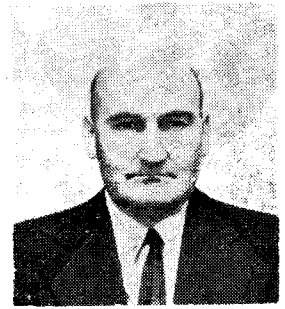


A hibatűrő rendszerek diagnosztikája

IX. nemzetközi konferencia szakmai tapasztalatai

KESSELYÁK PÉTER
BHG Fejlesztési Intézet



ÖSSZEFOGLALÁS

A beszámoló áttekinti az integrált áramkörök és számítógépi rendszerek tesztelési eljárásaival, a szoftvermegbízhatóság növelésével, a rendszerek hibatűrő képességének fokozásával és mikroprocesszor bázisú eszközök szervizelésével kapcsolatos, legérdekesebbnek ítélt előadásokat.

1. Bevezetés

1986. június 25—27. között a Csehszlovák Mérnökegyesület (CSVTS) szervezésében Brnoban került megrendezésre a „Hibatűrő rendszerek diagnosztikája” c. IX. nemzetközi konferencia, 17 országból mintegy 250 résztvevővel.

A konferencia szóhasználata szerint hibatűrő rendszereken nagy bonyolultságú integrált áramköröket, valamint számítógépeket és célorientált számítógépes hálózatokat kell érteni.

A jelen beszámoló az elhangzott előadásokból válogatva kíván ízelítőt adni e nemzetközi sereg szemle szakmai mondanivalójából.

2. A konferencia előadásainak témái

Mintegy 60 előadás hangzott el, egyetlen szekció keretén belül. Az előadásokat az alábbi témakörökbe lehetett sorolni:

- Integrált áramkörök (főként memóriák) tesztelhetősége, tesztelési eljárások és hibafelderítési határfokok;
- Integrált áramkörök tesztelhetőségre való tervezése. Önellenőrző áramkörök;
- Hibatűrő rendszerek (főként számítógépek és hálózatok) tulajdonságai, diagnosztikai és rekonfigurációs algoritmusok;
- Rendszer-megbízhatósági mutatók számítás-módja, Markov modellek;
- Integrált áramkörök és funkcionális számítógépi egységek tesztelő eszközei. Teszt-minta generátorok. Diagnosztikai műszerek.

Az előadásoknak kerekén 50%-a egyetemi, további 38%-a kutatóintézeti tevékenységek eredményeiről számolt be — az ipari és szolgáltató (karbantartó) ágazat konkrét gyártmányokra vonatkozó tapasztalatai együttvéve az előadásoknak 12%-át tették ki.

Beérkezett: 1987. II. 12. (#)

KESSELYÁK PÉTER

A Szegei Tudományegyetem matematika-fizika szakán 1958-ban szerzett diplomát. 1959 óta a BHG Híradástechnikai Vállalat fejlesztő mérnöke. Államközi műszaki-tudományos együttműködés keretében éveken át dolgozott szakértőként Dél-Kínában, majd Kubában híradástechnikai gyártmányok trópusállósági és megbízhatósági vizsgálatait végezve. E témában számos szakmai cikk és konferencia-előadás szerzője. Tagja az Európai Minőségügyi Szervezet és az IEC 56. Megbízhatósági Szakbizottságai hazai munkacsoportjának. A hibakapacitás, mint új rendszer-megbízhatósági-jellemző bevezetéséért megkapta az Európai Minőségügyi Szervezet 1983 évi nívódíját. 1986-ban a HTE Puskás Tivadar díjjal tüntette ki.

3. A szakterületen érvényesülő fejlődési irányzatok

John P. Hayes, a Michigani Egyetem Elektronikai és Számítástechnikai Intézetének professzora áttekintést adott a digitális eszközök és vizsgálati módszereik fejlődésének jelenéről és közeljövőjéről, a 90-es évek elejéig [1]. Az integrált logikai áramkörök funkciósűrűsége hamarosan eléri a 100 000 kapu/morzsa jellemző értéket, a RAM memóriák tároló képessége pedig a 4 Mbit/morzsa értéket. Megjelennek a RAM és ROM területeket egyben tartalmazó áramköri morzsák. A jövőben számolni kell a nagy tesztelési időmegtakarítást biztosító, párhuzamos szervezésű öntesztelő áramkörök tömeges megjelenésével.

A nagy bonyolultságú áramkörök gépi tervezési és gyártási ideje gyors csökkenésben van, ezzel együtt a számítógépes áramköri tervezés (CAD) eszközeinek és a VLSI technológiáknak az ára is csökken. — Ugyanakkor az áramköri tesztelő eszközök bonyolultsága és ára tovább növekszik, mivel a VLSI áramkörök növekvő kivezetés-száma, funkció-sűrűsége és működési sebessége ezt szükségesszerűvé teszi. A tesztelési költségek emelkedő irányzata miatt az alkalmazott kutatások már most is és a közeljövőben is az IC vizsgálatok költségeinek csökkentésére irányulnak, mégpedig új, hatékonyabb tesztelési elvek és nagyobb letapogatási sebesség bevezetése, valamint az IC tesztelhetőségre való tervezése útján. E törekvések közt fontos szerepet kap az az irányzat, hogy a tesztelési stratégia ne pusztán matematikai statisztikai megfontolásokra épüljön, mert ez az út az áramköri bonyolultság növekedtével egyre járhatatlannabb, hanem súlyozottan vegye figyelembe a konkrét hibalehetőségeket és a hibák feltárásához

vezető legcélrányosabb algoritmusokat. A műszaki-gazdasági optimumot jelentő tesztelési eljárás kiválasztása mindig kompromisszum a működési sebesség, a hibafeltárási hatások, a morzsanagyság, az áramkör rendeltetése és a külső eszközigeny között.

4. Integrált áramkörök tesztelési módszerei

E. J. McCluskey, a Stanfordi Egyetem Számítógépes Rendszerek Intézetének professzora „*Tesztminta generálási módszerek összehasonlítása*” címmel [2] egyszerű logikai IC-k vizsgálatának példáján keresztül mutatta be, hogyan javítható a Boole-algebrán alapuló funkcionális tesztelés hibafeltárási hatásfoka és melyek a tesztelési módszer korlátai. A hatékony, jó hatásfokú hibafeltárás — a statisztikai megfontolások mellett — nem nélkülözheti a konkrét meghibásodási modellekre épülő, célirányos tesztminta generálást. Emellett a funkcionális (logikai) és parametrikus áramköri vizsgálatok szétválasztása sem célszerű. Külön kitért az előadó a Boole-algebra segítségével nem tesztelhető hibák fajtáira. Ilyenek azok,

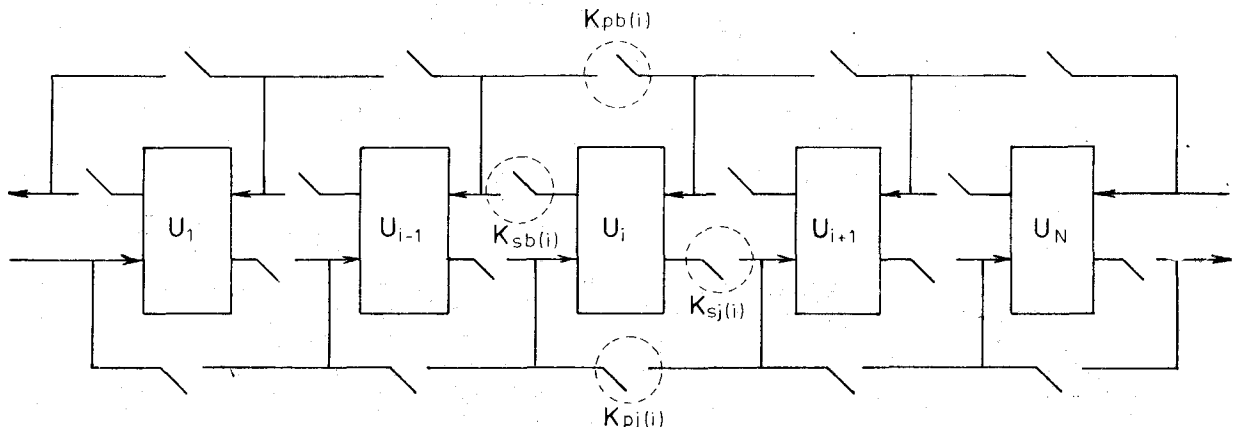
- amelyek az áramkör lehetséges logikai állapotainak számát megszorítják;
- amelyek az áramkörnek hardver szempontjából redundáns részében keletkeznek;
- amelyeket a belső logikai elrendezés kisöntöl.

A hibafeltárás hatásfokának helyes becslése a vizsgált eszköz gyakorlati megbízhatóságának szempontjából igen lényeges feladat, bonyolultabb áramköri struktúrák esetén azonban még elvileg sem mindig megoldott kérdés.

Stephen Y. H. Su — a New-Yorki Állami Egyetem Számítástechikai Intézetének professzora és *Kewal K. Satuja*, az ausztráliai Newcastle egyetemének munkatársa „*Hibatűrő VLSI szisztolikus architektúra*” címen [3] tartottak beszámolót a jel/képfeldolgozásban, számítástechikai osztályozó és string-manipulációs műveletekben alkalmazott, több száz azonos típusú műveleti egységből sorosan felépített morzsaáramkörök öntesztelési módszeréről. Az 1. ábra egy ilyen szisztolikus

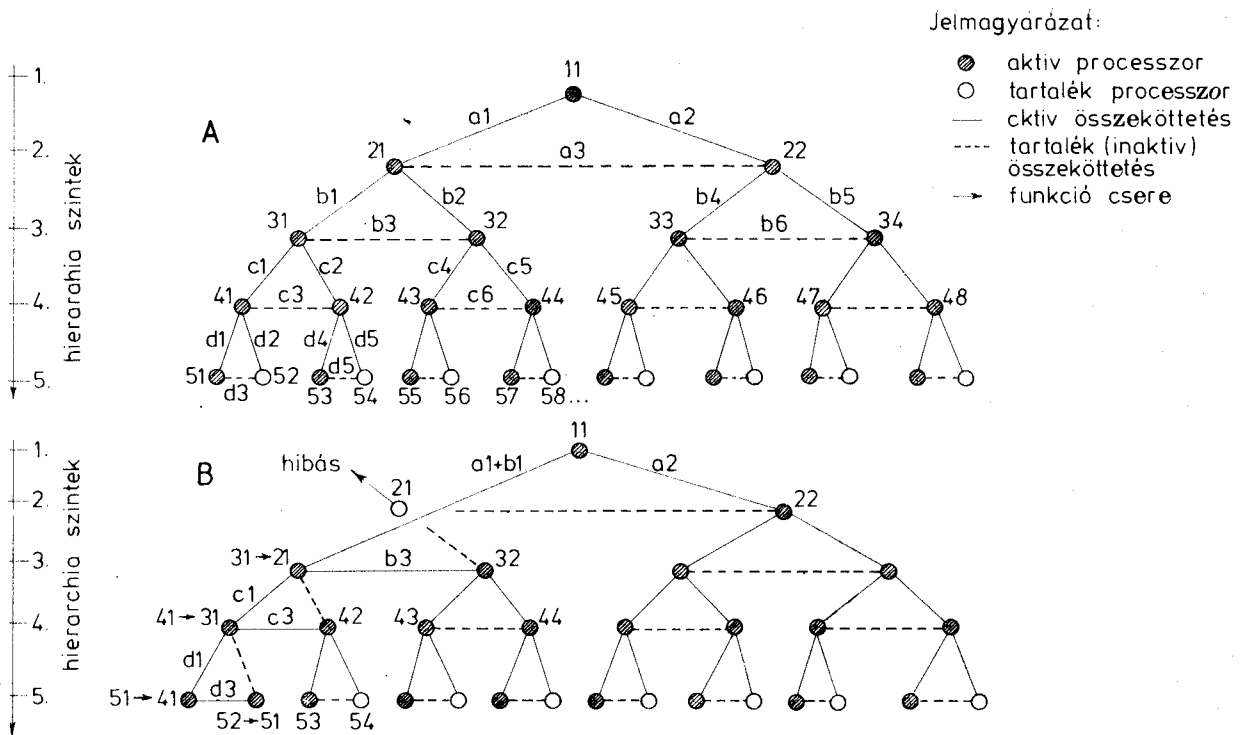
VLSI architektúrát mutat. A $K_{sb}(i)$, $K_{sj}(i)$, $K_{pb}(i)$, $K_{pj}(i)$ soros és párhuzamos kapcsolók megfelelő vezérlésével minden egyes i -edik műveleti egység egymástól függetlenül be- illetve kiiktatható a sorból. — A műveleti egységekbe öntesztelő áramköri rész is be van építve. Teszt üzemmódban mindegyik műveleti egység öntesztje szinkronban indítható, két közös jelvezeték felhasználásával. Az öntesztelés egységenként két beépített tesztminta generátor segítségével történik, amelyeknek a jelsorozatából az önteszt során konvolúció képződik. Ez a konvolúció — mint komprimált adat és egyben az önteszt végeredménye — egy regiszterben eltárolódik. Szinkronban ugyanez az eseménysorozat játszódik le a szomszédos műveleti egységekben is. Amikor valamely egység az öntesztet befejezi, az eltárolt végeredményt közli szomszédjaival és várja azok viszont közlését. Ha megkapta, akkor a szomszédos eredményeket összehasonlítja a sajátjával és többségi elv alapján vagy jónak vagy rossznak minősíti önmagát. A minősítés eredményéről értesíti a szomszédokat. Ezen kívül ún. jobb- és baloldali szindróma jeleket is képez, melyeknek értéke \emptyset , ha az összevetett két szomszédos végeredmény egyezik és 1, ha nem egyezik. A műveleti egységek által kibocsátott szindróma jelek közös shift-regiszterbe kerülnek és — második lépcsőben — szekvenciális jelanalízis dönt arról, hogy a műveleti egységek „önértékelése” abszolút értelemben helyes volt-e. Az öntesztelés végső eredménye alapján azután a hibásnak minősült műveleti egységeket a hozzájuk tartozó, 1. ábra szerinti K_{sb} , K_{sj} , K_{pb} , K_{pj} kapcsolók megfelelő állásba vezérlésével automatikusan kiiktatják a műveleti sorból és helyettük a műveleti sor végén álló tartalékok közül iktatnak be újat.

Az ismertetett szisztolikus architektúrájú öntesztelés előnyei három pontban foglalhatók össze: — a műveleti egységek (cellák) teszt-jel képzése és ön-minősítése időben párhuzamosan történik; — a szekvenciális jelanalízis útján, második lépcsőben történő diagnosztizálás ideje sem nő arányosan a cellák számával;



H313-1

1. ábra



H313-2

2. ábra

— hibásnak talált cella esetén az IC automatikusan átkonfigurálja önmagát.

5. Szoftver megbízhatóság növelése

C. Zurak—Owczarek, a lengyelországi Lodz egyetemének munkatársa *Szoftver megbízhatóság növelési modell* címen tartott előadásában [4] minden egyes szoftver programhoz hozzárendelte az input adatmezőnek azt a tartományát, amelyen operálva a program hibás eredményt szolgáltat, vagyis az output adatmezőnek egy hibás résztartományát generálja. Amikor egy programhibát elhárítanak, a kritikus input- és output-tartomány szűkülni fog és a következő programhiba észrevételéig a működési idő várható értéke növekszik. A programban rejlő szoftver hibák száma ismeretlen és mindegyik hibához tartozik egy jellemző meghibásodási intenzitás, amely valószínűségi változónak tekinthető. Ha feltételezzük, hogy az egyes szoftver hibákhoz tartozó meghibásodási intenzitások eloszlása azonos — pl. gamma-eloszlás (ami első közelítésben jogos feltételezés) — akkor az előadó bizonyítása szerint az eredő, közös eloszlás is csak gamma-eloszlás lehet. A meghibásodási intenzitás eloszlásának sűrűségfüggvényére a szerző rekurzív formulát adott az összes és az elhárított szoftver-hibák számának, valamint az első i db hiba elhárításáig eltelt időnek a függvényében. A formulának gyakorlati szempontból szépséghibája az, hogy a programban rejlő szoftver hibák ismeretlen N száma is szerepel benne, amire vonatkozólag feltételezéssel kell élnünk.

Ladislav Hudec, a Pozsonyi Műszaki Egyetem munkatársa „Elosztott watchdog időzítés mikro-számítógépek programfutásának ellenőrzésére” témájú előadásában [5] abból indult ki, hogy jelenleg a mikro-számítógépes rendszerekbe beépített watchdog időzítő eszközök nincsenek kellőképpen kihasználva. Sokkal intenzívebben lennének használhatóak a hibás programfutás gyors felismerésére és a hibák elszigetelésére, a következőképpen: bontsuk a mikro-számítógép programját egészen rövid futásidejű (néhány-szor $10 \mu\text{s}$ -os) szegmensekre és mindegyik szegmens futásához rendeljünk hozzá watchdog időzítést. Ily módon a hibafeltárási késedelem nagyságrenddel csökkenthető és a hibafeltárási hatásfok jelentősen növelhető. A Pozsonyi Egyetem gyakorlatában használt mikroprocesszoros eszközöknél a hiba keletkezésétől az indikációig eltelt időt $1000\text{--}4000 \mu\text{s}$ -ról néhányszor $10 \mu\text{s}$ -ra csökkentették, a hibafeltárási hatásfokát pedig $0\text{--}20\%$ -ról $15\text{--}45\%$ -ra sikerült növelniük.

F. Malabocchia és L. Simoncini, a torinói CSELT cég képviselőinek „On-line adatvédelem osztott hozzáférésű számítógépes rendszereknél” c. előadása [6] egy nagy biztonságú adatvédelmi módszernek az elvét ismertette, amely a fejlesztés szakaszában a hibahely behatárolását is segítheti. A módszer lényege az, hogy az előfizetők számára hozzáférhető szabad programkönyvtár és a tiltott programkönyvtár olyan memóriaterületeken van elhelyezve, melyeknek normál címkódja azonos, van azonban egy extra SELECT bit (jogossági kód) amelynek az értékét az előfizető nem képes befolyásolni. Ez a bit tesz különbséget a két

memória terület között. Ennek a jogossági bit-nek a beállítását a belső monitor program vezérli. Ha a monitor a tiltott területhez kíván hozzáférni, akkor a SELECT bitet egyszerű OUT utasítással, a programszámláló léptetése nélkül állítja be. További védelmet biztosít az a szervezőmód, hogy a tiltott programkönyvtár memória területén nincs minden cím hasznos információval betöltve. A kihasználatlan címekre interrupt-kérés van beírva, ezért ha az adott területre a program illegálisan vagy hiba folytán ráfut, akkor a rendszer késedelem nélkül leállítja az illegális programfutást és alarmjelzést ad.

6. Rendszerek hibátűrő képességének fokozása

A konferencia előadásai azt tükrözték, hogy a számítógép-vezérelt berendezések hibátűrő képességének fokozására továbbra is a „klasszikus receptek” vannak érvényben:

- redundáns egységek alkalmazása;
- az egységek közötti kommunikációs összeköttetések topológiájának megválasztása;
- üzenetek kódolása;
- szavazási elv alkalmazása;
- átkonfigurálási algoritmusok.

Elvi újdonságot ezen a téren nem hozott a konferencia, néhány hasznos gyakorlati módszert azonban körvonalazott.

Matthew B. Lowrie és W. Kent Fuchs, az Illinoisi Egyetem Tudományos Laboratóriuma Számítógépi Csoportjának munkatársai fa-struktúrájú multiprocesszoros rendszerek konfigurációs algoritmusairól tartottak érdekes előadást [7]. A 2. ábra egy 5-hierarchia szintű fa-struktúrát mutat. Az ábrán szaggatott haránt összekötő vonalak hideg-tartalékként meglévő összeköttetéseket jelentenek a processzor egységek között. Processzor tartalékolás csak a legalsó, ötödik szinten van. (A tartalék processzor egységeket az ábrán üres karika jelzi.) Ha valamelyik üzemelő processzor meghibásodik, akkor a hierarchiában alája rendelt egyik processzor (pl. először mindig a „baloldali”) lép be helyette és a szükséges haránt összeköttetések aktivizálódnak, bizonyos meglévők pedig bomlanak. Ha mondjuk az ábrán 21-gyel jelölt processzor egység meghibásodik, akkor az automatikus konfiguráció az alábbi szerepcseréket jelenti:

21 → hibás	a1 + b1 → a1
31 → 21	b3 → b2
41 → 31	c3 → c2
51 → 41	d3 → d2
52 → 51	

A rekonfiguráció vezérlését elláthatják maguk a csomóponti processzorok, vagy egy külön rekonfiguráció vezérlő egység mindegyik processzor mellett.

7. Mikroprocesszoros rendszerek tesztelő eszközei

E fontos szakterületen viszonylag kevés előadás hangzott el, amelyek közül említést érdemel *Jobbágy Á.—Pataricza A.—Setényi E.* beszámolója [8] a Budapesti Műszaki Egyetemen kifejlesztett μ SER'84 diagnosztikai szerviz műszerről.

Ez a hordozható, 2,8 kg súlyú műszer mikroprocesszor-vezérelt, 10—20 Euro-kártya terjedelmű kis berendezések széles skálájának szervizelését képes segíteni, elsősorban akkor, ha a javítandó berendezés ún. „kemény magja” hibásodott meg (CPU, tápellátás, buszrendszer). A műszer sokoldalú használatát a ROM tárolóban helyet foglaló és cserélhető, célorientált szerviz-programok biztosítják. (A szerviz programok PASCAL nyelven írhatók.) A műszer 7-szegmenses kijelzővel van ellátva. A szerviz-programok futása közben megjelenített kódolt üzenetek irányítást adnak a szerviz személyzet tevékenységéhez. A μ SER'84 Z 80 mikroprocesszort, 8K ROM és 2K RAM tárolót, analóg mérő egységet, jel-analizátort, buszkapcsoló adaptert, tasztaturát és kijelzőt tartalmaz.

8. A konferencia jelentősége

A konferencia hírt adott az elektronika és számítástechnika ágazatának teszteléssel és diagnosztikával kapcsolatos legfrissebb eredményeiről és körvonalazta a fejlődés irányvonalát. A hazai mikroelektronikai alkatrész- és berendezésgyártók részéről a konferencia sorozat témái nagyobb figyelmet érdemelnek a jövőben. A soronkövetkező X. konferenciát Várnában tartják 1987 szeptemberében, az 1988. évi konferenciára Gdanskban kerül sor. 1990-től kezdve lehetőség látszik arra, hogy Magyarország is bekapcsolódjék a rendezésbe.

IRODALOM

- [1] *John P. Hayes*: Trends in Digital System Testing. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 1—10, 1986. június.
- [2] *E. J. McCluskey*: A Comparison of Test Pattern Generation Techniques. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 11—20, 1986. június.
- [3] *Stephen Y H. Su—Kewal K. Satuja*: Fault Tolerant VLSI Systolic Architecture. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 36—44, 1986. június.
- [4] *C. Zurak-Owczarek*: Software Reliability Increasing Models. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 79—84, 1986. június.
- [5] *L. Hudeo*: Distribution of Watchdog Timer into Program of Microcomputer. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 233—237, 1986. június.
- [6] *F. Malabocchia—L. Simoncini*: On-line Error Detection in the Access of Shared Resources. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 58—63, 1986. június.
- [7] *Matthew B. Lowrie—W. Kent Fuchs*: Reconfiguration Algorithms for Tree Architectures Using Subtree Oriented Fault Tolerance. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 45—50, 1986. június.
- [8] *Jobbágy Á.—Pataricza A.—Setényi E.*: Service System and Instrument for Microprocessor Based Devices, the Extension of the Self-test. IX. Fault Tolerant Systems and Diagnostics Conference Volume, pp. 293—289, 1986. június.