ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2002
Seria: ELEKTRYKA z. 181 Nr kol.1540

Ryszard MIELNIK
Instytut Metrologii Elektrycznej
Politechnika Krakowska

SYNTEZA MIKROPROCESOROWEGO SYSTEMU POMIAROWO – STERUJĄCEGO DLA ZASTOSOWAŃ KRYTYCZNYCH

Streszczenie. Budowa nowoczesnych mikroprocesorowych systemów pomiarowo – sterujących wykorzystywanych w procesach, których niewłaściwe nadzorowanie bądź sterowanie może doprowadzić do dużych strat materialnych, śmierci ludzi lub katastrof ekologicznych środowiska, wymaga stosowania szczególnych zasad i metod projektowania oraz wytwarzania urządzeń nadzorujących i sterujących takimi procesami.. W artykule przedstawiono możliwości wykorzystania sieci Petriego do syntezy przykładowego mikroprocesorowego systemu pomiarowo – sterującego dla potrzeb urządzeń sygnalizacji przejazdowej znajdujących się na skrzyżowaniu linii kolejowej z drogową.

SYNTHESIS OF MICROPROCESSOR MEASUREMENT – CONTROL SYSTEM FOR CRITICAL USES

Summary. The paper presents assumption for a microprocessor measurement-control system (MMCS) of the automatic railway crossing signaling. For synthesis of this system the Petri net was used. On the basis of the analysis of the operation of MMCS there were formed sets of elementary events and conditions defining when particular events could take place, or conditions resulting from a given event. On this basis a Petri net for MMCS was worked out. Using formally prepared specification of the task, a general idea of software was worked out. MMCS was applied and tested in laboratory.

1. WPROWADZENIE

Budowa nowoczesnych mikroprocesorowych systemów pomiarowo-sterujących w wielu obszarach zastosowań wymaga specyficznego podejścia do filozofii ich projektowania, wytwarzania i eksploatacji. Wynika to z faktu, że w przypadku uszkodzenia lub niezgodnego z wcześniej założonymi specyfikacjami funkcjonalnymi systemu może dojść do zagrożenia bezpieczeństwa nadzorowanego procesu lub jego otoczenia. Może to prowadzić do dużych strat materialnych, śmierci ludzi lub skażenia środowiska. Dlatego też należy zwrócić szczególną uwagę na zapewnienie systemom pomiarowo-sterującym wymaganego stopnia niezawodności i bezpieczeństwa funkcjonowania. Pojęcia niezawodności i bezpieczeństwa pracy (funkcjonowania) systemów pomiarowo-sterujących wykorzystujących w swej budowie mikroelektronikę, prowadzą, ogólnie rzecz ujmując, do zapewnienia rzetelności działania systemów komputerowych i mikroprocesorowych w zastosowaniach krytycznych.

Dobrym przykładem mikroprocesorowych systemów pomiarowo-sterujących w zastosowaniach krytycznych są urządzenia samoczynnej sygnalizacji przejazdowej - SSP, umieszczane na jednopoziomowych skrzyżowaniach dróg kołowych z kolejowymi. Niniejszy artykuł przedstawia syntezę takich urządzeń na podstawie sieci Petriego.

2. URZĄDZENIA SYGNALIZACJI PRZEJAZDOWEJ

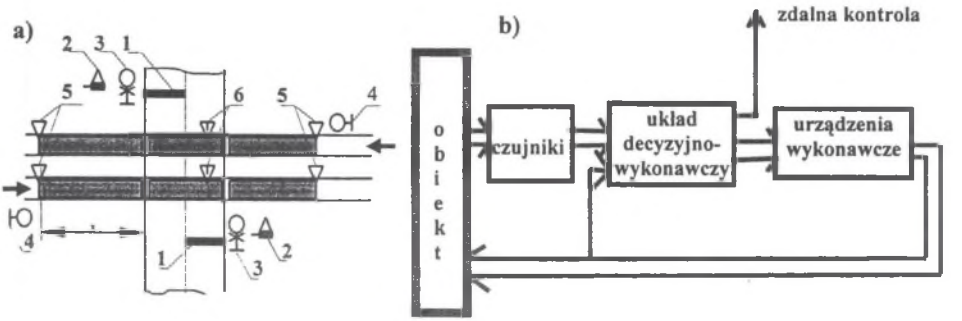
Bezpieczeństwo ruchu na przejeździe zapewnia aparatura pomiarowo-sterująca współpracująca z urządzeniami ostrzegania i zamykania w ten sposób, by dzięki zamknięciu przejazdu dla pojazdów drogowych nie doszło do kolizji między nimi a pojazdami szynowymi. Aparatura pomiarowo-sterująca urządzeń SSP musi spełniać dwie podstawowe funkcje polegające na:

- zapewnieniu wymaganego sterowania urządzeniami ostrzegania i zamykania zgodnie z zasadami zapewnienia płynnego, efektywnego i bezpiecznego ruchu pojazdów na przejeździe,
- kontrolowaniu poprawności działania czujników, urządzeń ostrzegania i zamykania oraz samokontroli działania aparatury pomiarowo-sterującej, a w razie jej nieprawidłowej pracy - doprowadzeniu do bezpiecznego stanu urządzeń SSP.

Typowe dla nowoczesnych systemów sygnalizacji przejazdowych wyposażenie przejazdu w urządzenia zabezpieczające pokazano na rys.1a. Są nimi:

- półzapory - (1),
- sygnalizacja akustyczna ostrzegająca kierowców - (2),
- sygnalizacja optyczna ostrzegająca kierowców - (3),
- czujniki wykrywające obecność pojazdu szynowego na odcinkach zbliżania - (5),
- czujniki stwierdzające opuszczenie strefy niebezpiecznej przez pojazd szynowy - (6),

- sygnalizator pociągowy - (4).



Rys.1. a) Wyposażenie przejazdu w urządzenia zabezpieczające
b) Struktura blokowa systemu pomiarowo – sterującego SSP
Fig. 1. a) Equipment of level crossing with devices protecting
b) Diagram-block of measurement – control system for SSP

3. MODEL SAMOCZYNNEJ SYGNALIZACJI PRZEJAZDOWEJ

Ogólną strukturę blokową rozważanego systemu pomiarowo-sterującego urządzeń SSP pokazano na rys.1b. Opis działania zasad obowiązujących w procesie zabezpieczenia ruchu na przejeździe podano poniżej w postaci przykładowych, wybranych reguł w postaci **JEŻELI** ... **TO**...:

Reguły działania procesu

JEŻELI *nadjeżdża pociąg*	**TO** *włącz sygnał ostrzeg. dla kierowców*
JEŻELI *upłynął wymag. czas od włącz. sygnału ostrzeg. dla kierowców*	**TO** *zamknij rogatki*
JEŻELI *nadjeżdża pociąg i rogatki są zamknięte*	**TO** *podtrzymuj zamknięcie rogatek*
JEŻELI *pociąg zjeżdża z przejazdu*	**TO** *otwórz rogatki, wyłącz sygnał ostrzegający dla kierowców i włącz sygnał zezwalający na sygnalizatorze pociągowym*
. . .	
JEŻELI *rogatki zamknięte*	**TO** *włącz sygnał zezwalający na sygnalizatorze pociągowym*

W wyniku przeprowadzonej analizy funkcjonowania system pomiarowo-sterujący powinien uwzględniać następujące, podane w postaci przykładowej, wybrane reguły:

Reguły działania systemu	
JEŻELI (1) *zamknij*	**TO** (1) *odmierz czas* $t' = t_0 - t$
JEŻELI (1) *zamknij*	**TO** (2) *odmierzaj czas zamykania*
JEŻELI (1) *zamknij*	**TO** (3) *włącz sygnalizator dla kierowców i wyślij komunikat do zdalnej kontroli*
JEŻELI (1) *zamknij*	**TO** (4) *włącz sygnaliz. akust. dla kierow.*
JEŻELI (2) *początek zamykania rogatki*	**TO** (5) *włącz układ stwierdz. przeszkodę*
. . .	
JEŻELI (14) *podtrzymuj*	**TO** (4) *włącz sygn. akust. dla pociągów*
JEŻELI (15) *uszkodzenie zapór*	**TO** (18) *awaria i wysł.kom. do zdal. kontr.*

4. SIEĆ PETRIEGO I GRAF ZNAKOWAŃ OSIĄGALNYCH

Na podstawie ww. reguł działania przyjmując, że miejsca odpowiadają warunkom po słowie **JEŻELI ...** , a przejścia działaniom wywoływanym po słowie **TO ...** , opracowano sieć Petriego systemu pomiarowo – sterującego urządzeń SSP. Analiza tej sieci pokazała, że:

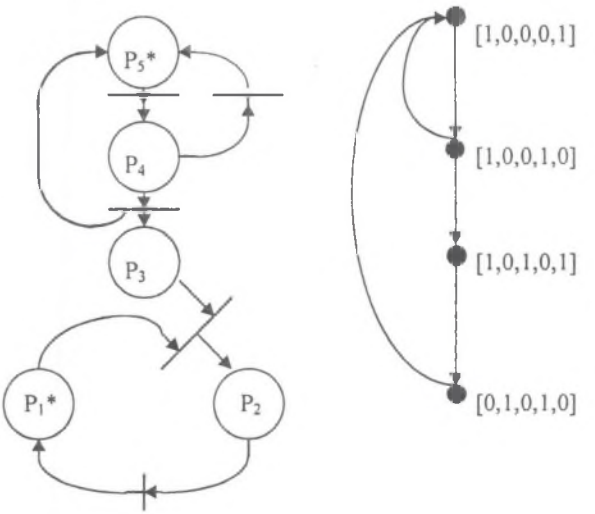
- w funkcjonowaniu systemu można wyróżnić trzy podstawowe procesy: informacyjny, decyzyjny i wykonawczy,
- pochłanianie znaczników przez sieć pozwala stwierdzić, że każdorazowe najechanie przez pojazd szynowy na odcinek zbliżania musi spowodować reakcję systemu w postaci procesu wykonawczego,
- sieć jest siecią zamkniętą (na podstawie analizy grafu znakowań osiągalnych).

Wykorzystując wnioski wypływające z analizy sieci stwierdzono, że:

- procesy informacyjne (wykrycie pojazdu szynowego na odcinku zbliżania i obliczenie czasu dojazdu pojazdu szynowego do przejazdu) są realizowane niezależnie,
- proces decyzyjny i wykonawczy (bez urządzeń wykonawczych zewnętrznych) może być wykonywany za pomocą mikroprocesora jednoukładowego.

Zredukowanie sieci Petriego dla urządzeń SSP umożliwiło (dla celów praktycznych) opracowanie nowej sieci współpracującej z otoczeniem, uwzględniającej ruch pojazdów szynowych na odcinku zbliżania. Na rys.2 pokazano tę sieć wraz z grafem znakowań osiągalnych. Miejsce P_1 w tej sieci reprezentuje warunki zachodzące podczas wykonywania procesów: zarządzającego, decyzyjnego, sterującego i kontrolnego. Miejsce P_2 odpowiada warunkom obsługi informacji nadchodzącej poprzez miejsce P_3 z procesu informacyjnego, miejsca P_4, P_5 odzwierciedlają sytuację ruchową na przejeździe i odcinkach zbliżania. Można zauważyć, że miejsca P_4, P_5 są generatorami znaczników, miejsca P_1 i P_2 pochłaniaczami znaczników, a miejsce P_3 przenosi znaczniki między procesem informacyjnym a procesami decyzyjno-wykonawczymi. Przedstawiony graf znakowań osiągalnych sieci warunków i zdarzeń charakteryzuje ją jako sieć żywą, aktywną, trwałą, trójograniczoną, bezpieczną i

zachowawczą - z jednym wyjątkiem, kiedy następuje przekazanie znacznika z procesu informacyjnego do pozostałych procesów. Przedstawiona sieć w wyniku przeprowadzonej analizy pozwala stwierdzić, że podczas działania dynamicznego (graf znakowań osiągalnych) nie występują w niej zakleszczenia, co oznacza, że układ przechodzi swobodnie do każdego z możliwych stanów.



Rys.2. Ogólna sieć Petriego oraz graf znakowań osiągalnych
Fig. 2. General Petrii net and graph of markings attainable

5. STRUKTURA SYSTEMU

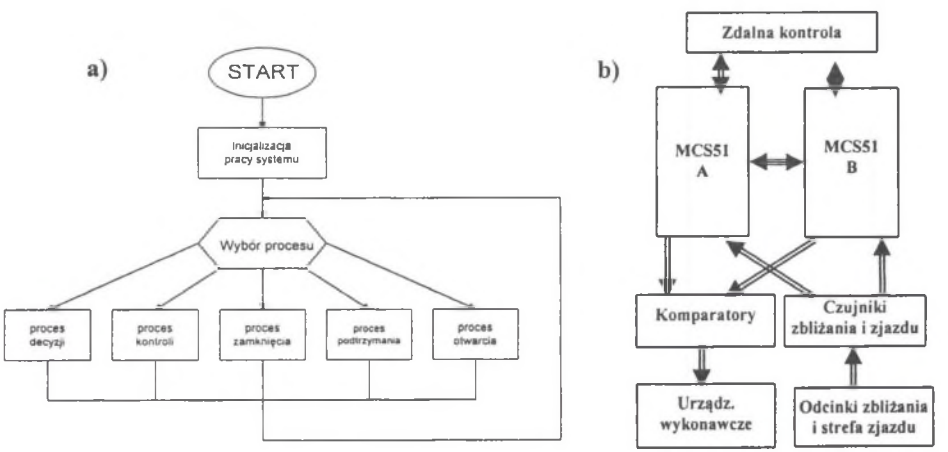
Omawiany system pomiarowo–sterujący dla urządzeń SSP został zrealizowany w technice mikroprocesorowej. Stosowanie takiej technologii dla aplikacji systemów do zastosowań krytycznych wymusiło na etapie specyfikacji, projektowania i budowy systemu uwzględnienie rozwiązań zapewniających wymagany stopień niezawodności i bezpieczeństwa. Zagadnienia niezawodności w zakresie mikroprocesorowych systemów pomiarowo – sterujących można rozpatrywać w dwóch aspektach:

- niezawodności urządzeń technicznych, tworzących infrastrukturę systemu pomiarowo – sterującego,
- niezawodności oprogramowania systemu.

5.1. Struktura sprzętowa systemu

W przypadku małych systemów pomiarowo – sterujących, do których można zaliczyć opracowany mikroprocesorowy system SSP, wymagane jest, by możliwa była detekcja każdego pojedynczego błędu, będącego efektem uszkodzenia infrastruktury systemu. W celu zrealizowania tego warunku przyjęto strukturę sprzętową systemu z „głosowaniem", pracującą w strukturze typu „k z n". W rzeczywistej aplikacji systemu zastosowano podwojoną strukturę sprzętową, zwaną jako „2 z 2", co pokazuje rys. 3b. W mikroprocesorowym systemie SSP można wyróżnić:

- 2 niezależne czujniki zbliżania się pojazdu szynowego i pomiaru czasu jego dojazdu do przejazdu,
- 2 niezależne czujniki stwierdzające opuszczenie strefy niebezpiecznej przez pojazd szynowy,
- 2 moduły decyzyjno-wykonawcze,
- urządzenia wykonawcze,
- bezpieczne komparatory sygnałów wyjściowych,
- komputer monitorujący (zdalnej kontroli).



Rys.3. a) Algorytm strukturalny układu decyzyjno–wykonawczego urządzeń SSP
b) Struktura sprzętowa systemu pomiarowo–sterującego dla SSP
Fig. 3. a) Algorithm of decision making and work system of devices SSP
b) The hardware structure of measurement–control system for SSP

Zastosowanie łącza transmisyjnego pomiędzy modułami decyzyjno–wykonawczymi pozwoliło zsynchronizować pracę obu kanałów oraz porównywać wewnętrzne, przejściowe, stany zmiennych i znaczników czasu. Zdublowano wszystkie wejścia i wyjścia, a sygnały

sterujące układami wykonawczymi urządzeń zewnętrznych generowane są przez bezpieczne komparatory. Zastosowana struktura sprzętowa pozwoliła również na zastosowanie zdalnej kontroli i sterowania systemu. Moduł decyzyjno–wykonawczy został zrealizowany na bazie struktury jednoukładowego mikroprocesora MCS 51. Zastosowano także niezbędne układy pośredniczące pomiędzy pozostałymi modułami systemu.

5.2. Struktura programowa systemu

Na podstawie sieci Petriego modelującej funkcjonowanie urządzeń SSP opracowano algorytm strukturalny modułu decyzyjno - wykonawczego. Przedstawia go rys. 3a. Algorytm ten obejmuje:

- moduł inicjalizacji pracy modułu decyzyjno-wykonawczego,
- moduł procesu decyzyjnego,
- moduł procesu zamykania,
- moduł procesu podtrzymania,
- moduł procesu otwierania,
- moduł procesu kontroli.

Po inicjalizacji pracy układu następuje wybór procesu do realizacji. Po zakończeniu jego realizacji następuje powrót do wyboru procesu. Następuje wtedy wybranie i realizacja następnego procesu. Sytuacja ta powtarza się cyklicznie. Przedstawiony algorytm pracuje w trybie jednozadaniowym. Może on być zatem wykonywany przez jeden mikroprocesor.
Każdy z modułów programowych został zrealizowany w asemblerze mikroprocesora MCS51. W celu zapewnienia wymaganej niezawodności systemu, przy stosowaniu struktury sprzętowej „2 z 2", każdy moduł decyzyjno – wykonawczy był oprogramowany przez niezależny zespół programistów. Podejście takie zmniejsza prawdopodobieństwo pojawienia się w oprogramowaniu błędów systematycznych.

6. WSKAŹNIKI NIEZAWODNOŚCIOWE SYSTEMU

Dla systemów pomiarowo – sterujących w zastosowaniach krytycznych istotne jest oszacowanie liczbowych wskaźników charakteryzujących poziom bezpieczeństwa. Podstawowym parametrem określającym poziom niezawodności i bezpieczeństwa jest intensywność uszkodzeń systemu. Procedura szacowania wskaźników niezawodnościowych i bezpieczeństwa zakłada dekompozycję systemu na struktury równoległo–szeregowe, złożone z podsystemów, modułów lub urządzeń. Analizę niezawodnościową opracowanego systemu SSP przeprowadzono z dokładnością do modułu i autonomicznych bloków funkcjonalnych. Zastosowano także uproszczony sposób prognozowania niezawodności, stosowany dla nowo

projektowanych systemów. Ogólne wyrażenie określające niezawodność urządzenia lub modułu ma postać:

$$\lambda_U = \sum_{i=1}^{N} N_i \lambda_i , \tag{1}$$

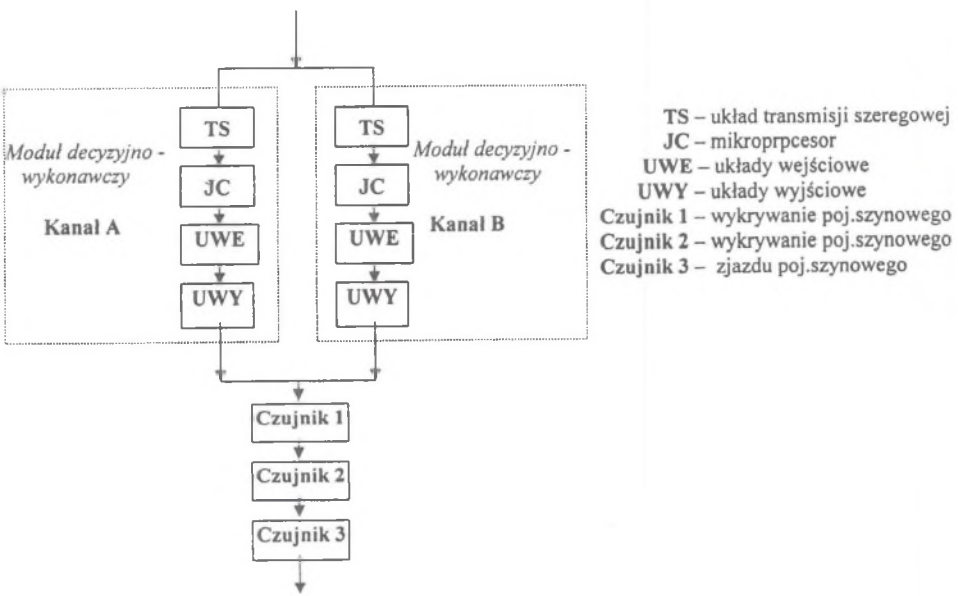
gdzie:

λ_U – współczynnik intensywności uszkodzeń modułu lub urządzenia,

N_i – ilość elementów i – tego typu,

λ_i – średnia intensywności uszkodzeń elementów i – tego typu.

Strukturę niezawodnościową systemu pokazano na rys. 4. Wyniki obliczeń współczynników intensywności uszkodzeń λ_U poszczególnych modułów systemu pokazano w tab. 1. Szacunkowa całkowita intensywność uszkodzeń λ systemu SSP wynosi 3.8 • 10-5 h^{-1}. W fazie eksploatacji mikroprocesorowy system pomiarowo–sterujący może się znaleźć w zbiorze stanów funkcjonalnych określanych jako stany niebezpieczne, zagrażające bezpieczeństwu. Bezpieczeństwo na poziomie systemu jest definiowane jako zdarzenie przeciwne do zdarzenia przebywania systemu w stanach niebezpiecznych.



Rys. 4. Struktura niezawodnościowa systemu SSP

Fig. 4. Reliability structures of measurement – control system for SSP

Tabela 1

Współczynniki intensywności uszkodzeń λ_U poszczególnych modułów urządzeń SSP

Lp.	Moduł	Intensywność uszkodzeń λ_U [h^{-1}]
1.	TS	$9.20 \cdot 10^{-6}$
2.	JC	$5.58 \cdot 10^{-6}$
3.	UWE	$6.58 \cdot 10^{-6}$
4.	UWY	$2.31 \cdot 10^{-6}$

Lp.	Moduł	Intensywność uszkodzeń λ_U [h^{-1}]
5.	CZUJNIK1	$3.58 \cdot 10^{-6}$
6.	CZUJNIK2	$3.58 \cdot 10^{-6}$
7.	CZUJNIK3	$3.61 \cdot 10^{-6}$

Przy założeniu, że suma zdarzeń przebywania systemu w stanach bezpiecznych i niebezpiecznych wyczerpuje cały zbiór zdarzeń, wartość bezpieczeństwa S określa wzór:

$$S = 1 - P_{NB} = 1 - \lim_{t \to \infty} \left\{ \sum_{i=1}^{n} P_i(t) \right\}, \tag{2}$$

gdzie :

P_{NB} – prawdopodobieństwo przebywania systemu w zbiorze stanów niebezpiecznych,

$P_i(t)$ –prawdopodobieństwo przebywania systemu w stanie zagrażającym bezpieczeństwu (niebezpiecznym).

Prawdopodobieństwo przebywania systemu w zbiorze stanów bezpiecznych, a zatem bezpieczeństwo S można określić w funkcji intensywności uszkodzeń λ oraz czasu reakcji t systemu na wykrycie błędu

$$S = 1 - (\lambda \cdot t). \tag{3}$$

Przyjmując że czas t reakcji systemu na wykrycie w nim błędu (uszkodzenia) wynosi 0,000278 s, a szacunkowa całkowita intensywność uszkodzeń λ opracowanego systemu SSP $3.8 \cdot 10^{-5}$, otrzymano wartość szacunkową prognozowanego bezpieczeństwa mikroprocesorowego systemu pomiarowo – sterującego urządzeń SSP na poziomie:

$$S = 1 - \frac{0,000278}{24572} \approx 1 - 1 \cdot 10^{-9} \tag{4}$$

Oprogramowanie jest niezwykle trudne do analizy niezawodnościowej ze względu na pozostałe po zakończeniu testowania błędy (logiczne, kompilacji i efektów ubocznych). W systemach sterowania można założyć istnienie jednego nie wykrytego błędu oprogramowania na 1000÷10.000 linii kodu źródłowego, w zależności od jakości:

- (kwalifikacji) zespołu programującego,

- posiadanego sprzętu komputerowego,
- posiadanego kompilatora i innych programów narzędziowych użytych do testowania i uruchamiania,
- procesu testowania.

Przyjmując, że ujawnienie błędu podczas normalnej eksploatacji programu może ujawnić się w granicach od 1 miesiąca do 1 roku, przyjęto, że szacunkowa intensywność uszkodzenia λ_S oprogramowania wynosi:

$$\lambda_S = \frac{\frac{n}{1000}}{0{,}083 \cdot 8760} \div \frac{\frac{n}{10000}}{1 \cdot 8760}, \tag{5}$$

gdzie:

n - jest liczbą linii programu.

Przy założeniu, że oprogramowanie modułów programowych wynosi ok. 1000 linii kodu źródłowego w asemblerze MCS51, szacunkowa intensywność uszkodzeń oprogramowania λ_S waha się w granicach $1.3\ 10^{-6} \div 1.1 \cdot 10^{-5}\ h^{-1}$

7. BADANIA SYSTEMU

Systemy pomiarowo–sterujące dla zastosowań krytycznych wymagają w czasie trwania, a w szczególności po zakończeniu każdego cyklu życia systemu, sprawdzenia zgodności parametrów funkcjonalnych i jakościowych systemu z parametrami założonymi w początkowej fazie cyklu życia systemu. Po zakończeniu fazy wytwarzania (budowy) należy przeprowadzić weryfikację parametrów wytworzonego (zbudowanego) systemu z parametrami założonymi we wstępnej fazie specyfikacji wymagań użytkownika.

Dla wykonanego mikroprocesorowego systemu urządzeń SSP opracowano program prób i badań laboratoryjnych. Założono, że należy przeprowadzić szczegółowo badania funkcjonalne. Badania i próby laboratoryjne zostały przeprowadzone z pozytywnym wynikiem. Podczas tych badań usunięto niedomagania programowe systemu. Dalszym etapem badań było opracowanie programu prób i badań terenowych. Miało to na celu zweryfikowanie posiadanych przez system parametrów funkcjonalnych i jakościowych w warunkach środowiskowych panujących w terenie. Badania te miały charakter krótkotrwały, a ich zakres uzupełniał zakres badań laboratoryjnych. Obecnie system jest poddawany takim próbom. Jeżeli wynik badań będzie pomyślny, to system będzie mógł przejść do fazy eksploatacji próbnej, która będzie trwać ok. 6 miesięcy. Ten okres czasu pozwoli ocenić zachowanie się systemu w warunkach środowiskowych panujących podczas różnych pór

roku. Jeżeli system uzyska pozytywną opinię z badań eksploatacyjnych, będzie mógł być stosowany powszechnie.

8. ZAKOŃCZENIE

Wykorzystanie mikroprocesorowych systemów pomiarowo–sterujących w zastosowaniach, w których wymagane jest zachowanie bezpieczeństwa funkcjonowania nadzorowanego procesu, wymaga stosowania specjalnych metod ich projektowania i budowy.

Na podstawie wymagań użytkownika oraz obowiązującego prawa i norm w obszarze, w którym zastosowano system pomiarowo–sterujący, działanie funkcjonalne mikroprocesorowego systemu pomiarowo–sterującego dla urządzeń SSP przedstawiono w postaci zbioru reguł **JEŻELI ... TO...** W celu uzyskania formalnego modelu działania systemu i dokonania jego syntezy konieczne było zamodelowanie działania systemu za pomocą Sieci Petriego.

Zapewnienie bezpiecznej pracy systemu, a więc zgodnej z przedstawionym modelem siecią Petriego, uzyskano dzięki dwukanałowej strukturze sprzętowej systemu. Porównywanie danych między kanałami zostało zrealizowane przez:

- wykorzystanie obwodu szynowego do pomiaru odległości pojazdu szynowego od przejazdu z wykorzystaniem dwóch niezależnych funkcji oddziaływania,
- porównywanie obliczonych czasów dojazdu,
- porównywanie danych pomiędzy modułami decyzyjno–wykonawczymi oraz wykorzystanie bezpiecznych komparatorów sygnałów wyjściowych.

Opracowanie szczegółowe systemu pomiarowo-sterującego przeznaczonego dla urządzeń samoczynnej sygnalizacji przejazdowej jest następstwem ogólnych rozważań teoretycznych dotyczących projektowania i budowy systemów komputerowych w zastosowaniach krytycznych z uwzględnieniem specyfiki określonego obszaru zastosowań i nie zawęża możliwości ich zastosowania również w wielu innych dziedzinach, jak np. w transporcie lotniczym, morskim, przemyśle zbrojeniowym, chemicznym itp. Należy jednak podkreślić, że szczególne wymagania stawiane komputerowo wspomaganym systemom pomiarowo-sterującym z przeznaczeniem do zastosowań krytycznych powodują, że systemy te winny być wyłącznie projektowane i wykonywane w specjalistycznych ośrodkach badawczych lub naukowych, w których zarówno wyposażenie aparaturowe, jak i wiedza przedmiotowa, doświadczenie i kwalifikacja kadry będą gwarantowały całkowitą wiarygodność ich późniejszego działania.

LITERATURA

1. Bartczak M.: Zasady kształtowania bezpieczeństwa systemów s.r.k wdrażanych na PKP. Materiały opracowane przez Biuro Fundacji na Rzecz Rozwoju Politechniki Warszawskiej, Warszawa 1996.

2. Górski J.: Bezpieczeństwo systemów komputerowych. Informatyka 9/1992.
3. Lewiński A., Perzyński T.: Nowe rozwiązania komputerów sterujących w systemach sterowania ruchem kolejowym na przykładzie SSP. Materiały konferencyjne „Transport w XXI wieku", Warszawa 2001,
4. Konopiński L., Lewiński A.: Metodyka przeprowadzania dowodu bezpieczeństwa komputerowych systemów srk wprowadzanych na kolejach polskich. Materiały konferencyjne „Transport w XXI wieku", Warszawa 2001,
5. Konopiński L., Lewiński A., Siergiejczyk M.: Prognozowanie niezawodności i bezpieczeństwa komputerowych systemów sterowania ruchem kolejowym. Przegląd Kolejowy 3/2000,
6. Mielnik R.: Petri Net as a tool for synthesis of microprocessor measurement-control system in critical applications. Materiały konferencyjne „Methods and Models in Automation and Robotics", Międzyzdroje 1995.
7. Mielnik R.: Sieć Petriego w syntezie systemu pomiarowo – sterującego w zastosowaniach krytycznych. Rozprawa doktorska, AGH,Kraków 1998,
8. Starke Peter H., Żurek J.: Sieci Petrii. Warszawa 1987.
9. Żurakowski E.: Systemy komputerowe w zastosowaniach związanych z bezpieczeństwem. Informatyka 3/1995,
10. Metody oceny niezawodności i bezpieczeństwa komputerowych systemów srk, zadanie 3. Biuro Konsultingowe Fundacji na rzecz Rozwoju Politechniki, Warszawa 1999.

Recenzent: Prof. dr hab. inż. Janusz Gajda

Wpłynęło do Redakcji dnia 1 grudnia 2001

Abstract

The design of modern microprocessor measurement-control systems applied to such fields as nuclear and power, chemical, metallurgical industries, air, sea and rail transport, military and telecommunications applications requires a special approach to the philosophy of design, manufacture and use of such systems. This follows from the fact that in case of damage or failure of the system the object or its surroundings might be exposed to danger, which could cause life loss and material waste. Therefore attention should be focused on safeguarding the required level of reliability and safety of working conditions of such systems. These two terms when referred to the applications mentioned above lead to the definition of reliability of computer systems in critical applications. Such systems are designed and produced after certain specifications which can be divided into four phases according to the cycle of microprocessor systems design: specification of tasks, software production, manufacture of hardware as well as verification and conformity confirmation of the whole system on an example of a microprocessor system for an automatic railway crossing signaling.