

WIELOPOZIOMOWE MECHANIZMY BEZPIECZEŃSTWA INTELIGENTNYCH ROZWIĄZAŃ PROCESOROWYCH

Marek Salamaj, Piotr Bubacz

**Instytut Informatyki i Elektroniki, Uniwersytet Zielonogórski
65-246 Zielona Góra, ul. Podgórna 50**

e-mail: [M.Salamaj, P.Bubacz]@iie.uz.zgora.pl

STRESZCZENIE

Ważnym elementem sterownia różnych obiektów, systemów zarządzających jest przede wszystkim bezpieczeństwo ich jednostek sterujących, procesorów. Z tego względu, że układy te stosowane są niemalże we wszystkich dziedzinach przemysłu, konieczne są opracowania coraz bardziej rozbudowanych, efektywniejszych, a przede wszystkim bezpieczniejszych jednostek sterujących. W artykule przedstawione zostały mechanizmy mające wpływ na zwiększenie efektywności i poprawności pracy całego systemu.

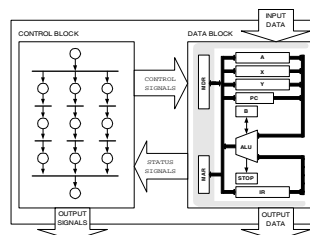
1. WPROWADZENIE

Na rynku cyfrowych układów sterowania, można wyróżnić liczne grupy wyspecjalizowanych, wielofunkcyjnych opracowań układowych, których przedstawicielami są różne rozwiązania procesorowe. Większość z tych rozwiązań jest wyspecjalizowanymi modułami logicznymi, które w bardzo wąskich i konkretnych dziedzinach zastosowań, zdolne są do realizacji wydajnych i bezpiecznych algorytmów sterowania. Realizacja właśnie takich algorytmów sprawia, że możliwe staje się osiąganie coraz wyższych szybkości, większej mocy obliczeniowej i bezpieczeństwa rozpatrywanych układów procesorowych. To przede wszystkim bezpieczeństwo pracy procesorowych układów sterowania jest głównym bodźcem, który popycha wielu naukowców do badań nad nowymi rozwiązaniami w tej dziedzinie.

W architekturach obecnie stosowanych, różnych rozwiązań procesorowych, wyróżnić można dwa moduły funkcjonalne (moduł sterujący i operacyjny) [1][3], które są zarazem jego elementami (blokami) składowymi (rys. 1.) W takim przypadku, każdy z nich realizuje całkowicie odmienne zadania w pracy całego systemu sterującego. W taki sposób, by po połączeniu rezultatów ich pracy uzyskać bardzo spójną, dokładną i poprawnie funkcjonującą jednostkę centralną.

Zastosowanie separacji bloku sterującego i operacyjnego w układach procesorowych miało na celu zwiększenie niezawodności układu, dokładności, precyzji, jego funkcjonalności, a przede wszystkim bezpieczeństwa działania całego układu. W ten sposób, stworzono całkowicie nowy, bezpieczny i efektywny mechanizm współpracy pomiędzy blokami. Jego idea polegała

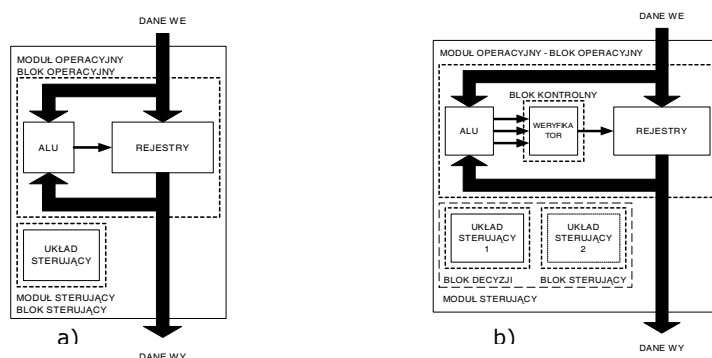
na tym, by głównym zadaniem bloku operacyjnego była możliwość realizacji wszelkich operacji związanych tylko z przetwarzaniem danych. Natomiast nad poprawnym i efektywnym wykorzystaniem wszelkich zasobów tego bloku, miał nadzorować blok sterujący. Jego zadanie polega na odpowiednim generowaniu sygnałów sekwencyjnych sterujących modulem operacyjnym i całym zewnętrznym systemem procesorowym.



Rys. 1. Architektura obecnie stosowanych układów procesorowych

Separacja bloku sterującego i operacyjnego kieruje się prostymi regułami [1][3]. Polega ona na tym, że blok sterujący realizuje algorytm sterowania, na podstawie, których generowane są w nim sygnały sterujące. Następnie sygnały te, przesyłane są do bloku operacyjnego, w którym realizowane są określone operacje na danych znajdujących się w chwili obecnej w jego elementach składowych. Po ich zakończeniu, rezultaty tych operacji, w postaci sygnałów statusowych, przesyłane są z powrotem do bloku sterującego, gdzie na ich podstawie podejmowane zostają decyzje o dalszej pracy całego systemu.

Omawianą architekturę oraz mechanizmy, jakie w niej funkcjonują można przedstawić w postaci struktury przedstawionej na rys. 2a. W strukturze można wyróżnić dwa potoki przetwarzania, w którym jeden z nich przesyła informacje bezpośrednio z wejścia układu do jego rejestrów oraz drugi potok, który przetwarza informacje wejściowe w jednostce ALU, a dopiero później przesyła je do odpowiedniego rejestru. Układ sterujący jest odpowiednikiem modułu sterującego, który zarządza wszystkimi elementami składowymi całej struktury procesorowej.



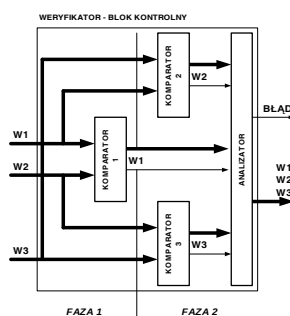
Rys. 2. Struktury procesorów: a) obecnie stosowana, b) nowa

2. MODUŁ OPERACYJNY

W celu zwiększenia stabilności, wydajności, a przede wszystkim bezbłędności działania układu przeprowadzono badania, których rezultaty doprowadziły do zmodyfikowania powyższej struktury [2]. Rezultatem tych działań było opracowanie nowej struktury procesora przedstawionej na rys. 2b.

Jest to struktura, która w ogólnym zarysie funkcjonuje identycznie jak poprzednie rozwiązanie, z tą różnicą, że w celu detekcji błędów, których głównym źródłem jest jednostka ALU, zastosowano w niej układ weryfikatora wyników [2]. Głównym zadaniem tego układu jest analiza wyników otrzymywanych z jednostki ALU. W przypadku wykrycia błędu układ sterujący wprowadza cały układ procesora do stanu bezpiecznego, bądź wymusza na ALU powtórzenie ostatniej operacji.

Zastosowanie w strukturze procesorowej układu weryfikatora, który składa się z odpowiedniej konfiguracji komparatorów (rys. 3) doprowadziło w znacznym stopniu do rozbudowy układu na poziomie algebraicznego przetwarzania danych. W tym przypadku, rozbudowie uległa jednostka arytmetyczno-logiczna ALU, która realizuje operacje przetwarzania danych. Ze względu, aby układ weryfikatora mógł prawidłowo funkcjonować, wykrywając powstałe błędy w jednostce ALU, założono, że będzie ona realizowała każdą operację trzema różnymi metodami obliczeniowymi. Następnie rezultaty tych operacji są ze sobą porównywane, w celu detekcji błędów powstałych w tej jednostce oraz określenia dalszej pracy całego systemu.



Rys. 3. Blok kontrolny – schemat weryfikatora wyników W1, W2 i W3

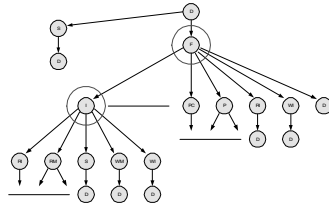
W pracy układu weryfikatora można wyróżnić dwie fazy. Pierwsza z nich, polega na porównaniu ze sobą rezultatów operacji W1 i W2 (rys. 3) przesłanych do niego z jednostki ALU. Na tym etapie analizy, możliwa jest weryfikacja zgodności wyników. Jeśli wyniki nie są jednakowe, to układ, poprzez moduł sterujący, może wprowadzić cały procesor do stanu bezpiecznego lub wymusić powtórzenie ostatnio realizowanej operacji w ALU. W przypadku stwierdzenia, w fazie pierwszej, różnicy porównywanych wyników W1 i W2, przeprowadzony zostaje kolejny etap analizy, w którym wyniki tych obliczeń (W1 i W2)

odnoszone są do wyniku W3. W module Analizatora następuje porównanie, po którym można stwierdzić, który z wyników operacji W1, W2 czy W3 jest wynikiem poprawnym. W przypadku, gdy otrzymane wyniki są różne moduł ten będzie wymuszał powtórzenie ostatniej operacji zrealizowanej w jednostce ALU, aż do osiągnięcia poprawnych rezultatów.

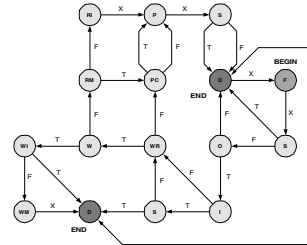
3. MODUŁ STERUJĄCY

W strukturze będącej odzwierciedleniem obecnie stosowanych rozwiązań procesorowych, został zastosowany układ sterujący (rys. 2a), który steruje i nadzoruje zasobami modułu operacyjnego [1][3]. Blok sterujący kieruje całym przepływem informacji, w taki sposób, by uzyskać jak najwyższą efektywność i wydajność pracy całego procesora przy jednoczesnym zachowaniu wszystkich elementów bezpieczeństwa. To właśnie bezpieczeństwo pracy takich jednostek sterujących jest ich najostrzejszym kryterium prawidłowego funkcjonowania, z tego względu, że stanowią one całą logikę sterowania, od której uzależniona jest praca całego układu procesorowego. W przypadku błędnej interpretacji instrukcji programu, bądź niewłaściwego zarządzania, przez moduł sterujący, układem procesorowym, może doprowadzić do nieodwracalnych zmian w zarządzanym systemie.

W celu zwiększenia szybkości i wydajności pracy oraz analizy współbieżnych mechanizmów funkcjonowania układu, wykorzystywany jest opis w postaci różnych konfiguracji sieci i grafów. Dzięki temu możliwa jest analiza stosowanych rozwiązań w modułach sterujących oraz określenie czy nowe układy są bardziej bezpieczne i efektywniejsze niż dotychczasowe rozwiązania. Przewagą wykorzystania sieci i grafów jest to, że istnieją mechanizmy, pozwalające na weryfikację różnych parametrów, a w rezultacie umożliwiają one otrzymanie rozwiązań, które będą bardziej bezpieczne [2]. Jednak pomimo ich wykorzystania w układach sterujących pojawiają się różne konflikty mogące wywołać błędną pracę całego układu. Występujące konflikty wyboru mogą dotyczyć m.in. zastosowania zbyt rozległych rozgałęzień w analizowanych sieciach (grafach). Na rys. 4 przedstawiono fragment grafu układu sterującego, w której występują liczne stany krytyczne (stany oznaczone okręgami) mogące doprowadzić w ekstremalnych warunkach do konfliktu wyboru. Aby stany krytyczne zostały wyeliminowane z sieci układu sterującego, konieczne jest zastąpienie ich stanami bezpiecznymi. Stany bezpieczne to takie stany, które posiadają, co najwyżej dwa wyjścia o określonych statusach. Wykorzystując właśnie taką ideę, w przeprowadzonych badaniach, opracowano całkowicie nową sieć działań, rys. 5, którą można wykorzystać do zwiększenia bezpieczeństwa pracy całego procesora.



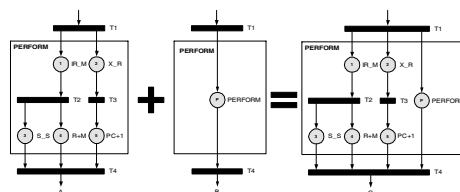
Rys. 4. Stany krytyczne w sieciach sterujących



Rys. 5. Sieć działań bloku decyzji

W strukturze układu procesorowego (rys. 2b) zastosowane zostały dwa różne moduły sterujące. Pierwszym z nich jest układ sterujący, którego sieć działań, opisana została tradycyjnymi metodami, stosowanymi w większości układów procesorowych. Natomiast sieć działań drugiego układu sterującego (rys. 5) zrealizowano przy wykorzystaniu idei bezpiecznych stanów logicznych procesora. Rezultatem takich działań, było otrzymanie dwóch różnych sieci, odseparowanych od siebie, które funkcjonowały indywidualnie oraz wspólnie nadzorowały pracą systemu.

Fragment sieci działań, modułu sterującego procesorem, w skład, którego wchodzi oba układy (bloki) sterujące przedstawiono na rys. 6c. Sieć C (rys. 6c) jest właśnie rezultatem połączenia dwóch indywidualnie funkcjonujących sieci działań A i B układów sterujących. Sieć A jest siecią bloku sterującego występującego w różnych rozwiązaniach układowych. Jest ona siecią bardziej rozbudowaną, kierującą całym przepływem informacji, w taki sposób, by każdy stan tej sieci, generował odpowiedni sygnał sterujący, wywołujący w module operacyjnym określone działanie. Natomiast sieć B, została ograniczona tylko i wyłącznie do samych stanów procesora. Takie rozwiązanie umożliwiło opracowanie sieci w sposób, który pozwalał na wyeliminowanie wszystkich stanów krytycznych, jakie mogły pojawić się w pracy układu.



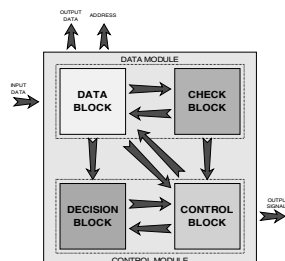
Rys. 6. Sieć działań modułu sterującego

Zastosowanie w tym rozwiązaniu mechanizmu współpracy pomiędzy obiema sieciami spowodowało zwiększenie wydajności i dokładności pracy układu sterującego. Sieć A zajmuje się kontrolą wszystkich możliwych stanów procesora oraz jego elementów składowych. Natomiast głównym zadaniem sieci B układu sterującego, jest nadzór nad prawidłowym działaniem sieci A.

4. ZAKOŃCZENIE

Procesor zrealizowany na podstawie pomysłu przedstawionego w tym artykule będzie układem znacznie bezpieczniejszym, niż dotychczasowe rozwiązania. Wynika to z faktu, że moduł operacyjny i sterujący procesora został rozbudowany o elementy zwiększające jego bezpieczeństwo. W architekturze procesora zostały umieszczone dwa dodatkowe bloki funkcyjne pełniące w nim funkcje kontrolne i diagnostyczne.

Architekturę opracowanego w ten sposób procesora, uwzględniającą wszystkie poruszone w tym artykule zagadnienia przedstawiono na rys. 7. Tego typu rozwiązanie, w porównaniu do ogólnie stosowanej architektury procesorów (rys. 1) zawiera rozbudowane mechanizmy odpowiedzialne za weryfikację poprawności działania całego układu procesorowego.



Rys. 7. Bloki funkcjonalne nowego procesora

Jak można zauważyć, przez zastosowanie różnych rozwiązań układowych w procesorach możliwe jest znaczne zwiększenie ich możliwości technicznych pod względem wydajności przetwarzania, poprawności i precyzji działania, a przede wszystkim bezpiecznego funkcjonowania.

LITERATURA

- [1] J. Kershaw: *The VIPER microprocessor*, Report No.85013, Royal Signal and Radar Establishment, Malvern, England 1987
- [2] M. Śnieżek, W. Halang: *Bezpieczny programowalny sterownik logiczny*, Politechnika Rzeszowska, Polska 1998
- [3] W.J. Cullyer, C.H. Pygott, *Application of formal methods to the VIPER microprocessor*, IEE PROCEEDING, No 3, page 133-141, England 1987