Marcin Bednarek
Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki, Katedra Informatyki i Automatyki

Tadeusz Dąbrowski
Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych

Lesław Będkowski
Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych

DIAGNOZOWANIE BEZPIECZNOŚCIOWE SYSTEMU KIEROWCA - SAMOCHÓD

Streszczenie: W pracy przedstawiono rozważania dotyczące diagnozowania w aspekcie bezpiecznościowym systemu kierowca-samochód-otoczenie. Scharakteryzowano zagadnienie diagnozowania eksploatacyjnego i diagnozowania projektowego tego systemu. Przeanalizowano właściwości diagnozowania sekwencyjnego i priorytetowanego inicjowanego przez system diagnozujący oraz diagnozowania inicjowanego przez dozorowane podsystemy samochodu z adresowaniem urządzeń lub komunikatów. Podano przykład zastosowania autorskich koncepcji organizacji komunikacji z użyciem magistrali CAN.
Słowa kluczowe: system transportu danych, sieć przemysłowa, system antropotechniczny, diagnozowanie systemu kierowca-samochód, magistrala CAN

1. DIAGNOZOWANIE BEZPIECZNOŚCIOWE

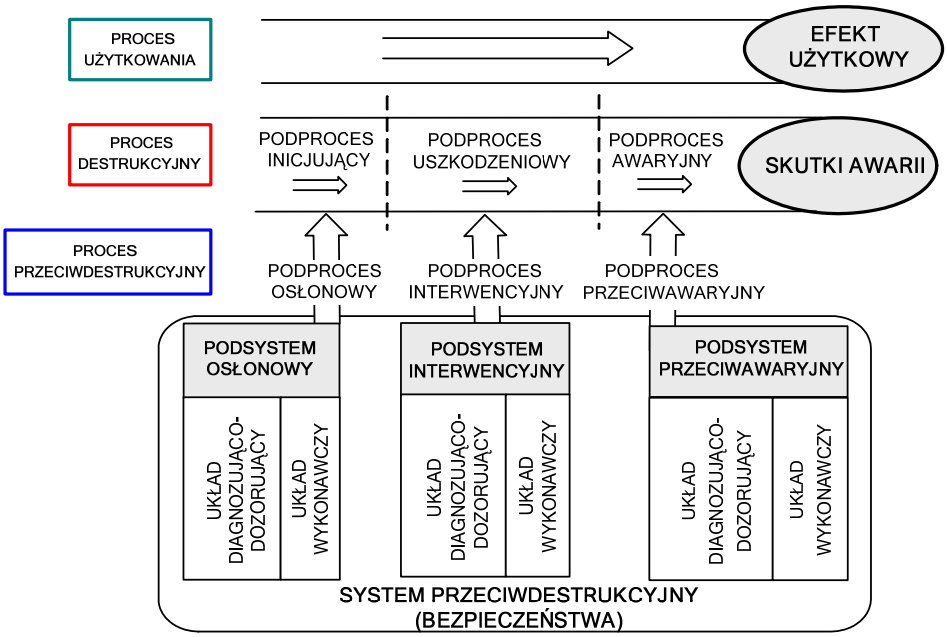
Proces diagnozowania jest zwykle postrzegany jako łańcuch działań prowadzący do powstania diagnozy stanu technicznego (i/lub funkcjonalnego) przedmiotowego obiektu zainteresowania [1]. W przypadku takiego systemu antropotechnicznego (SAT) jakim jest system Kierowca-Samochód-Otoczenie (K-S-O), niezwykle istotny jest proces dozorowania stanu tego systemu w aspekcie bezpiecznościowym tj. pod względem właściwości systemu zapewniających utrzymanie w stanie bezpieczeństwa wszystkich elementów systemu – a zwłaszcza znajdujących się w nim ludzi.

Użytkowanie systemu K-S-O można interpretować jako trójproces [2], na który składają się podprocesy (rys.1):

- użytkowania; proces ten ukierunkowany jest na zrealizowanie transportowego zadania użytkowego, polegającego np. na przemieszczeniu określonego ładunku między określonymi miejscami, w określonym czasie;

- destrukcyjny; proces ten wynika z fizycznej natury systemu K-S-O i polega na degradacji właściwości elementów systemu oraz relacji między nimi; końcowym efektem tego procesu jest stan niezdatności systemu – często o charakterze rozległej awarii lub katastrofy;

- przeciwdestrukcyjny; proces ten realizowany jest przez system bezpieczeństwa i obejmuje: pozyskiwanie informacji o stanie właściwości elementów systemu oraz wszelkie działania terapeutyczne ukierunkowane na przeciwdziałanie procesom destrukcyjnym.



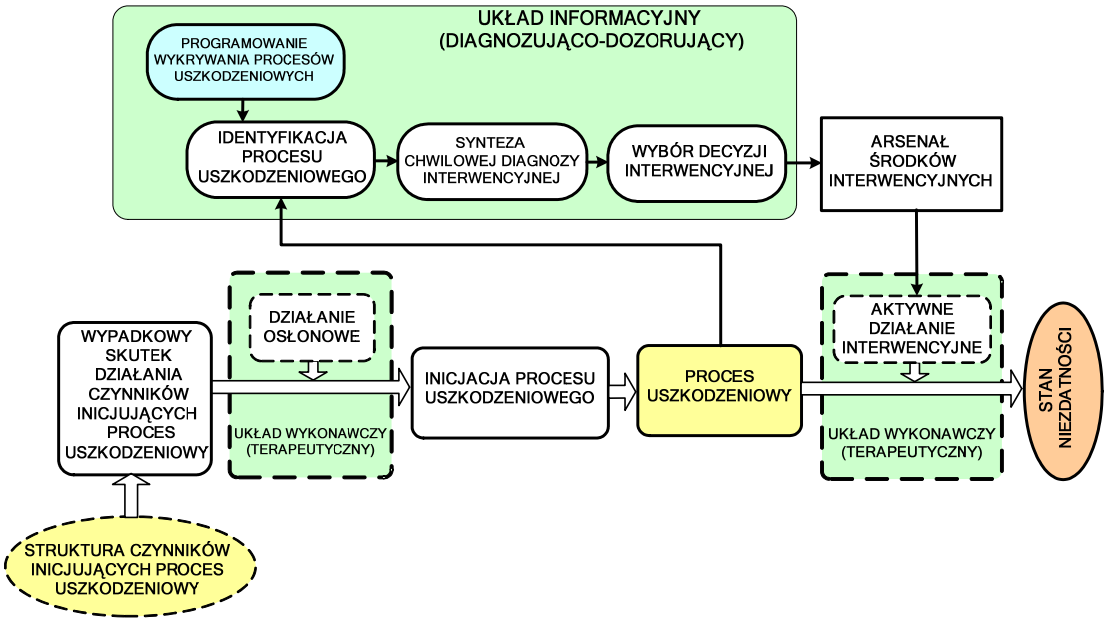
Rys. 1. Trójwarstwowy model procesu eksploatacji systemu K-S-O

Proces przeciwdestrukcyjny realizowany jest przez elementy systemu przeciwdestrukcyjnego, będącego swoistym systemem bezpieczeństwa w systemie K-S-O.

W procesie destrukcyjnym można wyróżnić charakterystyczne fazy: inicjującą, uszkodzeniową i awaryjną. Zasadnicza różnica między nimi polega na zaawansowaniu i intensywności procesu destrukcyjnego. Najbardziej pożądane – z punktu widzenia bezpieczeństwa systemu – jest blokowanie czynników inicjujących destrukcję. Działanie takie realizuje podsystem osłonowy. Jeśli mimo aktywności tego podsystemu pojawia się proces uszkodzeniowy, to zareagować na ten fakt powinien podsystem interwencyjny. Pożądanym efektem tego działania jest przerwanie (albo przynajmniej spowolnienie) procesu uszkodzeniowego. W przypadku, gdy mimo podejmowanych interwencji, proces uszkodzeniowy przybiera rozmiar awarii lub katastrofy, uruchamiany jest podsystem przeciwawaryjny (ratunkowy), którego zadaniem jest ograniczenie skutków katastrofy i ochrona zdrowia oraz życia ludzi znajdujących się w systemie K-S-O.

Jak łatwo zauważyć, poszczególne podsystemy systemu bezpieczeństwa mogą realizować przypisane im zadania jedynie w przypadku pozyskania odpowiednich informacji o stanie procesu użytkowania oraz o stanie ewentualnego procesu destrukcyjnego. Informacji tych muszą dostarczać układy diagnozująco-dozorujące w poszczególnych podsystemach systemu przeciwdestrukcyjnego. Efektywność działania układów i procedur pozyskiwania informacji decyduje w zasadniczym stopniu o skuteczności systemu bezpieczeństwa.

Strukturę i zadania układu diagnozująco-dozorującego na przykładzie podsystemu interwencyjnego ilustruje rys.2.



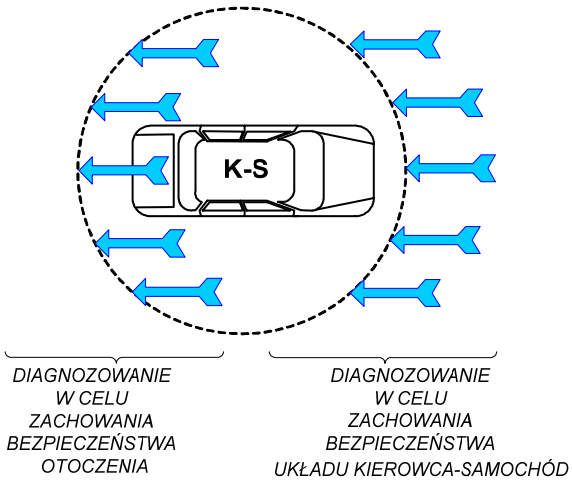
Rys.2. Model struktury podsystemu interwencyjnego

Stan bezpieczeństwa systemu kierowca-samochód-otoczenie należy rozumieć jako stan charakteryzujący się brakiem zagrożenia katastrofą [1]. Diagnozowanie i wnioskowanie bezpiecznościowe należy prowadzić dwukierunkowo, tak by efektem były diagnozy odnośnie (rys. 3):

- bezpieczeństwa układu kierowca-samochód; bezpieczeństwo to warunkowane jest utrzymaniem stanu zdatności układu „atakowanego” czynnikami wewnętrznymi i zewnętrznymi, sprzyjającymi przechodzeniu w stan niezdatności (a tym samym w stan niebezpieczeństwa);
- bezpieczeństwa otoczenia (np. innych uczestników ruchu); bezpieczeństwo to zależy od stanu układu kierowca-samochód oraz od stanu relacji samochód-otoczenie.

Zauważmy, że w celu utrzymania systemu kierowca-samochód-otoczenie w stanie bezpieczeństwa niezbędne jest pozyskiwanie informacji diagnostycznych o stanach technicznych i funkcjonalnych (oraz o istotnych zmianach tych stanów) licznego zbioru podsystemów pojazdu oraz o stanie psychomotorycznym kierowcy i stanie bliskiego otoczenia pojazdu. Rozwój elektroniki i technik informacyjnych umożliwia obecnie

dozorowanie stanu szeregu podzespołów sterujących pracą silnika, układu napędowego, hamulcowego, systemów wspomagających funkcje kierowcy i wielu innych [4]. Proces diagnozowania opiera się na informacjach pochodzących z rozproszonych terytorialnie urządzeń pojazdu. Coraz powszechniejsze jest sterowanie oraz testowanie układów pojazdu za pośrednictwem specjalizowanej sieci komputerowej. Sieć taka charakteryzuje się cechami sieci przemysłowej [5]. Najważniejszym parametrem tej sieci jest dostatecznie krótki i stały czas przesyłu danych pomiędzy współpracującymi podsystemami pojazdu. Determinizm czasowy oznacza znaną a'priori zwłokę dozorowania.



Rys. 3. Kierunki diagnozowania bezpiecznościowego w systemie K-S-O

Rozpatrzmy zatem proces diagnozowania bezpiecznościowego w kontekście wpływu różnych procedur przesyłu danych w magistrali komunikacyjnej pojazdu na czas pozyskania informacji diagnostycznych. Opóźnienia czasowe w otrzymywaniu tych informacji mają istotne znaczenie dla skuteczności działania mechanizmów terapeutycznych zapewniających bezpieczeństwo układu kierowca-samochód. Poniżej rozpatruje się to zagadnienie w aspekcie diagnozowania eksploatacyjnego (głównie użytkowego) oraz diagnozowania projektowego.

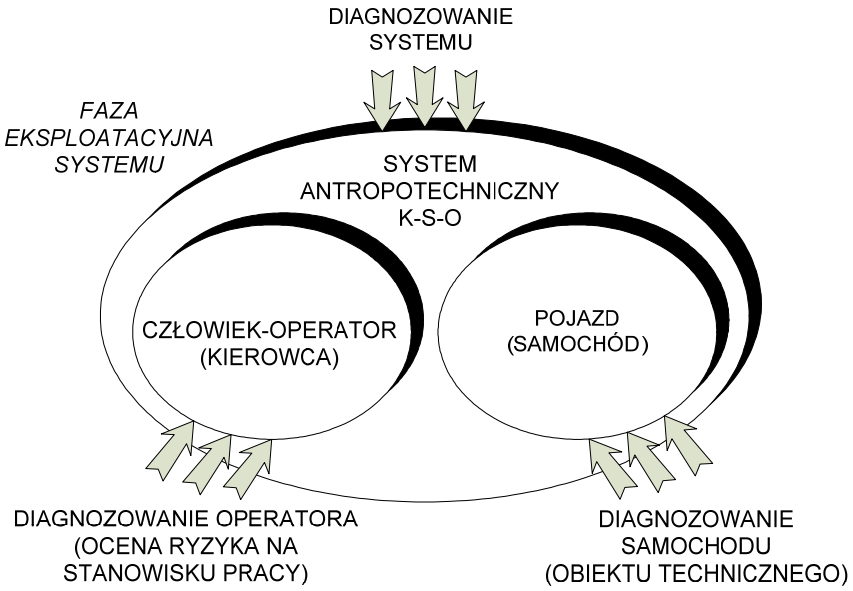
1.1. Diagnozowanie eksploatacyjne

W fazie eksploatacji systemu antropotechnicznego K-S-O można mówić o dwuwątkowym diagnozowaniu bezpiecznościowym (rys. 4).

Pierwszym wątkiem jest diagnozowanie obiektu technicznego jakim jest samochód, a co za tym idzie – podsystemów pojazdu odpowiedzialnych za bezpieczeństwo. Proces diagnostyczny ma głównie na celu informowanie pozostałych podsystemów pojazdu oraz kierowcę-operatora o zmianach stanu diagnozowanego układu (tj. o zmianach wartości zmiennej diagnostycznej transmitowanej magistralą komunikacyjną).

Drugim wątkiem rozpatrywanym w kontekście bezpieczeństwa systemu jest bezpiecznościowe diagnozowanie operatora-kierowcy oraz związana z tym ocena poziomu bezpieczeństwa. W celu oceny bezpieczeństwa kierowcy wskazane jest przeprowadzanie

analizy ryzyka związanego z wykonywaną przez niego funkcją. Polega ona na oszacowaniu oraz ewentualnej akceptacji wspomnianego ryzyka [6]. To postępowanie może być analogiczne do procedury oceny ryzyka na stanowisku pracy, stosowanej przez specjalistów z dziedziny BHP [7].

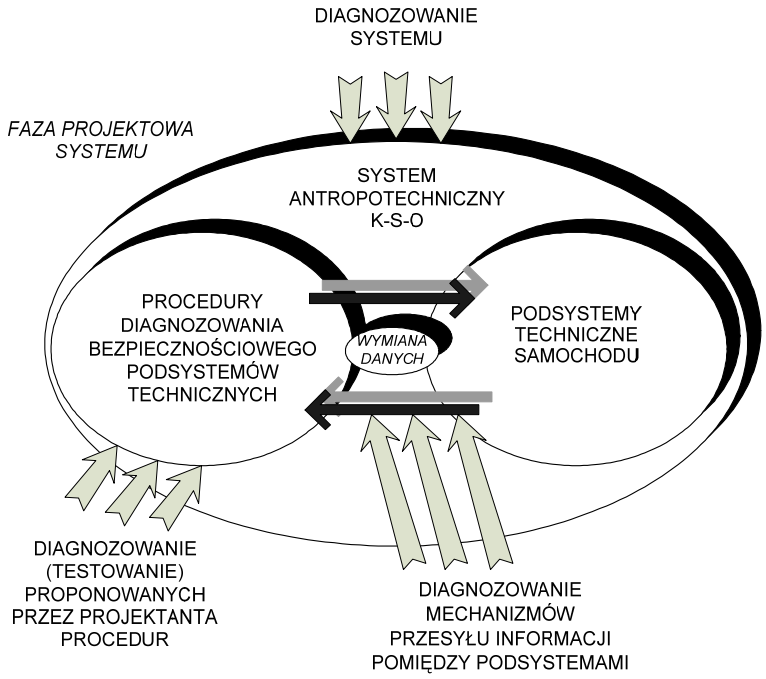


Rys. 4. Diagnozowanie eksploatacyjne systemu K-S-O

1.2. Diagnozowanie projektowe

Jak wspomniano wcześniej, diagnozowanie bezpiecznościowe systemu K-S-O realizowane jest w oparciu o informacje diagnostyczne przesyłane w postaci komunikatów. Komunikaty są transmitowane magistralą komunikacyjną pojazdu. Obecnie nawet samochody klasy popularnej wyposażone są w takie magistrale. Zamiast oddzielnych przewodów dla każdego sygnału przesyła się dane przy pomocy standardowych protokołów komunikacyjnych dwoma (CAN), lub nawet jednym sygnałowym przewodem (LIN) [9]. Sprzyja to oszczędnościom dotyczącym liczby zastosowanych połączeń. Dzięki temu można znacznie ograniczyć długość przewodów łączących podsystemy pojazdu (w samochodzie klasy popularnej łączna długość przewodów osiąga kilkanaście setek metrów [9]). Korzyść związana ze wspomnianą oszczędnością materiałową okupiona jest niestety problemami związanymi z wielodostępem do magistrali oraz z ewentualnymi kolizjami równocześnie nadających urządzeń. Procedury diagnozowania bezpiecznościowego powinny wykorzystywać takie mechanizmy dostępu do warstwy łącza danych sieci komunikacyjnej, które umożliwiają (sprzyjają) systemom terapeutycznym utrzymanie pojazdu w stanie zdatności.

Bezpiecznościowe diagnozowanie projektowe pozwala na (rys. 5):
- przetestowanie mechanizmów przesyłu danych pomiędzy podsystemami połączonymi magistralą komunikacyjną;
- przetestowanie proponowanych przez projektanta procedur diagnostycznych.



Rys. 5. Diagnozowanie projektowe systemu K-S-O

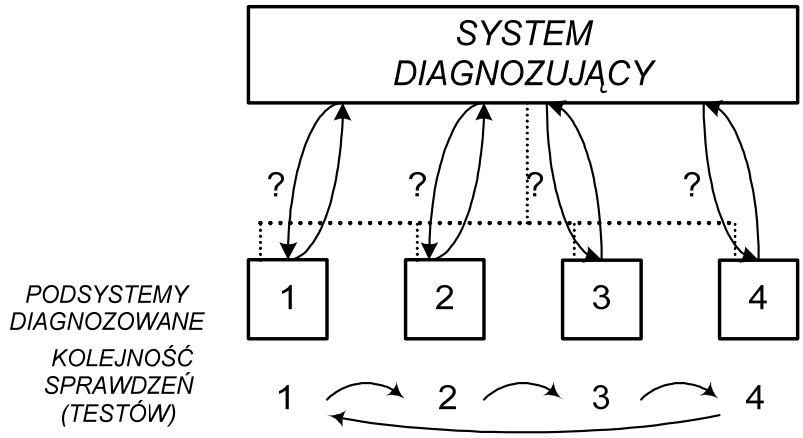
W tym kontekście należy wspomnieć o bardzo ważnej części procesu projektowania, którą jest sprawdzenie scenariusza wymian komunikatów proponowanego przez projektanta. Wiele rozproszonych systemów sterowania komunikuje się według ściśle określonego cyklu komunikacyjnego. Określona jest tam m.in. częstotliwość nadawania komunikatów przez poszczególne podsystemy. Newralgiczne, z punktu widzenia diagnozowania bezpieczności owego pojazdu, podsystemy powinny komunikować się z inną (wyższą) częstotliwością niż podsystemy mniej istotne. Projektowe diagnozowanie bezpieczności owe ma na celu sprawdzenie ułożonego scenariusza oraz wprowadzenie odpowiedniej terapii (polegającej np. na korekcie ustawień częstotliwości).

2. KOMUNIKACJA W PROCESIE DIAGNOZOWANIA BEZPIECZNOŚCIOWEGO

W sieciach przemysłowych, polowych (ang. *fieldbus*), do których zdaniem autorów można też zaliczyć sieci komunikacyjne występujące w pojazdach, występuje kilka modeli wymian komunikatów. Są to m.in.: *przekazywanie znacznika*, *master-slave*, *producent-dystrybutor-konsument*. Poniżej zostaną rozpatrzone dwa warianty diagnozowania bezpieczności owego: diagnozowanie inicjowane przez system diagnozujący oraz diagnozowanie inicjowane przez podsystem diagnozowany. W rozpatrywanych przypadkach każdy układ pojazdu może być, w zależności od wykonywanej w aktualnej chwili funkcji, podsystemem diagnozowanym lub systemem diagnozującym.

2.1. Komunikacja inicjowana przez system diagnozujący

Na rys. 6 przedstawiono najprostszy sposób diagnozowania podsystemów pojazdu. Na podstawie scenariusza utworzonego w fazie projektowej urządzenie nadrzędne (*master* - system diagnozujący) kolejno (zgodnie z planem) „odpytuje" urządzenia podrzędne (*slaves* - podsystemy diagnozowane) o wartości sygnałów diagnostycznych.

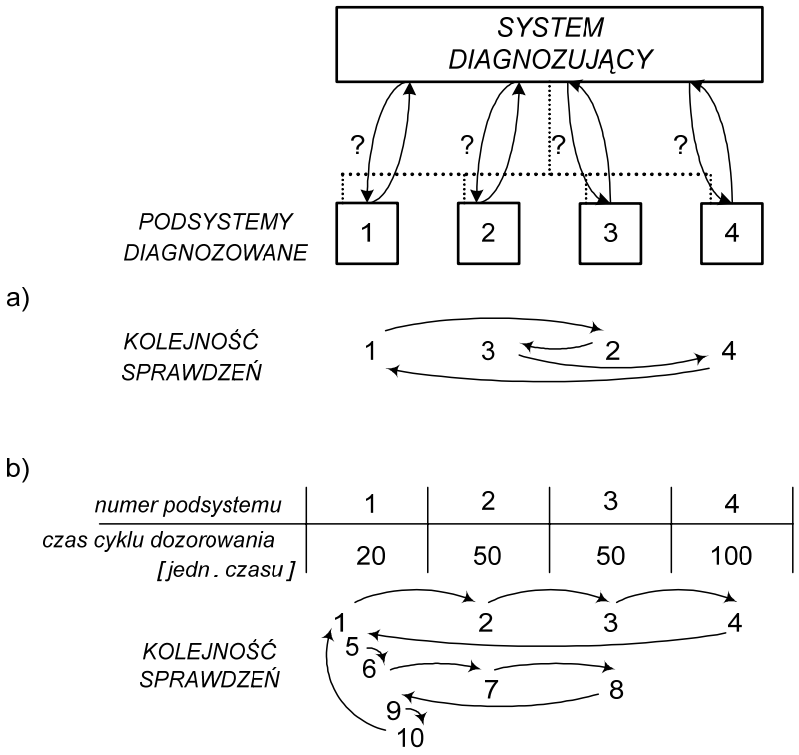


Rys. 6. Dozorowanie sekwencyjne inicjowane przez system diagnozujący ze stałym repertuarem sprawdzeń

Diagnozowanie bezpiecznościowe oparte na takiej zasadzie z założenia powinno być deterministyczne czasowo. Jest to jedyna korzyść wynikająca z zastosowanej metody. System diagnozowania bezpiecznościowego powinien reagować szybko na niewłaściwe zmiany wartości sygnałów diagnostycznych. W opisywanym przypadku kolejne diagnozowanie możliwe jest dopiero po zrealizowaniu całego cyklu transmisji.

Tę niedogodność można nieco ograniczyć stosując modyfikację przedstawioną na rys. 7. Wprowadzone tu zmiany dotyczą scenariusza wymian komunikatów. Najpierw stosuje się priorytetowanie z uwzględnieniem ważności informacji (rys. 7a). Umożliwia to zdalny odczyt najważniejszych - z uwagi na bezpieczeństwo - parametrów na początku całego cyklu diagnozowania urządzeń podrzędnych. W kolejnym kroku (rys. 7b) stosuje się zmianę polegającą na zróżnicowaniu odstępów czasu pomiędzy kolejnymi cyklami przesyłu komunikatów. W tym rozwiązaniu komunikaty niosące ważne bezpiecznościowo dane są realizowane z większą częstością. Takie rozwiązania przyjmuje się w sieciach przemysłowych łączących rozproszone systemy sterowania pracujące wg zasady *master-slave*.

To także nie jest doskonałe rozwiązanie z punktu widzenia bezpieczeństwa systemu. W razie pojawiających się błędów transmisji, podczas odpowiedzi podsystemu diagnozowanego (w wyniku np. zakłóceń) następują automatyczne retransmisje komunikatów. Wprowadza to dodatkowe opóźnienie. Stwierdzenie błędu transmisji (braku odpowiedzi) następuje tu - w najbardziej pesymistycznym przypadku - po odczekaniu przez system diagnozujący czasu równego czasowi oczekiwania na odpowiedź t_{to}.



Rys. 7. Dozorowanie bezpiecznościowe inicjowane przez system diagnozujący: a) priorytetowane; b) wykorzystujące tablicę częstości sprawdzeń diagnostycznych

Z każdym błędnie przesłanym komunikatem czas pełnego cyklu odpytań wszystkich urządzeń zwiększa się o t_{zdb}:

$$\forall(t_o > t_{to} \Rightarrow t_{zdb} = t_{to} + t_p) \tag{1}$$

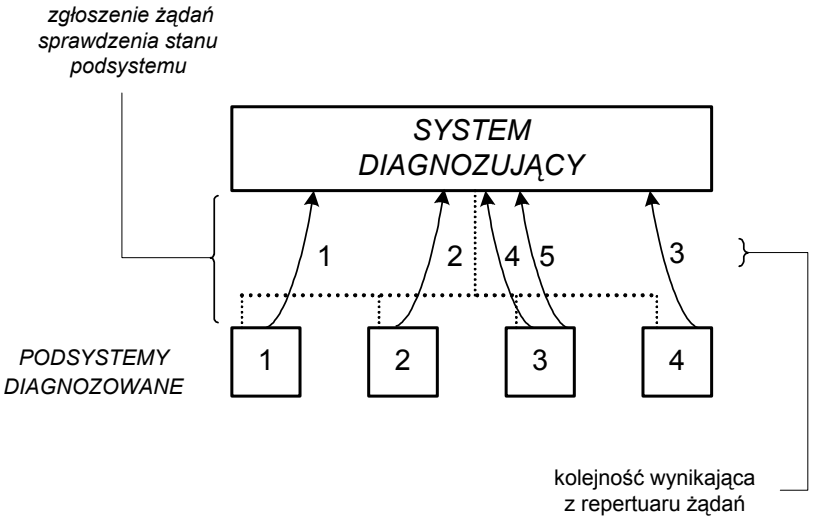
gdzie:

t_o - czas oczekiwania na odpowiedź podsystemu diagnozowanego
t_{to} - maksymalny czas oczekiwania systemu diagnozującego na odpowiedź
t_{zdb} - czas, o który zwiększa się czas pełnego cyklu odpytań
t_p - czas transmisji komunikatu-pytania systemu diagnozującego o wartość zmiennej.

2.2. Komunikacja inicjowana przez diagnozowane podsystemy

Analiza przedstawionych sposobów komunikacji miedzy systemem diagnozującym a podsystemami diagnozowanymi wykazuje zasadniczą niedoskonałość rozwiązania opartego na nadrzędnym wyborze przez system diagnozujący diagnozowanego podsystemu. Mając na uwadze diagnozowanie w celu utrzymania systemu K-S-O w stanie bezpieczeństwa, należy dostatecznie szybko reagować na zmiany stanu dozorowanych urządzeń. Przy założonym centralnym sterowaniu kolejnością dozorowania system diagnostyczny jest nieczuły na zdarzenia zachodzące pomiędzy kolejnymi wyznaczonymi turami sprawdzeń.

W celu zmiany tej sytuacji należy wprowadzić metodę samodzielnego zgłaszania potrzeby obsłużenia (odczytu wysyłanej wartości zmiennej diagnostycznej) przez podsystemy diagnozowane.. Negocjacja pierwszeństwa równoczesnych zgłoszeń, w takim przypadku, może odbywać się na zasadzie porównania priorytetów żądań (rys. 8). Im wpływ diagnozowanego podsystemu na bezpieczeństwo pojazdu jest większy, tym większy priorytet powinno uzyskać jego żądanie.



Rys. 8. Dozorowanie bezpiecznościowe inicjowane przez diagnozowane podsystemy

Dla newralgicznych bezpiecznościowo podsystemów autorzy proponują dodatkowo wprowadzić specjalne, oddzielne linie zgłoszeniowe. Wiąże się to z dodatkowym okablowaniem, jednak poprzez specjalne, oddzielne linie diagnozowane podsystemy mogłyby zgłaszać potrzebę obsłużenia transmisji komunikatów. To system diagnozujący decydowałby wtedy w pełni o kolejności obsłużenia urządzeń, mając do dyspozycji w międzyczasie dodatkową informację od diagnozowanych podsystemów. W ramach oszczędności można przyjąć, że wprowadzenie dodatkowych linii zgłoszeniowych ograniczałoby się tylko do kilku najważniejszych – z punktu widzenia bezpieczeństwa – urządzeń. Takie zgłoszenie następowałoby niezwłocznie. Zmiana stanu na przeciwny na linii zgłoszeniowej oznaczałaby żądanie obsłużenia. Wprowadzając dodatkowo adresację komunikatów, a nie całych urządzeń (unikalny adres miałby każdy komunikat), można uzyskać priorytetowanie także w ramach danego podsystemu.

2.3. Przykład zastosowania

Ostatni z przedstawionych wariantów koncepcji bezpiecznościowego diagnozowania (pkt. 2.2) można częściowo zastosować wykorzystując instalowane w pojazdach magistrale komunikacyjne bazujące na standardzie CAN (*Controller Area Network*). Mają one możliwość pracy z adresacją urządzeń lub komunikatów. Dostęp do magistrali jest priorytetowany. Im wyższy jest priorytet komunikatu, tym mniejsza jest wartość pola

nagłówka komunikatu. Arbitracja dostępu następuje poprzez wycofywanie się kolejnych urządzeń o niższym priorytecie komunikatu [5].

3. PODSUMOWANIE

Przedstawione w pkt. 2 rozważania prowadzą do wniosku, iż dobrym rozwiązaniem komunikacji pomiędzy podsystemami w bezpiecznościowym systemie diagnozowania jest rozwiązanie z inicjowaniem transmisji przez podsystemy diagnozowane z jednoczesną sygnalizacją chęci obsłużenia oddzielną linia sygnałową. Daje to najmniejsze opóźnienia w obsłużeniu komunikatu przez system diagnozujący. Rozwojowymi trendami przedstawionych zagadnień bezpiecznościowego diagnozowania systemu antropotechnicznego kierowca-samochód mogą być:

1. W celu zabezpieczenia jak najmniejszego obciążenia magistrali komunikacyjnej zastosowanie grupowania komunikatów. Polega to na zgromadzeniu i transmitowaniu w jednym komunikacie kilku wartości dozorowanych (szerszy opis w [10]).
2. Wspomniane grupowanie może odbywać się także na zasadzie wydzielania dla pewnych grup urządzeń oddzielnych magistrali komunikacyjnych. W najważniejszych pod kątem bezpieczeństwa przypadkach może to być personalna magistrala dla podsystemu.

Bibliografia

1. Dąbrowski T.: Diagnozowanie systemów antropotechnicznych w ujęciu potencjałowym. Wydawnictwo WAT Warszawa 2001.
2. Będkowski L., Dąbrowski T.: Podstawy eksploatacji, część 2. Wydawnictwo WAT, Warszawa 2006.
3. Będkowski L.: Elementy Diagnostyki Technicznej. Wydawnictwo WAT, Warszawa 1992.
4. Bosch R.: Sieci wymiany danych w pojazdach samochodowych. WKŁ, Warszawa 2008.
5. Kwiecień A.: Analiza przepływu informacji w komputerowych sieciach przemysłowych, Wydawnictwo Politechniki Śląskiej, Studia Informatica, Gliwice 2002.
6. Bednarek M., Będkowski L., Dąbrowski T.: Diagnozowanie bezpieczeństwa systemu antropotechnicznego w ujęciu potencjałowym. Przegląd Elektrotechniczny, 87-92, 2009, nr 11.
7. Romanowska-Słomka I., Słomka A.: Zarządzanie ryzykiem zawodowym. Wydawnictwo Tarbonus, Kraków 2009
8. Będkowski L., Dąbrowski T.: Analiza niezawodności użytkowej systemu antropotechnicznego. Zimowa Szkoła Niezawodności, Szczyrk, 2009.
9. http://elektronikasamochodowa.com
10. Bednarek M., Będkowski L., Dąbrowski T.: Potencjałowe wskaźniki niezawodności przesyłu zbioru komunikatów. Diagnostyka, 37, 45-50, 2006, nr 1.

SAFETY DIAGNOSING OF THE DRIVER-VEHICLE SYSTEM

Abstract: The paper presents a discussion concerning the driver-vehicle-environment diagnosing process, in terms of safety. The problems of operational and design diagnosing were formulated. The properties of the sequential diagnosing and diagnosing with priorities, initiated by diagnosing system as well as by the car supervised subsystems, both with device and message addressing were discussed. An application example of the author's concept of communication with use of the CAN bus was presented.

Keywords: data transport system, industrial network, human-engineering system (HES), diagnosing process of driver-vehicle system, CAN bus