CAPITOLUL 4

ECHIPAMENTE TOLERANTE LA DEFECTĂRI

4.1. Introducere

Dezvoltarea tehnologică din ultimele decenii a condus la apariţia unor domenii de activitate ce necesită echipamente care să nu se defecteze pe durata misiunii (centrale nucleare, sateliţi de telecomunicaţii, transport aerian şi cosmic etc). În unele cazuri, starea de defectare poate avea consecinţe catastrofale, iar în altele, odată cu prima defectare, se termină şi durata de viaţă a echipamentului, datorită faptului că intervenţia operatorului uman nu este posibilă (ex. sateliţii de telecomunicaţii, sondele spaţiale etc). Rezolvarea problemei defectărilor în aceste cazuri a condus la elaborarea unor structuri de echipamente tolerante la defectări. Un echipament tolerant la defectări este acel echipament care îşi poate continua execuţia corectă a funcţiilor sale de *intrare / ieşire*, fără o intervenţie din exterior, în prezenţa unei anumite mulţimi de defectări ce apar în timpul funcţionării sale.

Prin execuţie corectă se înţelege că rezultatele obţinute (mărimile de ieşire) nu sunt afectate de erori, iar timpul de execuţie nu depăşeşte o limită precizată.

O *defectare* ce apare în timpul funcţionării operaţionale a unui echipament este o schimbare în valoarea uneia sau a mai multor variabile de ieşire sau de stare ce caracterizează echipamentul, defectarea fiind consecinţa imediată a evenimentului “defect”. Evenimentul fizic “defect” poate fi o imperfecţiune fizică a unui element al echipamentului, care conduce la o funcţionare permanent, temporar sau intermitent eronată sau poate fi un factor extern (variaţii necontrolabile ale parametrilor mediului ambiant: temperatură, umiditate, vibraţii, şocuri etc; perturbaţii prin câmp electric sau electromagnetic etc.) care pot conduce la nefuncţionarea echipamentului. Defectările se clasifică după durată în *permanente* sau *temporare*, iar după extindere pot fi *singulare* sau *multiple*.

Defectările permanente sunt cauzate de defectele permanente ale componentelor echipamentului. Protecţia împotriva acestor defectări se poate face fie prin utilizarea de componente de rezervă care vor fi puse în funcţiune în locul celor defecte, fie prin măsuri de reconfigurare în urma cărora componenta defectă este izolată, iar funcţiile ei sunt preluate de altă componentă aflată în rezervă.

Defectele temporare sunt de durată limitată, fiind cauzate de nefuncţionări temporare ale componentelor sau de interferenţe externe, echipamentul revenind la parametrii normali de funcţionare fără o intervenţie externă.

Defectările pseudo-temporare sunt defectări determinate de defectele permanente ale componentelor echipamentului, pentru a căror manifestare este necesară o anumită combinaţie a valorilor semnalelor de intrare.

Defectările singulare (locale) afectează o singură variabilă corespunzătoare unui semnal de ieşire sau unei stări interne, în timp ce *defectările multiple* (distribuite) afectează mai multe variabile de ieşire sau de stare ale echipamentului.

Eroarea este un simptom al unui defect, fiind cauzată de prezenţa unei defectări. Se consideră că în momentul utilizării unui echipament au fost deja eliminate erorile de proiectare şi de fabricaţie. Eliminarea acestor erori/defecte se realizează în timpul testelor de laborator efectuate în vederea omologării echipamentului respectiv.

O interpretare mai generală dată toleranţei la defectări presupune ca aceasta să includă şi totalitatea erorilor de proiectare, nedetectate înainte de utilizarea operaţională a echipamentului. Prin tolerarea defectelor nu se înţelege o amânare a defectării echipamentului, ci posibilitatea localizării automate a elementelor defecte şi a dezactivării elementului afectat de erori, echipamentul continuând să funcţioneze corect pe baza elementelor redundante.

Defectările de proiectare sunt de regulă consecinţa unor specificaţii de proiectare incomplete sau incorecte şi se pot manifesta atât pe partea de *hardware* cât şi pe partea de *software* a unui echipament. Toleranţa la defectări este un aspect esenţial al realizării echipamentelor fiabile şi, în sensul cel mai general, înseamnă execuţia corectă a unui set de operaţii specificate în prezenţa unui anumit număr de defecte.

Pentru ca echipamentul să fie considerat tolerant la defectări este necesar ca dezactivarea elementului defect să se execute automat de către echipamentul în cauză.

Atunci când se utilizează forme ale redundanței de tip static pentru a implementa toleranța la defectări a unui echipament, se spune că echipamentul are o *toleranță statică la defectări,* iar când se utilizează procedee de detecție a defectărilor elementelor echipamentului urmate de înlocuirea modulului defect cu unul de rezervă, sau se realizează reconfigurarea automată a acestuia, echipamentul va fi cu *toleranță dinamică la defectări.*

Pentru implementarea toleranței la defectări a echipamentelor se pot utiliza următoarele trei tipuri de strategii:

- strategii bazate pe diagnosticarea defectărilor şi înlocuirea elementelor defecte;
- strategii bazate pe mascarea defectărilor;
- strategii hibride bazate pe mascarea defectărilor, diagnosticarea şi înlocuirea elementelor defecte.

În toate strategiile intervine "redundanța": fie la nivel *hardware* sau *software,* fie o redundanță a funcțiilor echipamentului. Metodologia de implementare a toleranței la defectări implică parcurgerea următoarelor etape:

- specificarea cerințelor de fiabilitate pentru echipament;
- selectarea metodelor de diagnosticare a defectărilor şi a algoritmilor de mascare a defectărilor sau de reconfigurare a echipamentului;
- evaluarea toleranței la defectări;
- calculul performanțelor de fiabilitate;
- determinarea avantajelor obținute din punct de vedere economic.

4.2. Algoritmi de detecție şi diagnosticare a defectărilor

Detecția şi diagnosticarea defectărilor constituie punctul de pornire a oricărei implementări a toleranței la defectări, atunci când aceasta este realizată prin reconfigurarea echipamentului. Algoritmul de diagnosticare a defectărilor conține de regulă şi toate acțiunile de localizare a acestora.

Într-un algoritm de diagnosticare a defectărilor se disting mai multe abordări [2]:

- Testarea inițială, care are loc înaintea utilizării normale a echipamentului. În această etapă se pot identifica erorile de proiectare sau de fabricație, elementele defecte (*hardware* şi *software*).
- Testarea ”*on-line*” ce are loc simultan cu funcționarea normală a echipamentului. Aceasta se poate realiza fie cu mijloace *hardware* fie cu mijloace *software*. Se pot utiliza circuite autotestabile, coduri detectoare de erori, module redundante etc. Această testare are avantajul că detecția sau diagnosticarea defectării se poate face înainte de a se produce pierderi importante în echipament.

- Testarea echipamentelor în vederea detecției sau diagnosticării defectărilor atunci când operarea normală este întreruptă. Această metodă de testare se realizează prin programe speciale de test sau prin execuții repetate ale aceleiaşi secvențe, pentru a se compara rezultatele obținute. Această testare se desfăşoară în timpul operațiilor de mentenanță preventivă, sau când s-a constatat defectarea echipamentului.

- Testarea modulelor redundante constă în verificarea dacă modulele de rezervă sunt în bună stare de funcționare. Se pot utiliza metode *on-line* (pentru echipamentele autotestabile) sau metode *off-line* ce utilizează programe de diagnoză, în funcție de tipul redundanței folosite.

4.2.1. Algoritmi de reconfigurare a echipamentelor

Implementarea toleranței la defectări a echipamentelor utilizând tehnici de reconfigurare presupune în primul rând diagnosticarea defectelor. Toate acțiunile întreprinse din momentul diagnosticării defectului şi până la repunerea în funcțiune, la parametri nominali, constituie algoritmul reconfigurării echipamentului [2].

Metodele de reconfigurare se pot clasifica în funcție de starea echipamentului după reconfigurare astfel:

- Metode ce realizează o *reconfigurare totală* a echipamentului, atunci când echipamentul este adus în starea anterioară defectării prin înlocuirea elementelor defecte.

- Metode ce realizează o *reconfigurare parțială,* adică aduc echipamentul într-o stare de funcționare, dar cu o restrângere a

funcţiilor sale anterioare. Aceasta se realizează prin înlăturarea elementului defectat şi prin preluarea funcţiilor sale de către alte elemente din structura echipamentului.

- Metode de *deconectare automată* a echipamentului. Acestea au drept scop evitarea unor pierderi sau avarii mai mari decât cele produse prin defectarea elementelor în cauză.

Algoritmii de reconfigurare a echipamentelor pot fi implementaţi atât la nivel hardware cât şi la nivel software

4.2.2. Algoritmi de mascare a defectărilor

Aceşti algoritmi se implementează utilizând structuri redundante statice (logică majoritară, logică cuadruplă, logică cablată etc). În cazul acestor algoritmi defectările componentelor nu sunt prezente la ieşirea echipamentului, decât numai atunci când ele afectează în totalitate, sau în majoritate elementele de rezervă.

Elementele de rezervă sunt conectate permanent, astfel încât mascarea defectărilor se realizează instantaneu. Folosirea tehnicilor de mascare a defectărilor se bazează pe presupunerea că defectările modulelor de rezervă sunt evenimente independente.

4.3. Structuri redundante pentru implementarea toleranţei la defectări

Teoria redundanţei foloseşte câteva "teoreme-limită" care ghidează proiectarea echipamentelor cu structură redundantă [2].

- *Redundanţa* este o metodă comodă de creştere a fiabilităţii echipamentelor dacă defectările elementelor din componenţa echipamentului sunt evenimente independente.

- *Probabilitatea de defectare* a unui echipament cu structură redundantă, scade exponenţial cu creşterea costului alocat echipamentului.

Implementarea redundanţei se poate face prin *tehnici de tip static*, numite şi tehnici de "*mascare*" a defectărilor şi prin *tehnici de tip dinamic* sau *de comutaţie.*

Realizarea echipamentele tolerante la defectări utilizând tehnicile de *tip static* prezintă următoarele avantaje:

- corecția defectării se face instantaneu;
- nu este necesară diagnosticarea defectărilor;
- trecerea pe la proiectarea unui echipament fără redundanțe la proiectarea unui echipament cu redundanțe este relativ simplă.

Redundanța de *tip dinamic* implică existența în componența echipamentului a mai multor module identice, din care doar o parte sunt operaționale, celelalte fiind în aşteptare pentru a fi comutate în momentul diagnosticării unui defect. Acest tip de redundanță este utilizat pentru a realiza echipamente autoreparabile, când comutarea rezervelor se face în mod automat, sau în realizarea echipamentelor reconfigurabile.

Redundanța de tip dinamic presupune îndeplinirea condițiilor următoare (uneori considerate dezavantaje):

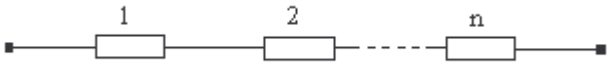
- echipamentul trebuie să tolereze întreruperile şi să poată executa o reluare a operațiilor pentru a corecta erorile;
- se presupune existența unui comutator sigur care să conecteze rezervele sau să execute reconfigurarea în caz de defectare a unui element;
- diagnoza se desfăşoară în timpul funcționării normale a echipamentului, ceea ce presupune utilizarea unor metode şi tehnici de diagnosticare mai complicate.

Avantajele utilizării redundanței de tip dinamic sunt următoarele:

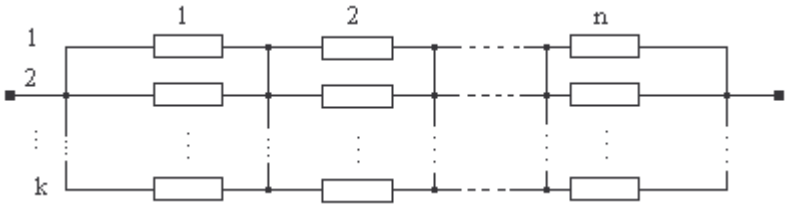
- se alimentează electric numai o rezervă a echipamentului;
- comutatorul realizează o izolare a defectului;
- numărul de rezerve poate fi ajustat fără a fi nevoie de modificarea proiectării echipamentului;
- nu apar probleme de cuplare *intrare / ieşire* a modulelor redundante.

Implementarea redundanței, în scopul alegerii schemei convenabile, presupune precizarea aprioric a nivelului la care aceasta trebuie aplicată: componentă, modul funcțional sau la nivelul întregului echipament.

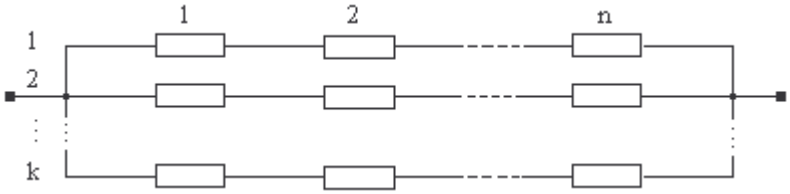
În continuare sunt prezentate exemple de structuri redundante statice de tip individual şi global rezultate prin multiplicare (figura 4.1):



a). Echipament cu structură neredundantă



b). Echipament cu redundanţă la nivel individual



c). Echipament cu redundanţă la nivel global

Fig. 4.1. Structuri redundante statice realizate prin multiplicare

Modul de conectare fizică a elementelor de rezervă poate să coincidă sau nu cu modelul logic de fiabilitate. Un exemplu de aplicare a redundanței la nivel global este prezentat în figura 4.2.

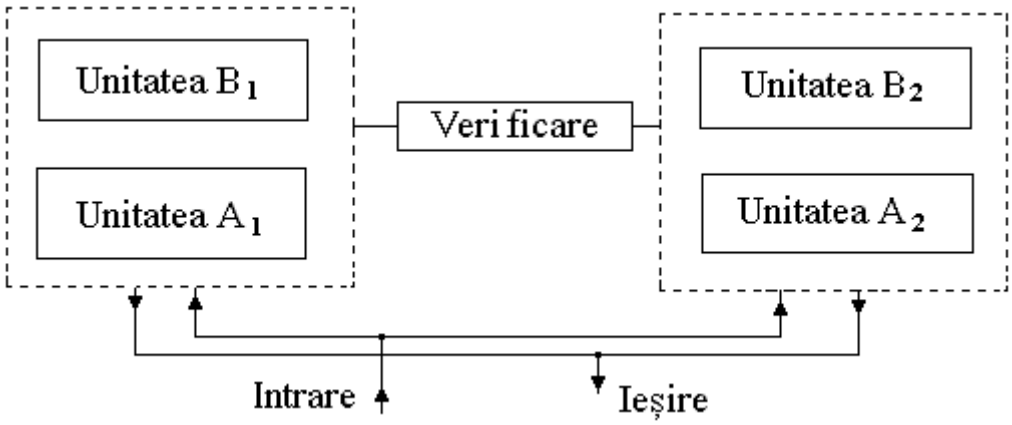


Fig. 4.2. Echipament cu redundanţă la nivel global

Echipamentul inițial format din unitățile *A, B,* a fost dublat, ambele echipamente lucrând *on-line* şi executând sarcini identice pentru a putea compara ieşirile. Echipamentul va fi în bună stare de funcționare chiar dacă unul dintre module se va defecta, identificarea şi izolarea elementului defect urmând a fi făcută de un modul suplimentar de verificare a funcționării corecte.

Dacă se consideră ipotezele următoare:

- modulele funcționale sunt nereparabile;
- circuitele care asigură conectarea modulelor sunt perfecte;
- defectările elementelor funcționale sunt independente şi staționare,

atunci se pot scrie în continuare expresiile funcțiilor de fiabilitate pentru structurile redundante de tip individual şi global (figura 4.1). Pentru prima structură avem:

$$R_{SI}(t) = \prod_{i=1}^{n} \left[1 - (1 - R_i(t))^{k_i}\right] \tag{4.1}$$

iar pentru structura redundantă la nivel global:

$$R_{SG}(t) = 1 - \left(1 - \prod_{i=1}^{n} R_i(t)\right)^{K} \tag{4.2}$$

unde $R_i(t)$ este funcția de fiabilitate a elementului *i*, iar k_i *- 1*, numărul de rezerve utilizate pentru elementul *i*.

Pentru acelaşi număr de rezerve, funcția de fiabilitate a structurii redundante individuale are o valoare mai mare decât funcția de fiabilitate a structurii redundante globale, ceea ce rezultă uşor din analiza calitativă a celor două structuri. În cazul structurii redundante la nivel global, defectarea unui element oarecare scoate din funcțiune şi celelalte *n-1* elemente aflate în serie cu el, ceea ce nu se constată la structura redundantă individuală, şansele de bună funcționare fiind mai mari pentru structura redundantă de tip individual.

Aplicarea redundanței individuale sau globale se poate face relativ simplu în cazul echipamentelor de tip analogic.

În cazul echipamentelor digitale aplicarea de redundanțe trebuie făcută luând măsuri speciale, în caz contrar putându-se observa o înrăutățire a performanțelor de fiabilitate.

Exemplu: Se consideră un circuit basculant monostabil (CBM) căruia i se aplică redundanța prin multiplicare, obținând schema din figura 4.3.

Dacă unul dintre circuite se defectează astfel încât nu va da impuls de ieşire, schema funcționează în continuare în mod normal, iar dacă circuitul defect va genera impulsuri cu durată incorectă (mai mare decât constanta de timp a CBM) sau va funcționa ca astabil, funcționarea echipamentului

va fi eronată. Rezultă de aici că este necesar să se cunoască toate modurile posibile de defectare ale echipamentului şi să se ia măsuri speciale de protecţie, specifice fiecărui caz în parte.

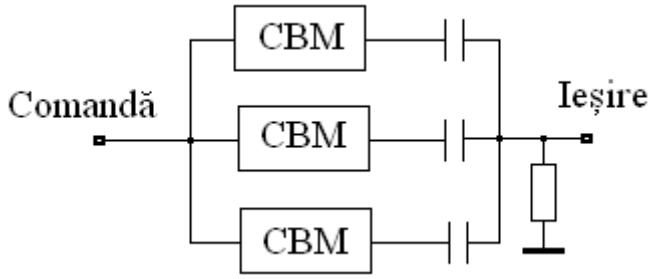


Fig. 4.3. Circuit basculant monostabil cu structură redundantă statică

Trebuie precizat faptul că dublarea componentelor unui echipament nu conduce întotdeauna la o creştere a fiabilităţii acestuia. Se poate exemplifica acest lucru cu ajutorul echipamentelor autotestabile realizate prin dublare (figura 4.4).

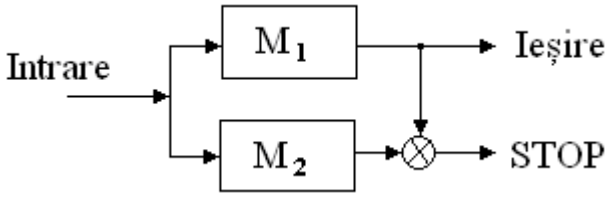


Fig.4.4. Echipament cu structură autotestabilă

Comparatorul evidenţiază defectarea unuia din cele două module identice prin formarea semnalului de STOP. Prezenţa unui defect în echipament este sesizată numai dacă cele două module nu sunt afectate simultan de aceleaşi erori (defecte).

4.3.1. Structuri redundante statice de tip individual şi global rezultate prin multiplicare

Pentru realizarea unei structuri tolerante la defectări, pornind de la echipamentul autotestabil din figura 4.4 se poate utiliza structura din figura 4.5. Defectarea unui modul *M* nu va mai produce apariţia semnalului de "*STOP*", informaţia eronată fiind blocată spre ieşire de una din porţile G_1. Semnalul de ieşire va fi dat doar de grupul de module aflate în bună stare de funcţionare.