ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 68 Nr kol. 1905

Damian PETRECKI, Ireneusz J. JÓŹWIAK, Jacek GRUBER
Politechnika Wrocławska,
Wydział Informatyki i Zarządzania

# PROPOZYCJA WYKORZYSTANIA SCENTRALIZOWANEGO SYSTEMU INFORMATYCZNEGO W SAMOCHODACH

**Streszczenie.** W artykule zaproponowano zastąpienie rozproszonego, skomplikowanego systemu informatycznego występującego w samochodzie nowym, autorskim rozwiązaniem. Opiera się ono na pojedynczym komputerze, który jest centralnym sterownikiem i konfiguruje elementy wykonawcze pojazdu podczas jazdy tak, aby jak najlepiej zrealizować decyzje kierowcy na podstawie informacji o otoczeniu i stanie pojazdu. Poprawiono bezpieczeństwo i jakość jazdy oraz zwiększono bezpieczeństwo informatyczne pomijane w tym zakresie we współczesnej motoryzacji.

**Słowa kluczowe:** inteligentny samochód, magistrala CAN, system wspomagania decyzji w motoryzacji.

# PROPOSITION OF USAGE A CENTRALIZED COMPUTER SYSTEM IN CARS

**Summary.** This article proposes to replace distributed, complex computer system present in the car with the original solution. That should base on a single computer that which is the central control car and which configures actuators to realize driver decisions and bases on known vehicle state and environment. In this way driving safety and quality as well as computer security neglected in the modern automotive industry can be improved.

**Keywords:** intelligent car, CAN bus, decision support system in automotive.

## 1. Wprowadzenie

Samochody produkowane na początku XXI wieku bazują na założeniach pochodzących z całego okresu rozwoju motoryzacji. Samochód został opatentowany w 1886 roku w Niemczech i od tej pory był ulepszany i unowocześniany przez specjalistów na całym świecie. Nie licząc kilku wyjątków, rozwój motoryzacji opierał się na dodawaniu nowych elementów do istniejących konstrukcji lub na komplikowaniu istniejących mechanizmów.

W drugiej połowie XX wieku w samochodach zaczęły pojawiać się sterowniki układów samochodu. Na początku były to bardzo proste układy elektroniczne przeznaczone do sterowania pokładową elektryką, jednak z czasem przejęły one role zarządzania pracą silnika czy poprawy bezpieczeństwa czynnego. Pojawiło się nawet określenie „komputer pokładowy", wskazujące na urządzenie wyliczające aktualny przebieg samochodu czy ilość spalanego paliwa.

Z czasem liczba niezależnych mikrokontrolerów w samochodach urosła do około 50, a sumaryczna długość łączących je przewodów – do kilkunastu kilometrów. Wartości te zależą od konkretnego modelu samochodu i jego wyposażenia, jednak od razu widać, że są one niebezpiecznie wysokie.

Problemem, który pojawił się w opisanej sytuacji jest spójność takiego systemu, a dokładniej niedoskonałość metod, które zostały użyte do osiągnięcia tej spójności. Z tego powodu proponuje się zastąpienie wszystkich mikrokomputerów sterujących jednym, z zachowaniem pewnych założeń gwarantujących zwiększenie bezpieczeństwa i jakości pracy systemu informatycznego w pojeździe.

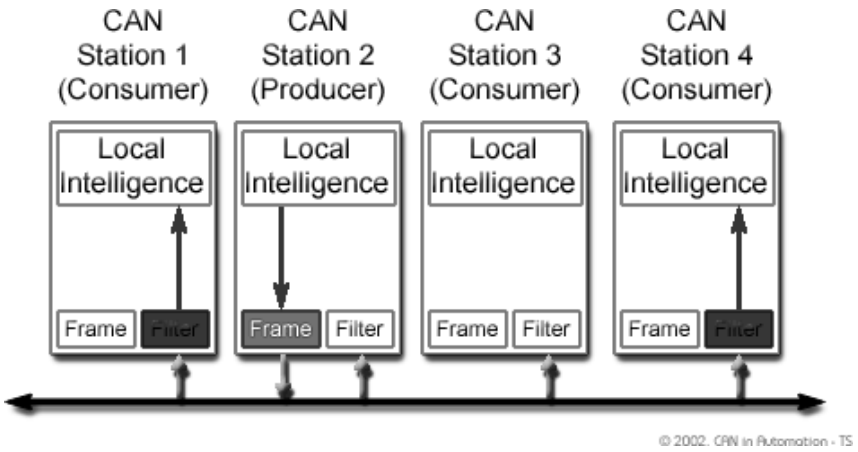
## 2. Obecne rozwiązania systemów informatycznych w samochodach

Dedykowane komputery sterujące używane w samochodach pełnią wiele ról: sterują światłami, wycieraczkami, mechanizmami szyb, klimatyzacją, fazami rozrządu, prędkością kół czy wysokością amortyzatorów. Do wielu czynności używa się kilku komputerów, np. oddzielny komputer steruje poziomowaniem reflektorów, a inny wykrywa pojazdy przed samochodem i na tej podstawie przełącza tryb pracy świateł. Z tego powodu wymaga się, żeby poszczególne jednostki mogły komunikować się ze sobą, ze swoimi czujnikami oraz z urządzeniami wykonawczymi, które realizują podjęte automatycznie decyzje. Aktualnie używa się do tego celu magistrali CAN [1].

Magistrala *Controller Area Network* (ang. skrót CAN) jest to magistrala szeregowa będąca podstawą sieci przemysłowych oraz sieci używanych w samochodach [2, 3, 4]. Schemat użycia magistrali CAN przedstawiono na rysunku 1. Jak widać na nim, magistrala

używa schematu komunikacji *multi-master broadcast*, czyli traktuje wszystkie urządzenia jednakowo i rozsyła każdą wiadomość do wszystkich podłączonych jednostek. Ta cecha stanowi podstawę budowy magistrali CAN i jednocześnie jej największą podatność w ujęciu bezpieczeństwa informatycznego. Stwarza ona zagrożenie podłączenia się do magistrali i nadawania wiadomości, które zostaną skutecznie rozesłane po całej sieci. Ta luka pozwala potencjalnemu agresorowi np. na wyłączenie świateł, odryglowanie zamków lub wyłączenie układu ABS [8, 9, 10].

Podłączone urządzenia same filtrują wiadomości i decydują, czy przekazać je z interfejsu sieciowego do lokalnej jednostki obliczeniowej. Używają do tego celu podpisów zawartych w każdej wiadomości, a nie podpisów nadawców czy odbiorców, co dodatkowo znacznie ułatwia ataki typu *spoofing* [5].




Rys. 1. Schemat użycia magistrali CAN [3]
Fig. 1. CAN bus usage schema

Magistrala CAN używa prostego medium transmisyjnego, którym jest skrętka dwuprzewodowa, co oznacza minimalną odporność na przesłuchy i wstrzykiwanie danych. Prędkość przesyłu danych wynosi tu 1 Mbit/s na odległości 40 m i maleje proporcjonalnie do wzrostu długości przewodu. W stosunku do prędkości, używanych w sieciach, opartych na światłowodach i miedzianych skrętkach ośmiożyłowych, wydajność CAN jest na tyle niska, że stała się przyczyną powstawania pierwszych alternatywnych rozwiązań, jak np. FlexRay, który z kolei rozwiązuje tylko niektóre problemy związane z bezpieczeństwem [11], ale nie upraszcza znacząco konstrukcji sieci komunikacyjnej.

Sprzętowa obsługa błędów, która jest elementem sieci CAN, stanowi kolejną, trudną do zaakceptowania podatność. Kody CRC, mechanizm ACK oraz *bit stuffing* umożliwiają potencjalnemu napastnikowi wykonanie ataku DoS przez zmuszenie magistrali do obsługi ciągle tych samych wiadomości lub uniemożliwienie odczytania wiadomości przez urządzenia odbiorcze. Podobnie można wykorzystać mechanizmy kontroli dostępu do łącza

danych. Magistrala wykorzystuje mechanizm dominacji bitowej podczas przyjmowania komunikatów, a w trakcie ich obsługi kolejkuje je względem długości kodu identyfikacyjnego.

Ostatnią, wartą uwagi cechą i podatnością omawianej magistrali, jest zestawienie jej z interfejsem diagnostycznym OBD-II [6]. Piny 6. oraz 14. z tego 16-pinowego złącza serwisowego podłączone są bezpośrednio do magistrali CAN, na równi z wszystkimi innymi urządzeniami informatycznymi. Dzięki temu możliwe jest nadawanie do magistrali oraz odczytywanie wszystkich informacji, które się w niej pojawiają. Do pełnej interakcji potrzebne są już tylko kody podpisujące wiadomości i prosty interfejs (np. bezprzewodowy, połączony z urządzeniem GSM/WiFi).

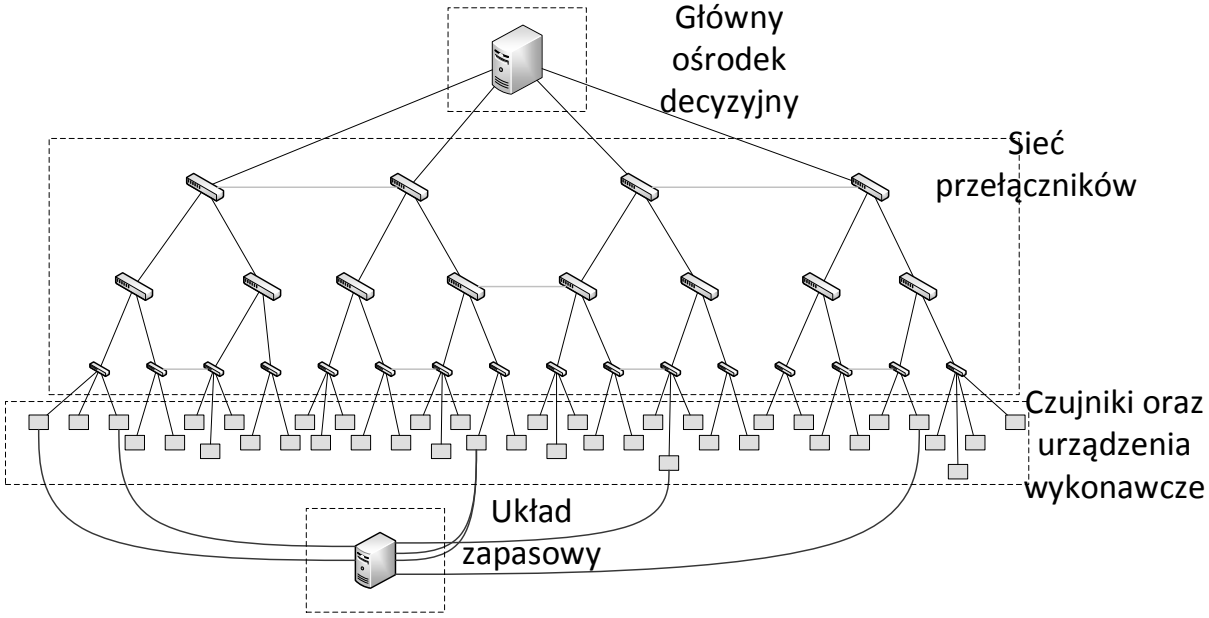
Kody identyfikacyjne wiadomości można zdobyć na wiele sposobów. Podstawowym jest zakup. Jednak jest to rozwiązanie bardzo drogie (dorównuje ceną samochodowi, którego dotyczą kody) i skuteczne tylko dla konkretnego modelu pojazdu z konkretnym wyposażeniem. Przeważnie, choć nie zawsze, książkami kodów dysponują autoryzowane serwisy, skąd można je zdobyć za pomocą ataków socjotechnicznych. Ostatecznie, duża liczba kodów dostępna jest w Internecie (część z nich za darmo i w pełni legalnie [7]) lub zaszyta w oprogramowaniu przeznaczonym do interakcji z CAN. Najprostsze, darmowe programy tego typu (np. wtyczka do popularnego *Wireshark*-a), zdolne są do wyświetlania w postaci heksadecymalnej wiadomości pojawiających się na magistrali, jednak drogie, komercyjne rozwiązania potrafią rozszyfrować dużą liczbę kodów i zaprezentować je w sposób czytelny dla użytkownika (wykresy, animacje, tabele). Większość dostępnego oprogramowania ma także wbudowaną możliwość wysyłania komunikatów do magistrali.

Potencjalny napastnik może wykorzystać fakt, że magistrala CAN jest dobrze opisana i samodzielnie opracować potrzebny interfejs OBD-II – PC oraz wykorzystać darmowe oprogramowanie wraz z kodami identyfikacyjnymi wiadomości zdobytymi eksperymentalnie.

## 3. Proponowane rozwiązanie systemu informatycznego

Celem badań było zwiększenie bezpieczeństwa użytkowników samochodu przez zastąpienie rozproszonego systemu informatycznego wykorzystującego wspólną magistralę przez jeden komputer sterujący połączony z siecią czujników i urządzeń wykonawczych. W ten sposób można poprawić bezpieczeństwo jazdy, bezpieczeństwo informatyczne oraz uprościć konstrukcję samochodu.

Proponuje się utworzenie sieci o strukturze drzewa, jak pokazane jest to na rysunku 2.




Rys. 2. Schemat proponowanej sieci z centralnym sterownikiem
Fig. 2. Diagram of the proposed network to a central controller
Źródło: opracowanie własne.

System informatyczny powinien składać się z czterech podstawowych elementów. Najważniejszym elementem omawianego systemu miałby być główny komputer sterujący, służący do podejmowania wszystkich decyzji w samochodzie. Każda operacja powinna składać się z żądania wysłanego do tego komputera i wychodzącego z niego sygnału sterującego. Powinien on pobierać z czujników informacje o stanie samochodu, otoczeniu samochodu oraz o intencjach kierowcy i na ich podstawie wysyłać sygnały sterujące do urządzeń wykonawczych. Główny komputer sterujący powinien dysponować szybkim magazynem danych, możliwością wielopotokowego przetwarzania danych (na przykład z użyciem GPGPU) i interfejsami odpowiedzialnymi za komunikację z siecią informatyczną w samochodzie.

Rolą głównego komputera byłoby podejmowanie atomowych decyzji dotyczących zachowania auta. Rozumie się przez to np. uruchomienie kierunkowskazów, podgrzewania szyb, odryglowanie zamków, ale także zmianę twardości zawieszenia, zmianę wysokości zawieszenia, zaciśnięcie hamulców czy skręt mechanizmu zwrotniczego. Lista takich operacji musiałaby być bardzo długa, jednak istotne jest to, że podejmowane byłyby one w wyniku pracy taniego i łatwego w aktualizacji oprogramowania, zamiast przez sprzętowe sterowniki, jak ma to miejsce w obecnych rozwiązaniach w samochodach.

Komunikacja głównej jednostki sterującej z czujnikami i urządzeniami wykonawczymi miałaby odbywać się przez sieć zbudowaną w topologii drzewa, uzupełnioną poziomymi połączeniami redundantnymi. Przełączniki takiej sieci powinny być zdolne wyłącznie do

przekazywania sygnałów z liści drzewa do korzenia i odwrotnie. Nie ma potrzeby, żeby czujniki i realizatory komunikowały się pomiędzy sobą, a proponowane rozwiązanie pozwoli na zastosowanie prostych, szybkich i niezawodnych przełączników.

Wyznaczanie trasy od korzenia do liści powinno opierać się na adresacji zawartej w ramkach. Nagłówek każdej wiadomości powinien zawierać krótkie (np. 4-bitowe) instrukcje dla każdego z przełączników, a każdy przełącznik powinien interpretować pierwsze bity wiadomości, jako cel wysłania ramki, odcinać instrukcję przeznaczoną dla siebie i przekazywać pozostałe dane do kolejnego urządzenia.

Na rysunku 2 widoczne są połączenia zapasowe. Każdy przełącznik powinien dysponować możliwością wykrycia awarii głównego połączenia i przekazania ruchu przez kanał dodatkowy z jednoczesną modyfikacją pól sterujących tak, żeby pakiet trafił do celu. Alternatywą wartą rozważenia jest możliwość zgłaszania awarii łącza do nadawcy ramek, który dokonywałby retransmisji na podstawie znajomości łączy zapasowych. W tej wersji każdy liść drzewa musiałby znać swoją trasę podstawową do korzenia, a także kilka tras zapasowych. Ze względu na fizyczny rozkład urządzeń, można to opisać na następującym przykładzie: wszystkie czujniki i urządzenia wykonawcze umiejscowione przy kole, łączyłyby swoje sygnały z użyciem kilku przełączników do jednego przewodu, który kierowałby komunikację w kierunku głównego ośrodka decyzyjnego; w wypadku awarii tego przewodu uruchamiane byłoby połączenie redundantne, kierujące transfer do przełącznika obsługującego transfer zawieszenia innego koła; dzięki zastosowaniu szybkich łączy miedzianych lub światłowodowych połączenie drugiego koła byłoby w stanie obsłużyć, oprócz przeznaczonego sobie transferu, dodatkowo ruch pochodzący z uszkodzonego łączą.

Ze względu na inną obsługę wyznaczania tras, od korzenia do liści oraz od liści do korzenia, problem obsługi uszkodzeń sieci wciąż jest sprawą otwartą.

W grupie, zwanej czujnikami i urządzeniami wykonawczymi, powinny się znaleźć wszystkie czujniki samochodu oraz wszystkie urządzenia, które wykonują w samochodzie fizyczne działania. Do czujników zaliczyć należy lidary i kamery obserwujące otoczenie, czujniki urządzeń sterujących (np. kierownicy i pedałów) oraz wszystkie urządzenia interakcji człowieka z samochodem (przyciski, przełączniki, czujniki, ekrany dotykowe). Urządzenia wykonawcze powinny być maksymalnie uproszczone tak, żeby zajmowały się tylko wykonywaniem akcji (przyspieszanie, hamowanie, włączanie świateł, otwieranie nawiewów), zamiast podejmować jakiekolwiek decyzje.

Ważną cechą liści omawianego systemu powinno być posiadanie certyfikatów podpisanych przez producenta samochodu. Dzięki temu komunikacja z głównym komputerem mogłaby zachowywać poufność danych i identyfikowalność stron komunikacji.

Przejdźmy teraz do układu zapasowego. Należy rozważyć przypadek awarii głównego komputera lub tak dużego fragmentu sieci, żeby omawiany system nie mógł funkcjonować. W tym wypadku podstawowe urządzenia wejściowe (czujnik położenia kierownicy, czujniki położenia pedałów) powinny zostać połączone z najważniejszymi realizatorami

(np. hamulcami, silnikiem, skrzynią biegów) przez prosty, zapasowy system decyzyjny. Nie musiałby on implementować wszystkich funkcjonalności głównego komputera, ale powinien zapewnić bezpieczne kontynuowanie jazdy samochodem. Dodatkowo, należy rozważyć zdublowanie najważniejszych czujników i urządzeń wykonawczych.

## 4. System decyzyjny

Podstawowym zadaniem omawianego systemu byłoby sterowanie kierunkiem oraz prędkością jazdy tak, żeby zachować maksymalne bezpieczeństwo i komfort. Oznacza to konieczność podejmowania decyzji w dyskretnych chwilach czasu. Proponowany system decyzyjny w postaci schematu blokowego specjalizowanego sterownika przedstawiony jest na rysunku 3. Jak widać, wszystkie zmienne ustalane są w danej, dyskretnej chwili czasu. W skład systemu wchodzą następujące elementy:

- modelowany obiekt – samochód, reprezentowany przez model symulacyjny lub model regresji,
- System Wspomagania Decyzji (SWD), który analizuje dane i generuje sygnały sterujące,
- wejścia modelu:

wektor $u_1(t)$ to sygnały z otoczenia samochodu – jest to opis parametryczny drogi i obiektów znajdujących się w pobliżu pojazdu,

wektor $u_2(t)$ to wejście od użytkownika, np. położenie pedałów i kierownicy,

- parametry modelu:

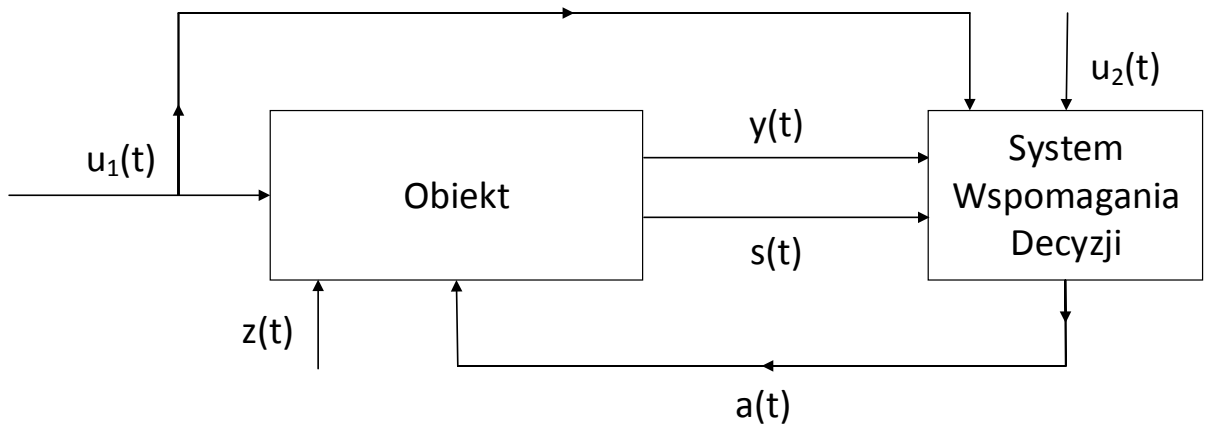
  wektor $a(t)$ zawiera sygnały sterujące pracą zawieszenia, silnika, hamulców i innych urządzeń wykonawczych,

- wyjście modelu:

  wektor $y(t)$ to wyjście z modelu – zestaw zmiennych opisujących zachowanie samochodu,

  wektor $s(t)$ reprezentuje aktualne położenie elementów wykonawczych (stan systemu),

- wektor $z(t)$ to niemierzalne zakłócenia, np. nierówności drogi mniejsze niż rozdzielczość urządzeń pomiarowych.




Rys. 3. Schemat blokowy specjalizowanego sterownika dla sytemu decyzyjnego
Fig. 3. Block diagram of a specialized driver for decision-making system
Źródło: opracowanie własne.

W każdej dyskretnej chwili czasu należałoby wykonywać następujące operacje:

1. Akwizycja danych o otoczeniu i poleceń do użytkownika.
2. Utworzenie żądanej trajektorii poruszania się pojazdu.
3. Skorygowanie trajektorii, jeśli sytuacja tego wymaga. Ten krok powinien polegać na poprawianiu decyzji kierowcy. Przykładowo, gdy kierowca próbuje ominąć przeszkodę, jednak wykonuje za mały skręt kołem kierownicy, komputer powinien sam przeanalizować sytuację i zmniejszyć promień łuku, po którym miałby poruszać się pojazd, tak żeby uniknąć zderzenia.
4. Wyznaczenie wektora zmiennych decyzyjnych i przekazanie ich do urządzeń wykonawczych – zawieszenia, silnika, hamulców itd.

Dokonano próby wyznaczania wektora zmiennych decyzyjnych na podstawie optymalizacji z wykorzystaniem modelu regresji, utworzonego na podstawie identyfikacji modelu symulacyjnego poruszającego się pojazdu. Badania zakończyły się powodzeniem [12, 13], jednak ze względu na ogromną złożoność obliczeniową tego rozwiązania badane są rozwiązania alternatywne – analiza zachowania ruchu pojazdu, programowanie dynamiczne lub równoległe symulacje w czasie rzeczywistym.

## 5. Kierunki dalszych badań

Niniejszy artykuł stanowi opis koncepcji proponowanego systemu. Ograniczone miejsce nie pozwala na bardziej szczegółowy opis rozwiązania. Każdy z elementów proponowanego komputerowego systemu sterowania wymaga struktury i algorytmów sterowania. Wymagane są też dalsze badania. W szczególności należy opracować protokół komunikacji

w zaproponowanej sieci oraz zaprojektować przełączniki i interfejsy urządzeń podłączonych do magistrali sieciowej. Oprócz tego należy dopracować system decyzyjny do zaimplementowania w postaci sterownika oraz zapewnić bezawaryjną pracę podsystemu poprawiania decyzji kierowcy.

**Bibliografia**


1. Bosch R, CAN Specification, version 2.0. Robert Bosch GmbH, Stuttgart, 1991.
2. Johansson K.H., Törngren M., Nielsen L.: Vehicle Applications of Controller Area Network, [in:] Handbook of Networked and Embedded Control Systems, Birkhäuser Basel, 2005, p. 741-765.
3. „Controller Area Network (CAN),” [Online]. Available: http://www.can-cia.org/index.php?id=16. [2 maj 2013].
4. „Magistrala CAN, cześci 1-5, Elektronika Praktyczna, 1-5 2000.
5. Guardigli M.: Hacking Your Car, 4 Październik 2010. [Online]. Available: http://marco.guardigli.it/2010/10/hacking-your-car.html [2 maj 2013].
6. „Adapters for Vehicle On-board Diagnostic,” [Online]. Available: http://www.obddiag.net/adapter.html [2 maj 2013].
7. Edytorzy Wikipedii, „OBD-II PIDs,” 5 Kwiecień 2013. [Online]. Available: http://en.wikipedia.org/wiki/OBD-II_PIDs [2 Maj 2013].
8. Czeskis A., Koscher K., Roesner F., Patel S., Kohno T., Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., Savage S.: Experimental Security Analysis of a Modern Automobile, [in:] Security and Privacy (SP), 2010 IEEE Symposium on, 2010, p. 447-462.
9. Wolf M., Weimerskirch A.: Paar C, Security in Automotive Bus Systems. Workshop on Embedded IT-Security in Cars, 2004, p. 11-12.
10. Hoppe T., Kiltz S., Dittmann J.: Security threats to automotive CAN networks–practical examples and selected short-term countermeasures. Computer Safety, Reliability, and Security 2008, p. 235-248.
11. Mazran E., Redzuan A., Badrul H., Adie M., Amat A.: Security System Using CAN Bus. Journal of Telecommunication, Electronic and Computer Engineering, 1 1 2009, p. 1-5.
12. Acocella N.: Zasady polityki gospodarczej. PWN, Warszawa 2002.
13. Petrecki D.: Opracowanie modelu matematycznego i komputerowego nowoczesnego samochodu na potrzeby zadania stabilizacji podwozia. Praca magisterska, Politechnika Wrocławska, Wrocław 2013.

**Abstract**

This paper describes original vision of centralized computer system dedicated to manage vehicle behaviour. In first part, present in-car network is described and some security susceptibility are pointed. After that there is a description of proposed network system, basing on tree topology with redundant connections. Next, there is a short explanation of the central decision-making unit, network switches and network tree leases – sensors and actuators. In last part of document, a decision-making system is drafted and future research are pointed.

Entire document presents authors original concept based on own idea and conducted research.