ИЗСЛЕДВАНЕ НА БЕЗОПАСНОСТТА НА КОЛЕКТОРНО-БАЗОВА ЛОГИКА

1993 г.

проф. дтн Христо Ангелов Христов
ст.ас. Нели Иванова Стойчева
ВВТУ "Т.Каблешков"

Опасността е случайно събитие или принудено състояние, в което възниква заплаха за здравето и/или живота и интересите на човека, за материални, морални и/или природни ценности.

Безопасността е свойство да не се допуска опасност.

В работоспособно състояние перфектно създадената система е безопасна. Неработоспособната система е опасна, ако следотказовото и поведение противоречи на възприетия критерий за безопасност. Ако пък се съгласува с критерия, поведението и е защитно. Този критерий не е универсален. Определя се конкретно за всяка система, устройство или елемент, като се изхожда от горното определение за опасност.

Тук се разглежда безопасността на логически елемент, използван в железопътната осигурителна техника.

Според [2] един логически елемент(ЛЕ) се нарича безопасен, ако интензивността на възникване на отказ е по-малка от пределното значение при дадено ниво на безопасност. Последното определение не е съвсем коректно, защото изключва от пространството на безопасните един съществен клас ЛЕ, за които решаващо се явява не това, изменя ли той своите функции, а в каква посока. Елементът може да е с ниска надеждност, но да е с висока безопасност, ако отказите му го довеждат в защитно състояние.

В системите за железопътна автоматика логическа "1" съответства на високоотговорното състояние (от гледна точка на безопасността). В това състояние се разрешава движението на влака или маневрения състав, подават се управляващи въздействия при наличие на условия за безопасност. Сигналите, носещи логическа "1", винаги са активни.

Логическа "0" съответства на състояние, в което движението е забранено. В общия случай е забранено изпълнението на недопустими за безопасността действия на човека или въздействия на техниката. Сигналите, носещи логическа "0", винаги са пасивни.

Според алгоритъма на функциониране и в зависимост от входните данни изправният елемент осъществява функционални преходи от двата вида "0-1" и "1-0". Но преходът може и да е нефункционален, а лъхлив. Лъхлив е преходът на елемента от едно състояние в друго вследствие на отказ.

Ако единият от двата нефункционални прехода на изходния сигнал ("0-1" или "1-0") е невъзможен (или малковероятен) при каква да е неизправност във вътрешната структура на елемента, то ЛЕ е елемент с несиметрични откази. В съответствие с дефинираните състояния "0" и "1" в ж.п. осигурителната техника невъзможен е лъхлив преход "0-1", защото е опасен.

ЛЕ с несиметрични откази е качествено безопасен, ако допустимите неизправности в неговата вътрешна структура се проявяват като невъзможност да се замени функционалния изходен сигнал, приет за логическа "0", с лъхлив сигнал, приет за логическа "1". ЛЕ е количествено безопасен, ако интензивността на възникване на отказите, предизвикващи лъхливи преходи "0-1" е по-малка от вероятността, определяща зададената безопасност.

Входния набор, при наличието на който може да се появява лъхлив преход "0-1", определяме като опасен входен набор. При различни неизправности или техни съвкупности опасни могат да бъдат различни входни набори.

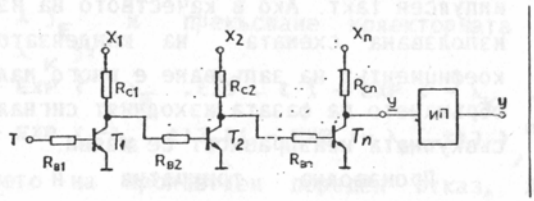
Съществуват качествена (логическа) и количествена (вероятностна) оценка на безопасността. Целта на качествената оценка е да се определят опасните входни набори. Ако при недопустимите неизправности такива няма, то ЛЕ е качествено безопасен. Целта на количествената оценка е да се определи вероятността за истинност на опасния отказ с отчитане на входните набори. Ако е зададена норма за безопасност и вероятността за опасен отказ се окаже $Q_o \leq Q_{доп}$, то ЛЕ е количествено безопасен. Като се изхожда от конвенционалните елементи на осигурителната техника, се приема $Q_{доп} = 1.10^{-13}$.

В електромеханическите елементи, използвани в системите за железопътна автоматика и телемеханика изискванията за безопасност се удовлетворяват по пътя на специални конструкции и технологии, изчислени на недопустими неизправности. В активните и пасивни компоненти, използвани в традиционните области на електрониката, като правило няма недопустими неизправности. Те са

елементи със симетрични откази. За тях вероятностите за възникване на неизправности от типа "късо съединение" и "прекъсване" са от еднакъв порядък. В изследваната схема са използвани такива елементи .Колекторно-базовата логика принадлежи към схемите с истинска безопасност и с некодиран сигнал на логическата променлива. При този, твърде широко разпространен клас, намирането на неизправностите и автоматическия преход в защитно състояние, се достига благодарение на непрекъсната импулсна работа на схемите, въпреки логическите единици на нейните входове във вид на непрекъснат потенциал. Схемите се превключват от външния такт T, постъпващ на специален вход. Изходният сигнал се получава в кодиран вид (такт), но за последващата му обработка той трябва непременно да се декодира.

В тази работа търсим качествената и количествената оценка на безопасността на колекторно-базова логика при внезапни откази..

Схемата представлява многовходов ЛЕ (фиг1.) и е разработена от нас в [1]. Правени са много изследвания върху нейната функционалност. Тук се прави за пръв път анализ на безопасността и.



Фиг.1.

Логическите променливи $X_1, X_2, \ldots X_n$ постъпват във вид на устойчиви потенциали в колекторната верига на транзисторите, свързани последователно в каскадна схема. Тактовите импулси T се подават на базовия вход на първия транзистор. При наличие на всички логически входове на високи потенциали, на изхода, в зависимост от броя на каскадите, се получава импулсен сигнал със същата (при четен брой) или обратна фаза (при нечетен брой). Реализира се булевата функция "И" $Y = X_1 \cdot X_2 \cdot \ldots X_n$.

Формулираме изискването към безопасността на колекторно-базовата логика чрез булевата функция на потенциално опасните откази F_0. За ЛЕ от типа "И" , какъвто е случая, тя има вида:

$$F_0 = \left(\bigcup_{\{M_{n,1}\}} \bigcap_{j=1}^{n} X_{ij} \right) \cup \left(\bigcup_{\{M_{n,2}\}} \bigcap_{j=1}^{n} X_{ij} \right) \cup \ldots$$

$$\ldots \cup \left(\bigcup_{\{M_{n,n}\}} \bigcap_{j=1}^{n} X_{ij} \right) = 0 \qquad /1/$$

където множествата $\{M_{n,1}\}$, $\{M_{n,2}\}$ .... $\{M_{n,n}\}$ се състоят от наборите, съответно с една, с две и т.н., с n - логически променливи $x_j = 0$.

Съгласно уравнение /1/ входните набори могат да бъдат опасни, ако макар и една от логическите променливи в набора е равна на "0".

Изследванията показаха, че произволна единична неизправност в схемата се контролира, т.е. няма опасен входен набор.. От двукратните заслужава внимание едновременното прекъсване на колекторния резистор и на емитерната верига на един и същ транзистор. Отбелязваме логическата променлива на неизправността със z_i^1. Ако такава съвкупна неизправност стане на тази каскада, където логическата променлива е нула (x_i^0), тактовите импулси ще преминат през каскадата, без да се инвертира фазата, както е нормално. На изхода се получава кодиран, но с обратна фаза, импулсен такт. Ако в качеството на изходен преобразувател е използвана схемата на кондензаторен декодер [1], а коефициентът на запълване е много малък (примерно K=0,1), с обръщането на фазата изходният сигнал рязко изчезва, когато съвкупната неизправност се изяви.

Произволна трикратна и повече-кратна нечетна неизправност води до прекъсване на тактовите импулси в тази каскада, където е първата по хода на импулсите неизправност. Вече четирикратна неизправност (две съвкупни) ще бъде опасна, защото ще имаме двукратно инвертиране на сигнала и отказът може да остане неразпознат, ако амплитудата му не затихне достатъчно. Втората съвкупна неизправност се комбинира опасно с вече възникналата, независимо от стойността на логическата променлива на съответния вход.

Ще определим вероятността за опасен набор.

Нека на първия вход с вероятност p има нулев сигнал (x_1^0). Булевата функция на опасния отказ има вида :

$$F_{O_1} = x_1^0 \cdot z_1^1 \cdot (z_2^1 \cup z_3^1 \cup \ldots\ldots \cup z_n^1) \qquad /2/$$

Логическата функция /2/ отчита възможните опасни съчетания на съвкупната неизправност на първата каскада с подобни неизправности на всички останали каскади.

Функцията /2/ е безповторна. За да преминем към вероятностна функция, е необходимо да я преобразуваме с теоремата на де Морган :

$$F_{O_1} = x_1^0 \cdot z_1^1 \cdot (z_2^0 \cup z_3^0 \cup \ldots\ldots \cup z_n^0) \qquad /3/$$

Тогава <u>вероятността за опасен отказ</u> по първи вход е:

$$Q_{O_1} = P_{X_1} \cdot Q_{C_1} \cdot (1 - P_{C_2} \cdot P_{C_3} \ldots\ldots P_{C_n}) \qquad /4/$$

където Q_C и P_C са съответно вероятности за съвкупна неизправност и за нейното отсъствие. Ако приемем, че всички каскади са еднакви:

$$Q_O = P \cdot Q_C \cdot \left[1 - [1 - Q_C]^{n-1} \right] \qquad /5/$$

В случай на експоненциално разпределение на отработката до отказ, какъвто е най-често случая, за невъзстановим ЛЕ с отчитане на независимостта на прекъсването на емитерната верига (с интензивност λ_E) и прекъсване колекторната верига (с интензивност λ_K):

$$Q_O = P \cdot [1 - EXP (- \lambda_E .t)] \cdot [1 - EXP (- \lambda_K .t)] \cdot \left[1 - (1 - [1 - EXP (-\lambda_E .t)].[1 - EXP (- \lambda_K .t)])^{n-1} \right] \qquad /6/$$

Ако след изявяването на произволен пореден отказ, ЛЕ се възстановява с интензивност μ, за <u>пределната вероятност на неготовността</u> получаваме:

$$Q_O = P \cdot \frac{\lambda_E \cdot \lambda_K}{(\lambda_E + \mu).(\lambda_K + \mu)} \cdot \left[1 - \left[1 - \left[\frac{\lambda_E \cdot \lambda_K}{(\lambda_E + \mu).(\lambda_K + \mu)}\right]\right]^{n-1}\right] \qquad /7/$$

Ако приемем, че всички каскади са еднакви и вероятностите за появяване на логическа нула на всички входове на схемата равни (т.е. $p = 1 / n$), то, за пределната вероятност на неготовността получаваме :

$$Q_O = \frac{1}{n} \cdot \frac{\lambda_E \cdot \lambda_K}{(\lambda_E + \mu).(\lambda_K + \mu)} \cdot \left[1 - \left[1 - \left[\frac{\lambda_E \cdot \lambda_K}{(\lambda_E + \mu).(\lambda_K + \mu)}\right]\right]^{n-1}\right] \qquad /8/$$

Изследванията върху /8/ са представени таблично на фиг. 2.

Q_0	$\mu = 1$	$\mu = 2$	$\mu = 10$
n = 4	$8{,}24.10^{-21}$	$5{,}15.10^{-22}$	$8{,}25.10^{-25}$
n = 8	$9.62.10^{-21}$	$6{,}01.10^{-22}$	$9{,}62.10^{-25}$
n = 16	$1{,}03.10^{-20}$	$6{,}45.10^{-22}$	$1{,}03.10^{-24}$
n = 32	$1{,}07.10^{-20}$	$6{,}66.10^{-22}$	$1{,}06.10^{-24}$

Фиг. 2.

За най-често използвания в практиката случай, когато входния набор е един полубайт (n = 4) и време на възстановяване 1 час (μ = 1 [1/час]), вероятността за опасна работа при еднаква интензивност на отказите в емитерната и колекторната верига ($\lambda_E = 10^{-5}$ [1/час]) е равна на $8{,}24.10^{-21}$.

С увеличаване броя на логическите входове се увеличава вероятността за опасна работа.

С намаляване на времето T за възстановяване, т.е. увеличаване на μ ($\mu = 1 / T$) , вероятността за опасен отказ намалява.

При по-малки интензивности на отказ (λ е от порядъка на 10^{-7} 1/час) , вероятността за опасен отказ е по-малка.

ИЗВОДИ:

В тази работа е направена качествена и количествена оценка на безопасността на колекторно-базова логика.

Получени са формули за вероятността за опасен отказ и пределната вероятност на неготовността.

Получените функции са изследвани при различни стойности на параметрите, участващи в тях. Установено е, че безопасността на колекторно - базовата логика - логически елемент "И" е на няколко порядъка по-висока от допустимата.

ЛИТЕРАТУРА:

1. Христов, Х.А., Основи на осигурителната техника, София, Техника, 1990.

2. Лисенков, В.М., Показатели и методи обеспечения безопасности ответственых технологических процессов на транспорте, Втора научно-техническа сесия, ВВТУ, 1991.

3. Рябинин, И.А., Черкасов, Г.Н., Логико - вероятностные методы исследования надежности структурно сложных систем, М., Радио и связь, 1981.