

VIKAPUUANALYYSI TUOTANTOJÄRJESTELMÄN LUOTETTAVUUDEN JA TURVALLISUUDEN MÄÄRITYKSESSÄ

SISÄLLYSLUETTELO

1	Johdanto	244
2	Alustavat toimenpiteet vikapuanalyysin suorittamiseksi: vioittumis- ja vaikutusanalyysi	245
3	Järjestelmän vikapuun laadinta	248
	3.1 Vikapuun laatimisen vaihejako	249
	3.2 Vikapuussa käytettävät symbolit	250
	3.2.1 Loogiset symbolit	251
	3.2.2 Tapahtuma-symbolit	252
	3.2.3 Esimerkkejä symbolien käytöstä	253
4	Vikapuun analysointi	257
	4.1 Kvalitatiivinen analyysi	257
	4.2 Kvantitatiivinen analyysi	258
	4.2.1 Simulointimenetelmät	259
	4.2.2 Analyytiset menetelmät	261
5	Esimerkki vikapuun laadinnasta ja sen ratkaisemisesta	262
	5.1 Huipputapahtuman todennäköisyys	264
	5.2 Huipputapahtuman vikataajuusfunktio	265
	Summary	268
	Lähteet	270

VIKAPUUANALYYSI TUOTANTOJÄRJESTELMÄN LUOTETTAVUUDEN JA TURVALLISUUDEN MÄÄRITYKSESSÄ

1 JOHDANTO

Luotettavuusanalyysin tehtävänä on useimmiten selvittää tarkasteltavan tuotanto- tai muun järjestelmän kyky suorittaa sille suunnitellut tehtävät. Nämä tehtävät voivat eri järjestelmillä olla luonteeltaan varsin erilaiset. Esimerkiksi säätöjärjestelmän on jatkuvasti toimittava tietyllä spesifioidulla tavalla; turvajärjestelmästä taas vaaditaan, että järjestelmä on toimintakunnossa sillä hetkellä, jolloin sen toimintaa tarvitaan. Tarkastettavasta järjestelmästä ja sen käyttötarkoituksesta riippuen voi luotettavuusanalyysin täsmällisemmin määritellyksi tehtäväksi muodostua yhden tai useamman seuraavassa lueteltavan seikan selvittäminen:

- todennäköisyys, että järjestelmä on toimintakunnossa tietyllä hetkellä (järjestelmän käytettävyys)
- todennäköisyys, että järjestelmä toimii tietyn ennalta valitun ajanjakson (järjestelmän luotettavuus)
- keskimääräinen järjestelmän vioittumisten väliaika
- järjestelmän vikataajuus (hasardifunktio)
- järjestelmän vioittumisen suhteen kriittisimmät komponentit tai osajärjestelmät (esim. minimitoimintakelvottomuustiet).

Kuten luettelosta helposti huomataan, selvitettävät asiat voivat olla luonteeltaan joko kvantitatiivisia tai kvalitatiivisia. Tässä kirjoituksessa esiteltävä vikapuanalyysi tarjoaa mahdollisuuden kumman tahansa lähestymistavan, kvalitatiivisen tai kvantitatiivisen tai molempien valitsemiseksi järjestelmän luotettavuusongelmien tarkastelemiseksi.

Vikapuuanalyysin historia käsitteiden ja perusmenetelmien osalta ulottuu 1960-luvun alkuun. Ensimmäisinä tämän tekniikan kehittäjinä mainitaan Bell Telephone Laboratories ja Boeing Company.¹

¹ Ks. esim. Fussell et al., Fault trees - a state of..., s.51 ja Nieuwhof, An introduction to fault tree..., s. 106.

Paitsi näiden yhtymien edustamalla tietoliikenne- ja ilma- liikennejärjestelmien aloilla vikapuuanalyysi on sittemmin saavuttanut merkittäviä sovellutuksia erityisesti atomivoimalaitosten, kemiallisen teollisuuden tuotantolaitosten ja sotilaallisten järjestelmien piirissä¹, ts. yleensä kaikkialla, missä järjestelmän luotettavuuteen on mahdollisten vikojen järjestelmän toiminnalle tai yleiselle turvallisuudelle aiheuttamien seuraamusten vakavuuden takia muutenkin kiinnitetty erityistä huomiota.

Vikapuunenettelmän suosio järjestelmien luotettavuuskysymysten analysoinnissa perustuu ennen kaikkea menetelmän monipuolisuuteen ja joustavuuteen.² Edellä jo viitattiin menetelmän tarjoamaan mahdollisuuteen valita analyysimuodoksi joko kvalitatiivinen (esim. järjestelmän heikkojen kohtien etsiminen) tai kvantitatiivinen analyysi (järjestelmän luotettavuuteen liittyvien tunnuslukujen määrittäminen). Vikapuun yksityiskohtaisuuden aste on myös helposti muunneltavissa järjestelmän komponenttitasosta laajojen osajärjestelmien tasolle saakka kulloistenkin käyttötarkoitusten mukaisesti. Valmiin vikapuun käyttömuodot ovat niin ikään "kaksisuuntaiset". Etenemällä puun latvoista sen juureen saadaan selville järjestelmän kustakin osasta lähtevät vikojen seurausketjut ja niiden vaikutukset koko järjestelmän luotettavuuteen. Todetun järjestelmävirian tapauksessa taas vikapuun tarjoaa välineen vian yhä yksityiskohtaisemmaksi paikallistamiseksi ja lopulta varsinaisen vian aiheuttajan löytämiseksi.

2 ALUSTAVAT TOIMENPITEET VIKAPUUANALYYSIN SUORITTAMISEKSI: VIOITTUMIS- JA VAIKUTUSANALYYSI

Järjestelmän luotettavuusanalyysin lähtökohdaksi tulee olla yksityiskohtainen kuvaus analysoidavasta järjestelmästä. Tämän kuvauksen tulee sisältää ainakin seuraavat asiat:³

¹ Edellisten lisäksi ks. myös Crosetti, Fault tree analysis..., s. 465 ja Powers and Tompkins, Fault tree synthesis..., s.376.

² Vikapuunenettelmän ominaisuuksista ja käyttötarkoituksista ks. tarkemmin esim. Fussel et al., mt. s.51 ja Nieuwhof, mt. s.105.

³ IEEE guide for general principles..., s. 11.

- (1) analysoitavan järjestelmän ja sen tehtävän määrittäminen
- (2) järjestelmän toiminnan ja suunnitellun käytön kuvaus
- (3) vikojen identifiointi
- (4) järjestelmän ympäristöolosuhteiden kuvaus.

Sen jälkeen kun järjestelmä ja sen suunniteltu käyttö on näin määritetty, voidaan suorittaa varsinaisen luotettavuusanalyysi. Luotettavuusanalyysi etenee tavallisesti vaiheittain seuraavasti:

- (1) identifioidaan merkittävät viat ja niiden seuraukset, ns. vioittumiset ja vaikutusanalyysi VVA (engl. Failure Mode and Effects Analysis - FMEA)
- (2) esitetään yllä mainittu informaatio taulukon, vikapuun tms. muodossa
- (3) suoritetaan edellisten kohtien perusteella järjestelmän kokonaisluotettavuuden määrittäminen ja ratkaistaan asetetut ongelmat.

Tämän esityksen tarkoituksena on keskittyä analyysin vaiheisiin 2 ja 3 erityisesti silloin, kun analyysivälineenä on vikapuunenettelmä. Vaiheen 2 muodostaa tällöin vikapuun konstruointi, vaiheen 3 laaditun vikapuun ratkaiseminen, sen kvalitatiivinen ja kvantitatiivinen analyysi. Tässä jaksossa luodaan lyhyt katsaus varsinaista vikapuuanalyysia edeltävään vaiheeseen, vioittumiset ja vaikutusanalyysiin.

Vioittumiset ja vaikutusanalyysi on järjestelmän luotettavuuden ja turvallisuuden induktiivinen analyysimenettelmä.² Siinä lähdetään liikkeelle järjestelmän yksityisistä komponenteista ja niiden mahdollisista vioista, määritetään vikojen vaikutukset ja seuraukset järjestelmän muihin osiin ja lopulta koko järjestelmän toimintaan.³

Vioittumiset ja vaikutusanalyysi on siten erityisesti järjestelmän suunnitteluvaiheessa esiin tuleva formalisoitu tekniikka, jolla

¹ IEEE guide for..., s.8 ja Komi, Vioittumiset ja vaikutusanalyysi, s.1.

² Lambert, System modeling for reliability..., s.4.

³ Powers and Tompkins, mt. s.376.

etsitään vastausta järjestelmän luotettavuutta ja turvallisuutta koskeviin, tyyppiä "entä jos" oleviin kysymyksiin.

Tarkemmin eriteltyinä vioittumis- ja vaikutusanalyysin tehtäväksi voidaan katsoa seuraavien osavaiheiden selvittäminen:¹

- (1) Identifioidaan järjestelmän kaikki komponentit tai alimman tason modulit ja määritetään niiden tehtävät ja tekniset tiedot.
- (2) Määritetään kunkin komponentin osalta kaikki mahdolliset vioittumisyyt, myös usean komponentin yhtäaikaisen vioittumisen syyt (esim. ympäristölämpötilan nousu).
- (3) Määritetään komponentin kaikki mahdolliset vioittumistavat (esim. venttiili: ei avaudu, ei sulkeudu, vuotaa).
- (4) Määritetään komponentin kunkin vioittumistavan välittömät seuraukset (esim. venttiilin sulkeutumattomuus aiheuttaa siihen liittyvän säiliön liikätyttymisen).
- (5) Määritetään ko. komponentin ko. vioittumistavan vaikutus koko järjestelmän toimintaan (esim. tietyn venttiilin vuotaminen ei merkitse järjestelmävikaa).
- (6) Määritetään, miten järjestelmän suunnittelussa on varauduttu ilmaisemaan ko. vika (esim. merkkilamppu, jaksottainen koestus).
- (7) Arvioidaan, onko vika seuraamuksiltaan turvallinen vai vaarallinen (esim. räjähdys).
- (8) Selvitetään komponentin kunkin vioittumistavan vika- taajuuden ja korjausajan jakautumat, mikäli mahdollista. Tätä vaihetta ei varsinaisesti lueta vioittumis- ja vaikutusanalyysiin kuuluvaksi, mutta välttämättömänä toimenpiteenä varsinaista vikapuuanalyysia varten se on kuitenkin mainittu tässä yhteydessä.
- (9) Selvitetään, onko järjestelmässä varauduttu ja miten havaitun vian kompensoimiseksi sopivilla järjestelyillä.

¹ Powers and Tompkins, mt. s. 378 ja IEEE guide..., s. 11 ja Komsa, mt. s. 5.

Vioittumis- ja vaikutusanalyysin tuloksena saadaan näin järjestelmän jokaisen yksityisen komponentin jokaisen eri vioittumis- muodon osalta yksityiskohtainen kuvaus siitä, miten järjestelmä reagoi ilmenneeseen komponenttivikaan tai niiden yhdistelmään, mikä vaikutus tällä on järjestelmän luotettavuuteen ja turvallisuuteen ja miten järjestelmän puitteissa on varauduttu tällaisten poikkeustilanteiden varalle.

3. JÄRJESTELMÄN VIKAPUUN LAADINTA

Järjestelmän esittäminen vikapuun muodossa ja tämän vikapuun analysointi on eräs tapa käyttää hyväksi ja edelleen jalostaa sitä informaatiota, joka on saatu edeltävän vioittumis- ja vaikutusanalyysin tuloksena. Ongelmien lähestymistapa on nyt täysin päinvastainen kuin vioittumis- ja vaikutusanalyysissä, so. deduktiivinen.¹ Tarkastelun lähtökohdaksi valitaan tietty järjestelmän toiminnan tai turvallisuuden kannalta ei-toivottu, järjestelmähäiriötä merkitsevä tapahtuma, nk. huipputapahtuma (esim. räjähdys, tulipalo, tuotantokoneiston pysähtyminen), ja siirtymällä tämän jälkeen asteittain alemman tason vikoihin selvitetään lopulta ne komponenttitason viat ja vikojen yhdistelmät, jotka ovat tai voivat olla ei-toivotun huipputapahtuman alkusyynä. Järjestelmällä voi siten olla useita eri vikapuita, jokaista vioittumis- ja vaikutusanalyysin perusteella määritettyä järjestelmävikaa lajia kohti omansa. Kussakin vikapuussa tarvitsee ottaa huomioon vain ne alemman tason viat, joilla valitun huipputapahtuman kannalta on merkitystä. Varsinainen vikapuu on puumuotoinen (vrt. esim. päätöspuu) looginen diagrammi, joka kuvaa informaatiovirtojen, so. komponenttivikojen vaikutusten ja seurausten, etenemistä tarkasteltavassa järjestelmässä. Vikapuun perusrakenteosot ovat tapahtumien loogisia kytkentöjä, nk. loogisia portteja.² Looginen portti määrittelee ne sisäänmenotapahtumia (alemman tason vikoja) koskevat ehdot, joilla ulosmenotapahtuma (ylemman tason vika) sattuu. Puun juuri vastaa ylimmän tason tapahtumaa, huipputapahtumaa,

¹ Powers and Tompkins, mt. s. 376, Lambert, mt. s. 5

² Powers and Tompkins, mt. s. 379, Nieuwhof, mt. s. 105, Fussell et al., mt. s. 52.

puun latvat ovat alimman tason tapahtumia, yksityisten komponenttien eri vioittumismuotoja. Seuraavissa jaksoissa kuvataan vikapuun laadintaa yksityiskohtaisemmin esittämällä työhön liittyvät eri vaiheet sekä yleisesti käytetyt symbolit.

3.1 VIKAPUUN LAATIMISEN VAIHEJAKO

Vikapuun laatiminen etenee normaalisti seuraavina vaiheina.¹

- (1) Määritellään tarkastelun kohteeksi otettava huipputapahtuma. Tämä huipputapahtuma on siis jokin vioittumis- ja vaikutusanalyysissä tunnistettu, järjestelmän toiminnan kannalta ei-toivottu tapahtuma. Koska järjestelmällä voi olla useita eri huipputapahtumia, on tärkeätä, että tarkasteltavan huipputapahtuman määrittely suoritetaan täsmällisesti.
- (2) Määritetään kaikki ne lähinnä alemman tason tapahtumat, joiden suoranaisena seurauksena huipputapahtuma voi esiintyä. Lisäksi määritetään se looginen kytkentä, joka huipputapahtuman sattumiseksi näiden alemman tason tapahtumien välillä vallitsee. Kukin tällainen alemman tason tapahtuma merkitsee oman haaran syntymistä vikapuuhun.
- (3) Valitaan jokin edellisessä kohdassa määritetyistä tapahtumista (haaroista) ja määritetään siihen liittyvät edelleen alemman tason tapahtumat ja niiden välinen looginen kytkentä (vikapuun haara jaetaan osahaaroihin).
- (4) Kohdan 3 mukaista menettelyä jatketaan niin kauan kunnes jokainen puun haara päättyy alkeistapahtumaan, so. tapahtumaan, jota ei voida tai ei ole tarpeellista enää jakaa alemman tason tapahtumiksi. Tällainen alkeistapahtuma on normaalisti yksityisen komponentin jokin yksityinen vika.
- (5) Alkeistapahtumiin liitetään niiden esiintymiseen liittyvät tiedot kuten esim. vian esiintymistodennäköisyys, vikataajuusfunktio, korjausajan jakautuma jne.

¹ IEEE guide..., s. 15 ja Crosetti, mt. s. 465-466.

Edellä kuvattu vikapuun laadintatekniikka on kyllin formaalinen mahdollistaakseen "hardware"-orientoituneen vikapuun laadinnan myös automaattisesti tietokoneella. Haluttaessa kuitenkin "täydellistä" vikapuuta, joka ottaa laitteiston puutteiden lisäksi huomioon myös ympäristötekijöistä ja inhimillisestä käyttäytymisestä aiheutuvat vikamahdollisuudet, joudutaan turvautumaan pääasiassa käsityönä suoritettavaan puun konstruointiin.¹ Tämä käsityönä suoritettava puun laadinta yhdessä puun helposti laajaksi paisuvan koon kanssa aiheuttaakin nyt sen, että vikapuun laadinta on yleensä varsin työläs työjakso. Esimerkkinä mainittakoon erään Yhdysvaltain atomivoimalan tietylle osalle laadittu vikapuu, joka vaati valmistuakseen 25 miestyövuotta.²

3.2 VIKAPUUSSA KÄYTETTÄVÄT SYMBOLIT

Seuraavassa käydään läpi tavallisimmat vikapuussa käytettävät symbolit. Esityksessä noudatetaan Crosetti'n³ mukaisia symboleja. Samat symbolit, joskaan eivät aivan yhtä täydellisenä luettelona, esiintyvät useimmissa tämän esityksen lähdekirjoituksissa. Valtion teknillisessä tutkimuskeskuksessa sen sijaan on omaksuttu hieman poikkeava käytäntö.⁴

Aluksi esitetään symboleista luettelo ja lyhyt kuvaus, jonka jälkeen symbolien merkitystä ja käyttöä havainnollistetaan yksinkertaisin esimerkein. Symbolit on esityksessä jaettu kahteen ryhmään: loogisia kytkentöjä kuvaaviin symboleihin ja tapahtumia kuvaaviin symboleihin.

¹ Fussell et al., mt. s. 52.

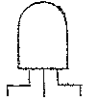
² Powers and Tompkins, mt. s. 380.

³ Crosetti, mt. s. 469-471.

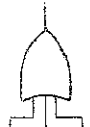
⁴ Ks. esim. Harju, Korjaamattoman järjestelmän... ja Harju, Monte Carlo...

3.2.1 LOOGISET SYMBOLIT

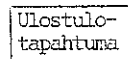
Ulostulo



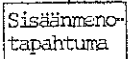
Sisäänmenot



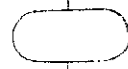
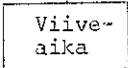
Sisäänmenot



Ehdollinen sisäänmeno



Ulostulo



Sisäänmeno

Ulostulo



Sisäänmenot

JA-portti: kaikkien sisäänmenotapahtumien samanaikainen esiintyminen on edellytyksenä ulostulotapahtuman esiintymiselle

TAI-portti: ulostulotapahtuma esiintyy jo yhdenkin sisäänmenotapahtuman esiintyessä

ESTO-portti: ulostulotapahtuma esiintyy sisäänmenotapahtuman esiintyessä vain jos ehdollinen sisäänmenotapahtuma esiintyy samanaikaisesti varsinaisen sisäänmenotapahtuman kanssa

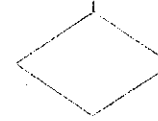
VIIVE-portti: ulostulotapahtuma esiintyy sen jälkeen kun viiveen ilmoittama aika sisäänmenotapahtuman esiintymisestä on kulunut

MATRIISI-portti: ulostulotapahtuma esiintyy yhden tai useamman sisäänmenotapahtuman esiintyessä; ulostulotapahtuman esiintymisen edellytyksenä olevien sisäänmenotapahtumien kombinaatio on vielä tarkemmin spesifioimatta, osa sisäänmenotapahtumista voi vielä olla määrittämättäkin

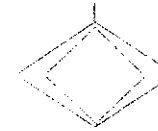
3.2.2 TAPAHTUMA-SYMBOLIT



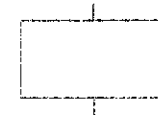
YMPYRÄ: alkeistapahtuma - tapahtumaa ei voida enää kehittää alemman tason tapahtumiksi; datat alkeistapahtumaa varten ovat olemassa tai hankittavissa



TIMANTTI: tapahtuma, joka vielä olisi kehitettävissä alemman tason tapahtumiksi, mutta jota tarkasteltavassa vikapuussa pidetään alkeistapahtuman luonteisena



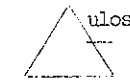
KAKSOISTIMANTTI: tapahtuma, joka tarkasteltavaa vikapuutakin varten on vielä kehitettävä alemman tason tapahtumiksi



SUORAKULMIO: edustaa tapahtumaa, joka on tuloksena alemman tason tapahtumien yhteisvaikutuksesta (nimen antaminen loogisen portin ulostulotapahtumalle)



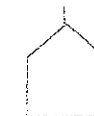
KOLMIO: yhdistävä tai siirtävä symboli. Viiva kolmion kärjessä merkitsee informaation (jo kehitetyn tapahtuman, osapuun tms.) liittämistä vikapuuhun, viiva kolmion sivulla merkitsee vastaanotetun informaation siirtämistä ko. puun kohdasta muualle



KÄRKIKOLMIO: symboliin liittyvä sisäänmeno on vastaava, ei kuitenkaan välttämättä sama tapahtuma kuin symbolissa on ilmoitettu

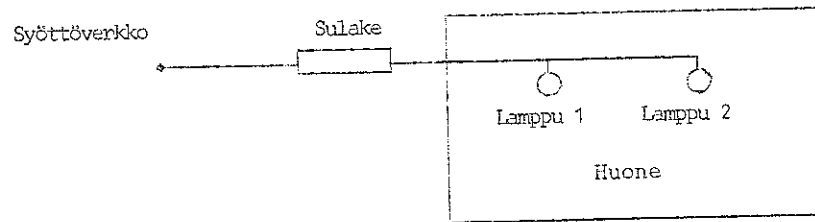


TALO: tapahtuma, jonka odotetaan normaalisti esiintyvän, mutta jonka ei-esiintyminen aiheuttaa muutoksen puun loogiseen rakenteeseen ("Häipäisy-tapahtuma")



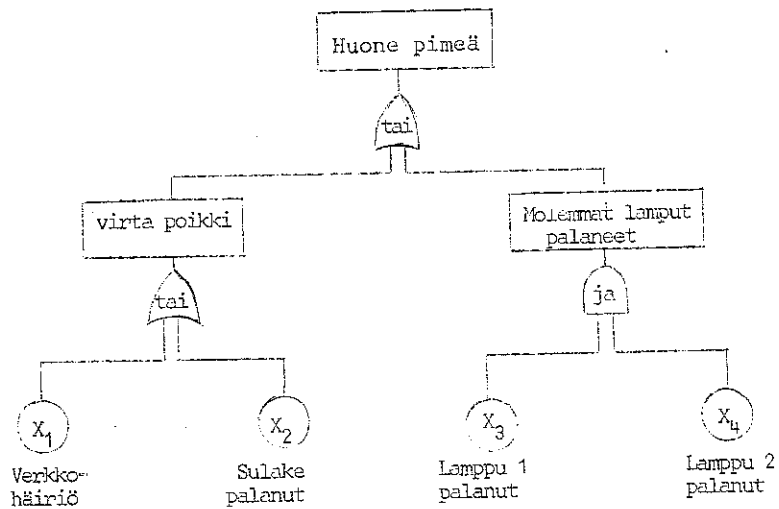
3.2.3 ESIMERKKEJÄ SYMBOLIEN KÄYTÖSTÄ

Esimerkkinä symbolien käytöstä tarkastellaan vikapuuta, joka on laadittu yksinkertaista valaistusjärjestelmää varten. Kuvassa 1 on pimeä huone, jonka valaistus hoidetaan kahdella lampulla. Lamput saavat virtansa yhteisestä verkosta saman sulakkeen kautta.



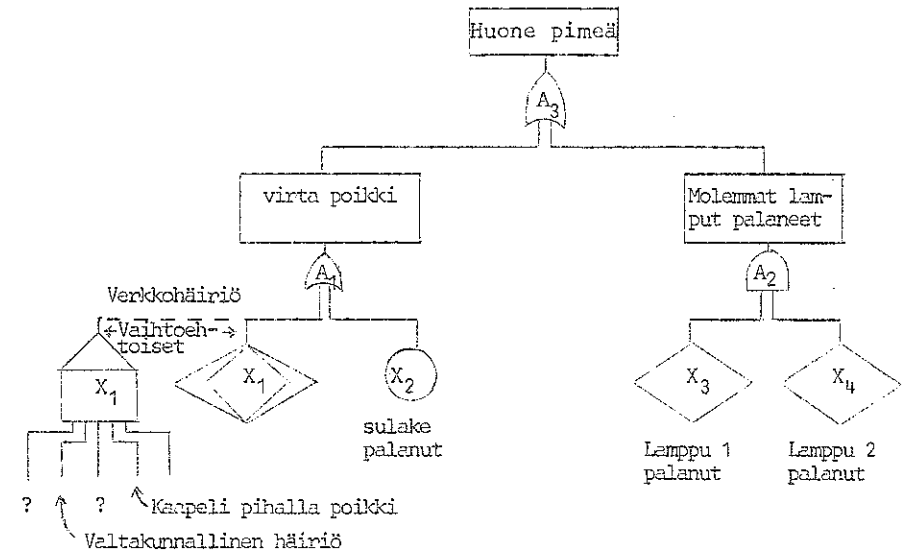
Kuva 1. Huoneen valaistusjärjestelmä

Ei-toivottu huipputapahtuma on nyt huoneen jääminen pimeäksi. Oletetaan, että huipputapahtuma esiintyy, kun joko molemmat lamput ovat palaneet tai lamput jäävät vailla sähkövirtaa. Sähkövirran taas oletetaan katkeavan sulakkeen palamisen tai verkkohäiriön seurauksena. Näillä edellytyksillä saadaan valaistusjärjestelmän huipputapahtumalle "huone pimeä" kuvan 2 vikapuu.



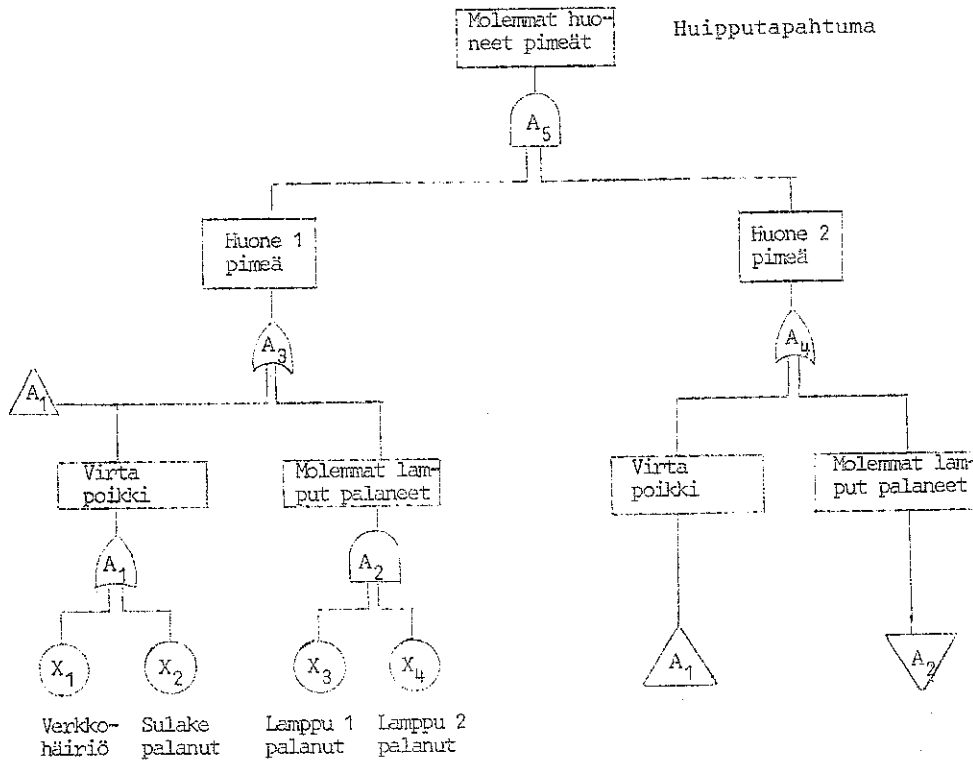
Kuva 2. Valaistusjärjestelmän vikapuu

Kuvan 2 vikapuussa tapahtumat X_1 , X_2 , X_3 ja X_4 oletettiin alkeis-tapahtumiksi. Voidaan kuitenkin heti huomata, että esimerkiksi tapahtumille X_3 ja X_4 on vielä löydettävissä useita eri syitä, kuten tärinä, ylijännite, valmistusvirhe jne. Koska lampun toiminta kuvaavat tiedot ovat kuitenkin useimmiten lamppukohtaisia, ei enää eri vikamuotoja eritteleviä, on tapahtuma "lamppu palanut" perusteltua valita perustapahtumaksi. Valitsemalla kuvan 3 vikapuussa X_3 :n ja X_4 :n symboleiksi timantit on haluttu korostaa näiden tapahtumien edelleen kehittämismahdollisuutta, vaikka tätä mahdollisuutta ei ko. vikapuussa olekaan käytetty hyväksi. Tapahtuman X_1 (verkkohäiriö) tapauksessa sen sijaan on lähdetty siitä, että ennen vikapuun lopullista muotoa ja sen analysointia tapahtuma X_1 on edelleen kehitettävä alemman tason tapahtumiksi. Tästä merkinä kaksoistimanttisymboli. Mikäli jo ennen lisäselvityksiä jotkin X_1 :n syistä ovat tiedossa, voidaan kaksoistimantti korvata matriisi-portilla ja luetella siinä yhteydessä jo tunnetut sisäänmenotapahtumat. Näillä lisäedellytyksillä valaistusjärjestelmän vikapuu saa kuvassa 2 esitetyn vikapuun sijasta kuvassa 3 esitetyn muodon.



Kuva 3. Vaihtoehtoinen vikapuu valaistusjärjestelmälle

Kolmio- ja kärkikolmio-symbolien käytön havainnollistamiseksi tarkastellaan kahden kuvassa 1 esitetyn kaltaisen huoneen valaistusjärjestelmää. Huoneisiin tulee virta samasta verkosta yhteisen sulakkeen kautta. Muuten ovat olettamukset samat kuin kuvan 2 vikapuuta laadittaessa. Tulos on esitetty kuvassa 4. Koska kummat-

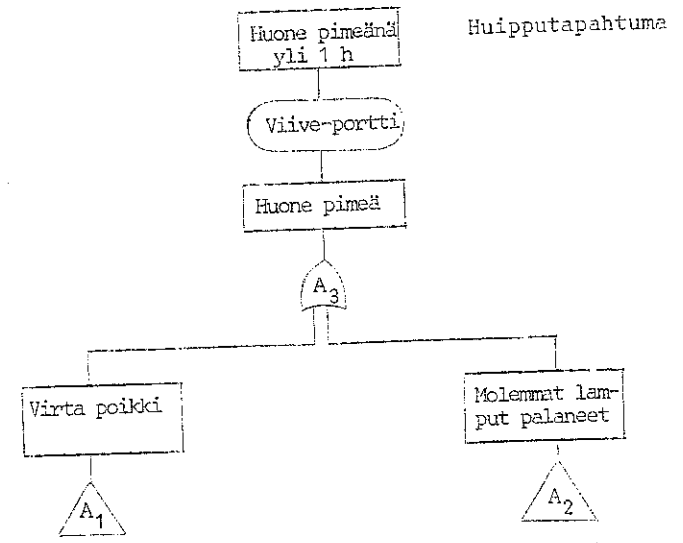


Kuva 4. Kahden huoneen valaistusjärjestelmän vikapuuta

kin huoneista käyttävät samaa virtalähdettä, on tapahtuman "virta poikki" muodostuminen alkeistapahtumista täysin samanlainen kummankin huoneen osalta. Vikapuussa tämä ilmenee siten, että huoneen 1 yhteydessä kehitettyä tapahtumaa A_1 ei enää kehitetä uudelleen huoneen 2 osalta, vaan kolmioiden avulla ilmoitetaan, että tapahtuma A_1 on sisäänmenotapahtumana paitsi tapahtumalle A_3 (huone 1 pimeä) myös tapahtumalle A_4 (huone 2 pimeä). Kärkikolmio ja siinä oleva tapahtuma A_2 puolestaan ilmoittavat, että tapahtuman "molemmat

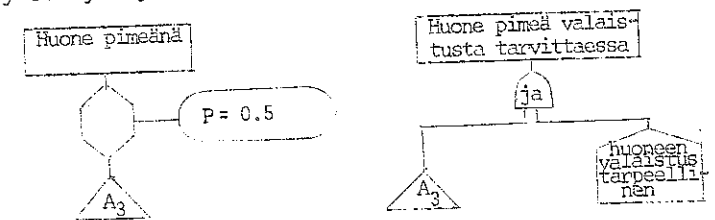
lamput palaneet" kehittämisen alkeistapahtumista on huoneen 2 osalta vastaavanlainen kuin huoneen 1 kohdalla (sekä lamppu 1 että lamppu 2 ovat palaneet). Tapahtumat eivät kuitenkaan ole välttämättä samat, esimerkiksi lamppuihin liittyvät datat saattavat olla erilaiset.

Viive-portin käyttöä havainnollistaa kuva 5. Siinä on oletettu, että ei-toivottu tapahtuma esiintyy vasta kun tilanne "huone pimeänä" on jatkunut yli tunnin. Tapahtumat A_1 ja A_2 viittaavat kuvan 3 vastaaviin tapahtumiin.



Kuva 5. Valaistusjärjestelmän vikapuun viive-portti

Esto-portin ja talon käyttöä havainnollistaa kuva 6. Esto-portti ja siihen liittyvä todennäköisyys 0.5 merkitsevät, että huipputapahtuma esiintyy A_3 :n (vrt.kuva 3) esiintyessä vain, jos ehdollinen sisäänmenotapahtuma, jonka esiintymistodennäköisyys on 0.5, esiintyy sen yhteydessä. Ehdollinen sisäänmenotapahtuma voisi tässä



Kuva 6. Valaistusjärjestelmän vikapuun esto-portti ja talo-symboli

yhteydessä olla esimerkiksi vaihtoehtoisen valolähteen, kuten päivänvalon, saatavuus (valaistusjärjestelmän pettäminen merkitsee huoneen pimeyttä vain vuorokauden 12 tunnin pituisena pimeänä ajanjaksona).

Talo-symbolia käytetään edustamaan tapahtumaa, jonka normaalisti oletetaan esiintyvän. Kuvassa 6 talo edustaa tapahtumaa "huone tarvitsee valaistusta", jolloin ei-toivottu huipputapahtuma on vastaavasti "huone pimeänä silloin kun valaistusta tarvittaisiin".

4 VIKAPUUN ANALYSOINTI

Tarkasteltavasta järjestelmästä laadittu vikapuun antaa jo sellaisenaan varsin paljon informaatiota ko. järjestelmästä ja sen toiminnasta. Vikapuusta selviävät erilaiset mahdollisuudet järjestelmän vioittumiseksi ja siitä nähdään komponenttinvian vaikutuksen eteneminen ja mahdollinen ulottuminen järjestelmävikaan saakka. Vikapuuta voidaan niin ikään käyttää oppaana paikallistettaessa järjestelmävikien tapauksessa vian alkuperää. Tässä tarkoituksessa lähdetään liikkeelle puun juuresta (huipputapahtumasta) ja suoritettujen tarkistusten jälkeen suljetaan pois kunnossa olevia järjestelmän osia vastaavat puun haarat, kunnes on "viollisia" haaroja ja pitkin edetty puun latvatasolle saakka ja paikallistettu näin vian perussyyt.

Varsinainen vikapuun käyttö perustuu kuitenkin siihen informaatioon, joka järjestelmästä on saatavissa vikapuun analysoinnin jälkeen. Analyysissa on erotettavissa kaksi päätyyppiä, kvalitatiivinen ja kvantitatiivinen.¹

4.1 KVALITATIIVINEN ANALYYSI

Vikapuun kvalitatiivinen analyysi käsittää lähinnä järjestelmävikien kaikkien mahdollisten yksikäsitteisten esiintymismuotojen määrittämisen. Tämä määrittäminen tapahtuu muodostamalla vikapuun minimitoimintakelvottomuusteiden joukko. Minimitoimintakelvottomuus-

¹ Fussell et al., mt. s. 52.

tie¹ on pienin mahdollinen joukko alkeistapahtumia (komponenttievikoja), joiden samanaikainen esiintyminen on välttämätön ja riittävä edellytys ko. minimitoimintakelvottomuustien aiheuttaman huipputapahtuman (järjestelmävikien) esiintymiselle. Kuvan 2 vikapuussa minimitoimintakelvottomuustiet ovat selvästi joukot $\{X_1\}$ (verkkohäiriö), $\{X_2\}$ (sulakehäiriö) ja $\{X_3, X_4\}$ (lamppuhäiriö).

Vikapuun yhteydessä ollaan yleensä kiinnostuneita tietyn, järjestelmän kannalta ei-toivotun tapahtuman esiintymisestä ja siihen liittyvistä olosuhteista. Luonnollisesti voidaan tarkastella myös edellytyksiä järjestelmän normaalia toimintaa varten. Kvalitatiivisen vikapuuanalyysin yhteydessä tämä merkitsee minimitoimintakelpoisuusteiden määrittämistä. Minimitoimintakelpoisuustiellä² tarkoitetaan pienintä sellaista joukkoa alkeistapahtumia, joiden samanaikainen ei-esiintyminen on välttämätön ja riittävä edellytys järjestelmän toimintakuntoisuudelle. Kuvan 2 vikapuun minimitoimintakelpoisuustiet ovat $\{X_1, X_2, X_3\}$ ja $\{X_1, X_2, X_4\}$.

Minimitoimintakelvottomuus- (ja -kelpoisuus) -teiden määrittäminen annettua vikapuuta on varsin helppoa myös automatisoivissa.³ Tämä on luonnollisesti seurausta puun hyvin jäsentyneestä rakenteesta ja siihen sisältyvistä loogisista lainalaisuuksista.

4.2 KVANTITATIIVINEN ANALYYSI

Täydelliseen vikapuun laadintaprosessiin kuului (vrt. jakso 3.1) myös alkeistapahtumien esiintymistä kuvaavien tietojen kokoaminen vioittumis- ja vaikutusanalyysin tuloksista ja näiden tietojen liittäminen vikapuuhun. Näitä tietoja ovat esim. vian esiintymistodennäköisyys, vian esiintymistiheys, vikataajuus (l. hasardi) funktio jne. Vikapuun kvantitatiivisen analyysin tehtävänä on johtaa näistä alkeistapahtumia koskevista tiedoista koko järjestelmän luotettavuuteen liittyvät tunnusluvut. Erään tätä tarkoitusta varten laaditun luotettavuusohjelmiston tulostamat tunnus-

¹ Engl. minimal cut, ks. esim. Fussell et al., mt. s. 52; suomenkielisestä nimestä ks. Harju, Monte Carlo..., s. 10.

² Harju, Monte Carlo..., s. 10.

³ Ks. Fussell et al., mt. s. 52 ja siinä viitattu kirjallisuus.

luvut esimerkiksi ovat:¹

- (1) huipputapahtuman esiintymistodennäköisyys
- (2) huipputapahtuman esiintymisten lukumäärän odotusarvo aikayksikköä kohti laskettuna
- (3) järjestelmän vikataajuus (hasardifunktio)
- (4) huipputapahtuman esiintymisten lukumäärän odotusarvo aikavälillä $(0, t)$.

Vastaavat tunnusluvut voidaan määrittää jokaiselle vikapuun tapahtumalle (portille) ja minimitoimintakelvottomuustielle.

Vikapuun ratkaisumenetelmän valintaan vaikuttavat ennen kaikkea järjestelmän tietyt ominaisuudet (järjestelmä korjattava/korjaamaton, loogiset portit riippuvat/riippumattomat) sekä ne tunnusluvut, jotka halutaan määrittää. Eräs perusjako vikapuuanalyysin yhteydessä käytetyille menetelmille on jako simulointimenetelmiin ja analyttisiin menetelmiin.²

4.2.1 SIMULOINTIMENETELMÄT

Vikapuun ratkaisumenetelmien kehitys on lähtenyt liikkeelle simulointimenetelmien alueella. Simulointi on edelleenkin tavallisin vikapuun ratkaisumenetelmästä.³ Yksityiset toteutukset poikkeavat luonnollisesti toisistaan, mutta perusratkaisuiltaan luotettavuussimulointiohjelmat noudattavat seuraavan jaottelun mukaisia toimintoja.⁴

- (1) Syöttötietoina luetaan järjestelmän vikapuu, alkeistapahtumiin liittyvät tiedot ja simuloinnin ohjaustiedot
- (2) Alkeistapahtumiin liittyvät tiedot generoidaan annetuista jakautumista satunnaislukuja käyttäen, tavallisimmin tapahtuman yksityinen esiintyminen kerrallaan.

¹ Fussell et al., mt. s. 52.

² Ks. esim. Crosetti, mt. s. 467 ja Harju, Korjaamattoman..., s.1.

³ Esim. Fussell, mt. s. 52 ja Harju, Korjaamattoman..., s.1.

⁴ Ks. Harju, Monte Carlo..., s. 12.

- (3) Ajan eteneminen voi tapahtua kahdella tavalla. Alkeellisemmässä menetelmässä jatkuva aika on jaettu lyhyihin osaväleihin. Kunkin välin lopussa tarkastetaan, onko välillä tapahtunut jotakin: komponentti vioittunut tai korjattu, seisokki alkanut jne. Kehittyneemmässä menetelmässä järjestelmän tila tarkastetaan ainoastaan niinä hetkinä, jolloin jokin tapahtuma esiintyy.
- (4) Järjestelmän vikapuu tutkitaan jokaisen uuden tapahtuman esiintyessä. Jos seurauksena on huipputapahtuma tai muu tarkkailtava tapahtuma, kerätään halutut tilastotiedot.
- (5) Simulointikertaa jatketaan kunnes järjestelmävikaa syntyy tai kiinnitetty simulointiaika ylitetään. Korjattavan järjestelmän käytettävyyttä tai muuta vastaavaa tunnuslukua simuloitaessa järjestelmävikien syntyminen ei katkaise simulointia vaan generoidaan korjaustapahtumaan liittyvät tiedot ja jatketaan simulointiaika loppuun. Järjestelmän stationääristä tilaa tutkittaessa tarvitsee kullekin alkeistapahtumalle suorittaa vain yksi generointi, tilan "tapahtuma esiintyy/ei esiinny" generointi. Tämä merkitsee vikapuunkin läpi käymistä vain kerran.
- (6) Simulointikertoja toistetaan ennalta kiinnitetty tai tulosten perusteella määräytyvä lukumäärä ja lasketaan kertyneen tilastoaineiston perusteella halutut tiedot ja suoritetaan tulostus.

Edellä kuvattu menetelmä on periaatteeltaan ns. suora Monte Carlo simulointi. Menetelmä tuottaa tunnusluvuille harhattomat estimaattorit.¹ Sen sijaan menetelmä ei välttämättä ole laskennallisesti tehokas. Tutkittaessa esimerkiksi hyvin pienen vioittumistodennäköisyyden omaavaa järjestelmää tarvitaan kohtuuttoman pitkä simulointiaika järjestelmävikien esiin saamiseksi. Simuloinnin nopeuttamiseksi on kehitetty useita nk. varianssinpienennysmenetelmiä. Luotettavuussimuloinnissa näistä tärkein on nk. importance sampling -menetelmä.² Importance sampling -menetelmän periaate on, että pyritään poimimaan vain kiinnostavia (tässä: vikatapahtumien esiintymisiä sisältäviä) näytteitä. Tämä tapahtuu muuttamalla

¹ Harju, Monte Carlo..., s. 16.

² Menetelmästä lähemmin ks. Harju, Monte Carlo..., s. 16-21 ja siinä viitattu kirjallisuus.

todellisia jakautumia niin, että tutkittavan tapahtuman esiintymistiheys kasvaa. Jakautuman muuttamisesta aiheutuva virhe on luonnollisesti otettava huomioon ja korjattava tuloksia laskettaessa.

4.2.2 ANALYYTTISET MENETELMÄT

Vikapuun ratkaiseminen analyytisesti tuo simulointiin verrattuna esiin tiettyjä etuja. Nämä edut ovat luonnollisesti paljolti samat kuin mitä analyytisillä menetelmillä yleensäkin on simulointimenetelmiin verrattuna. Tulokset ovat tarkkoja arvoja eivätkä vain näiden estimaatteja. Tulokset saadaan niin ikään yksityisten numeroarvojen sijasta yleisessä muodossa, kaikki saman tyyppiset, vain vakio- ja parametrisarvoiltaan toisistaan poikkeavat järjestelmät kattavina. Tämä luo esimerkiksi selvästi paremmat mahdollisuudet tietyn parametrin suhteen suoritettavan herkkyysanalyysin toteuttamiseksi.

Lietai on kuitenkin todettava, että analyytisillä menetelmillä on myös haittapuolensa. Suurimpana puutteena on se, että menetelmät sopivat vain tietyn tyyppisten järjestelmien tarkasteluun. Kysymykseen tulevat lähinnä korjaamattomat järjestelmät, korjattavat järjestelmät vain tietyissä erikoistapauksissa.¹ Eräät järjestelmän luotettavuuteen liittyvät tunnusluvut, kuten käytettävyys, jäävät niin ikään menetelmien ulottumattomiin. Korjaamattoman järjestelmän yhteydessä käytettävyys ei ole edes mielekäs käsite, korjattavan järjestelmän tapauksessa sen määrittämistä ei pystytä suorittamaan.

Mikäli vikapuu sisältää vain loogisia ja- ja tai-portteja ja nämä portit ovat toisistaan riippumattomat (alkeistapahtumat riippumattomat ja porteilla ei yhteisiä sisäänmenotapahtumia), on vikapuun ratkaiseminen tiettyjen tunnuslukujen (huipputapahtuman esiintymistodennäköisyys, huipputapahtuman hasardifunktio) suhteen varsin yksinkertaista. Ratkaisu toisistaan riippuvien porttien, kuitenkin riippumattomien alkeistapahtumien, tapauksessa on niin ikään löydettävissä esim. Boolean algebraa käyttäen. Kaikissa näissä

tapauksissa ratkaisu saadaan tarkasti suljetussa muodossa.¹ Muissa analyytisesti ratkaistuissa tilanteissa on jouduttu turvautumaan likimääräismenetelmiin.² Seuraavan jakson esimerkissä on suoritettu yksinkertaisen vikapuun analyytinen ratkaiseminen järjestelmän kahden eri tunnusluvun osalta.

5 ESIMERKKI VIKAPUUN LAADINNASTA JA SEN RATKAISEMISESTA

Tarkastellaan esimerkkinä vikapuun laadinnasta ja sen ratkaisemisesta järjestelmää, jonka muodostavat tavallinen polttomoottorilla varustettu rüchonleikkuukone ja sen käynnistämiseen liittyvät toimenpiteet.³ Moottori voidaan käynnistää akun tai käynnistinarun avulla. Tarkasteltava ei-toivottu huipputapahtuma tässä yhteydessä on tapahtuma "moottori ei käynnisty".

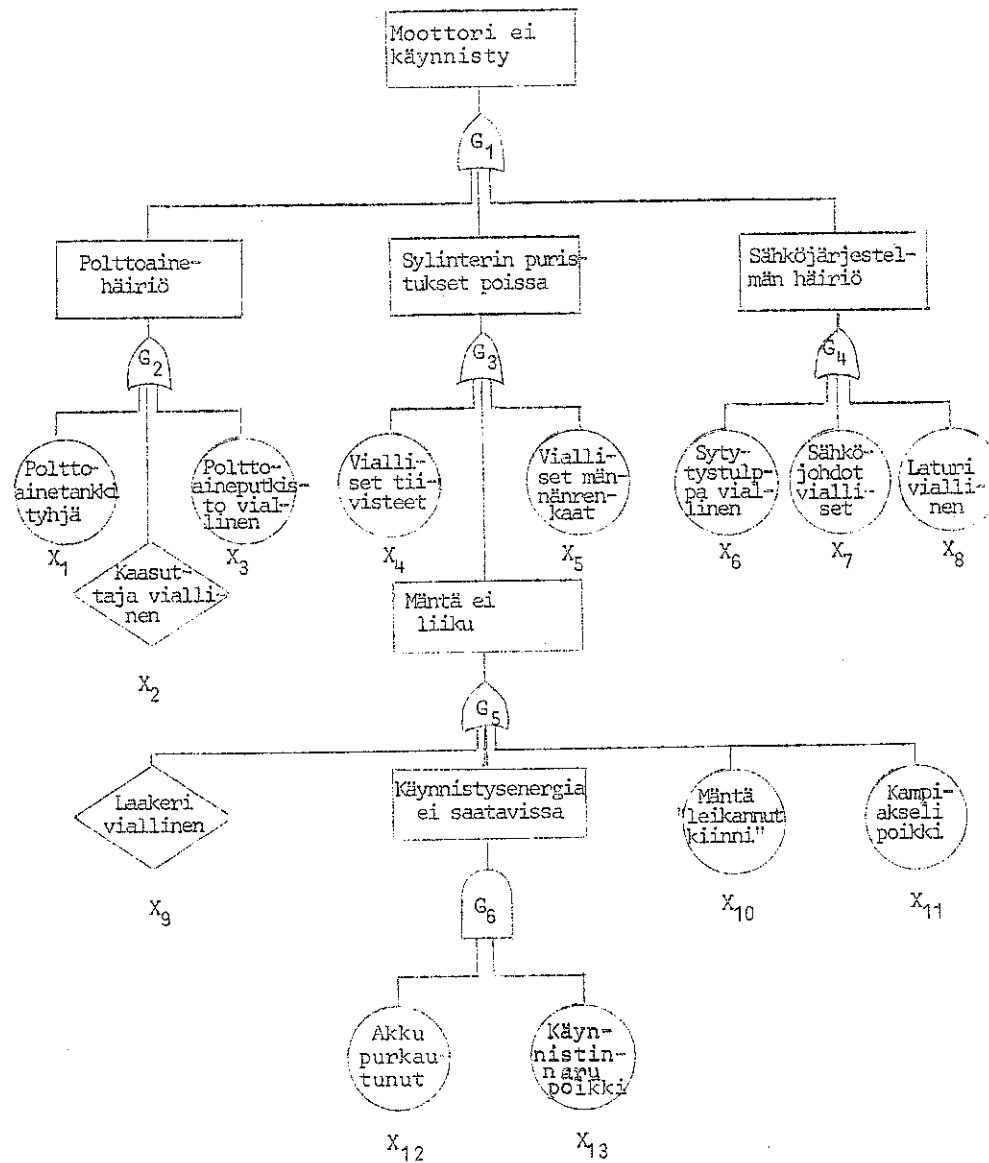
Eräs mahdollisuus vikapuun laatimiseksi valitulle huipputapahtumalle on esitetty kuvassa 7. Vikapuuta ei ole laadittu kovinkaan yksityiskohtaiseksi. Useat alkeistapahtumiksi merkityt tapahtumat olisivat helposti edelleen kehitettävissä. Esimerkin havainnollistamistarkoituksia varten vikapuu lienee kuitenkin riittävän pitkälle kehitetty.

¹ Fussell et al., mt. s. 52 ja Harju, Korjaamattoman ..., s.18.

¹ Ks. Harju, Korjaamattoman..., esimerkki s. 7-18 ja Nieuwhof, mt. s. 107-117.

² Crosetti, mt. s. 467.

³ Esimerkki osittain mukaeltu Nieuwhofin esimerkistä, s. 107-117.



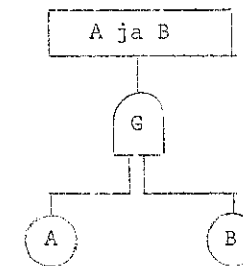
Kuva 7. Vikapuun ruohonleikkuukoneen moottorin tapahtumalle "moottori ei käynnisty"

5.1 HUIPPUTAPAHTUMAN TODENNÄKÖISYYS

Oletetaan, että vikapuun alkeistapahtumat X_1, X_2, \dots, X_{13} ovat toisistaan riippumattomat. Koska eri haaroissa olevilla porteilla ei ole yhteisiä sisäänmenotapahtumia, ovat myös eri haarojen portit riippumattomat. Tämä yhdessä sen kanssa, että puussa on vain ja- ja tai-portteja, tekee puun ratkaisemisen mahdollisimman yksinkertaiseksi. Olkoot alkeistapahtumien esiintymistodennäköisyydet seuraavan taulukon mukaiset.

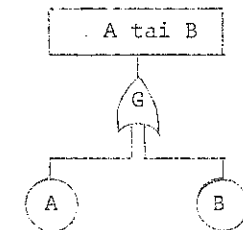
$X_1:$	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}
$P(X_i):$.0016	.03	.01	.001	.001	.02	.01	.01	.01	.01	.01	.04	.03

Riippumattomien tapahtumien tapauksessa saadaan nyt ja-portille



$$P(A \text{ ja } B) = P(A) P(B)$$

ja tai -portille



$$P(A \text{ tai } B) = P(A) + P(B) - P(A \text{ ja } B) \\ = P(A) + P(B) - P(A)P(B)$$

Esimerkkivikapuussa saadaan em. tuloksia käyttäen ja yleistäen

$$P(G_6) = P(X_{12})P(X_{13}) = 0.04 \times 0.03 = 0.0012$$

$$\begin{aligned}
 P(G_5) &= P(X_9) + P(G_6) + P(X_{10}) + P(X_{11}) - P(X_9)P(G_6) \\
 &\quad - P(X_9)P(X_{10}) - P(X_9)P(X_{11}) - P(G_6)P(X_{10}) - P(G_6)P(X_{11}) \\
 &\quad - P(X_{10})P(X_{11}) + P(X_9)P(G_6)P(X_{10}) + P(X_9)P(G_6)P(X_{11}) \\
 &\quad + P(X_9)P(X_{10})P(X_{11}) + P(G_6)P(X_{10})P(X_{11}) - P(X_9)P(G_6)P(X_{10})P(X_{11}) \\
 &= 0.0309
 \end{aligned}$$

$$\begin{aligned}
 P(G_2) &= P(X_1) + P(X_2) + P(X_3) - P(X_1)P(X_2) - P(X_1)P(X_3) \\
 &\quad - P(X_2)P(X_3) + P(X_1)P(X_2)P(X_3) \\
 &= 0.0412
 \end{aligned}$$

$$\begin{aligned}
 P(G_3) &= P(X_4) + P(G_5) + P(X_5) - P(X_4)P(G_5) - P(X_4)P(X_5) \\
 &\quad - P(G_5)P(X_5) + P(X_4)P(G_5)P(X_5) \\
 &= 0.0328
 \end{aligned}$$

$$\begin{aligned}
 P(G_4) &= P(X_6) + P(X_7) + P(X_8) - P(X_6)P(X_7) - P(X_6)P(X_8) \\
 &\quad - P(X_7)P(X_8) + P(X_6)P(X_7)P(X_8) \\
 &= 0.0395
 \end{aligned}$$

$$\begin{aligned}
 P(G_1) &= P(G_2) + P(G_3) + P(G_4) - P(G_2)P(G_3) - P(G_2)P(G_4) \\
 &\quad - P(G_3)P(G_4) + P(G_2)P(G_3)P(G_4) \\
 &= 0.1092
 \end{aligned}$$

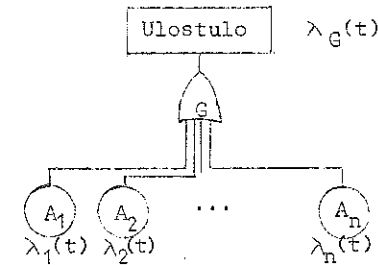
Huipputapahtuman "moottori ei käynnisty" todennäköisyydeksi saatiin siis 0.1092.

Vikapuuta ratkaistaessa approksimoidaan tai-portille usein $P(A \text{ tai } B) = P(A) + P(B)$. Näin laskut huomattavasti yksinkertaistuvat (vrt. erityisesti portti G_5). Approksimaation käytön edellytyksenä on luonnollisesti todennäköisyysarvojen pienuus. Esimerkissä saataisiin approksimaatiota käyttäen huipputapahtuman todennäköisyydeksi 0.115, minkä virhe on n. 0.006 eli n. 5.5 %.

5.2 HUIPPUTAPAHTUMAN VIKATAAJUUSFUNKTIO

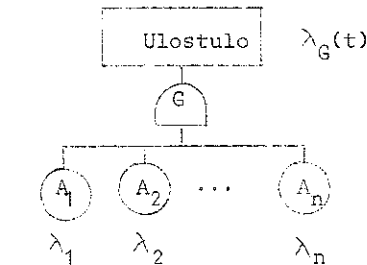
Tapauksessa, jolloin alkeistapahtumat ovat riippumattomat ja jolloin niiden vikataajuus- l. hasardifunktiot ovat vakioita (ts. alkeistapahtuman ensimmäiseen esiintymiseen l. vian syntymiseen kuluva aika on eksponentiaalisesti jakautunut satunnaismuuttuja), voidaan

huipputapahtumankin vikataajuusfunktio määrittää. Riippumattomien tapahtumien tapauksessa saadaan tai-portin vikataajuusfunktio sisäänmenotapahtumien vikataajuusfunktioiden summana. Tulos on voimassa paitsi vakiovikataajuuden omaaville tapahtumille myös aikariippuvan vikataajuusfunktion omaaville tapahtumille.¹



$$\lambda_G(t) = \lambda_1(t) + \lambda_2(t) + \dots + \lambda_n(t)$$

Ja-portin vikataajuusfunktion määrittäystä tarkastellaan tässä vain alkeistapahtumien vikataajuuksien ollessa vakioita. Tällöin saadaan²



$$\lambda_G(t) = \frac{\sum_{i=1}^n \lambda_i [\alpha_i(t) - 1]}{\prod_{i=1}^n \alpha_i(t) - 1}$$

$$\text{missä } \alpha_i(t) = (1 - e^{-\lambda_i t})^{-1}.$$

Siis ja-portin ulostulotapahtuman vikataajuusfunktio on ajasta riippuva, vaikka sisäänmenotapahtumien vikataajuusfunktiot eivät tätä ole. Tämä ehkä yllättävältäkin kuullostava tulos johtuu luonnollisesti siitä että komponenteilla häiriön esiintymiseen kuluva aika on eksponentiaalisesti jakautunut satunnaismuuttuja, jonka tiheysfunktio on ajasta riippuva.

¹ Nieuwhof, mt. s. 112-113.

² Nieuwhof, mt. s. 114.

Oletetaan esimerkkivikapuun alkeistapahtumille seuraavat vikataajuudet (muunnettuna kaikki samoiksi yksiköiksi, h^{-1}):¹

X_i	X_1	X_2	X_3	X_4	X_5	X_6		
λ_i	6×10^{-5}	2×10^{-5}	2×10^{-5}	5×10^{-6}	5×10^{-6}	1×10^{-4}		
							X_7	X_8
	5×10^{-5}	5×10^{-5}	2×10^{-6}	2×10^{-6}	1×10^{-6}	5×10^{-5}	5×10^{-5}	X_{13}

Huipputapahtuman vikataajuusfunktio saadaan siten vaiheittain:

$$\lambda_{G_6}(t) = \frac{5 \times 10^{-5} (e^{0.00005 \cdot t} - 1)^{-1} + 5 \times 10^{-5} (e^{0.00005 \cdot t} - 1)^{-1}}{(1 - e^{-0.00005 \cdot t})^{-1} (1 - e^{-0.00005 \cdot t})^{-1} - 1}$$

$$= \frac{10^{-4} (e^{0.00005 \cdot t} - 1)}{(1 - e^{-0.00005 \cdot t})^{-2} - 1}$$

$$\lambda_{G_5}(t) = \lambda_9 + \lambda_{10} + \lambda_{11} + \lambda_{G_6}(t) = 5 \times 10^{-6} + \lambda_{G_6}(t)$$

$$\lambda_{G_2}(t) = \lambda_1 + \lambda_2 + \lambda_3 = 1 \times 10^{-4}$$

$$\lambda_{G_3}(t) = \lambda_4 + \lambda_{G_5}(t) + \lambda_5 = 1 \times 10^{-5} + \lambda_{G_5}(t)$$

$$= 1.5 \times 10^{-5} + \lambda_{G_5}(t)$$

$$\lambda_{G_4}(t) = \lambda_6 + \lambda_7 + \lambda_8 = 2 \times 10^{-4}$$

$$\lambda_{G_1}(t) = \lambda_{G_2}(t) + \lambda_{G_3}(t) + \lambda_{G_4}(t)$$

$$= 3.15 \times 10^{-4} + \lambda_{G_5}(t)$$

Huipputapahtuman vikataajuusfunktio on näin

$$\lambda_{G_1}(t) = 3.15 \times 10^{-4} h^{-1} + \lambda_{G_5}(t).$$

Tämän raja-arvoina saadaan erikoisesti:

$$\lambda_{G_1}(0) = 3.15 \times 10^{-4} h^{-1} \quad \lambda_{G_1}(\infty) = 3.65 \times 10^{-4} h^{-1}$$

¹ Esimerkkijärjestelmän yhteydessä vikataajuus-käsitteen käyttö ei ehkä sel-laisenaan ole täysin perusteltua. Sopivasti tulkittuna käsitteen sisältö on kuitenkin mielekäs tässäkin yhteydessä. Esimerkin vikataajuusfunktion määrittästä havainnollistavaan merkitykseen tämä pienehkö käsitteellinen epätasällisyys ei sen sijaan mitenkään vaikuta.

S U M M A R Y

FAULT TREE ANALYSIS IN RELIABILITY AND SAFETY EVALUATION OF A PRODUCTION SYSTEM

This paper outlines the basic concepts for a systematic approach to the reliability and safety analysis of a complex system. The principal method for identifying system failures - with their causes and consequences - and for evaluating probabilities of failure occurrences is the fault tree analysis.

The fault tree analysis has rapidly gained favor with reliability analysts of complex systems. The main feature of the fault tree technique is the versatility in the degree of detail in which the analysis can be carried out. Also the analyst has options for qualitative and quantitative analysis. And further, the simple logic of the fault tree approach makes it a visibility tool for both engineering and management. These general properties of the fault tree technique are discussed in section 1.

The first step in reliability analysis is the identification of all system failure modes. This step is called the Failure Mode and Effect Analysis (FMEA). During FMEA all component failures are hypothesized and the possible adverse effects on the system are determined by investigating how the system responds to each failure and failure combination. Section 2 contains a brief discussion about this preceding step for the actual fault tree analysis.

In section 3 the general procedure for constructing a fault tree is dealt with. Fault tree is a tool by which failures that can contribute to an undesired event in the system (e.g. fire, explosion) are organized deductively and represented pictorially. Fault tree is so one way to diagram and relate the information developed in the preceding FMEA. The resulting arrangement is a treelike logical structure with information flows from the branches (component failures) to the top of the tree (the undesired event, system failure). The general construction principle of the fault tree and the commonly used fault tree symbols - logic gates and fault events - as well as the main steps involving

in the tree construction are included in the discussion of section 3.

Section 4 deals with the analysis of a fault tree. Two different approaches are possible: qualitative or quantitative analysis. In the qualitative analysis the fault tree is inspected in order to determine all the combinations of component failures that can lead to the undesired event (minimal cut set evaluation). In the quantitative analysis such quantitative reliability measures as

- the probability of occurrence of the undesired event
- the failure rate for the undesired event
- the expected number of occurrences of the undesired event during the time interval from 0 to t
- the expected number of undesired event occurrences per unit time

can be obtained. Similar information can also be determined for the minimal cut sets and primary events (component failures). There is a great number of methods available for carrying out the fault tree evaluation, both analytical and simulation methods. These methods are also touched upon in section 4.

The construction and evaluation of a fault tree is illustrated in section 5 by means of a simplified system. The system is a lawn mower internal combustion engine. The engine can be started by batter power or by a pull cord. The undesired event is "Engine does not start". Figure 7 shows one possible fault tree for the undesired event of this system. For the fault tree of the example both qualitative and quantitative analysis are carried out.

L Ä H D E K I R J A L L I S U U S

- Crosetti, P.A. Fault tree analysis with probability evaluation
- Fussell, J.B. -
Powers, G.J. --
Bennetts, R.G. Fault trees - a state of the art discussion, IEEE Transactions on Reliability, Vol. R-23, No.1, 1974, pp.51-55
- Harju, T. Korjaamattoman järjestelmän vikapuun analyttinen laskeminen, VTT:n luotettavuusryhmän muistio 4/74
- Harju, T. Monte Carlo simuloinnin käyttö luotettavuusanalyysissa, VTT:n luotettavuusryhmän muistio 18/74
- IEEE guide for general principles of reliability analysis of nuclear power generating station protection systems, IEEE Standard 352-1975, New York 1975
- Komsi, M. Vioittumis- ja vaikutusanalyysi, VTT:n luotettavuusryhmän muistio 15/73
- Lambert, H. System modeling for reliability and safety evaluation in chemical processes, Lawrence Livermore Laboratory, University of California, Livermore California 1974
- Nieuwhof, G.W.E. An introduction to fault tree analysis with emphasis on failure rate evaluation, Microelectronics and Reliability, Vol.14, No. 2, 1975, pp. 105-119
- Powers, G.J. -
TOMPkins, F.C.Jr. Fault tree synthesis for chemical processes, AIChE Journal, Vol. 20, No.2, 1974, pp. 376-387.