Алгоритъм за изследване и компютърно моделиране на безопасността на електронни fail- safe схеми

проф. дтн. Христо Ангелов Христов,
гл.ас. Нели Иванова Стойчева

Висше Военно Транспортно Училище „Т.Каблешков“

1. Увод.

Новото поколение системи за жп автоматика и телемеханика е построено на конвенционални микропроцесорни и микроелектронни елементи. Безопасността на устройствата се постига на макониво, с помощта на апаратни и програмни средства за контрол и превключване (СКП) , а не на елементно ниво. Средствата за контрол и превключване регистрират неизправностите в апаратурата и грешките в програмирането и превключват системата към защитно (неопасно) състояние или към контролируемо развитие. Но за да бъде достигнато необходимото ниво на безопасност, трябва СКП сами да не допускат опасни откази.

Специфичният интерфейс на системите, осигуряващи въвеждането на контролната и управляващата информация и изведането на управляващите въздействия към обекта на управляние също се реализира с помощта на безопасни електронни устройства, които са построени на основта на логияески, аналогови или прагови електронни схеми. Възниква въпросът за синтеза на безопасни схеми и анализ на достигнатата безопасност.

Моделирането на безопасността на електронните схеми за контрол, превключване и входно-изходна организация се явява част от анализа и доказателството на безопасността на системите.

Целта на тази работа е компютърно моделиране на безопасността на електронните схеми, построени на дискретни електронни еелементи.

Решението на проблема за моделирането на безопасността на електронните схеми се свежда до следните задачи:

1. Определяне на критерия за опасен отказ и опасното състояние на схемата.
2. Определяне на изходния сигнал на работоспособна схема.
3. Логическо моделиране на безопасността - качествена оценка на безопасността.
4. Изчисляване на показателите за безопасност - количествено оценяване на безопасността.

Проблемът за автоматизирания анализ на надеждността на електронните схеми е обсъждан в редица публикации [7,8,9, 10,]. В достъпната литература отсъства изследването на безопасностат на електронни схеми с отчитане на всички многократни неизправности.

2. Проблемът за безопасността на електронните схеми.

Безопасността на жп транспорт се разбира като отсъствие на аварии и катастрофи, застрашаващи живота, здравето и интересите на хората, загуба на големи материални, духовни и природни ценности.

Най-общо ***критерият за безопасност след отказ (fail- safe)*** на СЖАТ може да се определи като свойство на сситемата да преминава в защитно състояние, забраняващо движението на подвижния състав или намаляващо скоростта му под допустимата.

Неработоспособната система е опасна, ако следотказовото и поведение противоречи на възприетия критерий. Всички следотказови състояния, в които тя попада в противоречие с критерия, са опасни, а отказите, които са ги предизвикали - **опасни откази.**

Защитният отказ е такова частично или пълно нарушаване на работоспособността на обекта, което предизвиква изключване на управляващото въздействие (или контрролния сигнал) върху управлявания от обекта процес, в резутат на което се постига желаното по възприетия критерий следотказово състояние или развитие на процеса. [3]

Защитният отказ е логически инверсен на опасния. Системата реагира *съобразно* критерия, а при опасен отказ - в *разрез* с критерия за желано следотказово поведение.

Ако електронният елемент винаги след активизиране на неизправност преминава в защитно по възприет критерии, то той се нарича елемент с безопасно след отказово поведение (***Fail- safe елементи***).

Недопустими (невъзможни) се наричат неизправности, възникването на които е изключено от природни закони, свойствата на използуваните материали, конструкцията и технологията на готовия компонент или изделия. За електронните елементи са известни каталози и отраслови стандарти [ ] , от които може да се установи какви неизправности да допустими в конвенционалната електроника и какви в специализираната продукция за изделията със специално предназначение.

3.Определяне на изходния сигнал на схемата.

Нека входните сигнали , подавани на схемата са X_i $i=\{1,2,...m\}$. Трябва да се определят изходните сигнали Y_i, $i=\{1,2,...I\}$, както при отсъствие, така и при наличие на откази. По зададен алгоруитъм ан функциониране всеки входен вектор X_i $<x_1,x_2,...\ x_r>$, където X_i, $i=1\div r$ е множеството от логически променливи ан входа на схемата, предизвиква функционален сигнал на изхода Y_i. В схемата могат да се появят допъстими логияески неизправности $z_1, z_2, z_3..., z_R$. Ако коя да е от тях се е случила (например първата), то z_1^1, ако не се е случила z_1^0.

Нека в схемата се е случила логическа неизправниост z_i^1. Наборът от входни променливи $X_K = <x_1, x_2, ... x_r>$, за които се е получил преход към сигнал $Y_j > Y_i$ се нарича опасен входен набор, булевата функция, съвкупност от опасните входни набори, равняващя се на 1 се нарича функция от опасни набори (ФОН). [3]

Нека на входа е зададен векторът $X_K = <x_{K1}, x_{K2}, ... x_{Kr}>$. Възможни са различни набори логически неизправности ((НН):

$$Z_1 = <z_1^0,z_2^0,... z_R^1>,$$
$$Z_2 = <z_1^0,z_2^1,... z_R^0>,$$
$$Z_3 = <z_1^0,z_2^1,... z_R^1>, \qquad (1)$$
$$.....$$
$$Z_2^R = <z_1^1,z_2^1,... z_R^1>,$$

Наборите Z_1, Z_2,... Z_2^R, за които се получава преход към сигнал $Y_j > Y_i$, се наричат опасни набори от неизправности (ОНН), а съответната булева функция, равна на 1, се нарича БФ ОНН за при даден входен набор.

В случай на аналогова схема са валидни същите съотношения, но входните $X_K = <x_1(t), x_2(t), ... x_r(t) >$ и изходните сигнали $Y_i = <y_{i1}(t), y_{i2}(t), ... y_{ij}(t),..., y_{iq}(t)>$ са непрекъснати функции. Ако схемата е с един вход и един изход, дадената система от отношения се опростява и свежда до прехода $Y_i(t) < Y_j(t)$.

Логическата оценка на безопасността на схемите се състои в определяне на БФ ОНН за всички входни набори.

4.Логическо моделиране на безопасността.

4.1. Алгоритъм N1.

За да се определят опасните набори от неизправности за даден входен набор е необходимо да се изпълни следния алгоритъм [ ]:

1. Последователно се задават всички основни набори X_i, където $i=\{1,2,....n\}$;

2. За всеки входен набор се определя съответстващия (по алгоритъм) изходен сигнал Y_i.

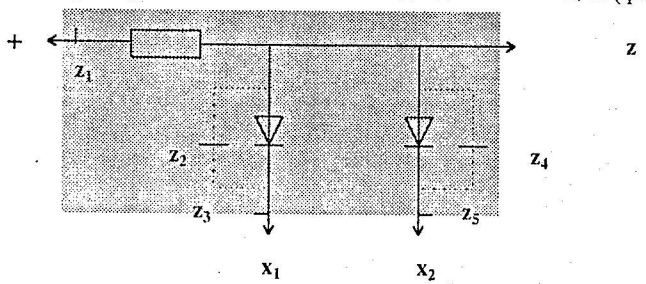
3. Изреждат се всички възможни набори от неизправности за зададения входен набор;

4. За всеки набор от неизправности Z_i, $i=\{1,2,..2^R\}$ се определя изходен сигнал Z_j и характера на лъжливия преход:

- ако $Z_j > Z_i$, то прехода е опасен;
- ако $Z_j = Z_i$, то прехода е скрит;
- ако $Z_j < Z_i$, то прехода е защитен.

5. Логическата функция на опасните набори от неизправности е дизюнкция от всички опасни набори. Ако няма опасен преход за нито един от неизправности при всички набори на входа, схемата е качествено безопасна.

Пример. Нека вземем схема на диодна конюнкция (фиг.1)



Фиг.1

1.Входните набори са: $X_1 = <0,0>$, $X_2 = <0,1>$, $X_3 = <1,0>$ и $X_4 = <1,1>$;

2.

	X_1	X_2	X_3	X_4
Y	0	0	0	1

3. и 4.Лъжливите сигнали, установени визуално са:

Z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
z1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1	1	1	1	0	1	0	1	0	1	0	1
z2	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
z3	0	0	0	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
z4	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
z5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Yj за X1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0
Yi за X2	0	0	0	1	0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0
Yi за X3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	1	1	0	0	1	1	1	1	0	1	0

5.Булевите функции на ОНН имат вида:

$F_{0.1} = z1^0.z2^0.z3^0.z4^0.z5^1 \vee z1^0.z2^1.z3^1.z4^0.z5^1 \vee z1^0.z2^0.z3^1.z4^1.z5^1 \vee z1^0.z2^1.z3^1.z4^1.z5^1$

$F_{0.2} = z1^0.z2^0.z3^1.z4^0.z5^0 \vee z1^0.z2^1.z3^1.z4^0.z5^0 \vee z1^1.z2^0.z3^1.z4^1.z5^0 \vee z1^1.z2^0.z3^1.z4^1.z5^0 \vee z1^0.z2^1.z3^1.z4^1.z5^0 \vee z1^1.z2^1.z3^1.z4^1.z5^0 \vee z1^0.z2^0.z3^1.z4^0.z5^1 \vee z1^0.z2^1.z3^1.z4^0.z5^1 \vee z1^0.z2^0.z3^1.z4^1.z5^1 \vee z1^0.z2^1.z3^1.z4^1.z5^1$

$F_{0.3}$ е аналогична $F_{0.2}$.

4.2. Алгоритъм N2.

От алгоритъм N1 се вижда, че с усложняване на схемата допустимите неизправности растат и реализирането на алгоритъм по метода на пълното изброяване[

] е практически невъзможно (*т.3. от Алгоритъм N1*). Ограничаването на анализа само до единична или съвкупна двойна неизправност е нецелесъобразно при схемите с висока отговорност за безопасността на движението. Ето защо в тази работа се предлага анализът да се извърши по метода Дърво на Откриващите Набори от Повреди (ДОНП) [ ].

Методът ДОНП се състои в следнато.

Построява се верига на неизправностите,започвайки със z_1. Изпълнява се стъпка 4 от алгортъм N1. Ако НН не се изявява, се добавя z_2 и и отново се изпълнява стъпка 4. Ако НН отново е скрит, веригарта се удължава до z_3 и т.н. до изявяване на отказ или до z_R. Ако обаче на някаква съвкупност от откази $к_i$ отказът се изявява, то се определя неговия характер и полученият набор се записва към множеството на защитните или опасните откази.

По- нанатък отстранявайки последната наизправност, съответстваща на върха на клона, веригата се намалява до $к_i$ -1.

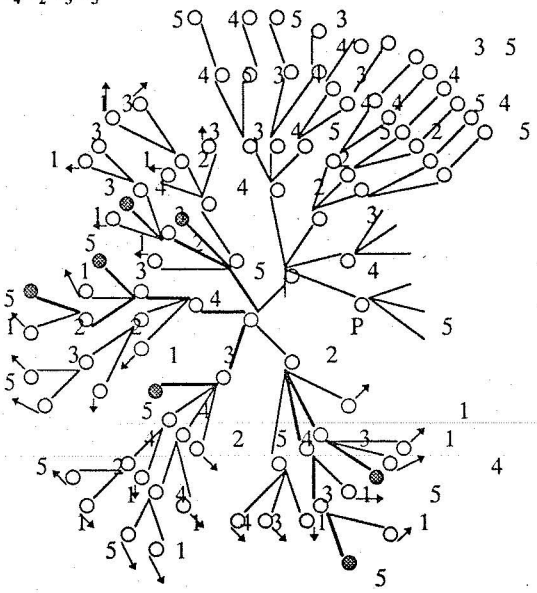
Тук се образува разклонение на веригата. Добавя се неизправността със следващ номер и веригата се удължава по същото правило.

Получава се дърво с разклонения, чийто корен е z_1. Когто е завършен пълният набот от неизправности, дървото е построено

Строи се ново дърво с корен z_2. Добавя се z_1, после z_3, и т.н. Веригата се удължава, но без z_i, които вече са включени във веригарта.

На фиг.4 е показано дървото за диодната конюнкция от фиг.3.
От него се вижда, че:

$F_{o.1} = z_2^1 z_3^1 z_5^1$
$F_{o.2} = z_2^1 z_4^1 z_3^1 z_5^1$
$F_{o.3} = z_2^1 z_5^1 z_3^1$
$F_{o.4} = z_3^1 z_2^1 z_4^1 z_5^1$
$F_{o.5} = z_3^1 z_4^1 z_2^1 z_5^1$
$F_{o.6} = z_3^1 z_5^1$
$F_{o.7} = z_4^1 z_2^1 z_3^1 z_5^1$
$F_{o.8} = z_4^1 z_3^1 z_2^1 z_5^1$
$F_{o.9} = z_4^1 z_3^1 z_5^1$
$F_{o.10} = z_5^1 z_2^1 z_3^1$
$F_{o.11} = z_5^1 z_2^1 z_4^1 z_3^1$
$F_{o.12} = z_5^1 z_4^1 z_2^1 z_3^1$
$F_{o.13} = z_5^1 z_4^1 z_3^1$



Фиг.4

$F_{онн} = F_{o.1} \vee F_{o.2} \vee F_{o.3} \vee F_{o.3} \vee F_{o.4} \vee F_{o.5} \vee F_{o.6} \vee F_{o.7} \vee F_{o.8} \vee F_{o.9} \vee F_{o.10} \vee F_{o.11} \vee F_{o.12} \vee F_{o.13} = z_3^1 z_5^1$

5. Изчисляване на показателите за безопасност.

След като се изпълни алгоритъм N1 и вградения в него алгоритъм N2 се получават n на брой ДОНП, толкова, колкото са входните набори.

БФ на ОНН се получава като конюнкция на опасните набори от повреди, записани към множеството на опасните откази за всеки входен вектор.

5.1. Изчисляване на вероятността за опасна работа.

Приемаме,че схемите са възстановими и ергодични и пребивават в различни надеждностни състояния. Предполагаме, че отказите възникват и се възстановяват поединично, т.е. потокът от откази и възстановявания е ординарен. Под състояние се разбира набора от еизправности, например $Z_1 = <z_{1o}, z_{2o},...z_{R1}>$. С интензивност λ_i в схемата се случва неизправност i , а с интензивност μ_i работоспособността на схемата се възстановява. Процесът на преминаване от едно състояние в друго е марковски. Всички състояния принадлежата към едно от трите пространства (глобални състояния) - работоспособно M_p, опасно M_o и защитно $M_з$. След достатъчно дълго време се достига пределната вероятност за пребиваване на схемата във всяко от трите състояния, която не се изменя с времето.

Невъзстановимата система се явява частенм случай , когато $\mu_i=0$, $i = \{1,2,....R\}$. Системата е неергодическа.

Изчисляване на вероятността за опасен отказ $Q_o.o(t)$ за невъзстановима система и вероятността за опасна работа $Q_{o.p}(t)$ за възстановима се определят по метода на преход от логически към вероятностни функции. [6,7].

БФ се преобразува във форма, подходяща за пълно заместване. След спазване на правилата на това преобразуване логическите променливи z_i^0 се заместват с вероятността за безотказна работа на съответния елемент - p(t), а z_i^1 - се замества с вероятността за отказ q(t).

На тази основа за схемата от фиг. 1. , за която е получена БФ на ОНН ( ) , за вероятността за опасна работа се получава:

$Q_{o.o}(t) = p_3(t).p_4(t)\ [p_5(t).q_8(t) + q_5(t).p_8(t) + q_5(t).q_8(t)] + (p_1(t).p_j(t) + q_1(t).q_0(t)]$

Ако схемата е невъзстановима и отработката до отказ има експоненциално разпределение, то $\lambda(t) = \lambda = const.$ и

$p_i(t) = \exp(-\lambda t)$, $q_i(t) = 1 - \exp(-\lambda t)$.

Ако схемата е възстановима, то вместо вероятността за опасен отказ критерий ще бъде вероятността за опасна работа $Q_o.p(t)$. В уравнение (6) вместо вероятността за безотказна работа $p_i(t)$ и вероятността за отказ $q_i(t)$ трябва да се поставят съответно готовността $\Gamma_i(t)$

$$\Gamma_i(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda}.\exp[-(\mu+\lambda)t]$$

и неготовността $\Pi_i(t)$

$$\Pi_i(t) = \frac{\lambda}{\mu+\lambda}\{1 - \exp[-\mu+\lambda)t\}$$

5.2 Средна отработка на опасен отказ (MTBHF).

Математическото очакване на времето мейду два опасни отказа MTBHF е показател за възстановими системи и може да определи о честотата H_O. Влизането в пространството на опасните състояния става с някаква честота Ho= 1/MTBHF.

Известно е [8], че честотата на прехода h от едно в друго състояние се определя по формулата:

$h_{ij} = p_i.\lambda_{ij}$, където **i** - е изходното състоянието, а **j** - състоянието на прехода.

Честотата на влизане в пространството на опасните състояния H_o се явява сума от всички честоти на прехода от състояние **i**, непринадлежащо към опасните , към произволно опасно състояние **j**.

$$H_o = \sum_{i \notin M_o} \left(p_i \sum_{j \in M_o} \lambda_{ij} \right)$$

За примера от фиг.1. по дадената формула получаваме:

$H_o = p_1p_5p_8p_o\lambda_s + q_1q_5p_8p_o\mu_1 + p_1q_5p_8q_o\mu_o + q_1p_5q_8p_o\mu_1 + p_1p_5p_8p_o\lambda_8 + p_1p_5q_8q_o\mu_o + q_1q_5q_8p_o\mu_1 + p_1q_5q_8q_o\mu_o + p_1p_5q_8q_o\mu_1 + q_1p_5p_8q_o\lambda_8 + q_1p_5q_8p_o\lambda_o + p_1q_5p_8q_o\lambda_1 + q_1p_5p_8q_o\lambda_5 + q_1q_5p_8p_o\lambda_o + p_1q_5q_8q_o\lambda_1 + q_1q_5q_8p_o\lambda_o$

6. Компютърно моделиране на безопасността

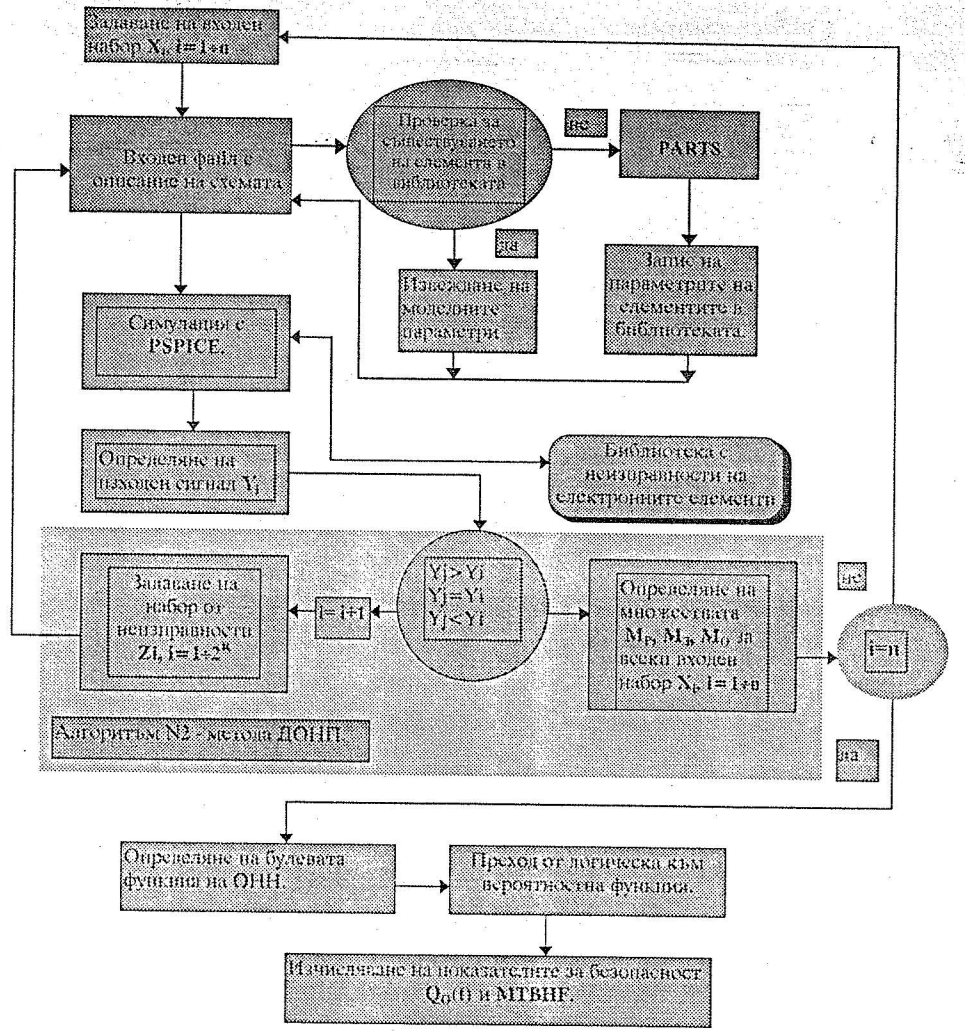
Тук се предлага компютърна програма, реализираща алгоритъма, показан в т.4, на основата на отказови модели на електронните компоненти, разработени в [.].

Структурната схема на алгоритъма е показана на фиг.5.

Програмата е написана на FORTRAN 77.

Литература:

1. MIL-HDBK-217C, Notice 1, Reliability Prediction of Electronic Equipment, 1980,
2. DEUTSCHE BUNDESBAHN, Allgemeine Richtlinien fur signaltechnisch sichere Schaltungen und Einrichtungen der Elektronik, 1990.
3. Сапожников,В.В.,Вл.В.Сапожников, Методы синтеза надежных автоматов, Энергия, 1980.
4. Linde,H., L.W.Schiweck. Der Sichrheitsnachweis auf Bauelementenebene.-Signal und Draht. 1981, N°9-10.
5. Христов,Хр.,Електронизация на осигурителната техника,Техника, 1984 ,
6. Хр. Основи на осигурителната техника, Техника, 1990.
7. Chenming Hu, The Berkeley Reliability Simulator BERT: an IC Reliability Simulator, Microelectronics Journal, N23, 1992, pp.97-102.
8. Стойчева,Н., Е.Иванов, Компютърен анализ на вида и последствията от отказитв в електронните схеми, Сборник доклади от научна конференция на ВВТУ "Т.Каблешков", 10-12.11.1993г., стр.513-518
9. Kalyan,R., S.Kumar, Comparison of a simulation and an exact method for reliability evaluation of a large networks using a personal computer, Microelecrtonics and Rel., Vol.29, N2, pp.133-136, 1989.
10. Lehtela,M., Computer-Aided Failure Mode and Effect Analysis of Electronic Circuits, Microelectronics and Reliability, Vol.30,N4, pp.761-773, 1992.
11. Pspice, User's guide. MicroSim Corporation, La Cadena Drive, Laguna Hills, 1989.


Задаване на входен набор X_i, i=1÷n
Входен файл с описание на схемата
Проверка за съществуването на елемента в библиотеката
не
PARTS
да
Въвеждане на моделните параметри
Запис на параметрите на елементите в библиотеката.
Симулация с PSPICE.
Определяне на изходен сигнал Y_i
Библиотека с неизправности на електронните елементи
Задаване на набор от неизправности Z_i, i=1÷2^N
i=i+1
Yj>Yi
Yj=Yi
Yj<Yi
Определяне на множествата M_0, M_1, M_2 за всеки входен набор X_i, i=1÷n
не
i=n
да
Алгоритъм N2 - метода ДОНП.
Определяне на булевата функция на ОНН.
Преход от логическа към вероятностна функция.
Изчисляване на показателите за безопасност $Q_0(0)$ и МТВНБ.

Фиг.5