Българска академия на науките. Bulgarian Academy of Sciences
Аерокосмически изследвания в България. 15. Aerospace Research in Bulgaria
София. 1999. Sofia

Контрол на работата на компютърни системи за управление и на системи за полунатурно моделиране в реално време чрез протоколен модел на Хоар[1]

Пламен Христов, Петър Гецов, Пламен Ангелов

Институт за космически изследвания, БАН

Съществуват различни методи за контрол на работата на една компютърна система за управление — методи на техническата диагностика, идентификация и оценка на качеството на управление в реално време и др. Тези методи контролират апаратната част на системата или общо нейното качество. Основната част на компютърните системи обаче е програмното осигуряване и то изисква по-специални методи за контрол. Когато системата е разработена на базата на CSP-модели, подходящо е приложението на протоколния модел на Хоар за контрол на работата на системата (изчислителните процеси в нея).

Този модел се основава на предварителна спецификация (спецификации и азбуки) на структурата и функциите на системата и процесите в нея и контрол (наблюдение) на работата чрез наблюдение на протоколите.

Същност на протоколния модел на Хоар

Протокол на поведението на процеса се нарича крайна последователност от символи, фиксиращи събития, в които процесът е участвал до определен момент от време. В CSP-нотацията протоколът се означава с последователност от символи, разделени със запетая — <x, y> — протокол, състоящ се от две събития, x и след него y; <x> — протокол, състоящ се от едно събитие; <> — празен протокол [1].

Примери:

Протокол на контурен процес:

prot(LoopProcess[i]) =<Adder[0], Prop[0.5], Stat1[0.2,0.1], SepPoint[3], ...> = $trace_x$;$trace_y$ = $s^n tr_x$.

[1] Изследванията се финансират от НФ„Научни изследвания“ — дог. И-305/93.

Протоколите на процесите се представят чрез последователността от агрегати (звена), които при текущата спецификация участват в процеса. Допустимостта на протокола се определя от това, дали съответният агрегат е включен в азбуката на процеса.

Протокол на агрегат — апериодично звено от първи ред:

AAZ1[i]= $\Sigma np_i, np_i'$; $np_i = np'_{i-1}; np'_i = y_k; y_k = -a_1 y_{k-1} + b_1 u_{k-1}$,

където np_i и np'_i са числови значения на входа и изхода на агрегата, np'_{i-1} — числови значения на изхода на предходния агрегат, y_k — реакция на звеното на произволен входен сигнал, a_1 и b_1 — коефициенти на характеристичното уравнение на звеното, u — входен сигнал на звеното.

Операции над протоколите

- **Конкатенация** — $s \hat{} t$, където s и t са протоколи. В резултат на конкатенацията на базата на два протокола се получава нов протокол, в който те са съединени в указания ред.
- **Свиване** — **(t |\A)** — означава протоколът t, свит върху множеството A, което обикновено е азбука на процес. Новият протокол се построява от t чрез отхвърляне на всички символи, които не принадлежат на A.
- **Глава и опашка** — s_0, s' — ако протоколът s е непразна последователност, то неговият пръв елемент се означава с s_0, а резултатът, получен след неговото изваждане, с s'.
- **Звезда** — **A*** — множество, представляващо набор от всички крайни протоколи, съставени от елементи на A.

$$A^* = \backslash s \mid s \mid \backslash A = s \backslash$$

- **Дължина на протокола** — **#** — брой на елементите на протокола.
- **Повторение** — s^n — протоколът s, повторен n-пъти.

Основни параметри на предлагания метод

- Методът е основан на протоколния модел на Хоар.
- Обединява контрол на работата на системата и верификация в реално време.
- Методът е предназначен за работата в средата на блоково-модулни системи с известен набор системни обекти, за които предварително могат да се изчислят протоколите на Хоар.

Същност на предлагания метод

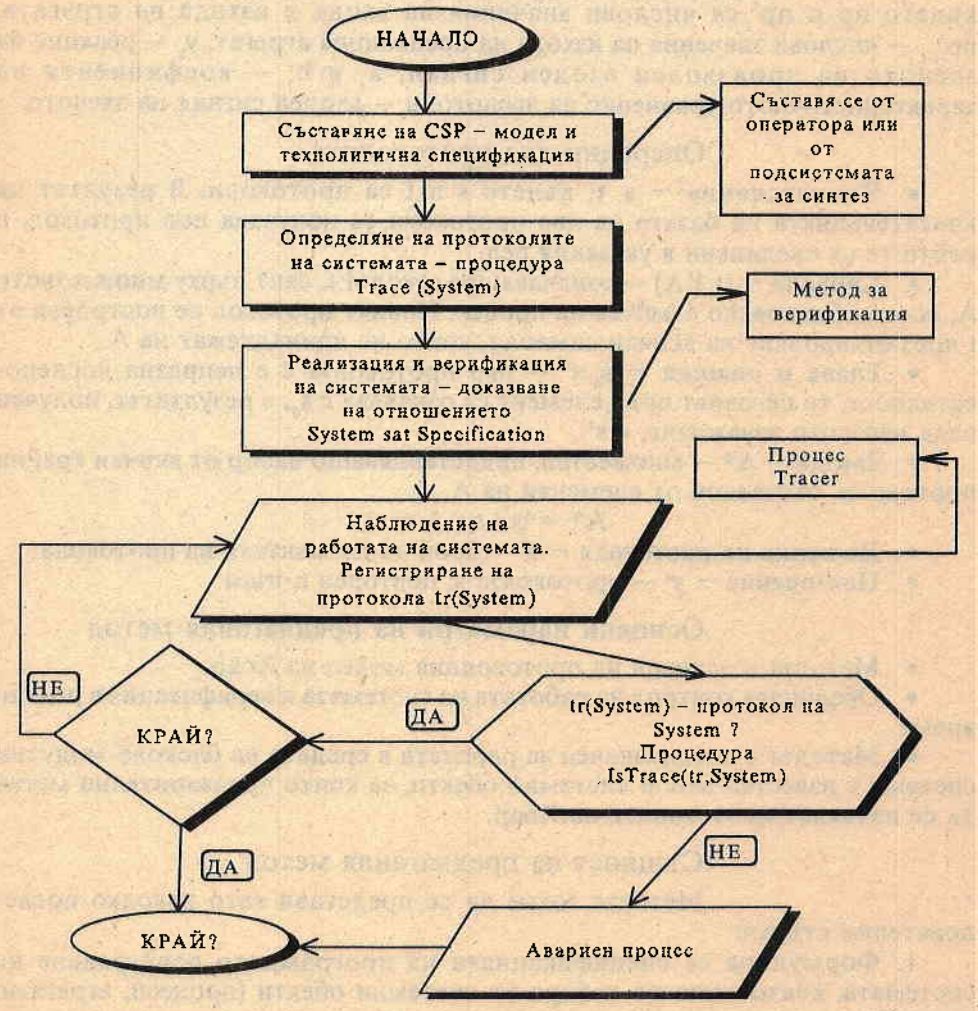
Методът може да се представи като няколко последователни стъпки:

1. Формулира се спецификацията на програмното осигуряване на системата, която включва набора от системни обекти (процеси, агрегати, канали);
2. Реализира се програмната система и се доказва нейната коректност (метод за доказване на коректността на спецификации на Хоар).
3. Определят се всички възможни протоколи на специфицираната система с процедурата **trace(P)**.
4. Стартира се системата.
5. Специален процес — протоколчик (tracer), следи и регистрира протоколите в системата и определя дали са валидни, т. е. — дали се явяват

подмножество на множеството предварително определени протоколи. Това се прави чрез процедурата **IsTrace(s,P).**

6. При регистриране на невалиден протокол се предприемат съответните действия за аварийна ситуация.

Блок - схемата на метода е представена на фиг. 1.



Фиг. 1

Основни проблеми при реализация на метода

• *Как протоколчикът да получава информация за протоколите в системата?* Процесът Tracer трябва да е разпределен между отделните компютри. Във всеки компютър диспечерът, след като управлението се върне към него, трябва да го предава на Tracer. Това решава

проблема с последователността от процеси, но не и с протоколите на всеки отделен процес. Тук трябва да се припомни, че обектът „контурен процес" играе ролята на диспечер на списъка от агрегати. В този смисъл той може след изпълнението на всеки агрегат да връща управлението на главния диспечер или директно да го предава на Tracer. Така Tracer ще може да следи всяко действие на системата чрез проверка на активните обекти в базата данни.

• *Как освен структурната коректност на изпълнението (последователността от процеси, агрегати и канали) да се контролира и функционалната коректност (коректното задаване на параметрите на обектите)?* Този проблем се отнася преди всичко за агрегатите. Решението се получава от това, че протоколите на агрегата се изчисляват по неговата спецификация, в която от своя страна участват неговите параметри.

Скелетът на функцията trace(P)е показан по-долу. Тя работи по типовите конструкции на Хоар (алтернативни процеси, паралелни процеси, рекурсивно определени процеси, процеси с избор и др.), протоколите на които са изведени в [1].

trace(P)= (R)* &
    if P = ($STOP_P$) then trace(P)= \<>\;
    elsif P = (c → P) then trace(P)= \<> U \<c> Λ t|t ∈ trace(P)\;
    elsif P = (c → P | d → Q)then trace(P)= \t|t = <> V (t_0 = c & t'∈ trace(P)V (t_0 = d & t'∈ trace(Q))\;
    elsif P = (x:B → P(x)) = \t|t = <> V (t_0 ∈ B & t'∈ trace($P(t_0)$))\
    elsif P = (mX : A.F(x))) = $\bigcup_{n\geq 0}$ trace($F^n(STOP_A)$);
  elsif P = (P || Q)then trace(P)= trace(P)∩ trace(Q);
      else t = trace(P||Q) then
trace(P||Q)=\t|(t |R) ∈ trace(P)& (t |Q) ∈ trace(Q)& t ∈ (αR ∪ αQ)*\
..... други конструкции на Хоар.....
    else
end.

По-долу е показан скелетът на процедурата IsTrace, определяща дали даден протокол е валиден за процеса.

IsTrace(s,P)=
    if s = NIL then TRUE;
      elsif $P(s_0)$ = BLEEP then FALSE;
      else IsTrace(s', $P(s_0)$);
end.

BLEEP е специален символ, използван в случай (само в този случай), че символът не може да бъде начално събитие на процеса.

Програмно осигуряване на метода

Програмното осигуряване на метода е реализирано на Modula-2 като отделен модул Tracer. Модулът се свързва по стандартни информационни канали с другите обекти на системата.

Изчислителни експерименти

Експериментите включват симулация на некоректни ситуации, при които може да възникне грешен протокол — повреди в датчиците, водещи до грешни сигнали, неправилна работа на диспечера, програмното осигуряване като цяло и др.

Изводи

Предлаганият метод дава възможност за контрол на работата на програмни системи на базата на строга математична теория (CSP).

Интерес представлява самият подход за контрол на работата на програмни системи в реално време чрез протоколи на Хоар, тъй като такъв подход не се прилага в известните системи. Методът е предназначен за работа с блоково-модулни системи и използва предварително изчислените протоколи на системните обекти.

Литература

1. Hoare, C.A.R. Communicating Sequential Processes. PRENTICE-HALL International, UK, LTD, 1985.
2. Concurrent Systems: Formal Development in CSP by Michael G.Hinchey (University of Cambridge) and Stephen A.Jarvis (University of Durham). McGraw-Hill International Series in Software Engineering published 12th January 1995. McGraw-Hill Book Company.

Постъпила на 21.IV.1997г.

A functional control of computer control systems and real time simulation systems by means of Hoare's trace model

Plamen Hristov, Peter Getzov, Plamen Angelov

(Summary)

Some possibilities of using Hoare's trace models for a software functional control of moving objects computer control systems and real time simulation systems are considered. A general description of the trace models is presented. A possibility for the main system objects trace calculation is inspected, and the main problems of the method implementation and the ways and means of their resolving too. The method algorithm and the main procedures of the method are presented.