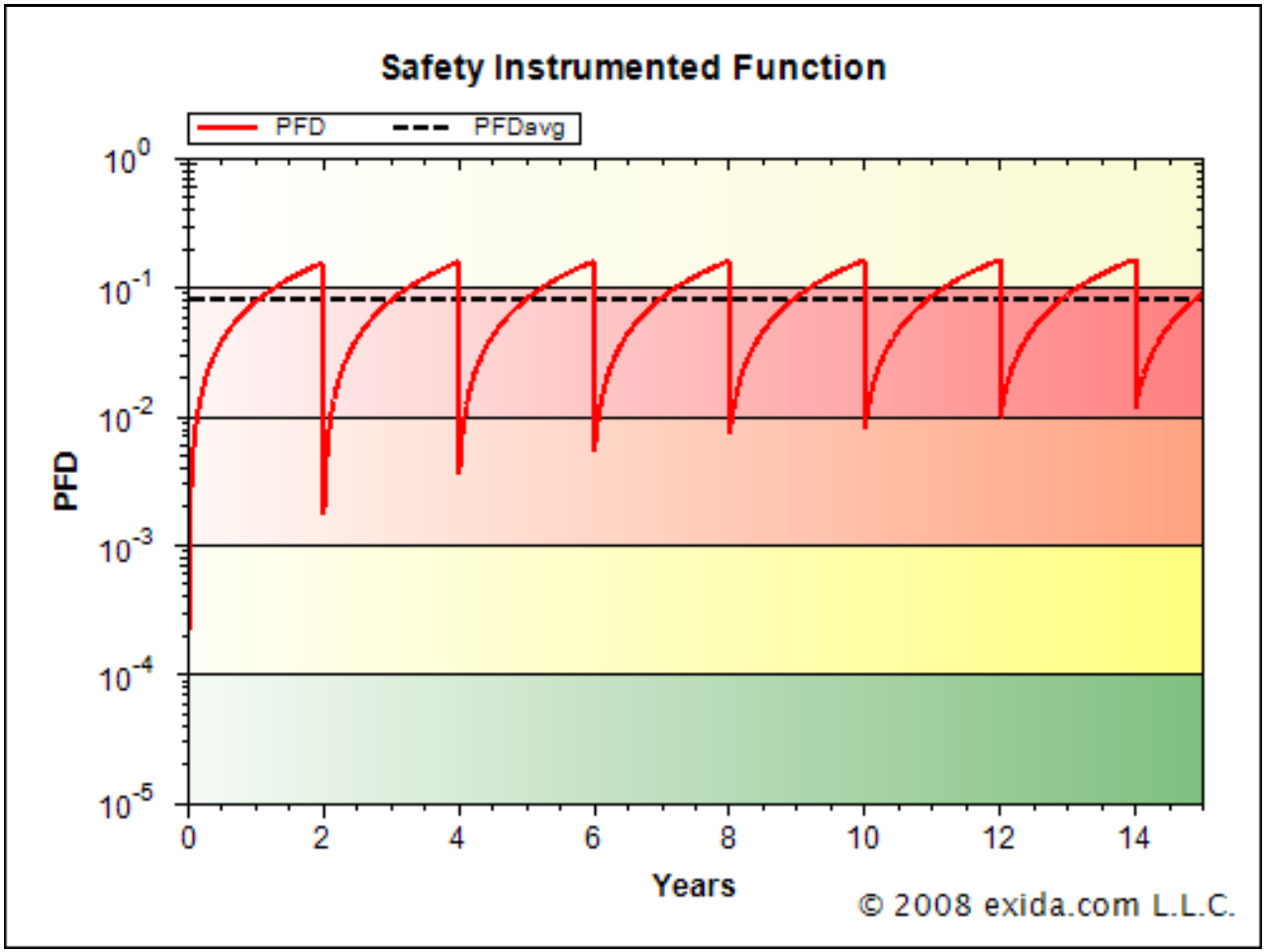
$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Hetkellinen vikaantumisen todennäköisyys PFD(t) (probability of failure on demand) riippuu tarkasteltavasta ajanhetkestä tarkasteluvälillä. Siksi käytännöllisempi suure on keskimääräinen vikaantumisen todennäköisyys tarkasteluvälillä PFDavg (average probability of failure on demand)

$$PFD_{AVG}(TI) = \frac{1}{TI}\int_{0}^{TI}(PFD)dt$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti



Innovation by experience

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Käyttövarmuus (availability)
  - Komponenteille, joilla on eksponentiaalisesti vähenevä todennäköisyyden tiheysfunktio ja siten myös vakioarvoinen vikatiheyden arvo, voidaan määritellä keskimääräistä vikaantumisaikaa kuvaava termi MTTF (mean time to failure):

$$MTTF = \frac{1}{\lambda}$$

  - Keskimääräisellä käyttövarmuudella A tarkoitetaan sitä suhdetta tarkasteluvälistä, jolloin se on käyttökunnossa.

$$A = \frac{MTTF}{MTTF + MTTR}$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- IEC 61508:n esimerkkilaskentamalli perustuu luotettavuuslohkokaavioihin
- Laskennassa määritetään PFD_{AVG} –lukuarvo, joka kuvaa todennäköisyyttä sille, että turvallisuuteen liittyvä toiminto ei toimi oikein vaadetilanteessa (harvojen vaateiden järjestelmä) tai PFH_{AVG} –lukuarvo, joka kuvaa vikaantumisen todennäköisyyttä tuntia kohden (tiheiden vaateiden järjestelmä)
- Standardin mukaisesti järjestelmäkonfiguraatiot koostuvat kanavista, jokainen kanava koostuu edelleen kahdesta komponentista
  - Paljastuva vikaantuminen
  - Piilevä vikaantuminen

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Piilevä vaarallinen vikaantuminen jää vaikuttamaan komponentin määräaikaiskoestusväliin asti, jolloin se määritelmän mukaan korjataan ”uutta vastaavaan kuntoon”. Paljastuvat vaaralliset vikaantumiset korjataan korjausajan, MTTR kuluessa
- Piilevästä vikaantumisesta johtuva kanavakohtainen vikaantuneenaoloaika t_{cl}

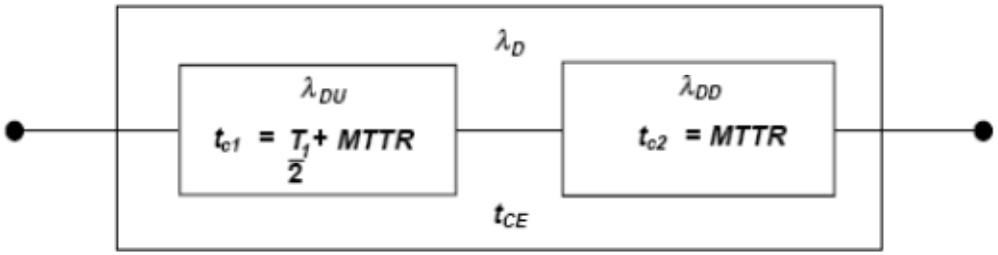
$$t_{cl} = E(T_1 - t) + MTTR = \frac{T_1}{2} + MTTR$$

- Paljastuvasta vikaantumisesta johtuva vikaantuneenaoloaika on MTTR mittainen. Näin ollen kanavakohtainen vikaantuneenaoloaika T_{CE} voidaan lausua:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

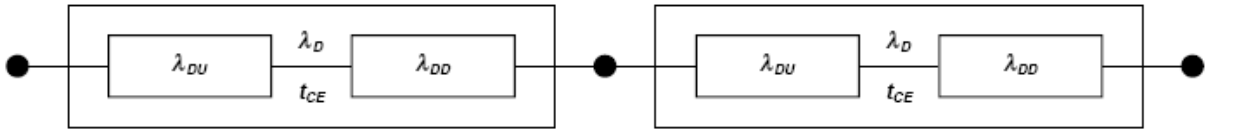
- 1oo1 –konfiguraatio vikaantuu vaarallisesti, kun konfiguraation ainoa laite vikaantuu vaarallisesti joko piilevästi tai paljastuvasti



$$PFD_{AVG}(1oo1) = (\lambda_{DD} + \lambda_{DU}) \cdot t_{CE}$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- 2oo2 –konfiguraation laskenta on samankaltaista 1oo1 –konfiguraation kanssa, sillä luotettavuuslohkokaaviomielessä laitteet ovat sarjassa. Käytännössä konfiguraatiossa on 2 kpl 1oo1 –



IEC 329/2000

- Konfiguraatio vikaantuu, kun kumpi tahansa laitteista vikaantuu vaarallisesti piilevästi tai paljastuvasti

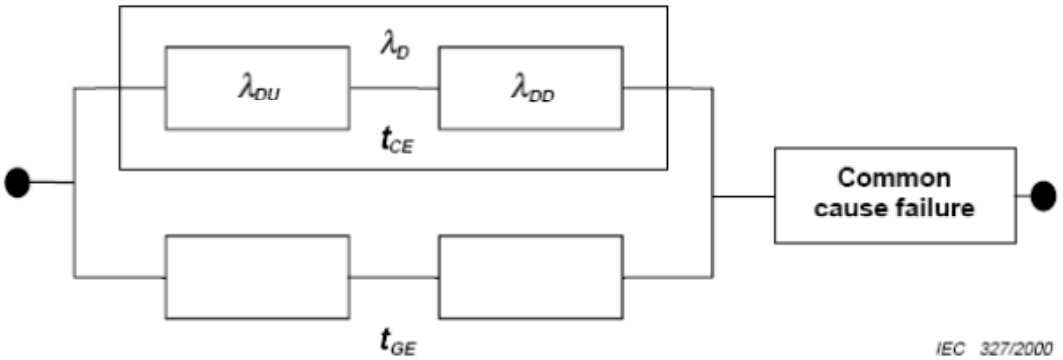
$$PFD_{AVG}(2oo2) = 2(\lambda_{DD} + \lambda_{DU})t_{CE}$$

Innovation by experience

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- 1oo2 –konfiguraatiossa on otettava huomioon myös äänestysporttikohtainen vikaantuneenaoloaika T_{GE} sekä yhteisvikaantumisen mahdollisuus

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$



Innovation by experience

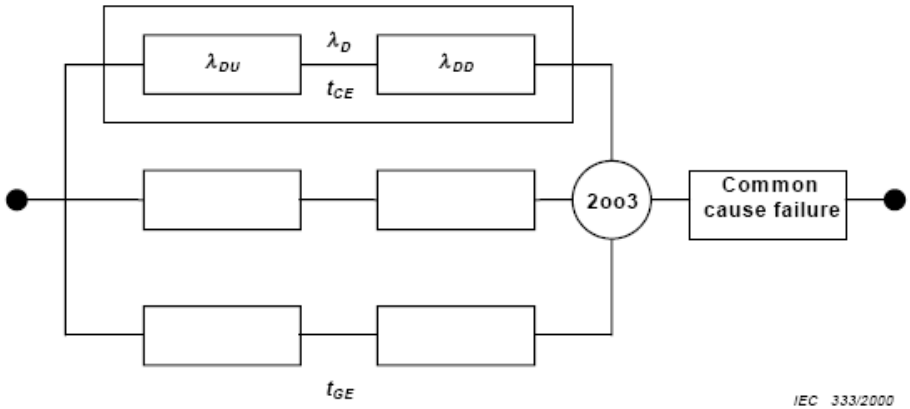
Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Yhteisviat jaotellaan myös piileviin sekä paljastuviin ja niiden vaikutusajat määritellään kuten 1oo1 –konfiguraation tapauksessa kanavakohtaisena vikaantuneenaoloaikana

$$PFD_{AVG}(1oo2) = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE} t_{GE}$$
$$+ \beta_D \lambda_{DD} MTTR + \beta_D \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- 2oo3 –konfiguraation vikaantuminen lasketaan lähes kuin 1oo2 –konfiguraation tapauksessa



$$PFD_{AVG}(2oo3) = 6\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE} t_{GE}$$
$$+ \beta_D \lambda_{DD} MTTR + \beta_D \lambda_{DU} \left(\frac{T_1}{2} + MTTR\right)$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- 1oo3 –konfiguraation tapauksessa laskenta samankaltaista 2oo3 –konfiguraation laskennan kanssa.

$$PFD_{AVG}(1oo3) = 6\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^3 t_{CE} t_{GE} t_{G2E}$$
$$+ \beta_D \lambda_{DD} MTTR + \beta_D \lambda_{DU} \left(\frac{T_1}{2} + MTTR\right)$$

- Lisänä kuitenkin termi T_{G2E}

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Esimerkki turvatoiminnon PFD_{AVG} -laskennasta
  - Riskianalyysissa päädytty turvatoimintoon, on tarkoituksena pysäyttää savukaasupuhallin, kun painemittaus ylittää sallitun raja-arvon
  - Turvatoiminnon TET –tasoksi on määritetty 2
  - Ratkaisuna toteutus, jossa turvalogiikkaan on yhdistettynä anturipuolella kaksi painelähetintä ja toimilaitepuolella kaksi laukaisurelettä ja yksi kontaktori, joilla pysäytetään savukaasupuhallin
  - Turvatoiminnon kokonais-PFD_{AVG} –arvo lasketaan summaamalla anturi-, logiikka- ja toimilaitealijärjestelmien PFD_{AVG} -arvot yhteen

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Painemittauksen (lähetin, impulssiputkitus, yms.) sekä laukaisureleiden ja kontaktorin vikatiheyden arvot etsitään vikatietokannasta
- Turvalogiikkana käytetään SIL 3 –tason turvalogiikkaa, jonka vikaantumistodennäköisyys etsitään valmistajalta itseltään tai sertifikaatista

Turvallisuuden eheystaso	Harvojen vaateiden toimintatapa (keskimääräinen toiminnan epäonnistumisen todennäköisyys suunnitellun toiminnan toteuttamisessa vaadetilanteessa)
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

SIL calculation of a safety related function

Component	Failure rate λ (10 ^ -6)	DC	Repair time (hours)	Dang. fail.	βd	β	TI (years)	Non-prefect proof test	PFDavg	SFF	Failure tolerance	Repair time (hours)	MTBFsp (years)	NooM voting		Total PFDavg
Sensor subsystem																
Pressure measurement fails																
Pressure measurement	5,0	0,6	8	0,5	0,025	0,05	4	0,99								
Cabling	1,0	0,6	8	0,2	0,025	0,05	4	0,99								
Terminal * 2	0,24	0,6	8	0,1	0,025	0,05	4	0,99								
Inmpulse piping	4,0	0,6	8	0,5	0,025	0,05	4	0,99								
Total	10,2		8				4	0,99	**3,02E-03**	**0,82**	**1**	**8**	**10**	1 *oo* 2		*3,02E-03*
Actuator subsystem																
Stopping of ID -fan fails																
Main contactor	1,2	0	8	0,35	0	0	4	0,99								
Terminals	0,24	0	8	0,1	0	0	4	0,99								
Total	1,44		8				4	0,99	**7,90E-03**	**0,69**	**0**	**8**	**115**	1 *oo* 1	OR	
Trip relay	0,4	0	8	0,35	0,025	0,05	4	0,99								
Cabling	1,0	0	8	0,2	0,025	0,05	4	0,99								
Terminal * 2	0,24	0	8	0,1	0,025	0,05	4	0,99								
Total	1,64		8				4	0,99	**3,69E-04**	**0,78**	**1**	**8**	**45**	1 *oo* 2		*8,27E-03*

SIF integrity	*PFDavg*	*MTBFsp*	*Safety integrity*		*PFDavg*	*SIL*
Sensor subsystem	3,02E-03		OR		**1,14E-02**	**TET 1**
Logic subsystem, Safety PLC	1,50E-04					
Actuator subsystem	8,27E-03					

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

- Esimerkin SIL2 –tason laskennalliset vaatimukset eivät täyty
- Arkkitehtuuristen vaatimusten suhteen tilanne on OK
- Mitä tehdään?

Turvatoiminnon vikaantumistodennäköisyyden laskenta IEC 61508 –standardin mukaisesti

SIL calculation of a safety related function

Component	Failure rate λ (10 ^ -6)	DC	Repair time (hours)	Dang. fail.	βd	β	TI (years)	Non-prefect proof test	PFDavg	SFF	Failure tolerance	Repair time (hours)	MTBFsp (years)	NooM voting		Total PFDavg
Sensor subsystem																
Pressure measurement fails																
Pressure measurement	5,0	0,9	8	0,5	0,025	0,05	4	0,99								
Cabling	1,0	0,9	8	0,2	0,025	0,05	4	0,99								
Terminal * 2	0,24	0,9	8	0,1	0,025	0,05	4	0,99								
Inmpulse piping	4,0	0,9	8	0,5	0,025	0,05	4	0,99								
Total	10,2		8				4	0,99	**5,01E-04**	**0,95**	**1**	**8**	**10**	1 *oo* 2		*5,01E-04*
Actuator subsystem																
Stopping of ID -fan fails																
Main contactor	1,2	0	8	0,35	0	0	4	0,99								
Terminals	0,24	0	8	0,1	0	0	4	0,99								
Total	1,44		8				4	0,99	**7,90E-03**	**0,69**	**0**	**8**	**115**	1 *oo* 1	OR	
Trip relay	0,4	0	8	0,35	0,025	0,05	4	0,99								
Cabling	1,0	0	8	0,2	0,025	0,05	4	0,99								
Terminal * 2	0,24	0	8	0,1	0,025	0,05	4	0,99								
Total	1,64		8				4	0,99	**3,69E-04**	**0,78**	**1**	**8**	**45**	1 *oo* 2		*8,27E-03*

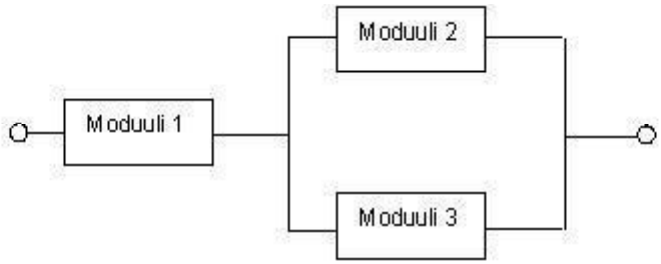
SIF integrity	*PFDavg*	*MTBFsp*	*Safety integrity*		*PFDavg*	*SIL*
Sensor subsystem	5,01E-04		OR		**8,92E-03**	**TET 2**
Logic subsystem, Safety PLC	1,50E-04					
Actuator subsystem	8,27E-03					

Vikaantumistodennäköisyyden laskentamenetelmistä

- Menetelmien vertailusta
  - Mielletään laskenta menetelmät ”mustina laatikkoina”
  - Laskentamenetelmät ottavat syötteinä informaatiota järjestelmästä ja tuottavat arvion järjestelmän turvallisuuden eheydestä
  - Verrataan menetelmiä sillä, kuinka paljon ne vaativat tietoa tarkasteltavasta järjestelmästä, mitä laskennan aikana tehdään ja mitä ne tuottavat tulosinformaationa

Vikaantumistodennäköisyyden laskentamenetelmistä

- Luotettavuuslohkokaaviot
  - Toimintavarmuuden laskentaan käytetty menetelmä, jolla on graafinen esitysmalli
  - Järjestelmä koostuu itsenäisistä moduuleista, joita voidaan asettaa rinnan tai sarjaan ja näistä edelleen muodostaa n-out-of-k –tason äänestysportteja
  - Yhden moduulin vikaantuminen ei aiheuta toisen moduulin vikaantumista

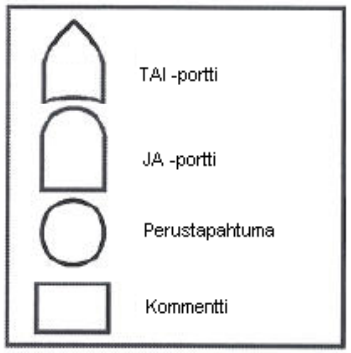


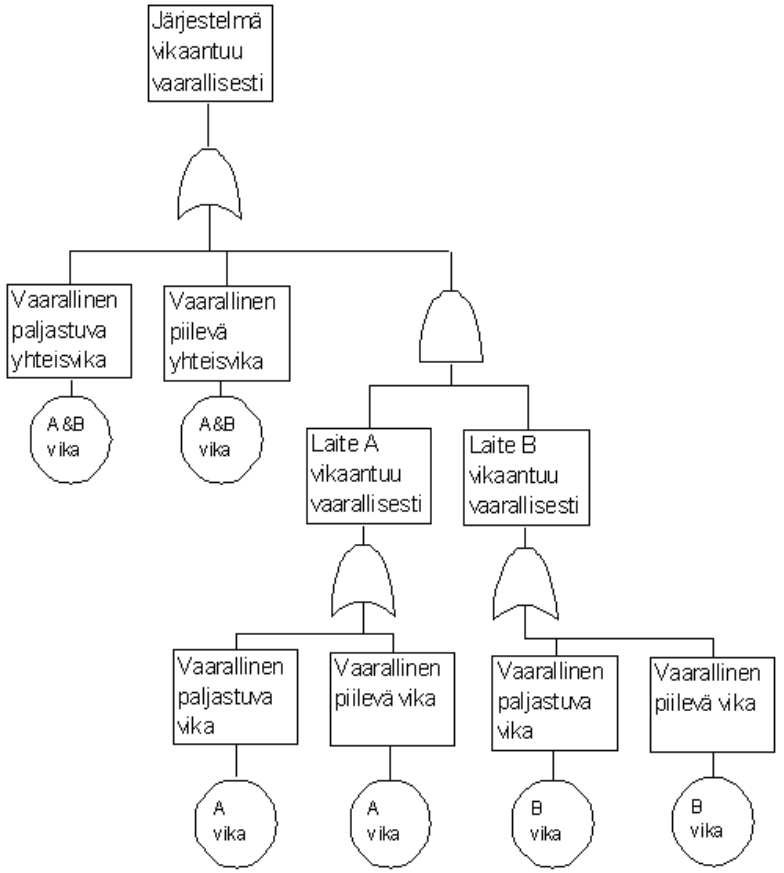
Vikaantumistodennäköisyyden laskentamenetelmistä

- Vikapuuanalyysi
  - Laskenta perustuu helposti ymmärrettävään graafiseen esitysmalliin, jossa tarkastelun kohteena on niin kutsutun ”top-tapahtuman” toteutuminen
  - PFD –laskennassa top-tapahtumana pidetään vaarallista vikaantumista
  - Vikapuun tapahtumat yhdistetään boolen logiikan mukaisesti JA sekä TAI -tapahtumiin

Vikaantumistodennäköisyyden laskentamenetelmistä

- Esimerkki vikapuun mallintamisesta 1oo2 –konfiguraation vikaantumista varten





Vikaantumistodennäköisyyden laskentamenetelmistä

- Markovin malliin perustuva analyysi
  - Malli koostuu tiloista ja tilasiirtymistä
  - Tilasiirtymät kuvaavat komponentin vikaantumista ja korjaustoimenpiteitä
  - Tilasiirtymien mahdollisuutta kuvaa vakioarvoiset vikatiheyksien arvot
  - Matemaattisesti malli koostuu joukosta differentiaalisia yhtälöitä
    - Analyyttinen ratkaisu tai numeerinen ratkaisu (iterointi)
  - Malli voi kasvaa hyvin monimutkaiseksi ja raskaaksi mallinnettava järjestelmän koon kasvaessa

Vikaantumistodennäköisyyden laskentamenetelmistä

- Esimerkki Markovin mallista, joka kuvaa 1oo2 – konfiguraation vikaantumista