Luento 4
Vikapuuanalyysi

Jan-Erik Holmberg
Systeemianalyysin laboratorio
Matematiikan ja systeemianalyysin laitos
Aalto-yliopiston perustieteiden korkeakoulu
PL 11100, 00076 Aalto
jan-erik.holmberg@aalto.fi

Influenssarokotus (1/3)

- Rokotuskampanja
  - Influenssaepidemian vakavuus vaihtelee vuosittain
  - Sairastumistodennäköisyys riippuu siitä, miten vakavasta epidemiasta on kyse
  - Erityisesti nuoret lapset, iäkkäät henkilöt ja kroonisesti sairastavat saattavat kärsiä influenssasta
  - Kannattaako koko väestöä tai sen osia rokottaa, jos rokotus alentaa sairastumisnäköisyyden 8 prosenttiin verrattuna tilanteeseen, jossa rokotusta ei annettu?

Influenssarokotus (2/5)

- Influenssan riskit

Probability of Developing Flu If Exposed to the Virus in Various Seasons

Type of Epidemic Season	Probability of Exposure and Flu Development
Severe epidemic	0.40
Mild epidemic	0.15
Nonepidemic	0.05

Probability of Severe and Mild Flu Cases and Subsequent Mortality Probability

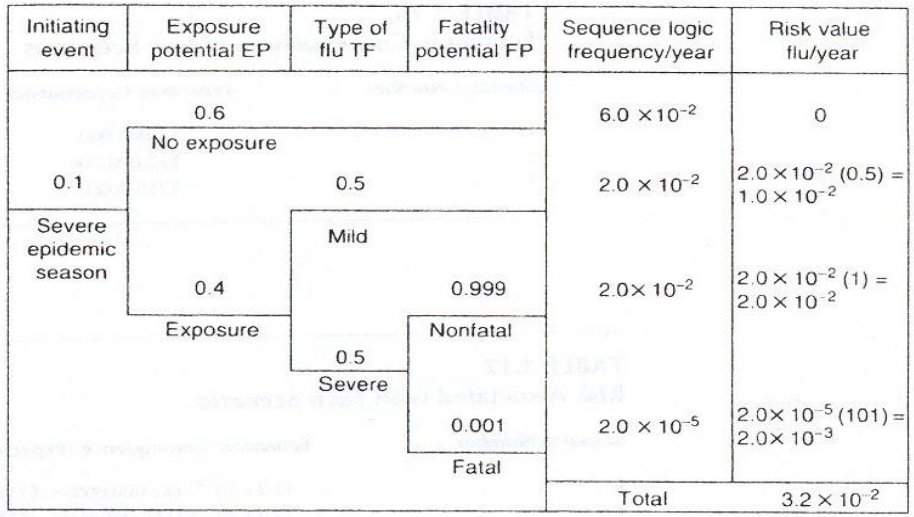
	Severe Case of Flu	Mild Case of Flu	Mortality Given a Flu Case
Severe epidemic seasons	0.500	0.499	0.001
Mild epidemic seasons	0.330	0.669	0.001
Nonepidemic seasons	0.100	0.899	0.001

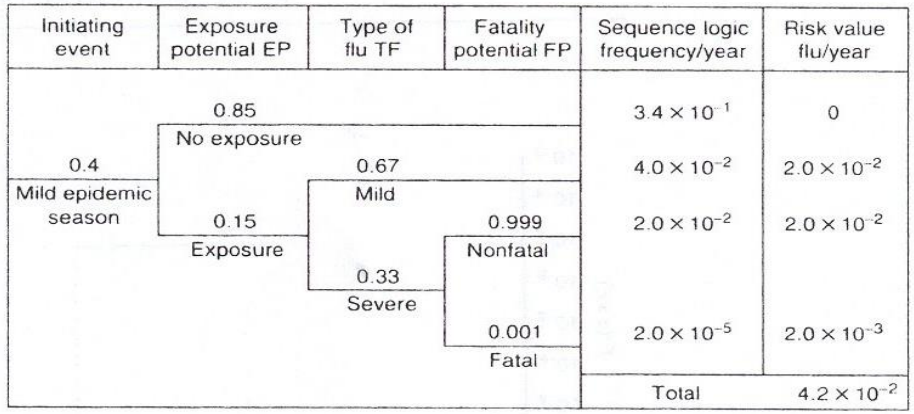
Consequence Values of Developing Flu

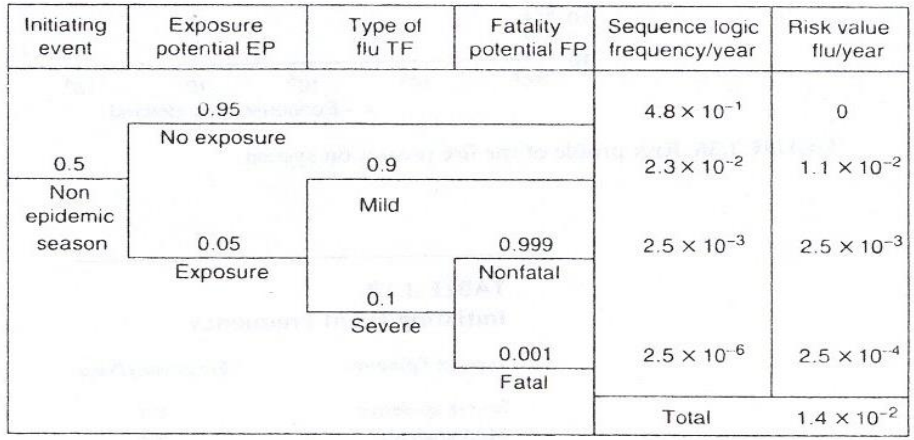
Consequence	Days Lost	FLU* Utility
Mortality (in severe cases of flu)	500–2000	100
Morbidity (state of disease)	2–20	1
Mild case of morbidity	3–9	0.5

Influenssarokotus (3/5)

- Tapahtumapuut
  - Ilman rokotusta







Influenssarokotus (4/5)

- Rokotuksella voi olla haittavaikutuksia

Consequences of Vaccination

Consequence	Days Lost	FLU Utility	Frequency
Chills and fever	3–10	0.9	0.3
Mild reaction	0–1	0.2	0.3
Sore arm	—	0.1	0.4

TABLE 3.24
Probability of Outcome of Flu on Subgroup Populations

	Young			Elderly and Chronically Ill		
Year	Severe Case	Mild Case	Mortality	Severe Case	Mild Case	Mortality
Epidemic	0.499	0.498	0.003	0.496	0.495	0.009
Mild epidemic	0.399	0.598	0.003	0.446	0.545	0.009
Nonepidemic	0.199	0.498	0.003	0.296	0.695	0.009

		Total Risk Values (in FLU units)	
Population	Type of Year	Without Vaccination	With Vaccination
General population	Epidemic year	3.2×10^{-2}	2.0×10^{-2}
	Mild epidemic year	4.2×10^{-2}	2.1×10^{-2}
	Nonepidemic year	1.4×10^{-2}	1.9×10^{-2}
Young	Epidemic year	4.9×10^{-2}	2.1×10^{-2}
	Mild epidemic year	8.2×10^{-2}	2.4×10^{-2}
	Nonepidemic year	4.9×10^{-2}	2.2×10^{-2}
Elderly and chronically ill	Epidemic year	7.4×10^{-2}	2.3×10^{-2}
	Mild epidemic year	1.2×10^{-1}	2.7×10^{-2}
	Nonepidemic year	8.3×10^{-2}	2.4×10^{-2}

Tapahtumapuu seuraavalla sivulla

Influenssarokotus (5/5)

- Tapahtumapuu
  - rokotus

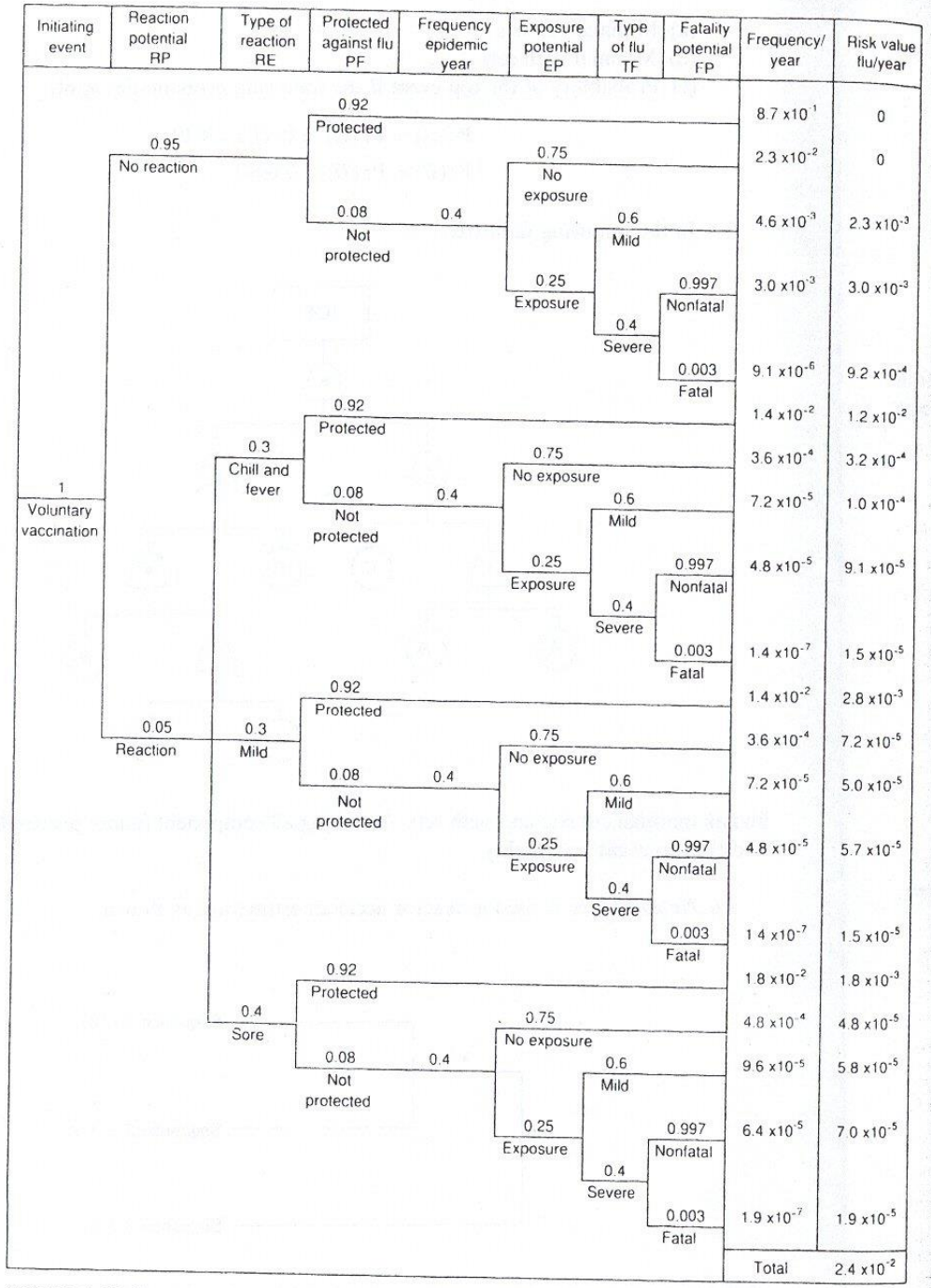


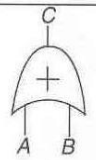
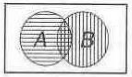
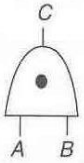
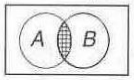
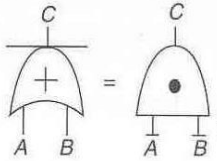
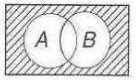
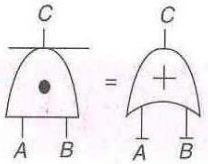
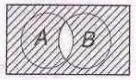
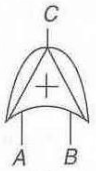
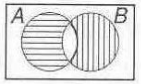
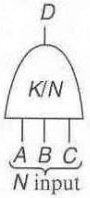
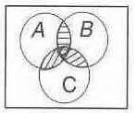
FIGURE 3.38 Scenarios of events for young population -- mild epidemic year (with vaccination).

Vikapuuanalyysi

- Tavoite
  - Löytää valittuihin järjestelmävikoihin vaikuttavat viat ja vikayhdistelmät (ml. ihmisen toimintovirheet)
  - Mahdollistaa onnettomuusmahdollisuuksien yksityiskohtaisen tutkimisen sekä vaihtoehtoratkaisujen kvantitatiivisen vertailun
- Periaate
  - Järjestelmäviasta (huipputapahtumasta) lähtien etsitään sen toteutumisen mahdollistavia tekijöitä
  - Rakennetaan graafinen esitys tekijöistä ja niiden välisistä kytkennöistä
  - Osoittaa vaaran kannalta tärkeät vikakombinaatiot sekä pienimmät vikakombinaatiot ja yhteisviat, jotka aiheuttavat järjestelmävian
- Rajoituksia ja puutteita
  - Ei sovellu hyvin huipputapahtuman seurausten analysointiin
  - Osittaisvikojen tutkiminen vaikeaa
  - Vikojen keskinäisiä vaikutuksia, aikariippuvuuksia ja ulkopuolisia tapahtumaketjuja vaikea huomioida
  - Ei anna hyvää kuvaa järjestelmän kokonaisturvallisuustasosta
  - Huipputapahtuman määrittely vaikuttaa lopputulokseen

Vikapuu

- Esittää järjestelmän vikatapahtuman (=huipputapahtuma) ja perustapahtumien (=komponenttien vikatapahtumat) väliset yhteydet loogisten kytkentöjen (= vikapuun porttien) avulla
- Porttityypit
  - AND = ulostulo toteutuu, kun kaikki sisäänmenot toteutuvat
  - OR = ulostulo toteutuu, kun yksikin sisäänmeno toteutuu
  - NOT = ulostulo toteutuu, kun sisäänmeno ei toteudu
  - K/N = ulostulo toteutuu, kun vähintään K kpl N:stä sisäänmenosta toteutuu
  - Käsittely Boolen-algebran lausekkeilla

Logic	Venn diagram representation (shaded areas show the gate output representation)	Boolean representation
 OR gate	Union operation 	$C = A \cup B = A + B$
 AND gate	Intersection operation 	$C = A \cap B = A \cdot B$
 Not OR gate NOR		$C = \overline{A \cup B} = \bar{A} \cap \bar{B} = \bar{A} \cdot \bar{B}$
 Not AND gate NAND		$C = \overline{A \cap B} = \bar{A} \cup \bar{B} = \bar{A} + \bar{B}$
 Exclusive OR		$C = [A \cap \bar{B}] \cup [B \cap \bar{A}] = [A \cdot \bar{B}] + [B \cdot \bar{A}]$
 Priority AND	Not applicable	$C = A$ first $\cap$ B next
 K-out-of-N		$D = [A \cap B] \cup [A \cap C] \cup [B \cap C]$ $= [A \cdot B] + [A \cdot C] + [B \cdot C]$ $K = 2, N = 3$ 2-out-of-3 gate

Vikapuuanalyysin vaiheet

- Ongelman ja reunaehtojen määrittely
- Vikapuun rakentaminen
- Minimikatkosjoukkojen ratkaiseminen
- Kvalitatiivinen analyysi
- Kvantitatiivinen analyysi

Ongelman ja reunaehtojen määrittely

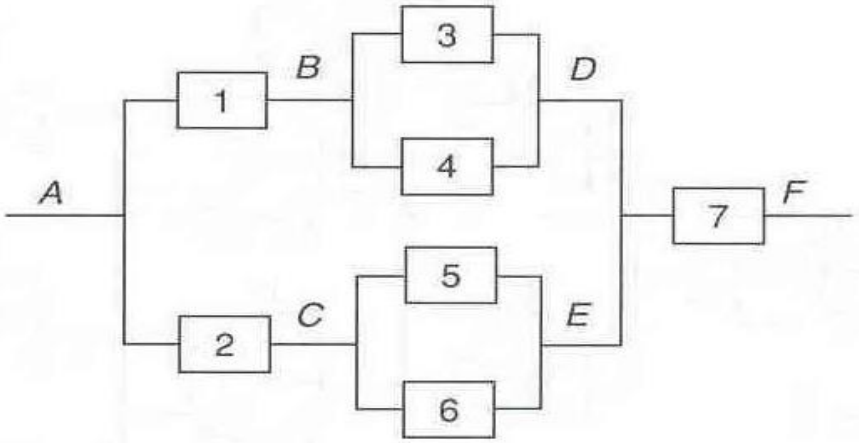
- Lähtökohtana huipputapahtuman ja reunaehtojen tunnistaminen
- Huipputapahtumalle annettava yksikäsitteinen ja selkeä määrittely
  - Tulee vastata täsmällisesti seuraaviin kysymyksiin:
    - » Mitä: tarkasteltavan tapahtuman tyyppi ja luonne (esim. tulipalo, jäähdytysveden syötön menetys, jne.)
    - » Missä: tapahtuman tarkka esiintymispaikka (esim. veden syöttö lauhdutinaltaaseen)
    - » Milloin: tapahtuman esiintymistilanne (esim. vuosihuoltoseisokin aikana)
  - Esim. ”Tulipalo polttoainesäiliössä vuosihuoltoseisokin aikana”

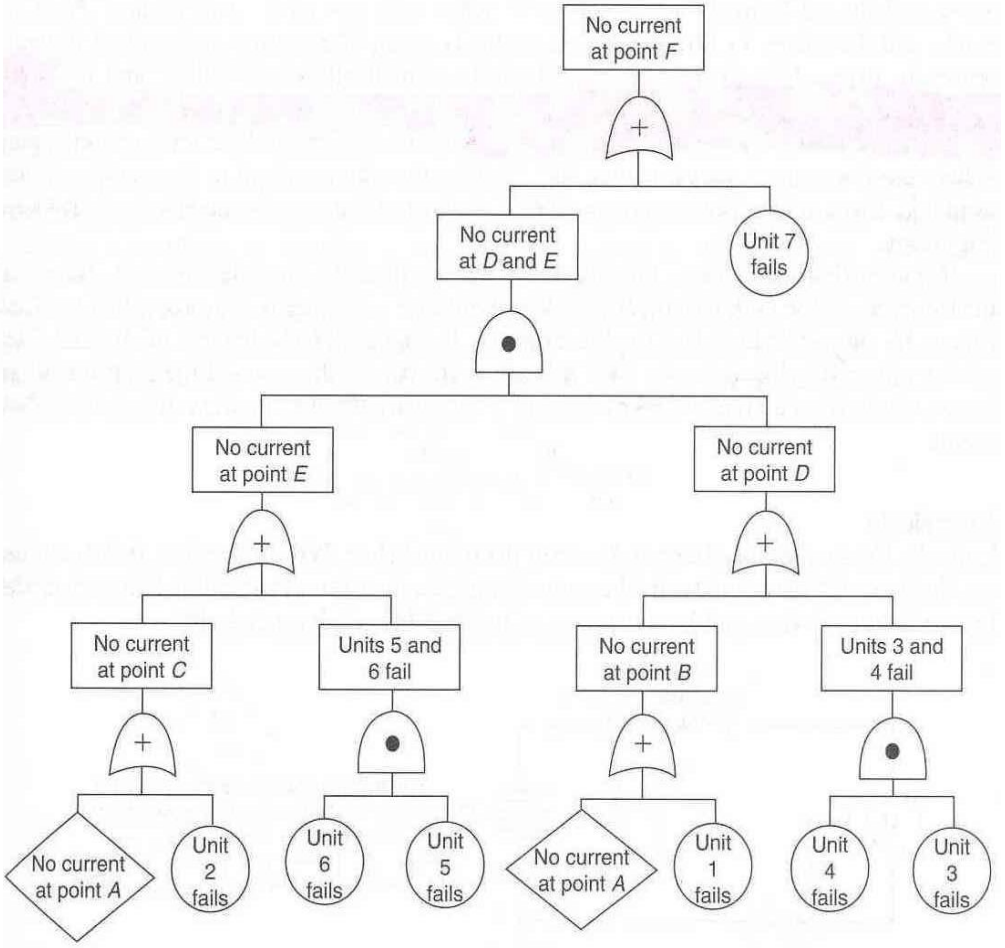
Ongelman ja reunaehtojen määrittely

- Reunaehtoja voivat olla
  - Järjestelmän fyysiset rajat
    - » Mitkä järjestelmän osat otetaan mukaan analyysiin?
  - Alkutilanteet
    - » Mikä on järjestelmän tila, kun huipputapahtuma esiintyessä? (esim. täydellinen toiminta, rajoitettu toiminta, huoltoseisokki jne.)
    - » Missä tilassa komponentit ovat? (esim. venttiilien asento, prosessilaitteiden tila jne.)
  - Ulkoisten tekijöiden vaikutus
    - » Mitkä ulkoiset tekijät otetaan mukaan? (esim. poikkeukselliset sääolot, sabotaasi, jne.)
  - Yksityiskohtaisuuden taso
    - » Miten tarkasti eri vikaantumistavat tai järjestelmän osat mallinnetaan? (esim. mitkä järjestelmät mallinnetaan komponenttitasolla, otetaanko inhimilliset virheet mukaan, jne.)
- Huomioita
  - Pyrittävä riittävän tarkkaan erittelyyn
  - Haettava tarkoituksenmukainen yksityiskohtaisuuden taso
  - Jäsentymätön ongelmankuvaus ja/tai epämääräiset rajaukset vievät pohjaa jatkoanalyyseiltä ja vaikeuttavat näiden tulkintaa

Vikapuun rakentaminen

- Aloitetaan huipputapahtuman analyysista:
  - Selvitetään huipputapahtuman välittömät, välttämättömät ja riittävät syyt
  - Syyt liitetään huipputapahtumaan vikapuun portilla
  - Edetään hierarkkisesti perustapahtumiin (esim. komponenttivikoihin)
    - » Kukin vikatapahtuma kuvataan ja esitetään porttina
    - » Kaikki porttien sisäänmenot määritellään täydellisesti
    - » Rakennetaan vikapuu tasoittain siten, että kukin taso kuvataan ennen etenemistä seuraavalle tasolle
  - Tehdään deduktiivinen analyysi
    - » Kunkin ylemmän tason kohdalla kysytään, mitkä voivat olla sen välittömät syyt
- Vikatapahtumien luokittelu (esimerkki)
  - Primäärivika (primary failure) tai sisäinen vika (internal vika)
    - » Vika, jonka aiheuttaa kohteen normaali ikääntyminen tai muu sisäinen vikamekanismi
  - Sekundäärivika (secondary failure)
    - » Vika, jonka aiheuttaa ulkopuolinen, poikkeuksellinen rasitus, toisen komponentin vikaantuminen tai toimintahäiriö, tai inhimillinen virhe
  - Ohjausvika (command fault, control failure, support system failure)
    - » Vika, joka aiheutuu virheellisestä tai puuttuvasta ohjaussignaalista tai muusta puuttuvasta tai virheellisestä tukitoiminnosta


A
1
B
3
4
D
7
F
2
C
5
6
E


No current at point F
No current at D and E
Unit 7 fails
No current at point E
No current at point D
No current at point C
Units 5 and 6 fail
No current at point B
Units 3 and 4 fail
No current at point A
Unit 2 fails
Unit 6 fails
Unit 5 fails
No current at point A
Unit 1 fails
Unit 4 fails
Unit 3 fails

Minimikatkosjoukkojen ratkaiseminen

- Vikaantumislogiikan tarkastelu
  - Huipputapahtuma, logiikkaportit ja perustapahtumat ovat ”vikaantumistapahtumia”, jotka esitetään Boolen algebran muuttujien avulla
  - Vikatapahtuma esiintyy <=> sitä vastaava Boolen muuttuja saa arvon ”tosi”, esim.

$$X = \begin{cases} 1, \text{komponentti vialla} \\ 0, \text{komponentti ehjä} \end{cases}$$

  - Kutakin porttia vastaa Boolen lauseke:
    - » OR = Boolen summa (+), AND = Boolen tulo (•), jne.

$$G = \begin{cases} 1, \text{portin tapahtuma toteutuu} \\ 0, \text{portin tapahtuma ei toteudu} \end{cases}$$

    - » Huom! piste vastaa siis leikkausta ja summa unionia
  - Huipputapahtumasta lähtien sovelletaan porttien määritelmiä (ks. seuraavat 2 kalvoa)
  - Saadaan perustapahtumien tulojen summa, jossa kukin summatermi on minimikatkosjoukko

Minimikatkosjoukkojen ratkaiseminen

- Minimikatkosjoukko
  - = Perustapahtumien joukko, joka aiheuttaa huipputapahtuman, mutta josta ei voida poistaa mitään perustapahtumaa siten, että huipputapahtuma edelleen toteutuu (so. mikään poistamisen jälkeen jäljelle jäävä perustapahtumien joukko ei johda huipputapahtumaan)

  - Katkosjoukko = Perustapahtumien joukko, joka aiheuttaa huipputapahtuman
  - Minimikatkosjoukko = Katkosjoukko, joka menettää katkosjoukko-ominaisuutensa, jos siitä poistetaan mikä tahansa perustapahtuma

Minimikatkosjoukkojen tunnistaminen

- Boolean algebran säännöt

$$X \cdot Y = Y \cdot X$$
$$X + Y = Y + X$$

$$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$$
$$X + (Y + Z) = (X + Y) + Z$$
$$X \cdot (Y + Z) = (X \cdot Y) + (X \cdot Z)$$

$$X \cdot X = X, \qquad X + X = X$$
$$X \cdot (X + Y) = X, \qquad X + (X \cdot Y) = X$$

$$X \cdot \bar{X} = \emptyset, \qquad X + \bar{X} = \Omega \text{ (koko avaruus)}$$

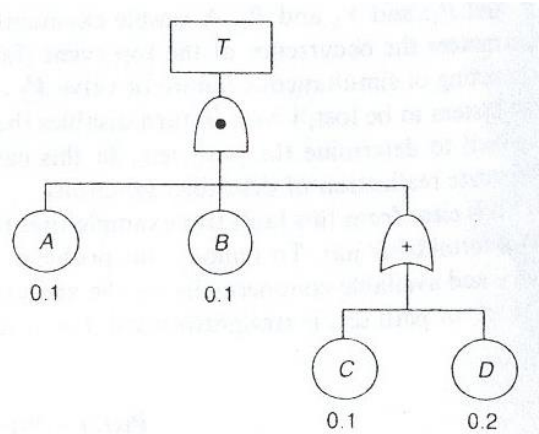
$$\overline{X \cdot Y} = \bar{X} + \bar{Y}, \overline{X + Y} = \bar{X} \cdot \bar{Y} \text{ (de Morgan)}$$

$$\bar{\bar{X}} = X$$

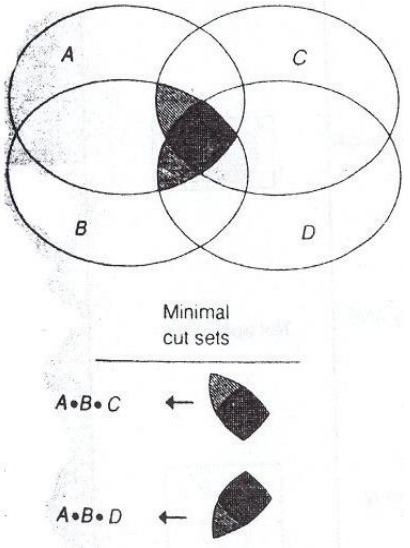
Esimerkki minimikatkosjoukoista (1/3)

- Vikaa kuvaava huipputapahtuma T toteutuu, kun

$$T = A \cdot B \cdot (C + D)$$
$$= A \cdot B \cdot C + A \cdot B \cdot D$$

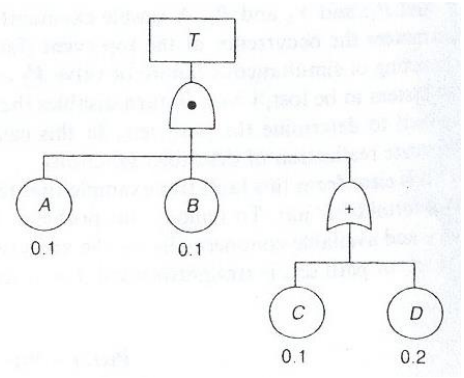


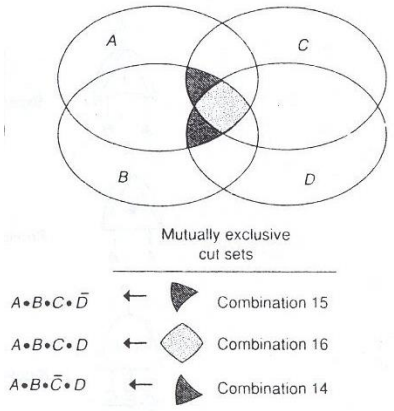
- Vennin kaavio (Venn diagram)
  - Kaavio ei kuitenkaan sikäli hyvä, että esim. A ja D voivat molemmat toteutua vain jos joko B tai C toteutuu (tosin vikapuun perusteella A:n ja B:n voidaan vaatia toteutuvan)



Esimerkki minimikatkosjoukoista (2/3)

- Havaintoja
  - Minimikatkosjoukot $A \cdot B \cdot C$ ja $A \cdot B \cdot D$ voivat esiintyä yhtä aikaa, koska $A \cdot B \cdot C \cdot D$ on molemmissa
  - Vikalogiikan purkaminen perustapahtumiksi Boolen algebran ei siis välttämättä anna toisensa poissulkevia (engl. mutually exclusive) katkosjoukkoja
  - Esimerkiksi edellisen kalvon esimerkissä tällaisia katkosjoukkoja on kolme





Esimerkki minimikatkosjoukoista (3/3)

- Minimikatkosjoukkojen $A \cdot B \cdot C$ ja $A \cdot B \cdot D$ todennäköisyyksien summa

$$P(A)P(B)P(C) + P(A)P(B)P(D) =$$
$$0.1 \times 0.1 \times 0.1 + 0.1 \times 0.1 \times 0.2 = 0.003$$

- Toisensa poissulkevien katkosjoukkojen todennäköisyyksien summa

$$P(A)P(B)P(C)P(D) + P(A)P(B)P(C)P(\bar{D})$$
$$+ P(A)P(B)P(\bar{C})P(D)$$
$$= 0.1 \times 0.1 \times 0.1 \times 0.2 + 0.1 \times 0.1 \times 0.1 \times 0.8 + 0.1$$
$$\times 0.1 \times 0.9 \times 0.2 = 0.0028$$

Päätöstaulukko – kaikki kombinaatiot

Combination Number	Combination Definition (System States)	Probability of C_i	System Operation T
1	$A_S\ B_S\ C_S\ D_S$	0.5832	S
2	$A_S\ B_S\ C_S\ D_F$	0.1458	S
3	$A_S\ B_S\ C_F\ D_S$	0.0648	S
4	$A_S\ B_S\ C_F\ D_F$	0.0162	S
5	$A_S\ B_F\ C_S\ D_S$	0.0648	S
6	$A_S\ B_F\ C_S\ D_F$	0.0162	S
7	$A_S\ B_F\ C_F\ D_S$	0.0072	S
8	$A_S\ B_F\ C_F\ D_F$	0.0018	S
9	$A_F\ B_S\ C_S\ D_S$	0.0648	S
10	$A_F\ B_S\ C_S\ D_F$	0.0162	S
11	$A_F\ B_S\ C_F\ D_S$	0.0072	S
12	$A_F\ B_S\ C_F\ D_F$	0.0018	S
13	$A_F\ B_F\ C_S\ D_S$	0.0072	S
14	$A_F\ B_F\ C_S\ D_F$	0.0018	F
15	$A_F\ B_F\ C_F\ D_S$	0.0008	F
16	$A_F\ B_F\ C_F\ D_F$	0.0002	F

$\sum C_i = 1.0000$

Kvalitatiivinen tulkinta

- Minimikatkosjoukkojen tulkinta
  - Minimikatkosjoukot antavat kuvan järjestelmän vikaantumisesta
  - Minimikatkosjoukkolistan perusteella voidaan tunnistaa tärkeimmät parannustoimenpiteet
- Käyttötapoja
  - Mitkä perustapahtumat esiintyvät minimikatkosjoukoissa useimmin?
    - » Näihin kannattaa kiinnittää huomiota, jos perustapahtumien todennäköisyyksistä ei tarkkaa tietoa
  - Onko perustapahtumista joku sellainen, että se ei kuulu mihinkään minimikatkosjoukkoon?
    - » Tällainen perustapahtuma ei voi aiheuttaa huipputapahtumaa

Kvantitatiivinen analyysi

- Lasketaan järjestelmän vikaantumistodennäköisyys
  - Vikaantuminen = huipputapahtuman toteutuminen
  - Laskenta perustuu minimikatkosjoukkoesitykseen
    - » Huipputapahtuma toteutuu jos ja vain jos joku minimikatkosjoukoista toteutuu
    - » Huipputapahtuman todennäköisyys on siis minimikatkosjoukkojen unionin todennäköisyys

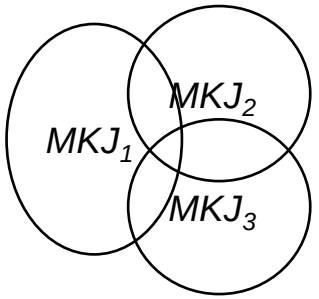
$$P(T) = P(MKJ_1 + MKJ_2) = P(MKJ_1) + P(MKJ_2) - P(MKJ_1 \cdot MKJ_2)$$

$$P(T) = P(MKJ_1 + \cdots + MKJ_n)$$

$$= \sum_i P(MKJ_i) - \sum_{i_1<i_2} P\left(MKJ_{i_1} \cdot MKJ_{i_2}\right)$$

$$+ \sum_{i_1<i_2<i_3} P\left(MKJ_{i_1} \cdot MKJ_{i_2} \cdot MKJ_{i_3}\right)$$

$$- \cdots (-1)^{n+1} \sum_{i_1<i_2<\cdots<i_n} P\left(MKJ_{i_1} \cdot \cdots \cdot MKJ_{i_n}\right)$$



Kvantitatiivinen analyysi

- Summalausekkeiden avulla voidaan muodostaa approksimaatiot

$$P(T) \approx \sum_i P(MKJ_i) = S_1$$

$$P(T) \approx S_1 - \sum_{i_1<i_2} P\left(MKJ_{i_1} \cdot MKJ_{i_2}\right) = S_1 - S_2$$

$$P(T) \approx S_1 - S_2 + \sum_{i_1<i_2<i_3} P\left(MKJ_{i_1} \cdot MKJ_{i_2} \cdot MKJ_{i_3}\right) = S_1 - S_2 + S_3$$

Kvantitatiivinen analyysi (jatkuu)

$$P(T) \leq S_1$$
$$S_1 - S_2 \leq P(T) \leq S_1$$
$$S_1 - S_2 \leq P(T) \leq S_1 - S_2 + S_3$$
$$S_1 - S_2 + S_3 - S_4 \leq P(T) \leq S_1 - S_2 + S_3$$
$$\vdots$$

- Pätee
  - Näistä S_1 (S1-summa ”rare event approximation”) on usein riittävä
  - Perustapahtumien tn:t otettava huomioon
    - » Jos nämä pieniä (esim. < 0.1), niin yhden lisätason mukaantuominen tarkoittaa vähintään yhtä kertaluokkaa pienempien kokonaistn:ien laskemista

Min Cut Upper Bound (MCUB) kvantifiointi

- Yleensä S1-summaa parempi approksimaatio (koherenteille järjestelmille) ja ylälikiarvo

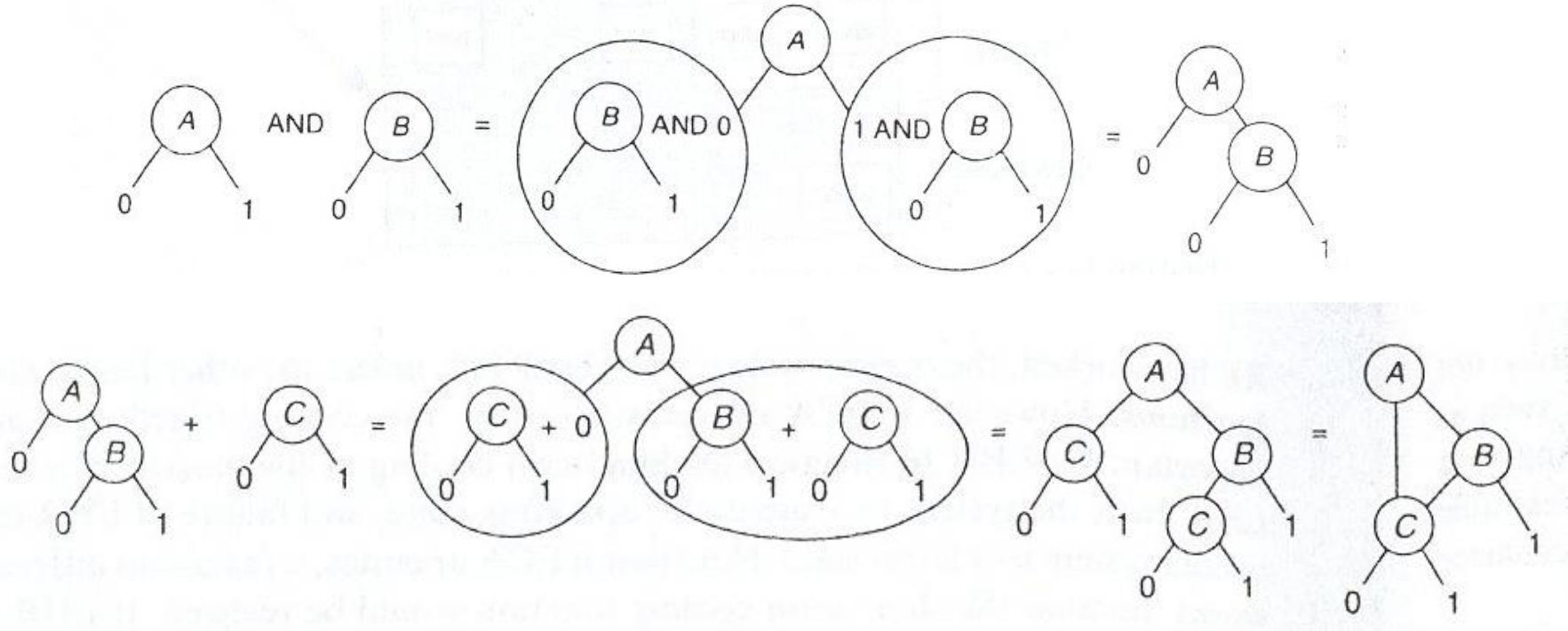
$$MCUB = 1 - \prod_{i=1}^{n} (1 - P(MKJ_i))$$

Katkosjoukkojen määrityksestä

- Huomioita
  - Minimikatkosjoukkojen tn:ien summa antaa ylärajan huipputapahtuman todennäköisyydelle
    - » Saatu arvo tarkka, jos minimikatkosjoukkojen leikkaus on tyhjä (näin käy vain harvoin)
  - Huipputapahtuman tarkan tn:n laskennassa ollaan kiinnostuneita minikatkosjoukkojen unionin esittämisestä toistensa poissulkevina katkosjoukkoina
    - » Nämä katkosjoukot eivät ole välttämättä minimaalisia
  - Nämä voidaan tuottaa binäärisillä päätöskaavioilla (engl. binary decision diagram, BDD)
  - Kunkin perustuman alla vasemmassa haarassa 0, oikeassa 1, yhdistelyt logiikkasäännöillä

Binääriset päätöskaavio (binary decision diagram, BDD)

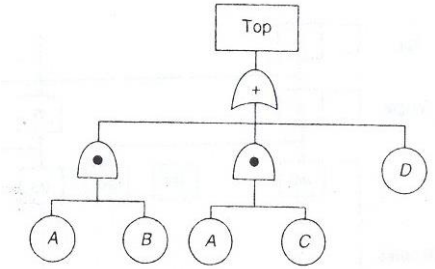
$$TOP = A \cdot B + C$$



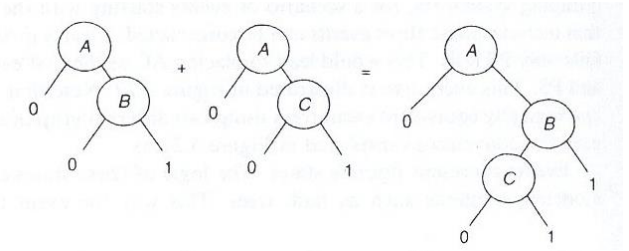
BDD:n rakentaminen

- Rakennetaan tasoittain vikapuun alaosasta ylöspäin
- Jokainen polku huipputapahtumasta ykköshaaraan vastaa katkosjoukkoa
- Ko. katkosjoukot ovat toisensa poissulkevia, koska polut ovat yksiselitteisiä, koska kukin haara vastaa joko nollaa 0:aa tai 1:tä

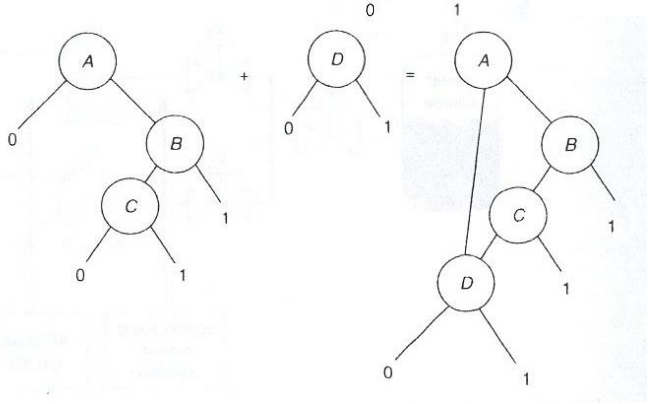
BDD:n rakentaminen



- 2. vaihe



- 3. vaihe

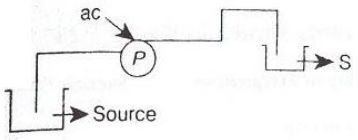


- saadaan katkosjoukkoesitys

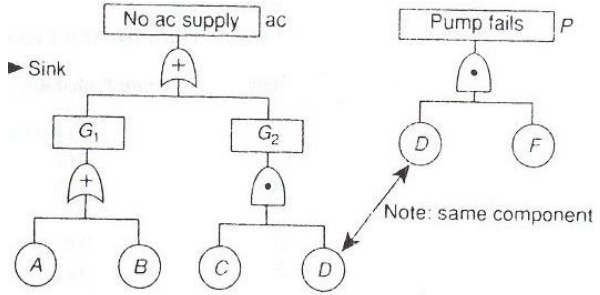
$$\bar{A}D + A\bar{B}\bar{C}D + A\bar{B}C + AB$$

Pumppujärjestelmän riskianalyysi (1/3)

- Järjestelmän toiminta
  - Pumppu siirtää nestettä lähtöaltaasta kohde-altaaseen, jos kohdealtaan nestemäärä laskee alle vaatimustason
  - Pumppu ei toimi, jos sähköä ei ole
  - Pumppu voi vikaantua komponenttivikojen takia, joista osa vaikuttaa sähkönsaantiin



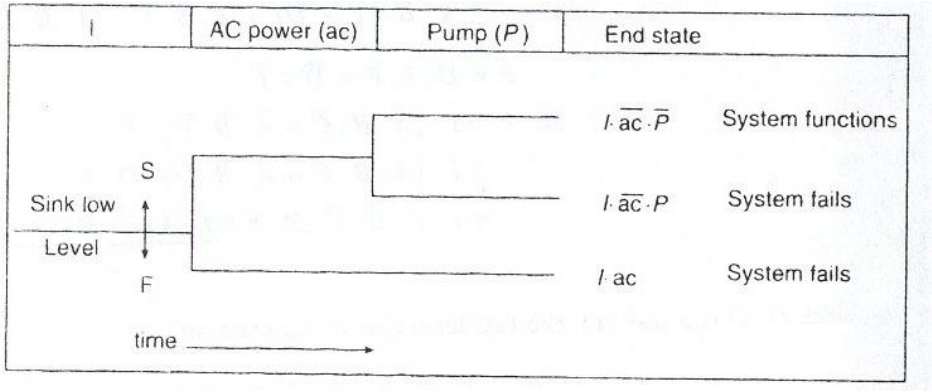
- Vikapuut



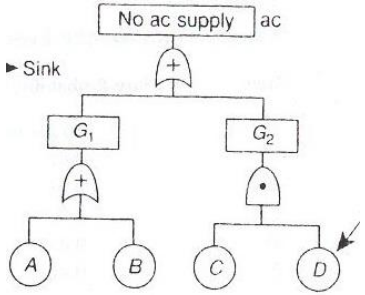
- Esiintymistaajuudet (/kk) alkutapahtuman ja komponenttien vikaantumiselle
  - Kohdeallas vajaa I, $f(I)$ =10 krt/kk
  - $P(A) = P(B) = P(F) = 0{,}01$
  - $P(C) = 0{,}02$
  - $P(D) = 0{,}05$

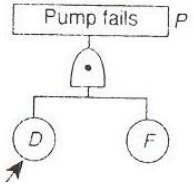
Pumppujärjestelmän riskianalyysi (2/3)

- Pumppujärjestelmän toimintaa kuvaava tapahtumapuu



- Järjestelmä ei toimi skenaarioissa
  $I \cdot \overline{ac} \cdot P$ ja $I \cdot ac$





- Vikapuista saadaan

$$ac = G_1 + G_2 = (A + B) + (C \cdot D) = A + B + C \cdot D$$
$$\overline{ac} = \overline{A + B + C \cdot D} = \bar{A} \cdot \bar{B} \cdot (\bar{C} + \bar{D}) = \bar{A} \cdot \bar{B} \cdot \bar{C} + \bar{A} \cdot \bar{B} \cdot \bar{D}$$
$$P = D \cdot F, \ \bar{P} = \bar{D} + \bar{F}$$

Pumppujärjestelmän riskianalyysi (3/3)

Vikaantumisen todennäköisyys:

$$I \cdot \overline{ac} \cdot P = I \cdot (\bar{A} \cdot \bar{B} \cdot \bar{C} + \bar{A} \cdot \bar{B} \cdot \bar{D}) \cdot (D \cdot F)$$
$$= I \cdot \bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F + I \cdot \bar{A} \cdot \bar{B} \cdot \bar{D} \cdot D \cdot F$$
$$= I \cdot \bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F \qquad (\bar{D} \cdot D = \emptyset)$$

$$I \cdot ac = I \cdot A + I \cdot B + I \cdot C \cdot D$$

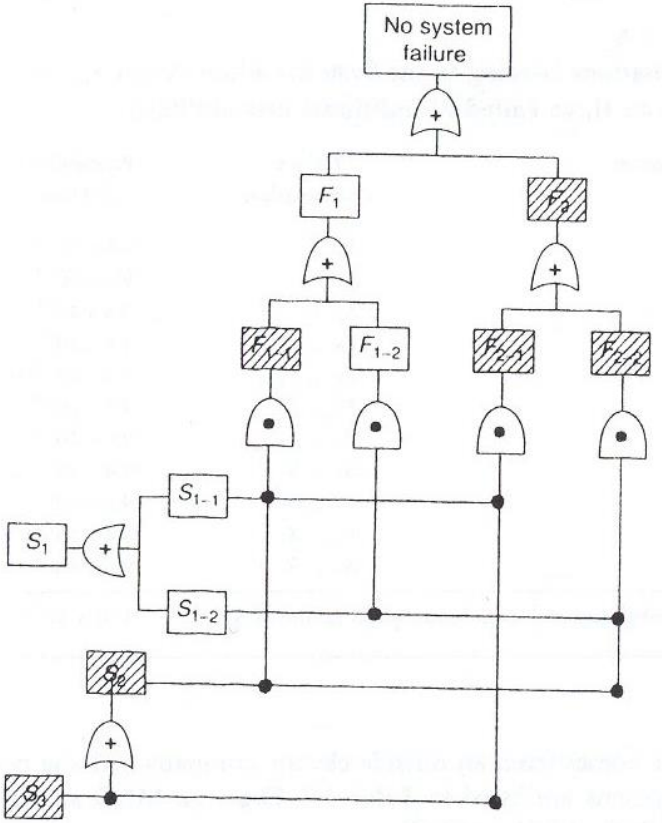
$$P(T) = P(I \cdot ac + I \cdot \overline{ac} \cdot P)$$
$$= P(I)\{P(A + B + C \cdot D) + P(\bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F)\}$$
$$= P(I)\{P(A) + P(B) + P(C \cdot D) - P(A \cdot B) - P(A \cdot C \cdot D) - P(B \cdot C \cdot D)$$
$$+ P(A \cdot B \cdot C \cdot D) + P(\bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F)\}$$
$$= P(I)\{0.01 + 0.01 + 0.02 \times 0.05 - 0.01 \times 0.01 - 2 \times 0.01 \times 0.02 \times 0.05$$
$$+ 0.01 \times 0.01 \times 0.02 \times 0.05 + 0.99 \times 0.99 \times 0.98 \times 0.05 \times 0.01\}$$
$$= P(I) \times 0.02136$$

- Huom! $P(\cdot)$ tarkoittaa tässä todennäköisyyttä, ei pumppua
- So. pumppujärjestelmä vikaantuu keskimäärin joka viides kuukausi

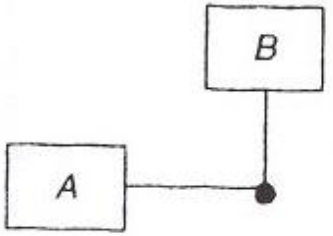
Logiikkakaavioiden käyttö

- Osajärjestelmien riippuvuuksia voidaan havainnollistaa logiikkakaavioina
  - Engl. master logic diagram, MLD
  - ”Huipputapahtuma” vastaa tällöin tyypillisesti järjestelmän toimimista, ei vikaantumista
  - Kiinnostuksen kohteena se, mihin tilaan järjestelmä joutuu riippumattomien osajärjestelmien pettäessä

MLD-esimerkki



Two rules are applied to MLD



(1) Failure of *A* causes failure of *B*
(2) Success of *B* requires success of *A*

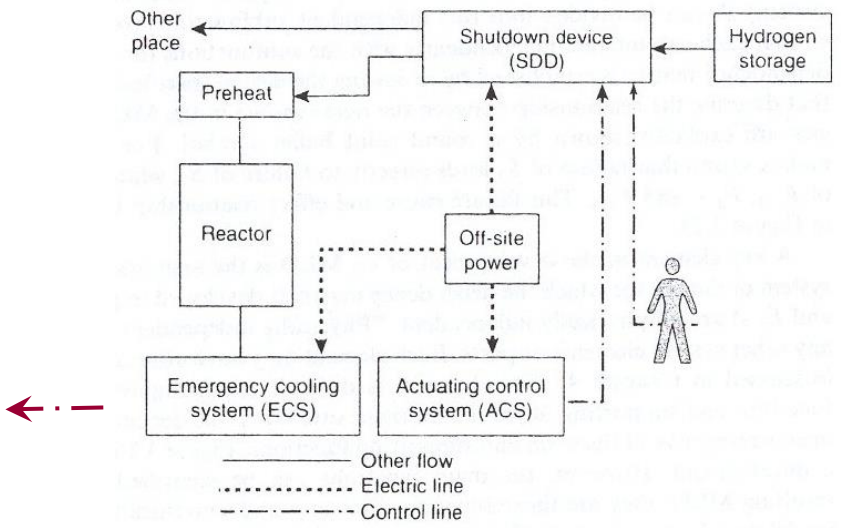
Jäähdytysjärjestelmä (1/3)

- Tarkasteltavana vetyreaktorijärjestelmää
  - Kriisitilanteessa vetyvirtaukset voidaan pysäyttää kriisitilanteessa ajasajojärjestelmällä (shutdown device, SDD)
  - Jos reaktorin lämpötila on liian korkea, jäähdytys vaatii, että hätäjäähdytysjärjestelmän toimii (emergency cooling system, ECS)
  - Molemmat järjestelmät toimivat säätöjärjestelmän varassa (actuator control system, ACS)
  - Operaattori (operating agent, OA) pystyy kuitenkin yksinään pysäyttämään vetyvirran
- Vikaantumistaajuudet

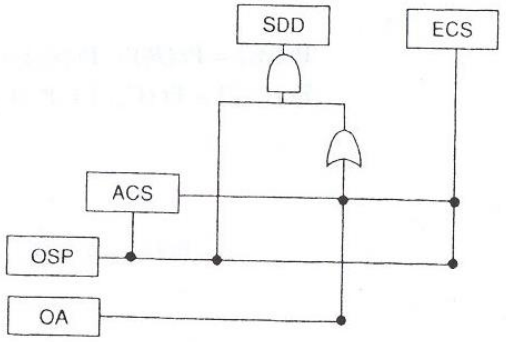
System Failure	
OSP	2.0×10^{-2}
OA	1.0×10^{-2}
ACS	1.0×10^{-3}
SDD	1.0×10^{-3}
ECS	1.0×10^{-3}

Jäähdytysjärjestelmä (2/3)

- Riippuvuussuhteet



- Logiikkakaavio



Jäähdytysjärjestelmä (3/3)

- Osajärjestelmien vaikutukset

State No. (i)	Failed Units	Probability*	Failed and inoperable Units	System State
1	None	9.67×10^{-1}	None	Success
2	ECS	9.68×10^{-4}	ECS	Success
3	SDD	9.68×10^{-4}	SDD	Success
4	ACS	9.68×10^{-4}	ECS, ACS	Success
5	OSP	1.97×10^{-2}	SDD, ECS, ACS, OSP	Failure
6	OA	9.77×10^{-3}	OA	Success
7	ECS, SDD	9.69×10^{-7}	SDD, ECS	Failure
8	ECS, ACS	9.69×10^{-7}	ECS, ACS	Success
9	ECS, OSP	1.98×10^{-5}	SDD, ECS, ACS, OSP	Failure
10	ECS, OA	9.78×10^{-6}	ECS, OA	Success
11	SDD, ACS	9.96×10^{-7}	ACS, ECS, SDD	Failure
12	SDD, OSP	1.98×10^{-5}	SDD, ECS, ACS, OSP	Failure
13	SDD, OA	9.78×10^{-6}	OA, SDD	Success
14	ACS, OSP	1.98×10^{-5}	SDD, ECS, ACS, OSP	Failure
15	ACS, OA	9.79×10^{-6}	ECS, ACS, OA	Success
16	OSP, OA	1.99×10^{-4}	SDD, ECS, ACS, OSP,OA	Failure
17	ECS, SDD, ACS	9.70×10^{-10}	ACS, ECS, SDD	Failure
18	ECS, SDD, OSP	1.9×10^{-8}	SDD, ECS, ACS, OSP	Failure
19	ECS, SDD, OA	9.79×10^{-9}	OA, ECS, SDD	Failure
20	SDD, ACS, OSP	1.98×10^{-8}	SDD, ECS, ACS, OSP	Failure
21	SDD, ACS, OA	9.79×10^{-9}	OA, ACS, ECS, SDD	Failure
22	ACS, OSP, OA	2.00×10^{-7}	SDD, ECS, ACS, OSP,OA	Failure

* Includes probability of success of elements not affected.

- Tärkeimmät riskitekijät

Failure Contributions from Failure of One and Two Units

Combination No.	Units Failed	Probability*	Contribution to Total Failure Prob. (%)
1	OSP	1.97×10^{-2}	98.69
2	ECS, SDD	9.69×10^{-7}	0.00
3	ECS, OSP	1.98×10^{-5}	0.10
4	SDD, ACS	9.96×10^{-7}	0.00
5	SDD, OSP	1.98×10^{-5}	0.10
6	ACS, OSP	1.98×10^{-5}	0.10
7	OSP, OA	1.99×10^{-4}	1.00
8	Sum of all others	2.60×10^{-7}	0.01

* Includes probability of success of elements not affected.

PRA:n prosessi