TOLERANŢA DEFECTELOR HARDWARE

Toleranţa defectelor hardware este abordarea cea mai evoluată în contextual general al tehnicilor de calcul tolerante la defecte.
S-au dezvoltat şi se utilizează multe tehnici de toleranţă a defectelor vizând aplicaţii care cuprind soluţii din domeniul telefoniei şi până în aplicaţii ale misiunilor spaţiale. Iniţial aceste tehnici aveau drept obstacol esenţial costurile asociate hardware-ului redundant. În timp costurile hardware-ului, în general, au scăzut şi nu mai constituie un impediment financiar utilizarea structurilor digitale în tehnicile de toleranţă a defectelor.
Mai mult, datorită costurilor convenabile actuale, se aşteaptă o creştere a utilizării volumului hardware-ului în proiectarea arhitecturilor hardware tolerante la defecte.

Alte considerente intervin în limitarea utilizării actuale extensive a hardware-ului. Printre acestea un rol important îl joacă puterea disipată în structurile digitale utilizate, în general.

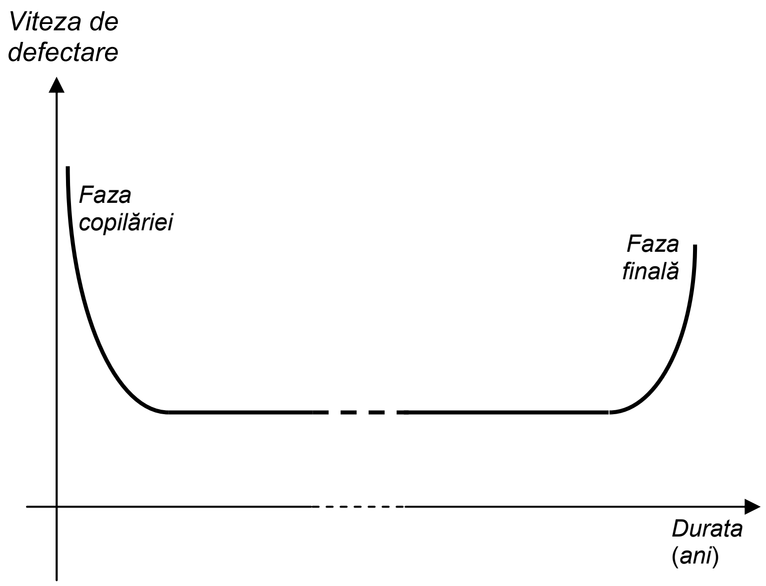


Figura 1. Curba caracteristică a vitezei de defectare pentru structurile digitale

Viteza de apariţie a defectelor hardware

Viteza de defectare a componentelor hardware este unicul şi cel mai important parametru utilizat în analiza fiabilităţii sistemelor hardware. Această viteză se referă la numărul de defecte în unitatea de timp ce urmează să afecteze o componentă, iniţial funcţionând corect, pe durata utilizării viitoare a acesteia într-un anumit sistem. Viteza de defectare este influenţată de vârsta respectivei componente dar şi de şocurile de tensiune ori ale altor parametri de funcţionare cum ar fi temperatura dar chiar şi tehnologia de manufacturare poate avea o contribuţie importantă în acest sens.

Pentru o structură digitală, o unitate de calcul, dependenţa faţă de durata de utilizare are, de regulă, alura unei căzi de baie, aşa cum se poate vedea în figura 1. Atunci când componentele structurii digitale sunt începutul la funcţionării acestora, viteza de defectare este pronunţată. Acest fapt se datorează întâmplării care face ca anumite componente să treacă prin controlul de calitate al manufacturării şi chiar să fie utilizate. Pe măsură ce trece timpul aceste componente sunt îndepărtate, viteza de defectare scade, iar circuitele parcurg grosul duratei lor de funcţionare cu o viteză relativ constantă de defectare. Pe durat utilizării lor aceste componente îmbătrânesc lent, în timp, efectele uzurii încep să se facă simţite iar viteza de defectare începe să crească din nou.

Impactul celorlalţi factori asupra unei componente este exprimat printr-o formulă empirică care determină viteza de defectare a respectivei componente:

$$\lambda = \pi_L \pi_Q (C_1 \pi_T \pi_V + C_2 \pi_E) \tag{1}$$

În relaţia (1) notaţiile au următoarele semnificaţii:
λ este viteza de defectare a componentei.
π_L acesta cuantifică maturitatea tehnologiei de fabricaţie a componentei.
π_Q reprezintă factorul de calitate, reprezentând controlul de calitate al procesului de manufacturare (cu valori cuprinse între 0,25 şi 20,00).
π_T simbolizează factorul de temperatură, cu valori cuprinse între 0,1 şi 1000. Acesta este proporţional cu $e^{-E_a/kT}$, unde s-a notat prin E_a energia de activare (în electron-volţi) asociată tehnologiei, k este constanta lui Boltzmann ($0{,}8625 \cdot 10^{-4}$eV/K) iar prin T s-a notat temperatura (măsurată în grade Kelvin).
π_V reprezintă factorul de stres în tensiune pentru circuitele CMOS. Acest factor are valori cuprinse în intervalul [1, 10], depinzând de tensiunea de alimentare şi de temperatură. Nu se aplică altor tehnologii (pentru alte tehnologii are valoarea 1).
π_E este factorul de şoc al mediului şi are valori foarte mici (aproximativ 0,4) atunci când componenta este plasată într-un mediu cu aer condiţionat, similar celui unui birou, dar poate lua valori mari (13,0) atunci când mediul este mai aspru.
C_1, C_2 sunt factori de complexitate; sunt determinaţi funcţie de numărul de porţi dintr-un circuit şi de numărul de pini ai capsulei.

Dispozitivele aflate, spre exemplu, la bordul autovehiculelor, ori în medii industriale se pot defecta mai des decât alte dispozitive, similare, dar situate în aparate care funcţionează în medii cu temperatură controlată (birouri cu aer condiţionat, bunăoară).

Viteza de defectare, fiabilitatea şi timpul mediu până la defectare

Se consideră o singură componentă, dintr-un sistem complex, care este funcţională de la momentul $t = 0$ şi până când se defectează. Toate defectările, care pot să apară, se presupune că sunt iremediabile şi au un caracter permanent.

Se notează, tradiţional, prin T durata de viaţă a componentei şi prin $f(t)$ şi $F(t)$ funcţia de densitate a probabilităţii a duratei de viaţă şi, respectiv, funcţia de distribuţie cumulativă a duratei de viaţă T. Aceste funcţii sunt definite doar pentru $t \geq 0$, deoarece timpul de viaţă nu poate fi negativ şi sunt exprimate analitic astfel:

$$f(t) = \frac{dF(t)}{dt}, \quad F(t) = \int_0^t f(\tau) d\tau \tag{2}$$

Funcţia $f(t)$ reprezintă, dar nu este egală cu, probabilitatea de defectare la momentul t. Astfel, pentru un interval de timp suficient de mic Δt, $f(t)\cdot \Delta t \approx \text{Prob}\{t \le T \le t + \Delta t\}$. Deoarece $f(t)$ este o funcţie densitate, aceasta trebuie să îndeplinească condiţiile:

$$f(t) \ge 0, \text{ pentru } t \ge 0 \text{ şi } \int_0^\infty f(t)dt = 1.$$

Funcţia $F(t)$ reprezintă probabilitatea defectării componentei la momentul t ori înaintea acestui moment t.

$$F(t) = \text{Prob}\{T \le t\}$$

Fiabilitatea unei componente, notate prin $R(t)$, este probabilitatea ca respectiva componentă să supravieţuiască cel puţin până în momentul t este calculată prin expresia:

$$R(t) = \text{Prob}\{T > t\} = 1 - F(t) \tag{3}$$

Funcţia $f(t)$ este asociată probabilităţii defectării unei noi componente la momentul t, în viitor.
O noţiune cu mai multă semnificaţie este probabilitatea ca o componentă cu vârsta curentă t să se defecteze într-un moment ulterior după un timp, suficient de scurt, cu durata dt.
Aceasta este o probabilitate condiţionată, deoarece se cunoaşte faptul că respectiva componentă a supravieţuit cel puţin până în momentul t.
Această probabilitate condiţionată este reprezentată de *viteza defectării* (numită de asemenea şi *viteza hazardului*) unei componente la momentul t, notată prin $\lambda(t)$, care este determinată astfel:

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \tag{4}$$

Deoarece $\frac{dR(t)}{dt} = -f(t)$, relaţia (4) devine:

$$\lambda(t) = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \tag{5}$$

Anumite tipuri de componente nu suferă vreo îmbătrânire, dar au o defectare care este constantă în timp, $\lambda(t) = \lambda$. Pentru astfel de situaţii,

$$\frac{dR(t)}{dt} = -\lambda R(t)$$

Iar soluţia acestei ecuaţii diferenţiale (cu condiţia $R(0) = 1$) este:

$$R(t) = e^{-\lambda t} \tag{6}$$

În consecinţă, o viteză de defectare constantă implică faptul că durata vieţii T a unei componente are o distribuţie exponenţială, cu un parametru care este chiar viteza constantă a defectării λ:

$$f(t) = \lambda e^{-\lambda t} \qquad F(t) = 1 - e^{-\lambda t} \qquad R(t) = e^{-\lambda t} \qquad \text{pentru } t \ge 0$$

În cazul unei componente ireparabile, timpul MTTF este egal cu media timpului de viaţă (media variabilei T este notată, tradiţional, prin $E[T]$):

$$MTTF = E[T] = \int_0^\infty tf(t)dt \tag{7}$$

Substituind $\frac{dR(t)}{dt} = -f(t)$ rezultă:

$$MTTF = -\int_0^\infty t\frac{dR(t)}{dt}dt = -tR(t)\,|_0^\infty + \int_0^\infty R(t)dt = \int_0^\infty R(t)dt \tag{8}$$

(termenul $-tR(t)$ este nul atunci când $t = 0$ dar şi atunci când $t = \infty$, deoarece $R(\infty)=0$).

În cazul în care viteza defectării este constantă, pentru care $R(t) = e^{-\lambda t}$, rezultă că

$$MTTF = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda}$$

Se consideră, în cele mai multe situaţii, o viteză constantă a defectării. Acest fapt este datorat, în primul rând, simplităţii calculelor.
Dar există cazuri în care această presupunere simplificatoare este inoportună. Zonele copilăriei şi uzurii din figura 1 sunt două exemple, în acest sens.
Pentru aceste zone se utilizează distribuţia Weibull. Această distribuţie are doi parametrii, λ şi β, şi are următoarea funcţie a densităţii timpului de viaţă T a unei componente:

$$f(t) = \lambda\beta t^{\beta-1}e^{-\lambda t^{\beta}} \tag{9}$$

Corespunzător viteza de defectare este:

$$\lambda(t) = \lambda\beta t^{\beta-1} \tag{10}$$

Această viteză de defectare este o funcţie crescătoare pentru $\beta > 1$, este constantă pentru $\beta = 1$ şi este o funcţie descrescătoare pentru $\beta < 1$. Aceste proprietăţi fac distribuţia aceasta foarte flexibilă şi în mod deosebit corespunzătoare pentru fazele copilăriei şi uzurii componentelor. Fiabilitatea unei componente cu distribuţie Weibull este:

$$R(t) = e^{-\lambda t^{\beta}} \tag{11}$$

Iar timpul MTTF al unei componente este:

$$MTTF = \frac{\Gamma(\beta^{-1})}{\beta\lambda^{\beta-1}} \tag{12}$$

Unde $\Gamma(x) = \int_0^\infty y^{x-1}e^{-y}dy$ este funcţia Gamma. Această funcţie este generalizarea funcţiei factorial pentru numere reale şi are următoarele proprietăţi:

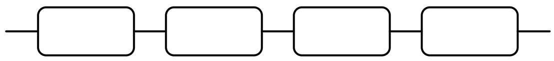
(i) $\Gamma(x) = \Gamma(x-1)$ pentru valori $x > 1$;
(ii) $\Gamma(0) = \Gamma(1) = 1$;
(iii) $\Gamma(n) = (n-1)!$, pentru n natural, $n > 0$.

Este de remarcat faptul că distribuţia Weibull include ca un caz particular (pentru $\beta =$ 1) distribuţia exponenţială cu viteză constantă a defectării.

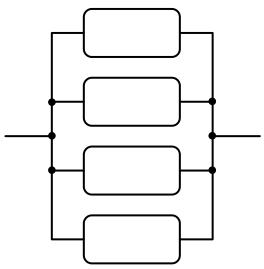
Structurile canonice şi resiliente

Se vor considera câteva dintre structurile canonice, cu ajutorul cărora se pot construi alte structuri mai complexe.
Pentru început se vor aborda structurile de bază, structurile serie şi paralele.

Sistemele serie şi paralele
Cele mai cunoscute structuri sunt structurile serie şi paralele de sisteme, aşa cum se pot vedea în figura 2. Un sistem serie se defineşte ca fiind un set de N de module conectate împreună astfel încât defectarea unui modul face ca întreg sistemul să cadă. Este de reţinut că diagrama din figura 2a este o diagramă de fiabilitate şi nu constituie întotdeauna şi o diagramă de funcţionare electrică.



(a) Sisteme Serie.



(b) Sisteme paralele.

Figura 2. Sisteme serie şi paralele.

Cele patru module din diagrama 2a pot reprezenta, spre exemplu, unitatea de decodificare a instrucţiunii, unitatea de execuţie, memoria imediată (*cache*) şi memoria imediată de instrucţiuni a procesorului. Aceste patru unităţi trebuie să funcţioneze fără erori pentru ca microprocesorul să funcţioneze corect. Se poate remarca diferenţa dintre diagrama de fiabilitate şi diagrama electrică.

Presupunând că modulele din figura 2a se defectează independent unul de celălalt, fiabilitatea întregului sistem serie este produsul fiabilităţii modulelor acestuia. Se notează prin $R_i(t)$ fiabilitatea modulului i şi prin $R_s(t)$ fiabilitatea întregului sistem:

$$R_s(t) = \prod_{i=1}^{N} R_i(t) \tag{13}$$

Presupunând că modulul i are o viteză constantă de defectare λ_i, atunci în conformitate cu relaţia (6), $R_i(t) = e^{-\lambda_i t}$, iar relaţia (13) se rescrie astfel:

$$R_S(t) = e^{-\lambda_S t} \quad (14)$$

În relaţia (14) s-a notat prin $\lambda_S = \sum_{i=1}^{N} \lambda_i$. Din (14) se poate vedea că sistemele serie au o viteză de defectare (cădere) constantă egală cu λ_S (suma vitezelor individuale de cădere) iar MTTF pentru sistemele serie este $MTTF_S = \frac{1}{\lambda_S}$.

Un sistem paralel se defineşte ca fiind un set de N module conectate laolaltă astfel încât sistemul se defectează atunci când toate modulele acestuia se defectează. Această proprietate conduce la următoarea expresie a fiabilităţii unui sistem paralel, notată prin $R_p(t)$:

$$R_p = 1 - \prod_{i=1}^{N} (1 - R_i(t)) \quad (15)$$

Presupunând că modul i are viteza de defectare λ_i, atunci

$$R_p = 1 - \prod_{i=1}^{N} (1 - e^{-\lambda_i t}) \quad (16)$$

Fiabilitatea unui sistem paralel care constă din trei module având vitezele constante de defectare λ_1, λ_2 şi λ_3, spre exemplu, este exprimată prin relaţia:

$$R_p(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} + e^{-\lambda_3 t} - e^{-(\lambda_1+\lambda_2)t} - e^{-(\lambda_2+\lambda_3)t} - e^{-(\lambda_3+\lambda_1)t} + e^{-(\lambda_1+\lambda_2+\lambda_3)t}$$

Se poate remarca, în cazul sistemelor paralele, că sistemul nu are o viteză constantă de defectare, de cădere. Viteza de cădere a unui sistem paralel descreşte odată cu fiecare defectare a unui modul.
Se poate arăta că timpul MTTF al unui sistem paralel, în cazul în care toate modulele au aceeaşi viteză de defectare λ, are expresia:

$$MTTF_p = \sum_{k=1}^{N} \frac{1}{k\lambda}.$$

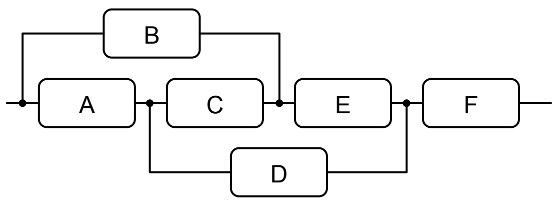


Figura 3. Sistem cu altă structură decât paralelă ori serie.

Sisteme cu alte structuri decât paralele ori serie

Există sisteme a căror diagrame de fiabilitate nu sunt conforme cu structurile paralele ori serie.
Un astfel de sistem este descris în figura 3. Fiabilitatea acestui sistem se nu se poate calcula prin formulele descrise pentru sistemele cu structură paralelă ori serie. Se

poate remarca existenţa mai multor căi în sistemul acesta. Calea *B*, *E* şi *F* arată că sistemul poate opera corect dacă modulele *B*, *E* şi *F* funcţionează corect.
O cale este corectă, validă, într-o astfel de diagramă doar dacă toate modulele sunt parcurse de la stânga spre dreapta. Din acest punct de vedere privind calea *B,C,D,F* se stabileşte că această cale nu este o cale validă. Nu sunt admise transformări ale grafului dacă acestea nu este respectată această regulă.
Pentru simplitatea scrierii, în cele ce urmează, dependenţa fiabilităţii în raport cu timpul va fi omisă, aceasta subînţelegându-se.

Utilizând formula clasică de probabilitate faţă de evenimentele condiţionate se va deduce formula fiabilităţii sistemului din figura 3 prin dezvoltarea acesteia în raport cu un modul oarecare *i* al acestui sistem:

$$R_{sistem} = R_i \cdot \text{Prob}\{\text{Sistemul funcţionează} \mid i \text{ este funcţional}\} + (1 - R_i) \cdot \text{Prob}\{\text{Sistemul funcţionează} \mid i \text{ este defect}\} \quad (17)$$

În formula (17) s-a notat prin = R_i fiabilitatea modulului *i* (*A, B, C, D, E, F*).

Utilizând formula (17) diagrama iniţială se poate descompune în două diagrame de fiabilitate ale sistemului iniţial din figura 3.
Prima corespunde situaţiei în care modulul *i* este funcţional, iar în a doua modulul este defect.
Alegerea modului *i* trebuie făcută astfel încât cele două diagrame nou introduse să aibă structuri cât mai apropiate de tipurile serie şi - ori paralel.
Pentru aceste structuri nou introduse se vor putea utiliza formulele deja stabilite pentru structurile serie şi paralele (13) şi (15).

Prin alegerea modulului *C* se obţin cele două diagrame din figura 4.

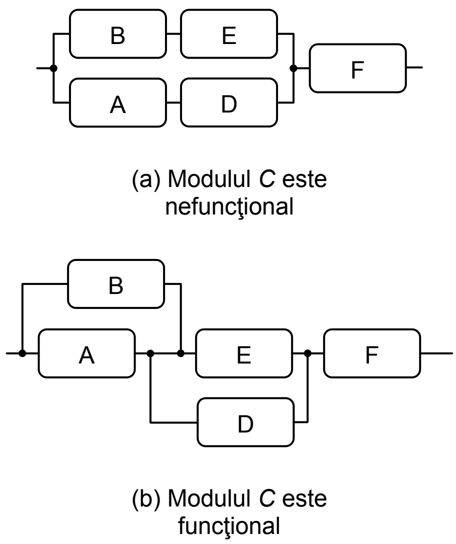


Figura 4. Descompunerea diagramei din figura 3, în raport cu modulul *C*.

Procesul de descompunere se poate relua, se poate re-itera, până când se obţin doar combinaţii de diagrame de tip serie ori paralel.

Aşa cum se poate remarca din figura 4.a aceasta este constituită doar din diagrame serie şi paralel.

Figura 4.b, spre deosebire de figura 4.a, nu este alcătuită exclusiv din combinaţii serie şi paralel. În acest sens trebuie remarcat faptul că modulele *A* şi *B* nu sunt în paralel, aşa cum s-ar putea aprecia la o primă privire.

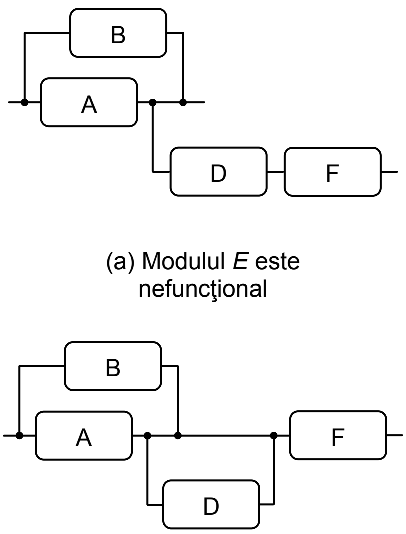
Dacă aceste module ar fi în paralel, aşa cum ar apare datorită funcţionării corecte a modulului *C*, atunci ar trebui să existe în diagrama iniţială, din figura 3, o cale *BCDF*, ceea nu se-ntâmplă să fie.

În figura 4.b acest fapt este marcat de sub-segmentul aflat între conexiunile modulelor *D* şi *B* (corespunzător prezenţei funcţional sigure a modulului *C*).

Cu aceste remarci, se poate rescrie relaţia (17) astfel:

$$R_{\text{sistem}} = R_C \cdot \text{Prob}\{\text{Sistemul funcţionează} \mid C \text{ este funcţional}\} + (1 - R_C) \cdot R_F \cdot [1 - (1 - R_A \cdot R_D)(1 - R_B \cdot R_E)] \quad (18)$$

Pentru calculul probabilităţii condiţionate a sistemului (în raport cu faptul că modulul *C* este funcţional) diagrama din figura 4.b va fi descompusă în raport cu modulul *E*, aşa cum se poate urmări în figura 5.



(a) Modulul *E* este nefuncţional

(b) Modulul *E* este funcţional

Figura 5. Descompunerea diagramei din figura 4.b, în raport cu modulul *E*.

Atunci când modulul *E* este nefuncţional diagrama de fiabilitate arată ca în figura 5.a. Este important de reţinut că modul *C* este funcţional atât în figura 5.a, cât şi în figura 5.b.

Expresia probabilităţii sistemului atunci când *C* funcţionează iar modul *E* este nefuncţional se calculează pentru conectarea în serie a modulelor *A, D şi F.*

Se poate remarca în această situaţie că modulul B este prezent în sistem dar nu este conectat la modul F de ieşire, întrucât nu există o cale între modulul B şi F în diagrama iniţială de fiabilitate a sistemului.

Expresia algebrică a probabilităţii sistemului condiţionat de faptul că modulul C este funcţional, iar modulul E este nefuncţional arată astfel:

Prob{Sistemul funcţionează | C este funcţional şi E este nefuncţional} =
$$(1 - R_E)R_A R_D R_F.$$

Iar cealaltă probabilitate arată astfel:

Prob{Sistemul funcţionează | C şi E sunt funcţionale} = $R_E\, R_F[1 - (1 - R_A)(1 - R_B)]$.

După determinarea acestei expresii se poate exprima fiabilitatea sistemului ca fiind:

$$R_{sistem} = R_C[R_E R_F(R_A + R_B - R_A R_B) + (1 - R_E)R_A R_D R_F] + (1 - R_C)[R_F(R_A R_D + R_A R_E - R_A R_D R_B R_E)] \quad (19).$$

Dacă blocurile acestei diagrame de fiabilitate au fiabilităţi identice:

$$R_A = R_B = R_C = R_D = R_E = R_F = R,$$

atunci fiabilitatea sistemului are expresia:

$$R_{sistem} = R^3(R^3 - 3R^2 + R + 2) \quad (20)$$

Atunci când o diagramă are o structură foarte complicată pentru aplicarea unei proceduri similare celei parcurse anterior se pot calcula margini inferioare şi superioare a fiabilităţii sistemului, R_{sistem}.

O margine superioară este determinabilă prin expresia:

$$R_{sistem} \le 1 - \prod (1 - R_{calea_i}) \quad (21)$$

Fiabilitatea unei căi se calculează ca pentru conectarea în serie a modulelor ce alcătuiesc acea cale.

Marginea superioară din expresia (21) presupune că toate căile sunt în paralele, pe de-o parte, şi independenţa respectivelor căi, pe de-altă parte.

Cazurile reale pot prezenta situaţii în care două astfel de căi au un modul în comun iar defectarea unui astfel de modul va conduce la defectarea ambelor căi.
Aceasta este raţiunea pentru care termenul din dreapta expresiei (21) constituie doar o margine superioară şi nu o valoare exactă.

O margine inferioară poate fi calculată în baza determinării unor seturi minimale de tăieturi ale diagramei de fiabilitate a sistemului.

Un set minimal de tăieturi este o listă de module cu proprietatea că prin îndepărtarea tuturor modulelor dintr-un set (datorită defectărilor) aceasta va conduce la defectarea sistemului, presupus iniţial perfect funcţional.

Marginea inferioară se calculează din expresia:

$$R_{sistem} \geq \prod (1 - Qcut_i) \qquad (23)$$

În relaţia (23) s-a notat prin $Qcut_i$ probabilitatea ca respectiva tăietură *i* să fie defectă. Referitor la figura 3, seturile minimale de tăieturi ale diagramei de fiabilitate din această figură sunt:

F, AB, AE, DE şi *BCD*.

Formula algebrică a marginii inferioare determinată prin seturile minimale de tăieturi arată astfel:

$$R_{sistem} \geq R_F[1-(1-R_A)(1-R_B)][1-(1-R_A)(1-R_E)][1-(1-R_D)(1-R_E)] \times[1-(1-R_B)(1-R_C)(1-R_D)] \qquad (24)$$

Dacă $R_A = R_B = R_C = R_D = R_E = R_F = R$, atunci:

$$R_{sistem} \geq R^5(24 - 60R + 62R^2 - 33R^3 + 9R^4 - R^5).$$