ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1978
Seria: AUTOMATYKA z. 45 Nr kol. 581

Andrzej Mencel, Marek Mokrosz, Jacek Wojciechowski

ZESTAW SPRZĘTOWO-PROGRAMOWY DLA PROCESÓW PRZEMYSŁOWYCH WYMAGAJĄCYCH PODWYŻSZONYCH PARAMETRÓW NIEZAWODNOŚCI NA PRZYKŁADZIE SYSTEMU KONTROLI RUCHU ZAŁOGI KOPALNI

Streszczenie: W referacie przedstawiono koncepcję konfiguracji systemu kontroli ruchu załogi kopalni. Koncepcja została opracowana na podstawie analizy cech obiektu i uwzględnienia wymagań podwyższonych parametrów niezawodnościowych kompleksu sprzętowo-programowego.

1. Wstęp

Etap projektowania współczesnych systemów informatycznych wymaga wnikliwej analizy procesu, ze szczególnym uwzględnieniem wagi zadań, jakie system przejmuje na siebie po okresie rozruchu. Mają one decydujący wpływ na wymagania niezawodnościowe, jakim system musi odpowiadać, a zatem i na jego strukturę.

Systemy informatyczne związane z bezpieczeństwem pracy ludzi muszą cechować podwyższone parametry niezawodnościowe. Dotyczy to szczególnie systemów instalowanych w kopalniach węgla kamiennego. Jednakże różnorodność wymagań w stosunku do systemu wynikająca ze specyfiki obiektów nie pozwala uogólniać wyników prac związanych z podwyższeniem niezawodności konktretnego systemu. Dlatego w dalszym ciągu referat poświęcony będzie oprogramowaniu i konfiguracji sprzętu informatycznego, spełniającego wymagania podwyższonej niezawodności dla wybranego typowego dyskretnego procesu, jakim jest kontrola ruchu załogi kopalni.

2. Analiza cech obiektu oraz określenie wymagań dla systemu kontroli ruchu załogi kopalni

Rodzaj oraz charakter sterowanego obiektu pozwala określić klasę i niezbędne elementy systemu sterowania. Dla omawianego systemu proces podlegający sterowaniu stanowią zjawiska związane z kontrolą ruchu załogi kopalni.

Podstawowym zadaniem systemu jest:

a. ewidencja czasu pracy całej załogi kopalni (dołowej i powierzchniowej) prowadzona wg rejestracji czasów wejść, zjazdów, wyjazdów z dołu i wyjść z kopalni w odniesieniu do całej załogi;
b. sporządzanie raportów (natychmiastowe na żądanie, zmianowe, dzienne, miesięczne, roczne, wydruki dla celów statystycznych i ewidencyjnych) w oparciu o stale uaktualnianą, bogatą bazę danych;

Cechy charakterystyczne obiektu to:

a. okresowe angażowanie systemu dla celów akwizycji danych,
b. jednorodny charakter informacji wejściowej w zakresie obsługi stref kontroli,
c. możliwość powtórnego wprowadzenia jednostkowej informacji wejściowej (potwierdzenie przyjęcia),
d. duże odległości między źródłem informacji a ośrodkiem jej przetwarzania,
e. duża ilość informacji związana z pracownikiem, konieczna do zapamiętania w systemie.

Pierwsza z cech wynika ze zmianowego charakteru pracy w kopalni. Dla wielozmianowego systemu pracy można wyróżnić w ciągu doby okresy, w których system będzie silnie obciążony obsługą stref kontroli pracowników. Przebieg obciążenia powtarza się cyklicznie z cyklem dobowym.
Jednorodny charakter informacji wejściowej upraszcza w dużym stopniu procedurę akwizycji danych. Cechy obiektu oraz funkcje systemu stanowią podstawę dla określenia wymagań, jakie system kontroli ruchu załogi powinien spełniać. Do wymagań tych należy zaliczyć:
a. ciągłą zdolność i sprawną obsługę pracowników w strefach kontroli,
b. dwukierunkową wymianę informacji ze strefami kontroli (potwierdzenie przyjęcia, dodatkowe informacje i polecenia dla rejestrującego się pracownika) przy stosunkowo dużych odległościach stref od ośrodka przetwarzania (ok. 5 km),
c. dostęp w każdej chwili do stale uaktualnianej dużej bazy danych na zasadzie raportowania (szczególnie w stanach zagrożeń BHP w kopalniach),
d. pełne zabezpieczenie bazy danych,
e. łatwość obsługi i konserwacji, czytelna forma raportów dostarczanych zainteresowanym komórkom administracji i zarządzania kopalni,
f. praktycznie niezawodna praca,
g. w przypadku wystąpienia uszkodzenia system powinna cechować łagodna degradacja [1] (ograniczenie funkcji na czas awarii lub łagodne wstrzymanie wszystkich funkcji dla uszkodzeń katastroficznych).

Na podstawie zadań i wymogów jakie powinien spełniać system SKRZ można zaszeregować go do systemów o działaniu bezpośrednim. Jest to system naprawialny, o długim czasie eksploatacji i o możliwości profilaktycznych przeglądów.

3. Ogólne metody podwyższania niezawodności systemów

Stosowane współcześnie metody podwyższania niezawodności systemów komputerowych dotyczą w głównej mierze samego sprzętu komputerowego. Z dwóch technik podwyższania niezawodności praktyka wykazała, że technika tolerowania uszkodzeń lepiej zdała egzamin zarówno pod względem ekonomicznym, jak i technicznych możliwości.
Podstawowymi metodami w zakresie tej techniki są metody nadmiarowe. Warunkiem skutecznego stosowania nadmiarowości w systemie komputerowym jest zachowanie właściwych proporcji każdej z trzech możliwych jej form:
- układowa (SNU, DNU)
- programowa (NP)
- czasowa (NCZ).

W zakresie układowej nadmiarowości złożonej rozróżnia się:
a. statyczną nadmiarowość układową (SNU)
b. dynamiczną nadmiarowość układową (DNU).

Cechą charakterystyczną SNU jest działanie "maskujące", ponieważ elementy nadmiarowe maskują fakt uszkodzenia elementu.
Metoda ta jest kosztowna ze względu na to, że każdy ważniejszy element systemu jest przynajmniej dublowany.
DNU charakteryzują dwa etapy postępowania. W pierwszym następuje wykrycie uszkodzenia, w drugim lokalizacja i jego usunięcie oraz odnowa systemu. W przeciwieństwie do SNU, DNU jest stosowana selektywnie. Podstawową zaletą metody DNU jest możliwość jej stosowania zarówno na poziomie elementarnych modułów, jak również na poziomie struktury systemu przy założeniu, że system posiada strukturę modularną. Metoda ta jest szczególnie wygodna przy projektowaniu systemu w oparciu o konkretny sprzęt komputerowy.
Nadmiarowość programowa (NP) obejmuje wszystkie dodatkowe programy, segmenty programowe, rozkazy i operacje mikroprogramowe, które są zbędne w systemie pracującym bez błędów operacyjnych. NP służy głównie do detekcji błędów lub procesu odnowy i najczęściej stosuje się ją w połączeniu z DNU.

Można wyróżnić kilka postaci NP:
a. wielokrotne pamiętanie newralgicznych programów i danych,
b. testy i programy diagnostyczne a także zabezpieczenie mikroprogramowe,
c. segmenty programowe w systemie operacyjnym, pozwalające na tolerowanie uszkodzeń w programach użytkowych.

Nowoczesny system komputerowy tolerujący uszkodzenia musi uwzględniać wszystkie wymienione formy NP.

Nadmiarowość czasowa (NCZ) polega na powtórzeniu lub weryfikacji operacji komputerowych na różnych poziomach: mikrooperacji, pojedynczych rozkazów, segmentów programowych lub całych programów. Używa się jej zazwyczaj w połączeniu z DNU lub NP. Podstawowe cele NCZ można określić następująco:
a. detekcja błędu przy pomocy powtórnego wykonania operacji lub weryfikacji rezultatu,
b. odnowa przez uruchomienie programu restartu lub ponowienie wykonania operacji po wykryciu błędu.

W systemach o działaniu bezpośrednim są ograniczone możliwości stosowania tej metody, wynikające z konieczności akwizycji danych na bieżąco. Powtórzenie dłuższej sekwencji programu może być równoznaczne z utratą informacji wejściowej.

Z praktyki stosowania systemów informatycznych do sterowania produkcją wynika, że najbardziej zawodnym ogniwem sprzętu informatycznego są urządzenia peryferyjne.

Aplikacja techniki tolerowania uszkodzeń do tych urządzeń powinna odbywać się w kilku etapach:
a. dobór odpowiednich urządzeń peryferyjnych,
b. określenie możliwej do wprowadzenia funkcjonalnej nadmiarowości w taki sposób, by funkcje uszkodzonego bloku mógł przejąć blok rezerwowy lub sam komputer,
c. opis algorytmiczny procedury ujawniania błędu i odnowy pod kontrolą komputera,
d. zaprojektowanie niezawodnego łącza pomiędzy urządzeniem zewnętrznym a kanałem we/wy komputera.

Ze względu na dużą zawodność urządzeń peryferyjnych prace nad ich ulepszaniem mają bardziej istotne znaczenie dla sprawności całego systemu niż zwiększanie niezawodności samego komputera.

Dla omawianego systemu kontroli ruchu załogi odnosi się to szczególnie do sprzętu specjalistycznego związanego z realizacją podstawowych zadań rejestracji czasu pracy.

4. Struktura środków aparaturowych systemu

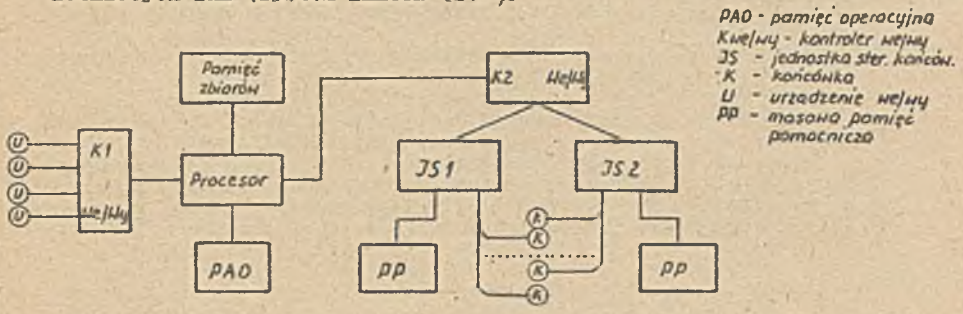
Wymagania stawiane systemowi kontroli ruchu załogi kopalni muszą znaleźć swoje odbicie w doborze odpowiedniej struktury środków aparaturowych. Przegląd możliwych do zastosowania konfiguracji sprzętowych rozpoczynamy od systemu jednomaszynowego.

Klasyczny układ, składający się z procesora, pamięci operacyjnej, pamięci zbiorów i systemu wejścia-wyjścia, jest rozwiązaniem najmniej przydatnym, ponieważ nie zapewnia:
- efektywnej protekcji danych wejściowych,
- zachowania minimum zdolności obliczeniowej, związanej z obsługą wejść i wyjść oraz bazy danych w sytuacjach krytycznych obiektu.

Dla zapewnienia ciągłej rejestracji danych napływających do systemu z końcówek (czytników dowodów kontrolnych) rozsianych na rozległym obszarze kopalni, system jednomaszynowy należy wyposażyć w co najmniej dwa wysunięte stałoprogramowe lub zmiennoprogramowe rejestratory (jednostki sterujące końcówek), zapisujące napływające informacje w pomocniczej pamięci masowej.

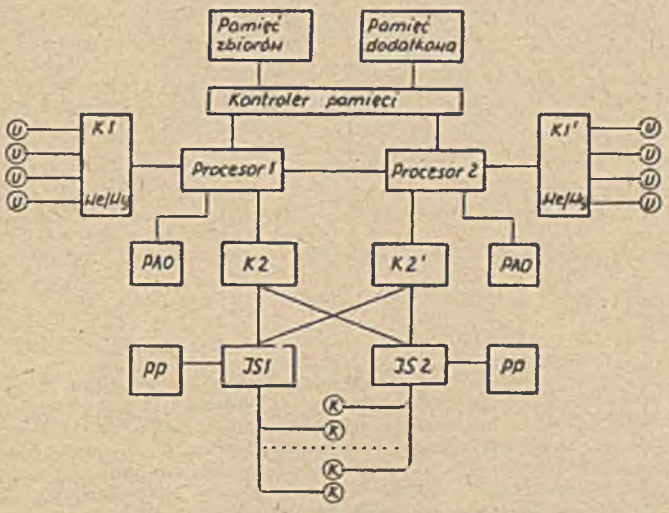
Końcówki są połączone z jednostkami sterującymi "w przeplocie", co oznacza, że jedna część końcówek znajdujących się w danej strefie kontroli połączona jest z jednostką nr 1, a druga część - z jednostką nr 2.

W przypadku awarii systemu komputerowego zachowana zostaje ciągłość rejestracji danych wejściowych, a dane zgromadzone w pamięciach pomocniczych mogą posłużyć do aktualizacji lub odtworzenia uszkodzonej bazy danych w pamięci zbiorów. Opisana konfiguracja została przedstawiona na rys. 1. Podobna koncepcja ochrony sieci danych wejściowych została sprawdzona w systemie rezerwacji miejsc brytyjskich linii lotniczych BEA (system BEACON [2]).



Rys. 1. System jednomaszynowy z nadmiarowymi wysuniętymi członami rejestrującymi

Po zabezpieczeniu w sposób opisany powyżej danych wejściowych należy wprowadzić do systemu dalszą nadmiarowość, pozwalającą uzyskać niezbędny minimalny poziom zdolności obliczeniowej dla obsługi bazy danych i raportowania w przypadku wystąpienia uszkodzeń urządzeń wchodzących w skład systemu komputerowego.
Jednym z najwcześniejszych rozwiązań tego typu jest system dwumaszynowy z częściowo wspólną pamięcią (rys.2).

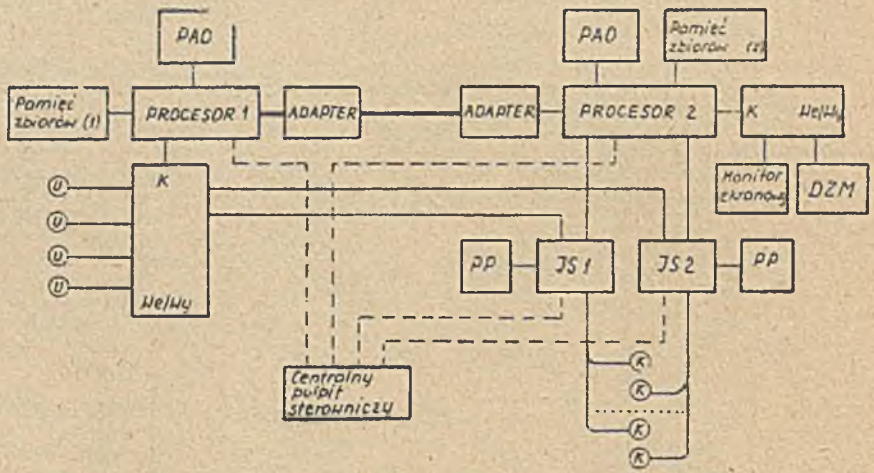


Rys. 2. System dwumaszynowy z częściowo wspólną pamięcią

W systemie można wyróżnić procesor komunikacyjny oraz procesor rezerwowy, przy czym jeden z nich wykonuje zadania związane z koordynacją. Informacje o stanie procesorów są nawzajem przekazywane przez szybkie łącze procesor-procesor, ale każdy z komputerów pracuje pod kontrolą własnego systemu operacyjnego. Obydwa procesory posiadają dostęp do pamięci zbiorów, w której przechowywana jest podstawowa baza danych systemu kontroli ruchu załogi. Przedstawione rozwiązanie posiada szereg wad, z których najważniejsze to:

- możliwość zniszczenia lub zablokowania bazy danych w niektórych, krytycznych momentach przełączania dostępu [3] ,
- słabe wykorzystanie zasobów sprzętowych systemu.
- trudności uzyskania dostępu do tablic (buforów) umieszczonych w pamięci operacyjnej komputera, który uległ awarii.

Ponieważ zapewnienie integralności bazy danych posiada decydujące znaczenie w systemach kontroli ruchu załogi autorzy proponują do realizacji inną konfigurację dwumaszynową, w której nie występuje przełączanie pamięci zbiorów (rys. 3).



Rys. 3. System dwumaszynowy z rezerwową bazą danych

Procesor 2 pełni rolę procesora komunikacyjnego, obsługującego dwie jednostki sterujące końcówek. Procesor 2 przesyła przez szybkie łącze procesor-procesor uporządkowane informacje otrzymane z końcówek do procesora 1, obsługującego główną pamięć zbiorów 1, w której są przechowywane i aktualizowane na bieżąco dane o pracownikach. Procesor 2 obsługuje rezerwową bazę danych, znajdującą się w pamięci zbiorów 2, w której przechowywane są tylko niektóre dane, mające kluczowe znaczenie dla systemu. Procesor 2 posiada rezerwę mocy obliczeniowej, pozwalającą na emisję najważniejszych z punktu widzenia bezpieczeństwa pracy raportów w przypadku awarii komputera głównego (np. sygnalizacja przebywania na dole kopalni powyżej określonego limitu czasowego).

W tym celu z procesorem 2 współpracuje monitor ekranowy i drukarka mozaikowa. W momencie wystąpienia awarii procesora komunikacyjnego procesor 1 przejmuje obsługę transakcji wejściowych, a jednostki sterujące J.S.1 i J.S.2 rejestrują dane z końcówek w pamięciach pomocniczych.

Dalsze zwiększenie współczynnika gotowości systemu, a także osiągnięcie lepszego wykorzystania zasobów aparaturowych (zwłaszcza urządzeń wejścia-wyjścia i pamięci operacyjnej) można uzyskać w systemach wieloprocesorowych, w których - zgodnie z definicją podaną w 4 - wszystkie procesory posiadające dostęp do wspólnej pamięci operacyjnej i pracują pod kontrolą zintegrowanego systemu operacyjnego.

Można rozróżnić trzy podstawowe typy wieloprocesorów [4] :

a) systemy ze wspólną szyną pracującą z rozdziałem czasowym,
b) systemy z matrycowym przełącznikiem,
c) systemy z wielowejściowymi pamięciami.

Stosunkowo prosty pod względem struktury sprzętowej system wieloprocesorowy dla potrzeb kontroli ruchu załogi można zrealizować wg modelu c . W przypadku systemu składającego się z dwu procesorów i dwu kontrolerów wejścia-wyjścia wymagane są pamięci o czterech wejściach, a więc o niewielkim jeszcze stopniu złożoności. Można sądzić, że taka struktura sprzętowa może okazać się korzystniejsza pod niektórymi względami od przedstawionej na rys. 3. Przykładem systemu wieloprocesorowego zrealizowanego według podanej zasady jest UNIVAC 1108, firmy Sperry Rand Corporation.

5. Wymagania w stosunku do oprogramowania zestawu.

Struktura systemu oprogramowania przedstawionego zestawu jest pochodną jego konfiguracji sprzętowej, realizowanych funkcji oraz wymagań specyfiki ruchowej systemu kontroli ruchu załogi.

Główną cechą struktury jest istnienie dwóch systemów operacyjnych o nieidentycznej budowie i funkcjach. Pierwszy z nich zlokalizowany w komputerze komunikacyjnym jest systemem operacyjnym specjalistycznym, o ograniczonych funkcjach, ukierunkowanym na obsługę specjalistycznych terminali systemu i umożliwiający dwustopniowe zapamiętanie treści transakcji. Realizacja funkcji rejestracji i informowania na bieżąco o stanie załogi na kopalni zmusza do przyjęcia struktury właściwej dla prac wykonywanych w czasie rzeczywistym w trybie bezpośrednim. Duża ilość transakcji do obsłużenia w określonych momentach czasowych narzuca ograniczony czas reakcji systemu, który stawia wysokie wymagania programowym modułom obsługi transakcji, które stanowią część składową obu systemów operacyjnych.
Drugi system operacyjny nadzorujący pracę komputera uniwersalnego jest rozbudowany w kierunku zarządzania obszerną bazą danych. Potrzeba ta wynika z prowadzenia przez system kontroli ruchu załogi ewidencji danych o pracowniku kopalni.
Konieczność wyposażenia obu systemów operacyjnych w mechanizmy umożliwiające szybką i bezbłędną odnowę bazy danych i stanu systemu po usunięciu awarii,wynika z ważności informacji o "historii" procesu rejestracji zjazdów i wyjazdów, znajomość której warunkuje możliwość określenia aktualnego obrazu stanu pracowników pod ziemią.
W celu organizacji współpracy międzykomputerowej systemy operacyjne wyposaża się w mechanizmy rozruchu i synchronizacji pracy zestawu, wymiany informacji użytkowej, wymiany informacji o stanie urządzeń, przełączania na pracę jednokomputerową w wypadku wykrycia usterek w drugim komputerze lub na zlecenie operatora, ponownego włączenia sprawnego komputera do zestawu, aktualizacja jego bazy danych oraz synchronizacja pracy bez naruszania ciągłości procesu rejestracji. Sygnały współpracy umożliwiają wymuszenie przez jeden system operacyjny przerwania pracy programów drugiego komputera, pozwalając w ten sposób na synchronizację realizacji programów obu komputerów.

Sygnały te są analizowane przez moduł nadzorujący wymianę informacji, inicjowany przez moduł obsługi przerwań.
Przed rozpoczęciem przesyłu informacji użytkowej następuje sprawdzenie stanu kanału współpracy. W tym celu przesyła się pewną liczbę stałych wzorcowych, które następnie są zwrotnie pobierane dla porównania z wartościami wyjściowymi. W przypadku niezgodności cykl się powtarza w celu stwierdzenia charakteru błędu. Błąd powtarzający się powoduje sygnalizację faktu uszkodzenia kanału wymiany oraz inicjację procedury przełączania procesu rejestracji na zestaw jednokomputerowy. Wykrycie stanu niesprawności kanału lub drugiego komputera następuje również w przypadku, gdy brak jest odpowiedzi na przepytanie w ciągu ustalonego odcinka czasu.
Drugim ważnym problemem oprogramowania zestawu jest koncepcja zbiorów danych systemu.
Organizacja bazy danych dla systemu kontroli ruchu załogi, który jest systemem o działaniu bezpośrednim, jest szczególnie ważna ze względu na jej pojemność, dynamiczny charakter i wrażliwość na awarie. Na bazę danych składa się szereg różnorodnych kartotek związanych z danymi podstawowymi o pracowniku, o miejscu i czasie jego pracy. Logiczna organizacja kartotek musi przede wszystkim zapewnić możliwość:
- odtwarzania bazy,
- ochrony przed niepożądanym dostępem,
- łatwego testowania poprawności aktualizowanych danych.

Baza danych jako integralna część zestawu o podwyższonej niezawodności wymaga specjalnych środków programowych i sprzętowych dla zabezpieczenia i odtworzenia jej zawartości na wypadek całkowitego lub częściowego zniszczenia. Muszą one uwzględniać konieczność zapewnienia bazie danych aktualności, kompletności i niesprzeczności oraz czasu odtwarzania narzuconego przez proces kontroli.
Położenie fizycznych nośników pamięci w strukturze prezentowanego zestawu oraz sposób ich aktualizacji wymaga cyklicznego porównywania obu zbiorów dla uniknięcia konfliktów logicznych wynikających z ich sprzeczności.
Ponieważ niezawodność pracy zestawu jest w znacznej mierze uzależniona od odporności oprogramowania na usterki sprzętu jak i samego oprogramowania, przy opracowywaniu jego struktury uwzględnia się technikę nadmiaru programowego i czasowego. Jednakże wielokrotne pamiętanie krytycznych programów i danych, rozbudowane testowanie i diagnostyka prawidłowości pracy programów jak i środki tolerancji usterek w egzekutorze powodują oprócz strat pamięci również narzuty czasowe na pracę systemu. Dlatego też zakres stosowanych środków zabezpieczenia programowego będzie kompromisem pomiędzy możliwościami sprzętowymi a wymaganiami obsługiwanego procesu.

6. Podsumowanie i wnioski

1. Dla realizacji systemu kontroli ruchu załogi kopalni proponuje się system dwumaszynowy z przełączanymi wejściami i rezerwową bazą danych. Zaproponowany układ spełnia wymogi stawiane systemowi kontroli ruchu załogi w zakresie protekcji podstawowej bazy danych i ochrony danych wejściowych.
2. Realizacja sprzętowa jest możliwa na bazie urządzeń krajowych (MERA-400, SMC-3).
3. Należy w dalszej perspektywie rozważyć bardziej szczegółowo możliwość realizacji systemu wieloprocesorowego (układ z wielowejściowymi pamięciami , co będzie się wiązało z dodatkowymi nakładami na adaptację dostępnego handlowo sprzętu (dotyczy głównie pamięci).

LITERATURA

[1] Avizenis A.: Architecture of fault-tolerant computing systems Mat. konferencji FTC 1975.

[2] Donald W. Davies, Derek L.A. Barber: Communication networks for computers, tłum rosyjskie, MIR, Moskwa 1976.

[3] Yourdon E.: Projektowanie systemów o działaniu bezpośrednim, WNT, Warszawa 1976.

[4] Philip H. Enslow: Multiprocessors and parallel processing, tłum. rosyjskie, MIR, Moskwa 1976.

НАБОР ОБОРУДОВАНИЯ И ПРОГРАММ ДЛЯ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ, ТРЕБУЮЩИХ ПОВЫШЕННЫХ ПОКАЗАТЕЛЕЙ НАДЁЖНОСТИ НА ПРИМЕРЕ СИСТЕМЫ КОНТРОЛЯ ДВИЖЕНИЯ РАБОЧЕГО СОСТАВА ШАХТЫ

Р е з ю м е

В работе дана концепция конфигурации системы контроля рабочего состава шахтн. Концепция была разработана на основе анализа свойств объекта при имеющихся повышенных требованиях к показателям комплекса оборудования и программ.

A HIGH-RELIABILITY HARDWARE-SOFTWARE SYSTEM FOR THE MANPOWER CONTROL IN COAL MINES

S u m m a r y

On the basis of a requirement analysis with regard to reliability of the hardware and softwere, a configuration for the manpower control system in coal mines is presented.