Sisteme de calcul tolerante la defectări

Prof.dr.ing. Aurel ŞERB
Academia Tehnică Militară, Bucureşti

Sistemele de calcul tolerante la defectări au capacitatea de a continua să-şi execute corect funcţiile lor de ieşire, fără o intervenţie din exterior, în prezenţa unei anumite mulţimi de defectări ce apar în timpul funcţionării lor. Tehnicile de bază utilizate pentru implementarea toleranţei la defectări folosesc fie codarea funcţiilor logice ale sistemului cu coduri redundante, fie recunoaşterea erorilor şi eliminarea acestora prin mascarea defectelor cu ajutorul elementelor multiple din sistem, sau reconfigurarea funcţională a sistemului prin activarea unui element de rezervă, care să înlocuiască elementul defectat. Sistemele tolerante la defectări prezintă o partiţionare funcţională ierarhică, la diferite niveluri ierarhice existând componente redundante şi mecanisme de restabilire. Restabilirea funcţională a sistemului se realizează prin mecanisme specifice atât nivelului ierarhic propriu, cât şi ale unui nivel ierarhic superior.
***Cuvinte cheie**:sisteme de calcul tolerante la defectări, detecţia şi corecţia erorilor, sisteme autotestabile, redundanţa, partiţionarea ierarhică a sistemelor, toleranţa ierarhică şi toleranţa de tip grup, restabilirea funcţională după defectare.*

1. Caracterizare generală

Domeniul actual al sistemelor de calcul tolerante la defectări este unul cu o arie de întindere destul de vastă, incluzând atât aspectele hardware cât şi pe cele software, atât prelucrările locale cât şi cele distribuite.
Sistemele de calcul tolerante la defectări au capa-citatea de a continua să-şi execute corect funcţiile lor de ieşire, fără o intervenţie din exterior, în prezenţa unei anumite mulţimi de defectări ce apar în timpul funcţionării lor. Prin *execuţie corectă* se înţelege faptul că rezultatele obţinute, ca efect al operaţiilor din sistem, nu conţin erori, iar timpul de execuţie a unei operaţii nu depăşeşte o limită specificată.
Obiectivul calculului tolerant la defectări este de a dezvolta şi certifica sisteme de calcul care funcţionează într-o manieră satisfăcătoare în prezenţa defectelor.
Domeniul calculului tolerant la defectări cuprinde teoria şi tehnicile de detecţie şi corecţie a erorilor, modelarea, analiza, sinteza şi arhitectura sistemelor de calcul tolerante la defectări, precum şi tehnicile de evaluare a acestor sisteme.
Tehnicile de bază utilizate pentru implementarea toleranţei la defectări folosesc fie codarea funcţiilor logice ale sistemului cu coduri redundante, fie recunoaşterea erorilor şi eliminarea acestora prin mascarea defectelor cu ajutorul elementelor multiple din sistem, sau reconfigurarea funcţională a sistemului prin activarea unui element de rezervă, care să înlocuiască elementul defectat. Sistemele tolerante la defectări prezintă o partiţionare funcţională ierarhică, la diferite niveluri ierarhice existând componente redundante şi mecanisme de restabilire care pot fi folosite pe diferite căi. Restabilirea funcţională a sistemului se realizează prin mecanisme specifice atât nivelului ierarhic propriu, cât şi ale unui nivel ierarhic superior.

2. Necesitatea toleranţei la defectări

Realizările de până acum au arătat că toleranţa la defectări este o necesitate în câteva domenii, precum ar fi:
Aplicaţii de calcul critice. Cerinţele de toleranţă la defectări cele mai stringente se pun pentru sistemele de control în timp real, la care calculele cu defecte pot primejdui viaţa omului, sau să distrugă echipamente scumpe. Astfel de aplicaţii în timp real cer nu numai ca să fie corecte calculele, dar şi ca orice întârziere asociată cu restabilirea după defectare să fie foarte mică.
Aplicaţii de timp de viaţă îndelungat. Sistemele de timp de viaţă îndelungat sunt acelea pentru care nu se face niciodată mentenanţă. Rachetele fără echipaj sunt exem-

plele cele mai dramatice. Sistemele de calcul pentru aceste aplicaţii au o redundanţă înaltă, furnizând suficientă rezervă hardware pentru a menţine performanţa nominală până la sfârşitul misiunii.

Aplicaţii care cer disponibilitate superioară. În sistemele mari, cu resurse partajate, pierderea ocazională a rezultatelor calculelor unui utilizator este acceptabilă, dar este inacceptabilă o cădere totală a sistemului sau distrugerea unei baze de date comune. Exemple de acest fel sunt calculatoarele de comutaţie telefonică şi unele servicii comerciale partajate în timp, sau sistemele utilizate în unele prelucrări numerice de semnal.

Amânarea mentenanţei. Într-un număr de aplicaţii costul de ciclu de viaţă a mentenanţei neplanificate poate să fie mai mare decât costul toleranţei la defectări.

Ultimele realizări şi studii privind perspectivele în domeniul structurilor şi arhitecturilor sistemelor de calcul, al sistemelor în general, indică faptul că toleranţa la defectări devine un atribut al tot mai multor calculatoare de uz general, încetând să mai fie un apanaj doar al unor domenii particulare.

3. Detecţia şi localizarea defectelor

Punctul de pornire al strategiilor de tolerare a defectărilor îl constitue detecţia şi localizarea "stării" eronate a sistemului, "stare" care, în absenţa oricăror măsuri de protecţie, va conduce la defectarea sistemului. Mai mult decât atât, succesul oricăreia dintre aceste strategii este dependent, în mod critic, de eficacitatea acestei detecţii. Odată detectată şi localizată o eroare este necesară utilizarea unor tehnici şi metode de tolerare a defectelor, care să permită restabilirea funcţională a sistemului defectat.

Din punctul de vedere al testabilităţii, sistemele tolerante la defectări se pot clasifica în două tipuri de bază. O categorie o reprezintă sistemele care pot detecta defectele interne concurent cu operarea normală, ceea ce se numeşte "sisteme cu autoverificare (autotestabile)" iar cealaltă categorie este cea a sistemelor care nu au capabilităţi interne de detecţie a defectelor şi care vor fi numite "sisteme fără autoverificare". Când sunt utilizate într-o partiţie redundantă, modulele cu autoverificare pot opera singure, deoarece defectele vor fi detectate prin mijloace proprii modulului, iar un mecanism extern de restabilire poate înlocui un modul care s-a defectat cu un modul de rezervă. Modulele fără autoverificare trebuie să fie duplicate şi să opereze câte două la un moment dat, cu ieşirile comparate pentru detecţia defectelor, sau trei la un moment dat, cu votare.

4. Redundanţa şi partiţionarea ierarhică a sistemelor

Metodele de bază folosite pentru realizarea sistemelor tolerante la defectări au ca element fundamental "redundanţa"- definită ca fiind utilizarea în cadrul sistemului a mai multor elemente decât sunt necesare pentru îndeplinirea funcţiilor acestuia, astfel încât sistemul să funcţioneze corect chiar şi în prezenţa unor defecte. Elementele suplimentare pot fi atât hardware cât şi software şi se pot aplica de la nivelul unor componente individuale, până la nivelul întregului sistem.

În mod natural, sistemele complexe sunt partiţionate pe câteva niveluri, partiţionare bazată pe funcţiile furnizate de subsistemul specific. Un sistem tolerant la defectări prezintă o partiţionare funcţională similară, dar în plus conţine componente redun-dante şi mecanisme de restabilire care pot fi folosite pe căi diferite, la niveluri ierarhice diferite. Este rezonabil de văzut un sistem tolerant la defectări ca un set ierarhic de subsisteme, fiecare dintre ele putând avea niveluri diferite de toleranţă la defectări.

O partiţie redundantă este un set de module care conţin suficientă redundanţă, astfel încât dacă unul dintre module se defectează, cu cele rămase să poată fi obţinută o performanţă acceptabilă. Partiţia redundantă poate conţine module de rezervă pentru a le înlocui pe cele care se defectează, sau, atunci când unul dintre module se defectează, modulele funcţionale pot să-şi redistribuie funcţiile şi să opereze într-o manieră cu performanţă degradată. Res-

tabilirea după un defect de la nivelul unei partiții redundante poate fi efectuată la nivelul domeniului însuși, sau se poate cere intervenția unui nivel ierarhic superior al sistemului. O partiție redundantă poate fi făcută din module diferite, iar un modul dintr-o partiție redundantă adesea va conține alte partiții redundante încorporate.

5. Tehnici de tolerare a defectelor și de restabilire funcțională utilizate în sistemele tolerante la defectări

În continuare vor fi prezentate cele două tehnici de bază utilizate pentru tolerarea defectelor: tolerarea ierarhică a defectelor; tolerarea de tip grup a defectelor.
Un comportament cu defecte poate fi clasificat numai prin respectare anumitor specificații ale unui subsistem, la un anumit nivel de abstractizare. Toleranța ierarhică a sistemelor utilizează mecanisme care au în vedere faptul că pentru a-și realiza sarcinile sale un subsistem depinde de subsistemele de nivel mai scăzut sau de nivel mai ridicat.
Pentru a exista siguranța că un serviciu rămâne disponibil pentru clienți în ciuda defectării subsistemelor, se poate implementa sarcina și printr-un "grup" de subsisteme redundante, independente fizic, astfel încât, dacă unele dintre subsisteme se defectează, cele care rămân furnizează sarcina specifică.
Toleranța de tip ierarhic și toleranța de tip grup sunt tehnici principale de mascare a defectărilor. În practică însă, adesea se întîlnesc abordări care combină elemente din amândouă. Restabilirea funcțională a unui sistem tolerant la defectări are ca scop continuarea funcționării sistemului cu date corecte după ce a apărut o eroare. Structura și arhitectura unui sistem tolerant la defectări trebuie să fie realizate sub forma modulară, pe cât posibil sub forma unor unități înlocuibile, astfel încât toate subsistemele principale să fie autonome și separate unele de altele prin interfețe bine definite. Avantajele majore ale unor astfel de structuri și arhitecturi constau în faptul că se face o verificare localizată, astfel încât detecția erorilor poate avea un caracter local, aceasta minimizând propagarea erorilor și contaminarea întregului sistem, iar restabilirea după defectare va putea fi simplificată.
O unitate înlocuibilă este o unitate de defectare, înlocuire și dezvoltare - adică o unitate care se defectează în mod independent de alte unități, care poate fi înlocuită fără a afecta celelalte unități și poate fi adaugată la un sistem pentru a-i îmbunătăți performanța, capacitatea și disponibilitatea.

Concluzii

Alegerea uneia dintre multiplele soluții posibile de management a redundanței la diferite niveluri hardware, sisteme de operare și aplicații este însă dificil de făcut nu numai din lipsa unor informații analitice și experimentale asupra costului diferitelor tehnici de management a resurselor, dar și din lipsa unor informații publicate despre tipurile de comportamente defecte pe care diferite componente le manifestă, precum și despre a ce fel de distribuțiile defectărilor asociate lor. Chiar dacă cineva ar avea disponibile toate costurile și datele de defectare teoretice și experimentale necesare, numărul de alegeri care ar trebui luat în considerație ar fi atât de mare încât este puțin probabil ca o căutare sistematică pentru optimalitate să poată avea loc. Pentru aceasta și pentru multe alte rațiuni este posibil ca realizarea sistemelor tolerante la defectări să rămână o artă în viitorul previzibil. Odată cu creșterea dependenței de sistemele de calcul, disponibilitatea serviciilor de prelucrare și de comunicații în prezența defectării componentelor va trebui să devină tot mai importantă.

Bibliografie

[1]. Aurel Șerb "Sisteme de calcul tolerante la defectări", Academia Tehnică Militară, Bucureşti, 1996
[2]. Vasile M. Cătuneanu, Angelica Bacivarof, "Structuri electronice de înaltă fiabilitate. Toleranța la defectări.", Editura Militară, Bucureşti, 1989