ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
Seria: ELEKTRYKA z. 164 Nr kol. 1409

Adrian HALINKA, Michał SZEWCZYK

KRYTERIA WARUNKUJĄCE PRAWIDŁOWĄ PRACĘ SYSTEMÓW ZABEZPIECZENIOWYCH ZŁOŻONYCH OBIEKTÓW ELEKTROENERGETYCZNYCH

Streszczenie. W artykule zostanie przedstawiona koncepcja inteligentnego systemu zarządzania funkcjami pomiarowymi, zabezpieczeniowymi i sterującymi oparta na strukturach sztucznych sieci neuronowych. Przyjęta struktura systemu pozwala przejąć podstawowe cechy ANN, takie jak szybkość przetwarzania dużej liczby danych (przetwarzanie równoległe), zdolność do uogólniania zdarzeń, mała wrażliwość na uszkodzenia poszczególnych elementów sieci. Zastosowanie sztucznych sieci neuronowych na poziomie przetwarzania podstawowego pozwala na wykorzystanie znacznie większej liczby sygnałów informujących o położeniu łączników w układzie, co zwiększa pewność prawidłowego odwzorowania aktualnej topologii układu.

PROPER POWER SYSTEM PROTECTION WORKING CRITERIA IN THE COMPLEX POWER SYSTEM UNITS

Summary. The paper presents a concept of an intelligent managing system overseeing measuring, protective and control functions, which is based on Artificial Neural Network (ANN) structures. The adopted structure of the system makes it possible to apply basic characteristics of ANN such as the speed at which a large amount of data is processed (parallel processing), the ability to generalize events, a negligible liability to damage of the constituent parts of the network. The application of ANN structures on the level of primary processing makes it possible to utilize a much bigger number of signals informing about the position of connectors within the system, which increases the reliability of the accurate representation of the system's topology.

1. WSTĘP

W elektroenergetyce istnieją obiekty o złożonej konfiguracji, rozumianej zarówno w sensie ilości i różnorodności urządzeń elektrycznych wchodzących w skład obiektu, jak i liczby zróżnicowanych konfiguracyjnie i funkcjonalnie trybów pracy obiektu.

Z punktu widzenia elektroenergetycznej automatyki zabezpieczeniowej możliwość kompleksowego (całościowego) zabezpieczenia złożonych obiektów pociąga za sobą konieczność zastosowania złożonych adaptacyjnych zespołów zabezpieczeniowych. Podstawowym zadaniem adaptacyjnych zespołów zabezpieczeniowych jest prawidłowa identyfikacja (logiczno-pomiarowa) aktualnego trybu pracy obiektu i na tej podstawie uaktywnianie odpowiedniej grupy funkcji zabezpieczeniowych przypisanych do tego stanu.

O skuteczności układów zabezpieczeniowych, określonej głównie poprzez poprawność generowanych decyzji klasyfikujących aktualny stan pracy zabezpieczanego obiektu do jednej z dwóch klas zdarzeń (stan pracy normalnej / stan zakłócenia), decyduje szereg wymogów, spośród których jako podstawowe należy wymienić: możliwość pozyskania i akwizycji dużej liczby informacji o zabezpieczanym obiekcie, prawidłową identyfikację aktualnego trybu pracy chronionego obiektu, szybkość przetwarzania danych i podejmowania decyzji, zdolności adaptowania swoich właściwości do aktualnego stanu pracy obiektu czy niewrażliwość na ogólnie pojęte „zakłócenia".

Wykorzystanie możliwości techniki cyfrowej pozwala na nowe podejście do zagadnień identyfikacji stanów chronionego obiektu i poprawnej adaptacji funkcji zabezpieczeniowych. Ilość i różnorodność pozyskiwanych informacji, możliwość ich przetwarzania z wykorzystaniem technik heurystycznych, szybkość przetwarzania danych, wstępna obróbka cyfrowa sygnałów pomiarowych, eliminująca m.in. składowe zakłócające, stanowią o zaletach techniki cyfrowej w złożonych układach zabezpieczeniowych [3]. Możliwość dostosowania się algorytmów pomiarowych, jak również algorytmów realizujących poszczególne funkcje zabezpieczeniowe do aktualnej częstotliwości (w stanach pracy obiektu charakteryzujących się zmienną w szerokich granicach częstotliwością sygnałów pomiarowych) oraz trybu pracy układu pozwala na uaktywnienie szeregu podstawowych funkcji zabezpieczeniowych (które w zespołach zabezpieczeń analogowych są blokowane), poprawiając tym samym jakość i skuteczność ochrony obiektu przed skutkami zakłóceń. Cyfrowe zespoły zabezpieczeniowe pozwalają na zwiększenie stopnia pewności prawidłowej identyfikacji stanów pracy układu wskutek możliwości korzystania z dodatkowych kryteriów zarówno pomiarowych, jak i logicznych czy też zastosowania nowych metod wykorzystujących elementy tzw. „sztucznej inteligencji", np. w postaci struktur sztucznych sieci neuronowych.

2. SYSTEM ZABEZPIECZENIOWY ZŁOŻONYCH OBIEKTÓW ELEKTROENERGETYCZNYCH

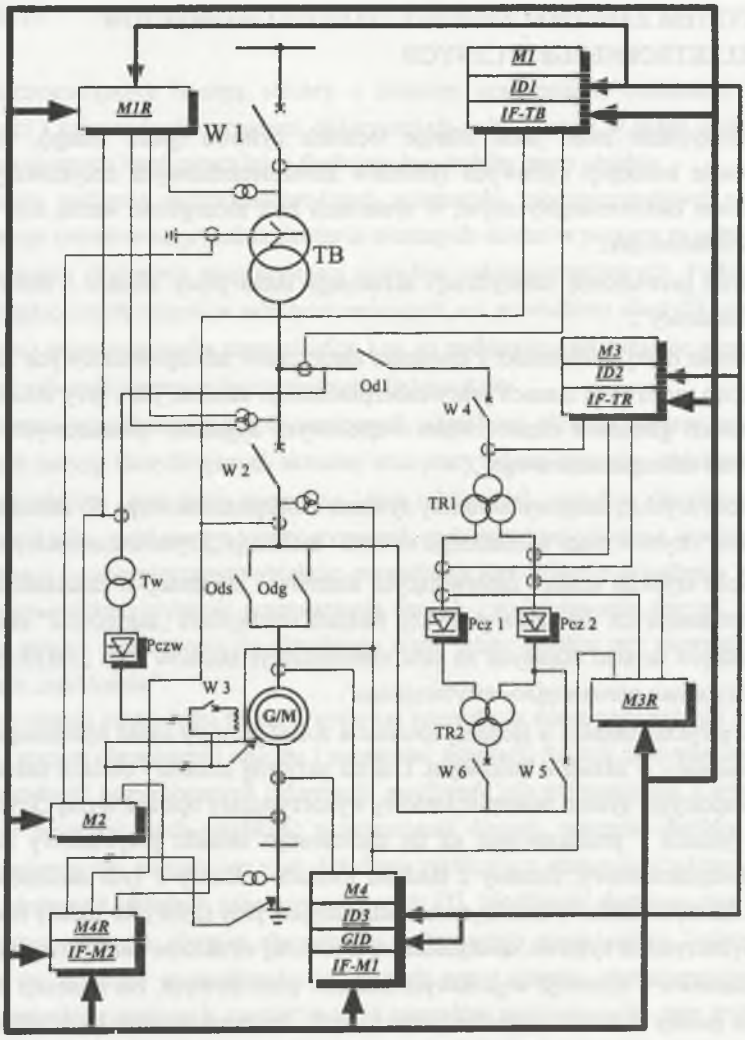
Wykorzystanie zalet, jakie oferuje technika cyfrowa (patrz wstęp), pozwala na sformułowanie koncepcji cyfrowych systemów zabezpieczeniowych dedykowanych złożonym obiektom elektroenergetycznym; w systemach tych szczególnie ważną rolę odgrywają takie ich własności, jak:

a) możliwość prawidłowej identyfikacji aktualnego stanu pracy obiektu - realizacja „kryterium struktury",
b) zapewnienie dużej dokładności i szybkości algorytmów zabezpieczeniowych zarówno we wszystkich możliwych stanach pracy zabezpieczanego obiektu, jak i przy zmieniającej się w szerokich granicach częstotliwości wejściowych sygnałów pomiarowych - realizacja „kryterium zabezpieczeniowego",
c) możliwość szybkiej adaptacji struktury systemu zabezpieczeniowego do zmieniających się warunków i trybów pracy chronionego obiektu - realizacja „kryterium adaptacyjnego",
d) możliwość szybkiej analizy napływających alarmów i informacji o zadziałaniach funkcji zabezpieczeniowych dla celów predykcji miejsca wystąpienia „zakłócenia" oraz podjęcia ewentualnych działań mających na celu minimalizację skutków tego „zakłócenia" -realizacja „kryterium prewencyjno-restytucyjnego".

Jako przykład obiektu o złożonej strukturze został przyjęty układ hydrozespołu odwracalnego pracujący w układzie blokowym. Dla tak przyjętej struktury obiektu został zaproponowany adaptacyjny system zabezpieczeniowy wykorzystujący opisane wyżej „kryteria".

Na rysunku 1 przedstawiono na tle chronionego obiektu przykładowy adaptacyjny system zabezpieczeniowy, złożony z siedmiu modułów. Każdy z tych modułów realizuje kryterium zabezpieczeniowe oraz kryterium adaptacyjne, przy czym jako układy realizujące te kryteria wykorzystano cyfrowe zabezpieczenia o otwartej strukturze konfiguracyjnej wyposażone standardowo w dziewięć wejściowych kanałów pomiarowych. Na ilustracji zaznaczono dodatkowo punkty pomiaru sygnałów wejściowych dla poszczególnych układów. Ponadto system wyposażony jest w trzy układy podstawowe (ID1, ID2, ID3) oraz jeden nadrzędny (GID), realizujące funkcje *kryterium struktury*. Do realizacji *kryterium prewencyjno-restytucyjnego* wykorzystano cztery układy analizy alarmów i predykcji miejsca wystąpienia zakłócenia o symbolu głównym IF....

Adaptacyjny system zabezpieczeniowy ze względu na złożoność obiektu został zdecentralizowany na moduły przypisane poszczególnym elementom obiektu. Decentralizacja pracy systemu zabezpieczeniowego na poszczególne moduły pozwala na rozbicie funkcji realizujących poszczególne kryteria zwiększając liczbę koniecznych procesorów, lecz wydatnie zmniejszając stopień ich obciążenia i czas koniecznych reakcji całego systemu na zmiany zachodzące w zabezpieczanym obiekcie.



Rys. 1. Adaptacyjny system zabezpieczeniowy hydrozespołu odwracalnego, gdzie:
ID1, ID2, ID3, GID - cyfrowy układ identyfikacji aktualnego trybu pracy,
M1, M1R, M2, M3, M3R, M4, M4R - układ realizujący kryterium zabezpieczeniowe i adaptacyjne,
IF-TB, IF-TR, IF-M1, IF-M2 - układ realizujący kryterium prewencyjno-restytucyjne

Fig. 1. Reverse hydro-generator adaptive protective system, where:
ID1, ID2, ID3, GID - digital current operation mode identification system,
M1, M1R, M2, M3, M3R, M4, M4R - modules which are responsible for protection and adaptation criteria,
IF-TB, IF-TR, IF-M1, IF-M2 - modules which are responsible for prevention and restitution criteria

Zbliżenie się modułów *"dedykowanych"* do wyróżnionych elementów chronionego obiektu zwiększa pewność i niezawodność akwizycji informacji; pomiędzy poszczególnymi modułami wymieniane są informacje już przetworzone, np. identyfikacja stanu pracy elementu obiektu chronionego, pozwalająca na zasadzie przewidywań na wstępną analizę trybu pracy całego układu zabezpieczanego. Zmniejszenie liczby operacji realizowanych przez procesory uzyskuje się również poprzez podział identyfikowanych stanów pracy na grupy i podgrupy aktywnych zabezpieczeń. W zależności od stopnia złożoności danego trybu pracy istnieje możliwość podziału danej grupy funkcji zabezpieczeniowych, np. poprzez *blok aktywacji* na podprzedziały definiowane na poziomie wypracowywania decyzji logicznych („kryterium struktury" - identyfikacja), jak i realizacji określonych funkcji zabezpieczeniowych za pomocą programowalnego planu funkcyjnego.

3. CYFROWY UKŁAD IDENTYFIKACJI AKTUALNEGO TRYBU PRACY ZABEZPIECZANEGO OBIEKTU

Dla zapewnienia prawidłowej pracy sytemu zabezpieczeniowego istotnym warunkiem jest prawidłowa identyfikacja trybów pracy zabezpieczanego obiektu na podstawie dostarczanych do systemu informacji (*kryterium struktury*). Przewiduje się trzy podstawowe grupy pozyskiwania informacji dla celów identyfikacyjnych [2]:

- za pomocą wejść logicznych odwzorowujących położenie wyłączników, odłączników i rozłączników w obrębie chronionego obiektu w ilości pozwalającej na jednoznaczne określenie aktualnej konfiguracji zabezpieczanego układu,
- wykorzystując wyniki pracy algorytmów pomiarowych, np. pomiaru napięcia, pomiaru aktualnej częstotliwości (w charakterystycznych punktach obiektu),
- poprzez wymianę informacji logicznych pomiędzy modułami wchodzących w skład systemu zabezpieczeniowego. Obiekt zabezpieczany został podzielony na kilka „układów elementarnych", w skład których wchodzi jedno lub grupa urządzeń (np. układ maszyny synchronicznej, układ transformatora blokowego). Każdy moduł identyfikuje poprzez logiczną lub logiczno-pomiarową informację o stanach położenia łączników aktualną konfigurację najbliższego mu „układu elementarnego" obiektu chronionego; pozwala to na podział identyfikacji stanu całego obiektu na poszczególne moduły funkcyjne, które w zależności od potrzeb wymieniają pomiędzy sobą informacje.

Obecnie zostaną przedstawione dwa przykładowe układy identyfikacji pracy układu zabezpieczanego: pierwszy oparty na doradczym systemie ekspertowym, drugi wykorzystujący struktury sztucznych sieci neuronowych. Jako obiekt zabezpieczany przyjęto hydrozespół odwracalny o konfiguracji przedstawionej na rysunku 1.

Pierwszy układ identyfikacji aktualnego trybu pracy zabezpieczanego obiektu bazuje na trzech *podstawowych jednostkach* identyfikacyjnych dedykowanych głównym urządzeniom

wchodzącym w skład obiektu. Poszczególne jednostki wykorzystują informacje w postaci sygnałów binarnych lub binarno-pomiarowych, dopiero na poziomie głównej jednostki identyfikacji (umieszczonej w module ***GID***) stosuje się doradczy system ekspertowy bazujący na regułach decyzyjnych.

Jednostki podstawowe oparte są na trzech głównych blokach logicznych:

- bloku wejściowym, w którym odbywa się wstępne sprawdzenie poprawności sygnałów wejściowych zawierających informacje o położeniu łączników,
- bloku zawierającym układy logiczne wiążące informacje z bloku wejściowego i dane z bloków wyjściowych sąsiednich jednostek podstawowych (opcjonalnie),
- bloku wyjściowym dokonującym wstępnego przyporządkowania danego „układu elementarnego" do jednego z identyfikowanych trybów pracy zabezpieczanego obiektu oraz komunikującym się z układem nadrzędnym (np. sterowania i zabezpieczeń stacji) i innymi jednostkami lub układami identyfikacji.

Jednostka podstawowa przypisana *transformatorowi blokowemu* wykorzystuje tylko informacje odwzorowujące aktualny stan łączników, nieodzowne do poprawnej identyfikacji czy to w postaci sygnałów dwustanowych, czy binarno-pomiarowych. Ze względu na pełnioną szczególną rolę transformatora blokowego jednostka dedykowana mu wypracowuje wstępną informację, z której korzystają pozostałe bloki. Jednostki dedykowane *układowi rozruchowemu* i *maszynie głównej* korzystają zarówno z informacji binarnych i binarno-pomiarowych o stanie łączników, z informacji z jednostki *transformatora blokowego*, jak i wymieniają informacje pomiędzy sobą. Dzięki temu uzyskuje się wzrastającą precyzję identyfikacji; coraz więcej informacji zostaje przetworzonych i wykorzystanych w celu podjęcia decyzji końcowej, tj. określenia aktualnego trybu pracy całego obiektu.

Główna jednostka identyfikacji korzysta z informacji wstępnie przetworzonych w jednostkach podstawowych, dedykowanych określonym „układom elementarnym" chronionego obiektu. Ponadto powinna wykorzystywać dodatkowe informacje, np. z systemu sterowania stacji o zaniku napięcia na sekcji, do której ma być przyłączony obiekt, z modułu sterowania i synchronizacji: z algorytmów pomiaru częstotliwości w celu określenia przedziału, w którym znajduje się aktualna częstotliwość sygnałów pomiarowych; informacje te stanowią istotną bazę dla podstawowych kryteriów identyfikacyjnych.

Jednostka główna identyfikacji oparta jest na systemie doradczym zdefiniowanym w oparciu o tzw. "reguły decyzyjne". Sprawdzane są odpowiednie relacje pomiędzy określonymi wejściami tej jednostki i w zależności od wyniku sprawdzenia podejmowane są dalsze decyzje mające na celu uzyskanie prawidłowej identyfikacji aktualnego stanu obiektu. Jednostka główna współpracuje bezpośrednio z blokiem aktywacji funkcji zabezpieczeniowych i komunikacji w celu wymiany danych i ewentualnych rozkazów sterujących dopasowaniem się funkcji zabezpieczeniowych do aktualnego trybu pracy chronionego obiektu (rys. 3).

Poszczególne zestawy aktywnych funkcji zabezpieczeniowych różnią się rodzajem zdefiniowanych funkcji, tj. rodzajem wielkości kryterialnych, wartościami wielkości kryterialnych i charakterystykami rozruchowymi [1].

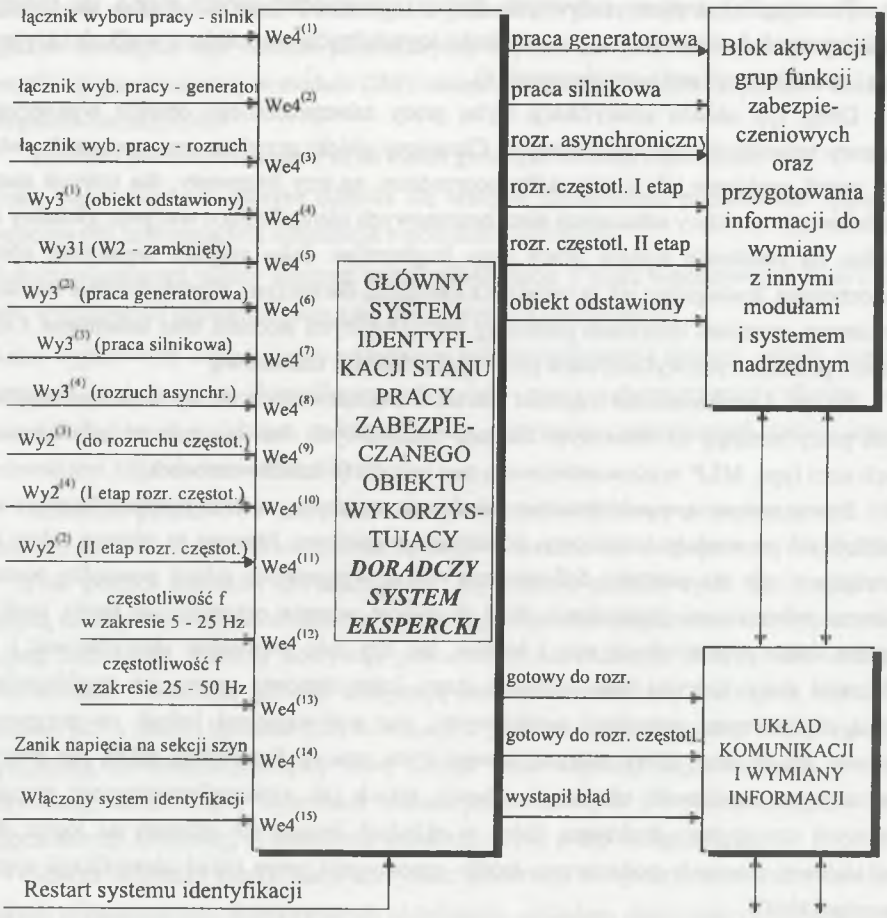
Drugi typ układu identyfikacji trybu pracy zabezpieczanego obiektu wykorzystuje struktury sztucznych sieci neuronowych. Chroniony obiekt przedstawiony na rys. 1 podzielony został, podobnie jak w przypadku poprzednim, na trzy fragmenty, dla których zostały zdefiniowanie struktury sztucznych sieci neuronowych identyfikujące wstępnie globalny stan obiektu na podstawie trybów pracy jego fragmentów. Jako sygnały wejściowe zostały wykorzystane, analogiczne jak w układzie z systemem doradczym, sygnały binarne i binarno-pomiarowe, wymiana informacji pomiędzy poszczególnymi sieciami oraz informacje z algorytmów pomiarowych wykorzystane przez nadrzędną sieć neuronową.

Na rys. 4 przedstawiono fragment schematu poglądowego struktury układu identyfikacji trybu pracy bazujący na sztucznych sieciach neuronowych. Jest to struktura jednokierunkowych sieci typu ***MLP*** wielowarstwowego perceptronu (o trzech warstwach).

Pewną nowością w porównaniu z układem poprzednim jest brak podziału każdej z sieci podrzędnych na moduły: wejściowy, powiązań i wyjściowy. Stanowi to główną zaletę tego rozwiązania - nie ma potrzeby definiowania wprost wzajemnych relacji pomiędzy poszczególnymi informacjami (sygnałami). Sieć w trakcie uczenia optymalizuje swoją strukturę poprzez dobór odpowiednich wag i biasów, tak aby móc poprawnie identyfikować i klasyfikować stany, którymi była uczona, i stany, które stanowią pewne ich uogólnienia, tj. różnią się pewnymi sygnałami wejściowymi, nie wpływającymi jednak na przyporządkowanie ich do innej klasy zdarzeń (innego trybu pracy). Szczególną zaletą tak przyjętej struktury jest możliwość eliminacji sytuacji, takich jak niekomplementarność sygnałów binarnych czy sygnały brakujące, które w układach bazujących głównie na logice dwuwartościowej stanowiły podstawowe źródło generowania przez układ identyfikacji sygnału „wystąpił błąd".

Dużego znaczenia w tak określonej strukturze układu identyfikacji nabiera problem odpowiedniego zdefiniowania bazy uczącej, pozwalający na uczenie sieci jak największą liczbą przypadków przynależnych do wszystkich możliwych klas zdarzeń - wszystkim możliwym trybom pracy zabezpieczanego obiektu.

W przypadku prezentowanego obiektu, jakim jest hydrozespół odwracalny pracujący w układzie blokowym, kolejne wywołanie opcji *"identyfikacja trybu pracy obiektu"* dokonywane jest co dwa lub trzy okresy podstawowej harmonicznej aktualnej częstotliwości w głównej jednostce identyfikacji, w przypadku któregokolwiek z rodzajów lub etapów rozruchu. Związane jest to z koniecznością aktywacji odpowiednich zespołów funkcji zabezpieczeniowych w zależności od aktualnej częstotliwości i trybu pracy obiektu. Konieczność wyposażenia systemu zabezpieczeniowego w oddzielne jednostki identyfikujące, zawierające własne, szybkie procesory i bufory pamięci jest podyktowana również dużą powtarzalnością i złożonością procesu identyfikacji.



Rys. 2. Główna jednostka identyfikacji trybu pracy zabezpieczanego obiektu oparta na "regułach decyzyjnych"

Fig. 2. The main module of the current operation mode identification unit based on the expert system

Dla trybów: praca generatorowa, praca silnikowa czy obiekt odstawiony powtarzalność identyfikacji może się odbywać w znacznie dłuższych przedziałach czasu, np. co 5 minut. Powtarzalność identyfikacji odbywa się we wszystkich jednostkach układu, jest ona zsynchronizowana poprzez moduł wyjściowy identyfikacji głównej i układ komunikacji systemu zabezpieczeniowego *"maszyny głównej"*.

Restart układu identyfikacji następuje natychmiastowo w przypadku stwierdzenia:

- pobudzenie lub zadziałanie aktywnej funkcji zabezpieczeniowej,
- stwierdzenie błędu przez jednostkę główną identyfikacji, bazującą na regułach decyzyjnych,

- pojawienie się informacji o wyłączeniu wyłącznika głównego układu W2, gdy poprzednio wyłącznik ten był załączony (wejście $W4^{(5)}$).

4. ADAPTACYJNY SYSTEM ZABEZPIECZENIOWY

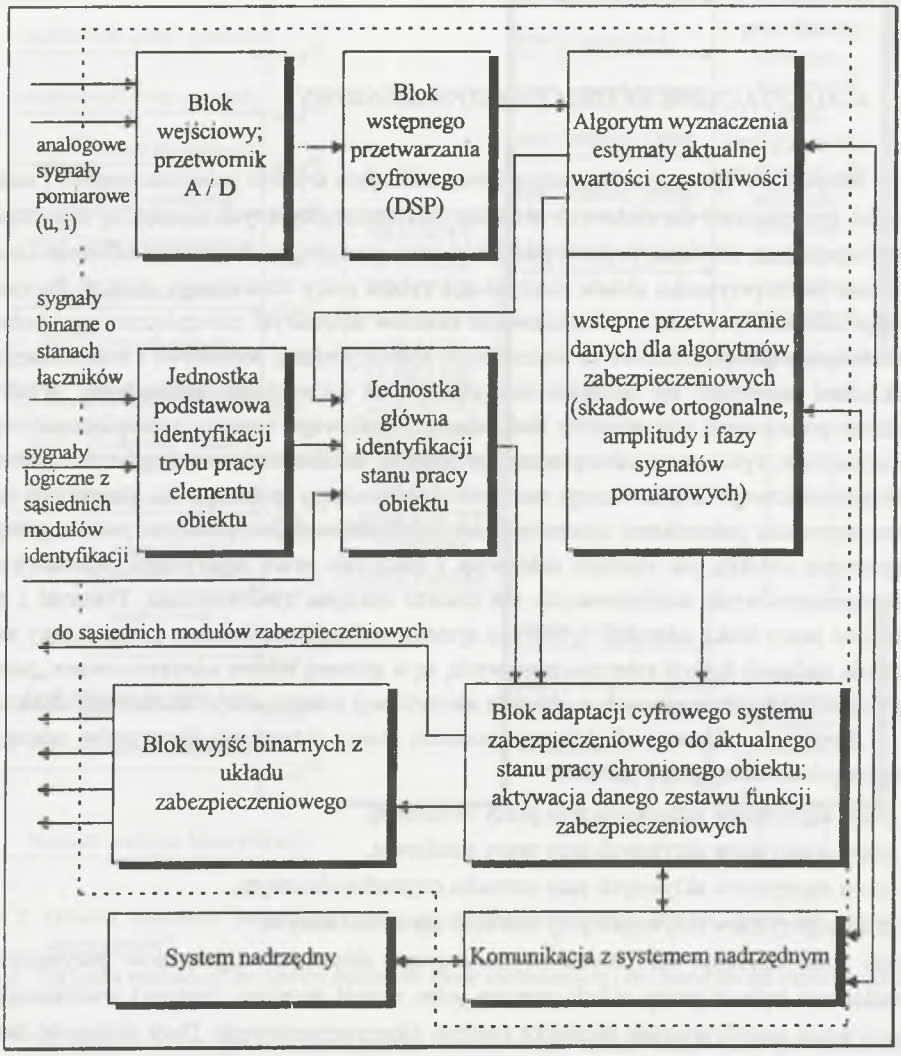
Adaptacyjne systemy zabezpieczeniowe, realizujące *kryteria zabezpieczeniowe* i *adaptacyjne*, przeznaczone dla złożonych obiektów elektroenergetycznych najczęściej mają strukturę rozproszoną, uzyskaną poprzez podział obiektu na mniejsze fragmenty zabezpieczane - podobnie jak w przypadku układu identyfikacji trybów pracy chronionego obiektu. Przyjęcie takiego założenia pozwala na sformułowanie układów automatyki zabezpieczeniowej pełniących funkcje zabezpieczeniowe (o własnościach adaptacyjnych), pomiarowe i komunikacyjne z układami sąsiednimi, np. układami identyfikacji, jak i z modułem nadrzędnym. W takim systemie podstawową rolę odgrywa blok adaptacji cyfrowego systemu zabezpieczeniowego do aktualnego trybu pracy zabezpieczanego obiektu, umieszczony we fragmencie systemu zabezpieczeniowego dedykowanego *maszynie synchronicznej* (patrz rys. 3). Stanowi on centrum sterowania jednostkami automatyki zabezpieczeniowej przypisanymi poszczególnym fragmentom obiektu, jak również uaktywnia i nadzoruje pracę algorytmów pomiarowych i zabezpieczeniowych zdefiniowanych dla obiektu *maszyna synchroniczna*. Pewność i poprawność pracy bloku adaptacji cyfrowego systemu zabezpieczeniowego, gwarantujący skuteczność realizacji funkcji zabezpieczeniowych, są w głównej mierze zdeterminowane „jakością" sygnałów wygenerowanych w układzie identyfikacji stanów pracy chronionego obiektu.

„Kryterium adaptacyjne" dokonuje podziału zbioru aktywnych algorytmów zabezpieczeniowych na cztery grupy główne:

* grupa algorytmów aktywnych przy pracy turbinowej,
* grupa algorytmów aktywnych przy pracy silnikowej,
* grupa algorytmów aktywnych przy rozruchu częstotliwościowym,
* grupa algorytmów aktywnych przy rozruchu asynchronicznym;

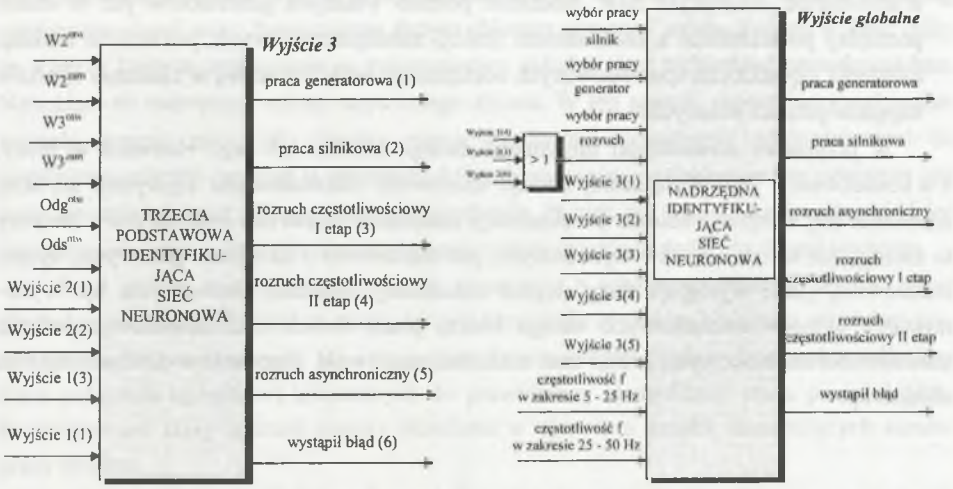
dzięki temu uzyskuje się łatwość wyboru grupy aktywnych algorytmów przypisanych określonemu trybowi pracy układu poprzez jeden sygnał sterujący (binarny) uruchamiający odpowiednio skonfigurowaną jednostkę systemu zabezpieczeniowego. Duża złożoność danego trybu pracy obiektu wymagająca sterowań aktywnymi funkcjami zabezpieczeniowymi w obrębie grupy pozwala na dalszą hierarchizację struktur funkcji zabezpieczeniowych, tworząc tzw. podgrupy.

Zastosowana w systemie technika cyfrowa umożliwia w dowolny sposób kształtowanie i adaptowanie charakterystyk rozruchowych i pomiarowych algorytmów realizujących złożone funkcje zabezpieczeniowe, uwzględniając np. różnice w konfiguracji elementów składowych chronionego obiektu.



Rys. 3. Schemat blokowy fragmentu cyfrowego systemu zabezpieczeniowego realizującego kryteria: struktury, zabezpieczeniowe i adaptacyjne dedykowany maszynie synchronicznej

Fig. 3. Scheme of the protective system dedicated to the synchronous machine



Rys. 4. Fragment układu identyfikującego stany pracy obiektu zabezpieczanego bazującego na sztucznych sieciach neuronowych typu MLP

Fig. 4. The part of current operation mode identification unit based on the artificial neural networks of the MLP type

5. ANALIZA ALARMÓW ORAZ LOKALIZACJA MIEJSCA ZAKŁÓCENIA DLA CELÓW AUTOMATYKI PREWENCYJNO-RESTYTUCYJNEJ

Istotna z punktu widzenia prawidłowej pracy zabezpieczanego obiektu jest również możliwość podejmowania przez system zabezpieczeniowy działań prewencyjnych (*kryterium prewencyjne*) w sytuacjach napływających alarmów o wystąpieniu zaburzeń w obiekcie lub w układach współpracujących z nim (utrata synchronizmu, odchyłki częstotliwości, przeciążenie prądowe, asymetria obciążenia, uszkodzenie w układach chłodzenia transformatorów). Celem tych działań jest próba utrzymania obiektu w pracy lub wydłużenia czasu jego pracy w warunkach zakłóceniowych poprzez ingerencje w działanie układów regulacji. Do działań tych należy zaliczyć m.in. [5]:

- obniżenie obciążenia obiektu mocą czynną i bierną,
- przejście z automatycznej na ręczną regulację napięcia w przypadkach alarmów o utracie wzbudzenia (przy zamkniętym wyłączniku odwzbudzania); istnieje duże prawdopodobieństwo uszkodzenia układu ARN,
- przejście na ręczną regulacje napięcia w sytuacjach pozyskania informacji o przeciążeniu prądowym wirnika, przewzbudzeniu; prawdopodobnie uszkodzeniu uległy ograniczniki w układzie ARN,

– uruchomienie automatyki SZR rozdzielni potrzeb własnych generatorów już w czasie pomiędzy pobudzeniem a zadziałaniem funkcji zabezpieczeniowych; pozwoli to uniknąć nałożenia się zakłóceń spowodowanych odciążeniem kotła i przerwą w zasilaniu silników napędów potrzeb własnych.

W przypadku niemożności utrzymania danego obiektu lub jego elementu w pracy, a w konsekwencji jego wyłączenia, istnieje możliwość sformułowania algorytmu szybkiej autonomicznej restytucji obiektu po eliminacji zakłócenia (*kryterium restytucyjne*). Dotyczy to szczególnie takich układów wytwórczych, jak elektrownie z turbinami gazowymi, hydroelektrownie, gdzie występuje duży stopień redundancji urządzeń pierwotnych, np. wykorzystanie układów rozruchowych innego bloku, praca dwóch hydrozespołów z jednym transformatorem blokowym, krótki czas rozruchu, możliwość ingerencji w sieć wewnętrzną obiektu itp.

6. UCZENIE I TESTOWANIE UKŁADU IDENTYFIKACJI TRYBU PRACY CHRONIONEGO OBIEKTU BAZUJĄCEGO NA STRUKTURZE ANN

Uczenie sieci neuronowej ma na celu znalezienie właściwego odwzorowania pomiędzy podawanymi na jej wejście sygnałami a oczekiwaną odpowiedzią sieci. Wynikiem procesu uczenia jest korekta wag i biasów poszczególnych neuronów sieci w stosunku do ich wartości początkowych [6].

W przeprowadzonych symulacjach zastosowano metodę uczenia z nauczycielem. Układy identyfikacji trybu pracy zostały zbudowane w oparciu o struktury wielowarstwowego perceptronu (MLP), a jako algorytm aktualizacji wag wybrano algorytm wstecznej propagacji błędów. Przyjęto, że każda z sieci neuronowych będzie miała strukturę trójwarstwową, gdyż tylko taka struktura umożliwia rozwiązanie dowolnego problemu nieliniowego. Założono, że w pierwszej warstwie będzie się znajdować 15 neuronów, w drugiej 10. Ilość neuronów trzeciej warstwy będzie równa ilości wyjść danego modułu układu identyfikacyjnego. Jako funkcję aktywacji pierwszej i drugiej warstwy wykorzystano tangens hiperboliczny; dla trzeciej warstwy funkcją aktywacji jest funkcja liniowa.

W procesie uczenia sieci neuronowej istotna jest kolejność prezentacji wzorców uczących. Należy unikać sytuacji, kiedy prezentowane są wszystkie wzorce jednej klasy, później następnej itd., ponieważ sieć „zapomina" wzorce wcześniej zapamiętane. Niebezpieczna jest również sytuacja, w której ilość wzorców należących do jednej klasy zdarzeń znacznie się różni od ilości wzorców należących do pozostałych klas. Sytuacja taka. powoduje „ukierunkowanie" sieci na rozpoznawanie klasy zawierającej największą ilość wzorców. Prowadzi to w efekcie do zatracenia przez sieć zdolności generalizacji (czyli zdolności do rozpoznawania wzorców nie podawanych w trakcie uczenia, ale należących do jednej z założonych klas zdarzeń). Może dojść również do sytuacji, w której „przeuczenie" sieci jedną

klasą spowoduje, że inne wzorce (nawet te, którymi sieć była uczona) nie zostaną przez nią rozpoznane. Jeżeli więc dysponujemy dużym zbiorem uczącym, należy z niego wybrać tylko te wzorce, których wystąpienie w rzeczywistym układzie jest najbardziej prawdopodobne. Natomiast do testowania należy użyć całego zbioru. W ten sposób zapewniamy optymalne warunki uczenia sieci, jak również mamy możliwość sprawdzenia zdolności sieci do uogólniania zdarzeń (testując ją wzorcami, których wystąpienie w układzie rzeczywistym jest mało prawdopodobne). W przypadku stwierdzenia, iż sieć nie jest w stanie odpowiedzieć poprawnie na wzorce, którymi nie była uczona, należy wzorce te dodać do zbioru uczącego.

Baza ucząca została wygenerowana w oparciu o analizę możliwych stanów pracy chronionego obiektu. Analiza ta miała na celu określenie sygnałów będących wynikiem pracy algorytmów pomiarowych, jak i sygnałów dwustanowych (będących odzwierciedleniem stanu położenia łączników) koniecznych do prawidłowej identyfikacji stanu pracy obiektu. Rozpoznawane klasy zdarzeń zostały określone w oparciu o analizę następujących stanów pracy obiektu:

- stany pracy „normalnej" (rozruch częstotliwościowy, rozruch asynchroniczny, praca silnikowa, praca generatorowa, kompensator synchroniczny),
- praca w układzie „redundancji", np. rozruch częstotliwościowy maszyny z wykorzystaniem układu rozruchowego maszyny sąsiedniej,
- stany „awaryjne" (np. odstawienie obiektu lub jego elementu, uszkodzenie styków pomocniczych łączników wykorzystywanych do odwzorowania struktury pracy obiektu).

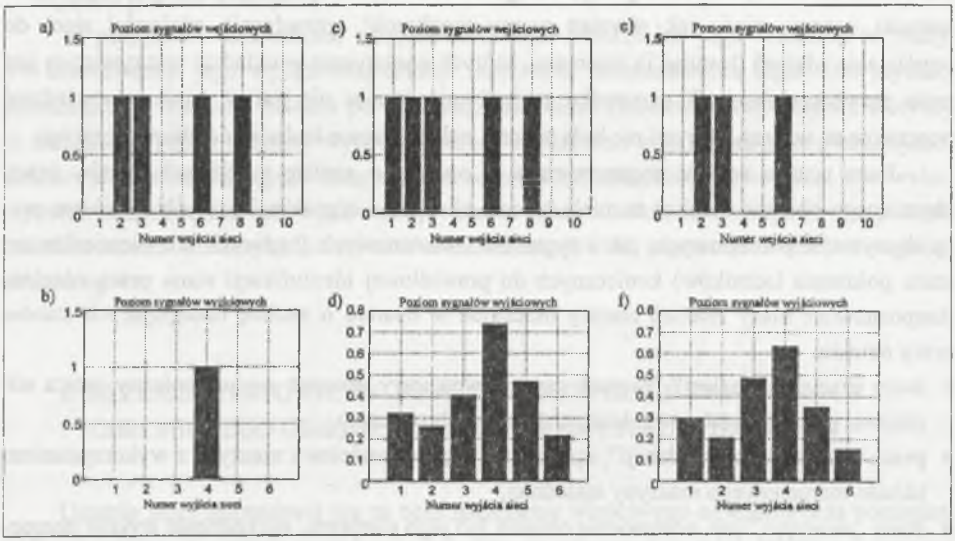
Generalnie, wzorce znajdujące się w bazie wiedzy uczącej podzielono na dwie grupy:

- grupę zawierającą sygnały niosące informację o tym, że obiekt znajduje się w danym trybie pracy,
- grupę sygnałów niosących informację „wystąpił błąd".

W procesie uczenia przyjęto zasadę prezentowania tych klas „na przemian" (najpierw wzorzec niosący informacje o danym trybie pracy obiektu, potem wzorzec niosący informację „wystąpił błąd"). Uwzględniono przy tym różnorodność trybów pracy (praca generatorowa, praca silnikowa, rozruch asynchroniczny, itd.), założono jednak, że część wzorców nie będzie podawana na wejście sieci neuronowej w celu sprawdzenia zdolności generalizowania zdarzeń przez nauczoną sieć.

Ważnym czynnikiem w procesie uczenia jest prawidłowe ustawienie wag początkowych. W przypadku programu MATLAB z pakietem Neural Network ustawienie wag początkowych realizowane jest przez polecenie *initff*. Polecenie to generuje początkowe wagi i biasy sieci korzystając z pierwszego wzorca bazy wiedzy uczącej. Ze względu na to, że algorytm wstecznej propagacji błędów nie gwarantuje znalezienia globalnego minimum funkcji w przestrzeni wag, gdy funkcja charakteryzuje się bogatą topologią, konieczne było podanie losowych sygnałów wejściowych, pochodzących jednak z zakresu, jakie one w rzeczywistości przyjmują (początkowy wektor wejściowy jest wprowadzany przez użytkownika programu). Proces uczenia przy pomocy algorytmu propagacji wstecznej opiera się na

metodzie największego spadku, która nie posiada zdolności wyznaczania minimum globalnego. W przypadku kiedy osiąga się optimum lokalne, proces uczenia należy powtórzyć.



Rys. 5. Odpowiedzi trzeciej sieci identyfikującej b), d), f) na poprawną a) i błędną c), e) sekwencję sygnałów wejściowych

Fig. 5. Responses of the third identification net b), d), f) to the signals with (c),e)) or without (a)) errors

Na rysunku 5 zaprezentowano przykładowe wyniki testów identyfikacji pośredniej realizowanej przez „trzecią identyfikującą sieć neuronową" (patrz rys.4). Przedstawiono trzy przypadki:

- pierwszy - na wejścia sieci neuronowej zostaje podana poprawna sekwencja sygnałów odwzorowująca drugi etap rozruchu częstotliwościowego zabezpieczanej maszyny (rys. 5a); najsilniejszy sygnał odpowiedzi sieci uzyskuje się na wyjściu czwartym, odpowiedzialnym za identyfikację drugiego etapu rozruchu częstotliwościowego (rys. 5b),
- drugi - sekwencja sygnałów wejściowych zawierała błąd (wystąpiła niekomplementarność sygnałów odwzorowujących położenia głównego wyłącznika generatora W2, rys. 5c); w tym przypadku również najsilniejszy sygnał generowany jest na wyjściu czwartym sieci (rys. 5d); pomimo błędnej informacji wejściowej przeprowadzona przez sieć neuronową identyfikacja jest poprawna,
- trzeci - sekwencja sygnałów wejściowych zawierała błąd (brak sygnału z innej jednostki rys. 5e). W tym przypadku również najsilniejszy sygnał generowany jest na wyjściu czwartym sieci (rys. 5f); pomimo błędnej informacji wejściowej przeprowadzona przez sieć neuronową identyfikacja jest poprawna.

7. ZAKOŃCZENIE

Przedstawiony system zabezpieczeniowy w sposób globalny pełni funkcje zabezpieczeniowe, pomiarowe, adaptacyjne i identyfikujące tryb pracy obiektu poprzez sieć wzajemnych powiązań pomiędzy modułami, które dedykowane są poszczególnym fragmentom chronionego obiektu. Sformułowanie dla takich systemów zabezpieczeniowych czterech podstawowych kryteriów, tj.: zabezpieczeniowego, adaptacyjnego, struktury i prewencyjno-restytucyjnego, znacznie rozszerza ich zakres i możliwości. Systemy te, bazując na inteligentnych układach identyfikacji, są w stanie automatycznie dostosować swoje funkcje pomiarowe i zabezpieczeniowe do zmieniających się warunków pracy chronionego obiektu - rozumianych w sensie zmiany powiązań poszczególnych elementów obiektu, jak i w sensie zmian parametrów charakteryzujących wejściowe wielkości pomiarowe (częstotliwość). Systemy te dedykowane są przede wszystkim układom wytwórczym o dużym stopniu redundancji urządzeń pierwotnych. Do układów takich zalicza się elektrownie kombinowane z turbinami parowymi oraz gazowymi [4], układy hydrozespołów odwracalnych, gdzie istnieje możliwość łatwego zastąpienia jednego urządzenia pierwotnego innym, ponadto układy te stanowią szybie źródła regulacji mocy, charakteryzują się również krótkim czasem rozruchu oraz złożoną strukturą. Własności te pozwalają na opracowanie autonomicznych algorytmów adaptacyjnej automatyki prewencyjno-restytucyjnej.

LITERATURA

1. Halinka A., Winkler W., Witek B.: Adaptive relaying for gas-turbine driven and hydro-turbine generators. Proceedings of the American Power Conference, vol. 59 - II, 59th Annual Meeting 1997, Chicago, p. 728-733.
2. Sowa P., Halinka A., Witek B., Szewczyk M.: Identification methods of complex power system units operation mode. French-Polish Seminar 98, Villeurbanne, France, 27-9 April 1998, pp. 21-26.
3. Kezunovic M.: Future requirements for digital substation control and protection systems. Workshop proceedings „Substation Automation Feedback and Trends", 21 March 1997, Paris.
4. Buck D.: Das elektrische System von ABB - Kombikraftwerken. ABB Technik 2/1995, s.15-23.
5. Cholewa S.: Możliwości modyfikacji sposobów impulsowania elektrycznych zabezpieczeń generatorów i bloków generator - transformator. „Automatyka Elektroenergetyczna", 3-4 1997, s. 12-16.
6. Osowski, S.: Sieci neuronowe, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 1994.

Recenzent: Dr hab. inż. Janusz Szafran, prof. Politechniki Wrocławskiej

Wpłynęło do Redakcji dn. 15 czerwca 1998 r.

Abstract

Generators of the type of top-load power plants equipped with reversible hydro-generators or so called "combined generating sets", which are a combination of traditional generating sets with steam turbines or generators with gas-turbine driven generators are becoming more and more important in the present structure of Electrical Power Systems (EPS). Such units, due to their specific properties, can become fast power-regulation units as well as power reserves in power-deficiency periods within the system. The structure of units of this kind is characterised by both complex configuration and a variety of operation modes (e.g. generator operation mode, motor operation mode and asynchronous start-up), for which groups of active algorithms responsible for protective functions must be established and their parameters provided. The need to employ adaptive protective automation in such systems is determined by two basic conditions:

- the change in frequency of current and voltage signals in certain areas of the protected unit. Thus, for example during a frequency start-up, signals of this kind become the primary source of data for measuring, protective and control functions,
- the changes in the configuration of particular units which constitute the protected unit and which are dictated by an operation mode, utilization conditions (overhauls or repairs of the basic systems), faults (full redundancy of start-up systems).

Designing a system which would identify in a global way the current condition of the whole of the unit and not merely the condition of its components is a basic condition for an appropriate configuration and activation both of the sets of measuring and protective algorithms and of control-regulatory ones in complex generating units. The units which have been used to date are characterised by a small amount and variety of the signals indispensable for such identification. The signals used nowadays are mostly binary signals which inform about the state of main switches (isolating switches and circuit-breakers). Information obtained in this way is frequently insufficient to work out an accurate decision about the state of the unit. Information is often falsified for example due to the incompatibility of the signals indicating the position of switches, missing data or the lack of other criteria which would verify the binary signals (utilizing information from measuring algorithms). Apart from that, the rules governing the processing of such signals are strictly determined. All these factors influence the accuracy with which the current state of the unit is identified, and, consequently, they influence the accurate functioning of main groups of algorithms, that is measuring, protective and control algorithms.

Identification system of the operation mode, which is one of the components of the intelligent managing system, as proposed in this paper, is made up of three basic modules dedicated to particular components of the unit (machine, unit transformer, start-up system -all of which should be based on their own processor) as well as of the main unit responsible for the global decision.

The other basic component of the intelligent managing system is a system identifying a spot of disturbance. Similarly to the identification system, it has a modular, ANN-based diffused structure. The system's modules are dedicated to the following components of the unit:

- machine with an excitation unit,
- transformer unit,
- frequency start-up unit.

Due to the large number of the places of potential disturbance, it was necessary to introduce three indirect networks whose outputs are simultaneously inputs of the main network

responsible for the final decision. The input signals of the system identifying a place of disturbance are the data from the protective systems, the identification system data concerning the last configuration of the unit, and additionally, the binary signals indicating the position of the switches.