Instrumente de testare

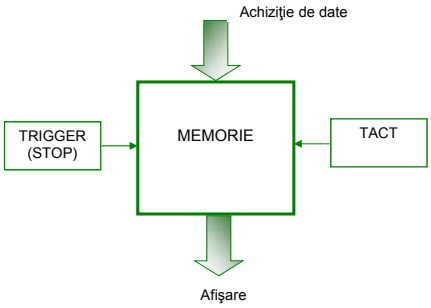
Instrumente de testare,adaptabile la testarea echipamentelor electronice industriale, sunt:

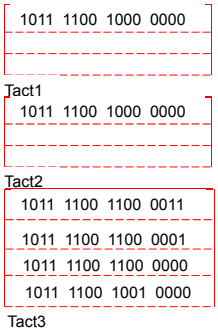
- Analizoarele logice
- Testarea convertoarelor de date
- Analizoarele de semnătură

Pe baza analizei datelor se poate caracteriza atât funcţia externă a maşinii testate cât şi cea internă – sub aspectul fluxului organizat al secvenţelor de date → starea regiştrilor, acumulatori, magistrale etc.

Analizoarele logice

Structura de bază a unui analizor logic constă dintr-un **sistem de achiziţie a datelor**, o memorie care funcţionează ca un registru de deplasare multiplu unde se înmagazinează datele prelevate din sistemul testat, care sunt afişate sub comanda unui tact şi în prezenţa unui semnal de declanşare.
Funcţionarea analizorului logic este controlată de către tactul sistemului care face ca la apariţia fiecărui semnal de tact, un eşantion din datele prezente la intrare să fie prelevat şi transferat în memorie.



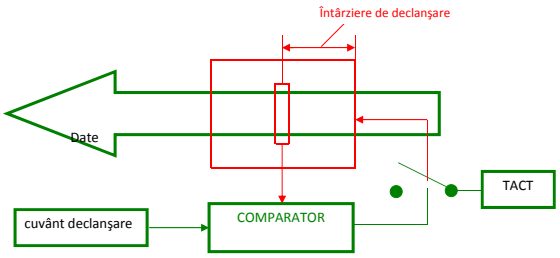


Analiza datelor – un set de tehnici de analiză ce privesc proiectarea, monitorizarea şi corecţia comportării unui sistem numeric (analiza de stări logice şi analiza de timp).

1

Funcţia de declanşare

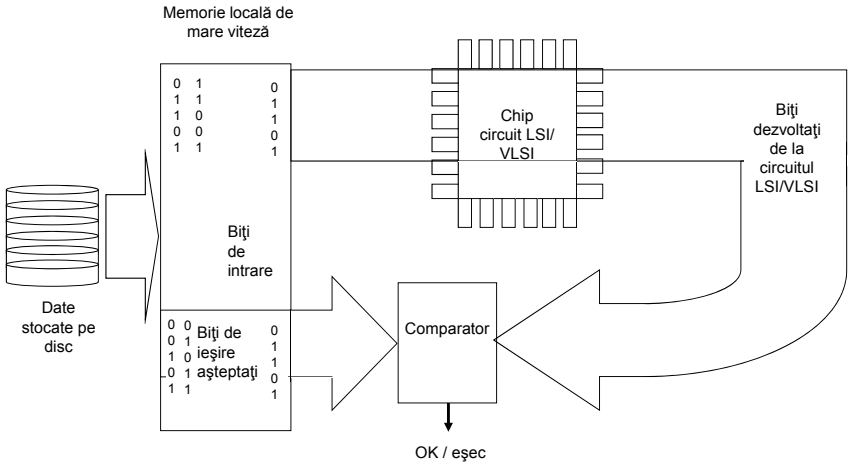
Analiza logică necesită o metodă de declanşare mai selectivă ca la alte instrumente (osciloscop) şi constă în compararea datelor stocate anterior cu un "cuvânt de declanşare, preselectat şi blocarea acestora în vederea analizei. Un circuit de comparare (vezi schema) va determina terminarea procesului de achiziţie şi la blocarea datelor prezente în memorie în acel moment.



Achiziţia datelor Se poate realiza prin intermediul unor sonde conectate la punctele de test.

Domeniile de aplicaţie ale analizoarelor logice se pot clasifica în funcţie de natura analizei efectuate: analiza de timp, analiza de stări logice şi analiza combinată.
Analiza de timp (asincronă) este asociată cu etapele de proiectare hardware, dezvoltare şi testare la nivel de modul funcţional.
Analiza de stări logice (sincronă) este utilizată în dezvoltarea şi testarea software, după implementarea dualităţii hardware/software.
Analiza combinată de timp şi stări logice este consacrată sistemelor de dezvoltare şi testare atât problemelor hardware cât şi software.

2



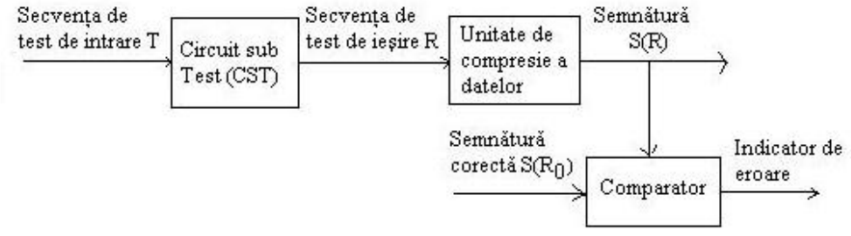
3

Principiul analizoarelor de semnătură

Principiul de testare pe baza analizei de semnătură se bazează pe ***comprimarea fluxului informaţional*** de lungime mare dintr-un nod sau de pe magistrala echipamentului, într-o formă concisă, uşor de interpretat şi care să semnifice dacă funcţionarea în nodul sau pe magistrala respectivă este corectă sau nu. Rezultatul comprimării poartă numele de **semnătură**, iar instrumentul care implementează această metodă poartă denumirea de **analizor de semnătură**.

Un analizor de semnătură face parte din clasa testoarelor cu control prin sumă. In funcţie de numărul de noduri din care se poate culege şi analiza fluxul informaţional, analizoarele de semnătură pot fi de tip ***serie*** sau ***paralel***. Primele analizoare de semnătură, de tip serial, au fost introduse de firma Hewlett-Packard în anul 1977.

Spre deosebire de analizoarele logice, dedicate în primul rând activităţilor de laborator, de proiectare şi de cercetare, analizoarele de semnătură au primordial rolul de a facilita procesul de testare în activitatea de producţie şi service. Prin simpla comparare a semnăturii culese din punctul de test cu semnătura corectă (determinată pe un etalon sau prin calcul), înscrisă în manualul de service, se poate verifica rapid funcţionarea circuitului sau echipamentului.



4

Metoda trebuie să poată fi implementată prin tehnici cât mai simple.

Tehnica utilizată nu trebuie să introducă întârzieri suplimentare în funcţionarea circuitului sau să afecteze major timpul de test.

Lungimea semnăturii trebuie să fie mult mai mică decât cea a răspunsului circuitului. Această performanţa este caracterizată de *gradul de compresie (GC)* definit ca raportul dintre lungimea secvenţei de ieşire şi lungimea semnăturii.

Metoda de compactare nu trebuie să piardă informaţia utilă din răspunsul circuitului, adică să nu mascheze manifestarea defectelor. Această performanţă este caracterizată prin *probabilitatea de mascare (P)* a erorilor.

- Răspunsul obţinut la ieşirea unui circuit constă într-o succesiune de valori binare 0 sau 1: $R=r_1,r_2,\ldots,r_m$. Metoda constă în numărarea valorilor binare 1 sau 0 din această secvenţă de ieşire. Dacă se numără valorile binare 1, atunci semnătura este dată de: $S(R)=\sum_i r_i$
- Lungimea semnăturii este variabilă, fiind determinată de numărul valorilor binare contorizate: $0 \le l_{S(R)} \le m$
- Tehnic metoda se implementează prin utilizarea unui numărător rezultând în felul acesta un grad de compresie: $GC = \log_2(m+1)$

5

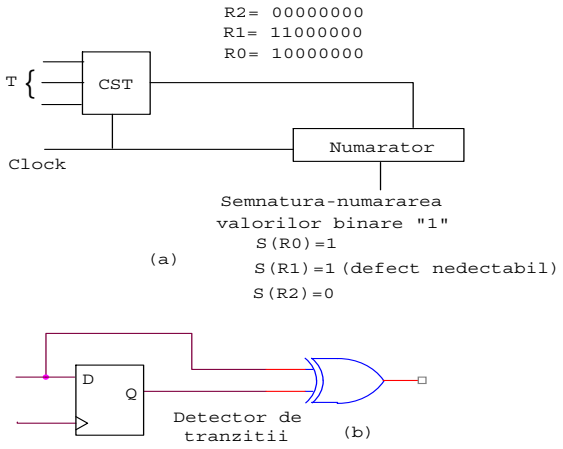
Metoda de compresie bazată pe numărarea tranziţiilor

- Prin această metodă se numără, se contorizează, tranziţiile care apar dintr-o stare logică în alta, din 0 în 1 şi din 1 în 0. Semnătura asociată răspunsului $R=r_1,r_2,\ldots,r_m$ este:

$$S(R) = \sum_{i=1}^{m-1} (r_i \oplus r_{i+1})$$

- Lungimea semnăturii obţinute este şi de această dată variabilă: $0 \le l_{S(R)} \le m-1$
- Tehnic metoda se implementează prin utilizarea unui detector de tranziţii urmat de un numărător care asigură gradul de compresie: $GC = \log_2 m$

6



- Considerăm că lungimea secvenţei de test T este *m* şi în răspunsul corect asociat acestei secvenţe apar *r* tranziţii, deci $S(R_0)=r$.
- Dacă considerăm o secvenţă de ieşire arbitrară de aceeaşi lungime *m*, atunci exista $2C_{m-1}^{r}-1$ combinaţii posibile care au acelaşi nr de tranziţii *r*.
- Luând în considerare toate combinaţiile posibile pentru secvenţa de lungime *m* rezultă următoarea probabilitate de mascare a erorilor pentru o secvenţă de lungime *m* cu *r* tranziţii:

$$P(M\,|\,m,r)=\frac{2C_{m-1}^{r}-1}{2^{m}-1}$$

În situaţia în care defectul din circuitul testat modifică un singur bit în secvenţa de ieşire, atunci probabilitatea de mascare a erorii devine:

$$P(M\,|\,m,r)=\frac{m-2}{2m}$$

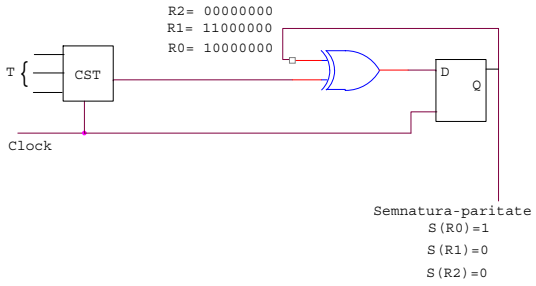
– Este importantă ordinea în care apar unităţile binare în şirul secvenţei.

Metoda de compresie bazată pe determinarea parităţii

- Circuitul de compresie prin care se implementează metoda realizează o funcţie dată de polinomul caracteristic:

$$p(x) = x + 1$$

- În polinomul anterior sumarea se realizează modulo 2.
- Pentru determinarea parităţii se introduce o reacţie. Dacă iniţial starea bistabilului este Q=0, atunci semnătura este dată de paritatea răspunsului, adică S(R)=0 pentru paritate pară şi S(R)=1 pentru paritate impară.
- Se remarcă faptul că prin această metodă lungimea semnăturii obţinute este fixă, fiind de un singur bit.

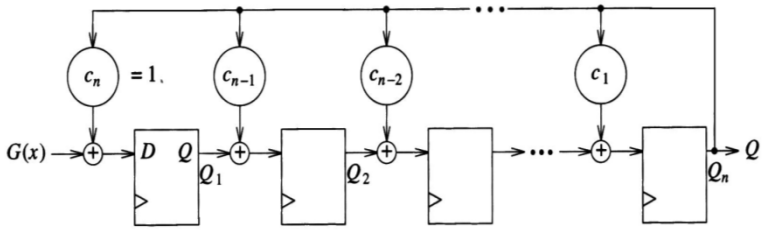


Circuit pentru determinarea parităţii

- Proprietăţi:
  - Metoda detectează toate erorile ce afectează un număr impar de biţi.
  - Defectele ce afectează un număr par de biţi nu sunt detectabile.
  - Pornind de la observaţiile anterioare rezultă că pentru $m \to \infty$ probabilitatea de mascare a erorilor tinde la valoarea 0,5.
  - Metoda poate fi uşor extinsă la circuite care au mai multe ieşiri. Ea poate fi implementată în mai multe moduri pentru această situaţie.
  - Metoda care presupune utilizarea unui număr mare de circuite, implementează câte un detector de paritate pentru fiecare ieşire, semnătura fiind un cuvânt reprezentat pe un număr de biţi egal cu numărul ieşirilor investigate.

Metoda de compresie bazată pe analiza de semnătură

- La baza metodei stă conceptul de verificare a redundanţei ciclice (*cyclic redundancy checking*, CRC).
- Circuitul de compresie constă de această dată într-un registru de deplasare liniar cu reacţie, LFSR, având o singură intrare.
- Semnătura este reprezentată de conţinutul acestui registru după momentul recepţionării ultimului bit din şirul de biţi ai secvenţei analizate.



- Metoda se bazează pe conceptul divizării polinoamelor.
- Circuitul efectuează o operaţie de împărţire între polinomul *G(x)* ce caracterizează secvenţa de intrare şi polinomul reciproc al polinomului caracteristic al registrului, $P^*(x)$.
- La ieşirea circuitului se obţine polinomul cât, *Q(x)*.
- Gradul cel mai mare al polinomului *G(x)* corespunde primului bit ce intră în registru iar gradul cel mai mare pentru *Q(x)* corespunde primului bit ce iese din registru după aplicarea a *n* impulsuri de ceas, unde *n* reprezintă numărul de celule din registru.
- Dacă în starea iniţială a registrului toate celulele sunt 0, atunci în starea finală registrul va conţine restul *R(x)* al împărţirii polinoamelor specificate. Deci, polinoamele respectă relaţia:

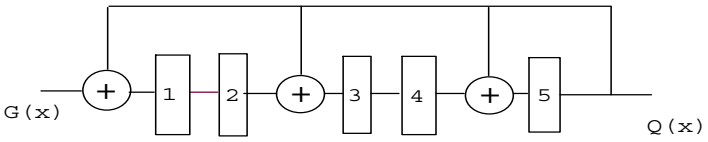
$$\frac{G(x)}{P^*(x)} = Q(x) + \frac{R(x)}{P^*(x)}$$

- Se utilizează polinomul reciproc $P^*(x)$ deoarece coeficientul a_m corespunde primului bit din şirul datelor de intrare.

Metoda de compresie bazată pe analiza de semnătură - ilustrare

Structură de analizor de semnatură cu 5 celule.
Acestui registru LFSR îi corespunde urmatorul polinom caracteristic reciproc:

$$P^*(x) = 1 + x^2 + x^4 + x^5$$



Presupunem că la intrarea registrului se aplică secvenţa: 11110101, acesteia corespunzându-i polinomul:

$$G(x) = x^7 + x^6 + x^5 + x^4 + x^2 + 1$$

Evoluţia în timp a conţinutului analizatorului de semnătură

Timp	Secvenţa de intrare	Conţinutul registrului	Secvenţa de ieşire
		1 2 3 4 5	
0	1 0 1 0 1 1 1 1	0 0 0 0 0 ← Starea iniţială	
1	1 0 1 0 1 1 1	1 0 0 0 0	
⋮	⋮	⋮	
5	1 0 1	0 1 1 1 1	
6	1 0	0 0 0 1 0	1
7	1	0 0 0 0 1	0 1
8	Restul →	0 0 1 0 1	1 0 1
		Restul	Câtul
		$R(x) = x^2 + x^4$	$1 + x^2$

Unitatea testată (UT) poate fi stimulată de condiţiile nominale de funcţionare în ansamblul din care face parte, permiţându-se verificarea sa funcţională **on-line**. De pe unitatea testată se culege fluxul informaţional de pe liniile importante pentru funcţionarea ecesteia.
Culegerea acestui flux, care constituie pentru analizorul de semnătură **datele de intrare**, se face prin intermediul ***blocului sondelor de date (BSD)***. Acest bloc trebuie să poată identifica nivelul logic al datelor preluate, fără a încărca însă suplimentar magistralele de pe care culege date şi fără a afecta în vreun fel fluxul recepţionat.

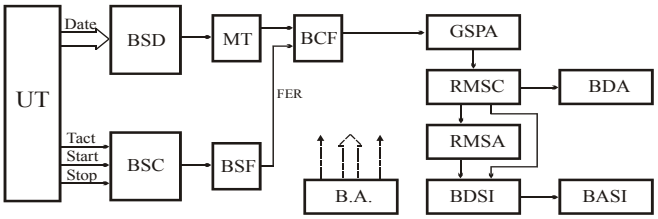


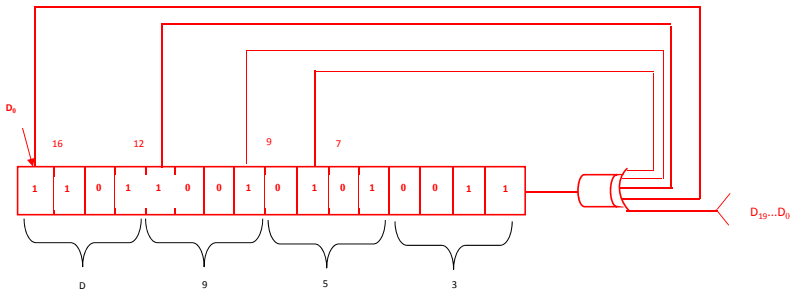
Fig. 4. Principiul analizorului de semnnătură

Culegerea fluxului de informaţie de pe magistralele unităţii testate se face sub controlul semnalelor *"Start"*, *"Stop"* şi *"Tact"*. Deoarece culegerea informaţiilor se face on-line, este necesar ca aceste semnale de control să aibă o strânsă legătură cu funcţionarea unităţii testate. Din acest motiv, ele sunt preluate tot de pe ***UT*** prin intermediul ***blocului sondelor de control (BSC***. Pentru a avea controlul asupra informaţiilor captate, tehnica analizei de semnături se utilizează în general în conjuncţie cu ***programe de test*** (sau autotest) rulate pe structura ***UT*** atunci când acesta se află în stare de aşteptare din punct de vedere al aplicaţiei rulate curent..

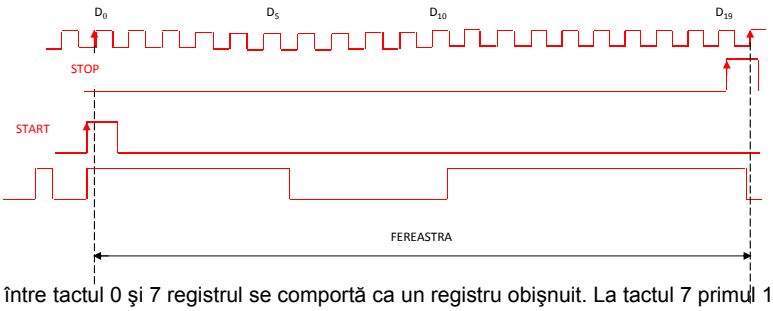
15

Blocul de formare a semnăturii (BFS) este alcătuit dintr-o schemă secvenţială liniară de codificare în cod ciclic.

O problemă în implementarea SSL costă în alegerea reacţiilor – tipul de polinom generator al codului



16



Iniţial, între tactul 0 şi 7 registrul se comportă ca un registru obişnuit. La tactul 7 primul 1 din secvenţa de intrare ajunge pe prima cale de reacţie şi împreună cu data de intrare 0 rezultă 1 care este transferat registrului la tactul 8 etc. Funcţionarea continuă până la închiderea ferestrei, tactul 20, când în registru rămâne un rest, $D953_H$

Semnătura va fi stabilă cât timp fereastra de măsurare, datele prelevate vor fi repetabile.

Analiza de semnătură este aplicabilă porţiunilor de circuit care operează în mod sincron cu tactul semnalului testat (memoria, procesorul, circuite periferice etc.). Circuitul de tip asincron (monostabile, sistemul de întreruperi, DMA) pentru a fi testate trebuie forţate într-o condiţie de funcţionare sincronă sau dezactivate

17

Pentru controlul fin al duratei de culegere a datelor, există prevăzută posibilitatea de selectare a fronturilor active pentru cele trei semnale de comandă: ***"Start"***, ***"Stop"*** şi ***"Tact"***, prin intermediul ***blocului selecţie fronturi (BSF)***. Acest bloc va genera un semnal numit ***fereastră (FER)***, care permite accesul datelor de la ***UT*** pe perioada în care este activ. Se mai utilizează în literatura de specialitate şi terminologia de ***"fereastră deschisă"*** pe durata culegerii datelor, respectiv de ***"fereastră închisă"*** atunci când dateele nu mai sunt preluate de către analizor.
După o posibilă memorare temporară în ***memoria tampon (MT)*** informaţia culeasă de pe magistralele ***UT*** este transmisă prin intermediul ***blocului control fereastră (BCF)*** către partea centrală de prelucrare a informaţiei din cadrul analizorului.

18