ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТА ОБЧИСЛЮВАЛЬНІ СИСТЕМИ І КОМПЛЕКСИ В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 681.335

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДУ ПОКОМПОНЕНТНОГО ДІАГНОСТУВАННЯ ЦИФРОВИХ ПРИСТРОЇВ

Перевозніков С.І., Савчук Т.А., Карач І.Ю.
Вінницький дкржавний технічний університет

Відмінною рисою методу покомпонентного діагностування (МПД) є можливість організовувати різні стратегії декомпозиційного тестового контролю цифрових пристроїв (ЦП). Це вдається виконати завдяки конструктивному доступу голок спеціального контактного пристосування до внутрішніх контрольних точок (КТ) об'єкта дослідження.

Доцільність використання МПД обумовлена існуванням низки практичних задач, вирішення яких дозволяє економити час, а також підвищувати якість продукції, що випускається. Так, в умовах серійного виробництва різних пристроїв РЕА, існує чимало технологічних та конструктивних особливостей виготовлення і складання друкованих плат ЦП, що потребують використання систем діагностування такого классу. Подібні проблеми з'являються при вирішенні наступних питань:

-пошук максимальної глибини діагностування ЦП в умовах обмежень складності фрагментів схем, що виділяються (наприклад, брак машиної пам'яті або у випадку , коли визначено спільний часовий ресурс при реалізації тестових програм контролю ЦП);

-в процессі тестового контролю пристроїв при наявності множини недоступних контрольних точок об'єкта (наприклад, при невідповідності значень координат внутрішних КТ відстані між контактними голками засобів діагностування або використанні мікросхем с планарними виводами);

-синтез компонентної структури об'єкта дослідження в умовах обмеженого числа голок контактного поля (аналогічні задачі виникають при високій щільності разміщення друкованих провідників на платі ЦП);

-розробка контролепридатних пристроїв для МПД при забезпеченні умов непошкоджуючого наведення тестових сигналів у вузли пов'язаних між собою компонентів цифрових об'єктів.

При цьому слід відзначити, що для вирішення розглянутих питань з використанням МПД необхідною умовою стає забезпечення спеціальних електричних умов подачі сигналів тестового контролю у множину внутрішніх КТ об'єкта. Результатом такого підходу є запобігання появи в об'єкті дослідження можливих вторинних дефектів (внаслідок порушення допустимих значень параметрів теплових режимів, що протікають при діагностуванні ЦП у вихідних каскадах мікросхем, наприклад, виготовлених по ТТЛ-технології). Модельний розрахунок умов електричного непошкодження елементів внутрішніх структур мікросхем об'єкта контролю (при заданих обмеженнях) дозволяє використовувати різні стратегії діагностування на основі синтезу тестопридатних структур компонентних утворень. З метою оптимізації значень параметрів тестового контролю ЦП подамо початкову структуру пристрою, що тестується, у вигляді, наприклад, орієнтованого графа $G(V,E)$, де $V=\{v1, v2, v3..., vn\}$ - множина вершин, що відповідає множині логічних елементів ЦП, а $E=\{e1, e2, ...,em\}$ - множина дуг, що відображають зв'язки між елементами пристрою. Тоді сформульовані раніше задачі формально можна звести до перетворення початкового графа $G \rightarrow G^*$, де $G^*(V^*,E^*)$ також є графом, для якого $|V^*| \le |V|$, $|E^*| \le |E|$. Останній являє собою множину компонентів V^* (а також зв'язки між ними E^*), які деяким чином покривають початкову множину елементів ЦП. При цьому для любого компонента (підграфа) $v_i \in V^*$ визначено підмножину внутрішніх дуг (КТ) $Ei \in E$ початкового графа G, подача в які наперед розрахованого вектора сигналів (установочний набір $L_i^{уи}$) забезпечує на виходах компонентів, які безпосередньо зв'язані з входами компонента v_i^*, що тестується, рівня напруги, що дорівнює потенціалу логичної одиниці (в позитивній логіці), або високоімпедансного стану (вектор початкових умов діагностування $L_i^{ну}$).

Проведений аналіз [1] показав, що час бездефектного наведення тестових сигналів у

внутрішні КТ пристрою знаходиться із наступних співвідношень параметрів теплових процесів, що протікають в період тестування об'єкта дослідження

$$P_{гран} \le (T_{к.гран} - T_{с.гран}) / R_T \ ; \tag{1}$$

$$t_з \le \tau_i \ln(1 - (T_{к.гран} - T_{с.гран}) / \ P_{гран\cdot} \cdot \sum_i R_{T_i} \ , \tag{2}$$

де $P_{гран}$, $T_{к.гран}$, $T_{с.гран}$ - гранично допустимі значення відповідно розсіюваної потужності, температури кристалу мікросхеми, температури навколишнього середовища;

R_T - тепловий опір;

$t_з$ - максимальний час примусової зміни рівня сигналів;

τ_i - коефіцієнт, що залежить від типу матеріалу корпусу мікросхеми.

Максимальна тривалість наведення сигналів вектора $L_i^{ун}$ компонента $v_i \in V$ при заданих параметрах для ТТЛ-схем (при потужності наведення 1,36 Вт, тепловій постійній $\tau_i = 10 \cdot 10^{-6}$ с та тепловому опорі R_T=60 С /Вт) становить 10 мкс. В цьому випадку найбільша глибина діагностування об'єкта досягається (при умові, що сумарний час установки вектора початкових умов діагностування (ПУД) і тривалості тестового контролю любого компонента не перевищує 10 мкс) за рахунок декомпозиції структури ЦП на мінімальні компоненти.

Визначення. Мінімальною компонентною структурою будемо називати максимальне число компонентів об'єкта, для кожного з яких існує вектор $L_i^{ун} = \{\varnothing\}$.

Методику синтезу мінімальних компонентних структур цифрових об'єктів узагальнює наступний алгоритм їх декомпозиції:

Крок 1. Покласти *i=0, j=0.*

Крок 2. Присвоїти *i:=i+1.*

Крок 3. Якщо *i*>$|\Gamma^+(v_i)|$, де $v_i \in V$, то присвоїти $V_i = v_i$. Перейти до кроку 8.

Крок 4. Визначити підмножину $E_S^{'} \subset E$ внутрішніх КТ, подача в $L_i^{ун}$ які вектору сигналів з множини векторів $\overline{L_i^{ун}}$ забезпечить умови ПУД елемента v_i.

Крок 5. Якщо існує таке $\overline{\kappa \in 1, |\Gamma^+(v_i)|}$, де $\kappa \ne i$, для якого виконується умова $L_i^{ун} \cap L_\kappa^{ун} \ne \{O\}$,то перейти до кроку 2, інакше усунути вектор $L_i^{ун}$ з множини векторів $\overline{L_i^{ун}}$.

Крок 6. Якщо $\overline{L_i^{ун}} \ne \{\varnothing\}$, то перейти до кроку 4.

Крок 7. Сформувати компонент V_i, об'єднавши елемент v_i з кожним елементом $V_c \in V$, для якого виконується умова $\Gamma^-(v_c) \cap \Gamma^+(v_i) \in E_S^{'}$.

Крок 8. Покласти *j:=j+1.* Зафіксувати компонент $V_j = V_i$. Сформувати повний вектор $L_j^{ун}$ компонента V_j.

Крок 9. Кінець алгоритму.

Згідно з алгоритмом, функція $\Gamma^+(\Gamma^-)$ для элемента $v_i \in V$ означає множину вхідних (вихідних) дуг, інцідентних вершині v графа *G(V,E)*; $\overline{L_i^{ун}}$ - множина векторів установочних наборів елемента $v_i \in V$.

Особливості розглянутого підходу іллюструють процес формування підсхем цифрового об'єкта, приведеного на рис.1, з урахуванням фактора часу. Так, згідно з приведеним алгоритмом та критеріями, запропонованими в [2], наприклад, для компонента схеми D6 початковий вектор

установочного набору $L_6^{уи}$ має такий вигляд:

$$L_6^{уи} = (XXXXXXXXXXXXX0XXXX), \text{ де } X \in \{0,1\}.$$

Остаточне формування умов електричного захисту компонента D5 здійснюється за допомогою подачі додаткових п'ятнадцяти імпульсів в КТ2, що складає $t^{ну}$ =4 мкс. При цьому вектор $L_6^{ну}$ визначиться наступним чином:

$$L_6^{ну} = (XXX1111XXXXXX0XX1X).$$

В даному випадку формується одноелементний компонент схеми, так як, згідно методики, існує $L_6^{уи} \neq \{O\}$, а також виконується умова ($t_6^{ну} + t_6^{к}$)<10мкс, де $t_6^{к}$ - час контролю елемента D6. Для элемента D8 умови забезпечення електричного захисту складаються із забезпечення начального вектора $L_8^{уи}$, рівного

$$L_8^{уи} = (XXXXXXXXXXXXX00XXX).$$

Після подачі необхідних п'ятнадцяти імпульсів в КТ2, а також серії з п'ятнадцяти імпульсів в КТ12, на виходах елемента D7 установлюється вектор $L_8^{ну}$ елемента D8.

$$L_8^{ну} = (XXXXXXX1111XX00XXX).$$

В цьому випадку час установки вектора $L_8^{ну}$ становить $t_8^{к}$ =8мкс+4мкс=12мкс. Ураховуючи, що $(t_8^{ну} + t_8^{к})$ > 10мкс ($t_8^{к}$ = 30нс), процес подачі тестових сигналів має свої особливості: фізично тест контролю фрагмента D8 має бути розподіленим на три однакових блоки, які реалізуються сумісно з вимушеними періодами охолодження вихідних напівпровідникових структур елемента D7 (такий підхід потребує не менш як 12,5 мкс).

Прискорити процес забезпечення умов діагностування компонента D8 можна тільки за рахунок введення в об'єкт додаткових елементів D9, D10 (як показано на рис.1). Достатньо в КТ18 и КТ19 подати рівень логічного нуля і час установки вектора $L_8^{уи}$ компонента D8 складе біля 100 нс. При цьому $(t_8^{ну} + t_8^{к})$ <10 мкс.

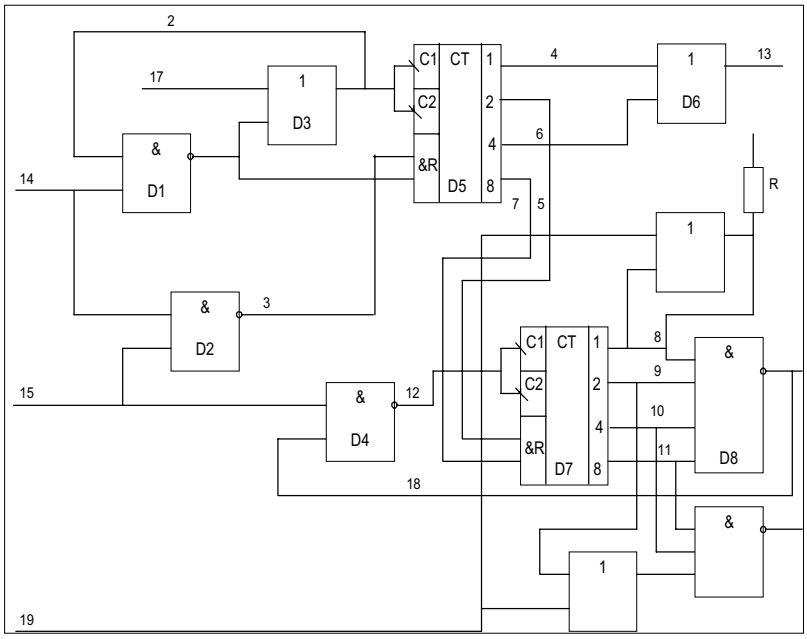

Рис 1

Особливістю систем розглянутого класу є конструктивна можливість змінювати структуру об'єкта дослідження в період тестового контролю. Адаптація об'єкта дозволяє, наприклад, шляхом створення генеруючих структур прискорити процес його перевірки. Це досягається

введенням додаткових штучних каналів передачі тестової інформації. Так, якщо на об'єкт подати відповідний вектор установочних сигналів ($L^{ун}$)

$$L^{ун} = (XXXXXXXXXXXX11X01)$$

та при цьому замкнути штучними ланцюгами КТ2 та КТ15, КТ3 та КТ18, а також КТ12 та КТ14, то в утвореному контурі зворотного зв'язку (D1, D3, D2 и D4) виникне генерація сигналів. Для таких компонентних утворень час контролю S-елементів синтезованого контуру зменшується в S разів. Узагальнений алгоритм синтезу генеруючих структур ЦП має наступний вигляд:

Крок 1. Визначити вектор $L_i^{ун}$ для елемента $v_i \in V$. Виконати це для всіх $i \in \overline{1,n}$.

Крок 2. Сформувати підмножину $V^* \subset V$ елементів схеми, для любих двох елементів якого виконується така умова $L_i^{ун} \cap L_j^{ун} \neq \{O\}; i, j \in 1, \left|V^*\right|; i \neq j$.

Крок 3. Розбити множину елементів V^* на підмножини $V^* = \{V_1^*, V_2^*, ..., V_s^*\}$ для кожної з яких виконуються наступні умови:

а) $\sum_{j=1}^{k} Z_j \geq \tau$, де $r_i = \left|V_i^*;\right|$;

б) для $p,q \in \overline{1,S}$, де $p \neq q$, справедливо $V_p^* \cap V_q^* = \{O\}$;

в) для кожного фрагмента схеми $V_i^* \subset V^*$ виконується умова непарного числа інверсій в штучному контурі.

Крок 4. Для кожної підмножини $V_i^* \subset V^*$ впорядкувати послідовність її елементів.

Крок 5. Якщо існує $V_i^* \subset V^*$, для якого умова (а) кроку3 не виконується, то ввести для такого фрагмента схеми в ланцюг штучного зворотного зв'язку елемент затримки.

Крок 6. Подати для всіх елементів фрагмента $V_i^* \subset V^*$ вектор $L_i^{ун}$, де $i \in \overline{1, \left|V_i^*\right|}$. Виконати це для всіх підмножин множини V^*.

Крок 7. Для всіх утворених контурів зворотних зв'язків $V_i^* \subset V^*$ подати блокуючі сигнали на вхід, наприклад, елемента $v_i \in V_i^*$ кожного фрагмента схеми $V_i^* \subset V^*$.

Крок 8. Замкнути вхід $v_i \in V_i^*$ з виходом $v_i \in V_i^*$. Виконати це для всіх $i \in \overline{1,S}$.

Крок 9. Зняти блокуючі сигнали з входів усіх контурів V_i^* схем.

Крок 10. Зафіксувати засобами СПД генерацію сигналів в кожному контурі. Видати діагностичне повідомлення.

Крок 11. Кінець алгоритму.

Таким чином, вибір тої або іншої стратегії тестового контролю цифрових об'єктів для систем покомпонентного діагностування в основному визначається особливостями конкретної топології включення елементів, що складають їх структуру, а також параметрами синтезу підмножини компонентів: глибиною діагностування, числом (або складністю) виділених (або штучно складених) фрагментів схем, часом тестового контролю, ціною введеної (додаткової) аппаратури у склад ЦП.

Найбільш перспективним у цьому відношенні є метод адаптивного діагностування, який дозволяє за рахунок утворення електричних умов її комутації певних внутрішніх КТ об'єкта суттєво спростити та прискорити час перевірки різних ЦП. Так, для розглядуваного фрагмента схеми (рис.1) одержуємо такі результати порівняння застосовуваних стратегій тестового контролю відносно загального часу процедур діагностування:

ДІАГНОСТУВАННЯ		
поелементне	пофрагментне	адаптаційне
21,7мкс	12,5мкс	100нс

Література

1. Чахмахсазян Е.А., Мозговой Г.П., Силин В.Д. Математическое моделирование и макромоделирование биполярных элементов электронных схем.-М.:Энергия,1989.-С.49-61.

2.Перевозников С.И. Методика алгоритмического поиска начальных условий покомпонентного диагностирования цифровых устройств//Электронное моделирование.-1993.-Т.15,№2.-С.50-55.

УДК 681.334

МАСКУВАННЯ ІНФОРМАЦІЇ У СИСТЕМАХ ОПРАЦЮВАННЯ ДАНИХ НА БАЗІ ТАЙМЕРНИХ ОБЧИСЛЮВАЛЬНИХ ПРИСТРОЇВ

Григорук П.М.

Технологічний університет Поділля, м. Хмельницький

Проблеми захисту інформації у системах обробки даних (СОД) вже багато років знаходяться в центрі уваги не тільки фахівців з розробки чи використання цих систем, але і широкого кола користувачів, причому особлива увага приділяється небезпеці несанкціонованого (випадкового чи зловмисного) одержання інформації особами, для яких вона не призначалась. Ця небезпека стала настільки гострою, що традиційні засоби , що існували раніше, у докомп'ютерну епоху, виявились недостатніми. Переконливим свідченням цього стали конкретні факти зловмисного одержання інформації. Тому наявність механізмів захисту (як апаратних, так і програмних) є одним із обов'язкових вимог при проектуванні СОД, причому не тільки спеціального призначення, але й чисто комерційних.

На початковому етапі розвитку концепції захисту інформації, коли панувало переконання, що захист інформації в СОД порівняно легко може бути забезпечений чисто програмним шляхом, здебільшого розвивалися саме програмні засоби, які доповнювалися необхідними організаційними заходами. Але коли виявилося, що як одними програмними засобами , так і додатковими організаційними заходами, надійний захист інформації не забезпечується, інтенсивний розвиток дістали різноманітні технічні пристрої і системи. Поступово, по мірі формування основних положень комплексного підходу до захисту інформації, зріло і переконання про необхідність комплексного розвитку всіх засобів захисту [1].

Маскування - засіб захисту інформації шляхом її криптографічного закриття. Вважається, що цей спосіб є ефективним як із точки зору власне захисту, так і із точки зору наочності для користувачів. За кордоном цей вид захисту застосовується як при обробці, так і при схові інформації. При передачі інформації по лініях зв'язку великої довжини маскування є єдиним засобом надійного її захисту.

Маскування, за визначеням зарубіжних фахівців, є найбільш універсальним засобом захисту, хоч практична реалізація алгоритмів шифрування пов'язана з подоланням значних труднощів [2]. Можна зашифрувати всю інформацію, призначену для схову, чи тільки ключі (паролі), які контролюють доступ до інформації, що зберігається. У будь-якому випадку шифрування підвищує безпеку схову інформації.

Існує багато способів перетворення вихідної інформації, що називається незашифрованим текстом, у зашифрований вигляд, що називається шифром, шифротекстом чи кодом. Всі вони можуть бути використані для захисту інформації у СОД, оскільки кожний із них цілком піддається алгоритмізації. Кожний із них характеризується своєю стійкістю і трудомісткістю при реалізації. Під стійкістю криптологічного закриття розуміють мінімальну довжину закритого тексту, із якого можуть бути виявлені такі статистичні закономірності, на основі яких може бути відновлений закритий текст. Наряду з цією характеристикою розглядають також обчислювальну стійкість. Криптоалгоритм вважається обчислювально стійким, якщо вартість обчислень для його розкриття робить це завдання невиконуваним. Під трудомісткістю криптоалгоритму розуміють мінімальне число елементарних операцій, необхідних для перетворення деякого фіксованого елемента відкритого тексту (наприклад, символу).

Сам процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно, проте апаратна реалізація володіє порівнянно із програмною рядом переваг : високою продуктивністю, спрощеною реалізацією тощо. Тому в ряді зарубіжних країн уже налагоджено промислове виробництво апаратури для шифрування і існує чималий досвід використання цієї апаратури [3]. Інтерес до теоретичних аспектів криптографії зумовив, з одного боку, поширення