st. asp. mgr inż. Krzysztof Biskup
Zakład Broni i Mechanoskopii Centralnego Laboratorium Kryminalistycznego Policji
krzysztof.biskup@policja.gov.pl
mgr inż. Krzysztof Ćwik
Wydział Samochodów i Maszyn Roboczych Politechniki Warszawskiej
krzysztofcwik@wp.pl
mgr Tadeusz Neumann
TOMSAD Tomasz Sadowski
tadeusz@programatory.com

Pozyskiwanie do celów procesowych informacji zakodowanych w podzespołach elektronicznych pojazdów i maszyn roboczych

Streszczenie

W artykule zaprezentowano wyniki otrzymane w trakcie badań dotyczących pozyskiwania do celów procesowych informacji zakodowanych w podzespołach elektronicznych pojazdów oraz wskazano możliwości ich wykorzystania w dalszej praktyce przez biegłych z zakresu badań mechanoskopijnych oraz funkcjonariuszy zajmujących się zwalczaniem przestępczości samochodowej.

Słowa kluczowe: projekt, pojazd, podzespół elektroniczny, sterownik, diagnostyka pojazdu, numer VIN

Geneza projektu sięga roku 2009, kiedy to w ramach ówczesnego Wydziału Mechanoskopii i Balistyki Centralnego Laboratorium Kryminalistycznego KGP uruchomiono pierwszą w kraju pracownię badań podzespołów elektronicznych pojazdów. Dynamiczny rozwój elektroniki samochodowej sprawił, że w pamięciach różnego rodzaju podzespołów elektronicznych większości samochodów wyprodukowanych po roku 2000 zapisywane były informacje dotyczące numeru identyfikacyjnego VIN pojazdu, w którym zamontowano dany podzespół (ryc. 1).

Zaistniała więc potrzeba rozszerzenia zakresu prowadzonych dotychczas badań identyfikacyjnych pojazdów o badania ich podzespołów elektronicznych

Ryc. 1. Podzespoły samochodowe, w których jest zakodowany numer VIN.

Ryc. 2. Urządzenia diagnostyczne wykorzystywane w badaniach.

w celu poszukiwania zapisanych w ich pamięciach numerów VIN. Początkowo badania te prowadzono z wykorzystaniem dostępnych na rynku urządzeń diagnostycznych (ryc. 2), urządzenia te charakteryzowały się jednak dwoma podstawowymi wadami:

– przeznaczone były dla określonych grup pojazdów, co powodowało konieczność zakupu wielu takich kosztownych narzędzi, aby zapewnić możliwość zbadania większości pojazdów,
– przeznaczone były do diagnostyki błędów i usterek w pojeździe, zatem pozyskanie informacji o numerze VIN wymagało sięgania w głębsze pokłady pamięci i wysokospecjalistycznej wiedzy biegłego.

Doświadczenia zebrane w ciągu pierwszych kilku lat wdrażania tych badań do policyjnej praktyki zaowocowały koncepcją zbudowania uniwersalnego urządzenia przeznaczonego dla biegłych identyfikujących pojazdy, które będzie obsługiwało szeroki zakres marek samochodów, miało przyjazne menu i z wykorzystaniem kilku prostych funkcji wyszukiwało zakodowany w podzespołach elektronicznych numer identyfikacyjny VIN badanego pojazdu oraz pokazywało go na własnym wyświetlaczu.

Zgłoszono więc do Narodowego Centrum Badań i Rozwoju propozycję tematu badawczego, po jego zaakceptowaniu złożono stosowny wniosek o finansowanie, a następnie w okresie od 23 grudnia 2013 r. do 31 marca 2017 r. w Zakładzie Broni i Mechanoskopii Centralnego Laboratorium Kryminalistycznego Policji zrealizowano projekt na rzecz bezpieczeństwa i obronności państwa pt. „Pozyskiwanie do celów procesowych informacji zakodowanych w podzespołach elektronicznych pojazdów i maszyn roboczych".

W celu wykonania projektu powołano konsorcjum naukowe, którego liderem było Centralne Laboratorium Kryminalistyczne Policji, a partnerami Wydział Samochodów i Maszyn Roboczych Politechniki Warszawskiej oraz firma TOMSAD Tomasz Sadowski.

W trakcie realizacji projektu firma TOMSAD zbudowała prototypy dwóch urządzeń do badań podzespołów elektronicznych pojazdów, które nazwano Smart Connect (ryc. 3) i Easy Dump (ryc. 4).

Smart Connect służy do uruchamiania urządzeń na stole warsztatowym lub bezpośrednio w pojeździe i sterowania nimi. Wyposażony jest w transceiver CAN w standardzie 2.0 oraz transceiver protokołu ISO 9141 (K-line BUA). Urządzenie zostało zaopatrzone w slot karty pamięci micro-SD, dzięki czemu możliwe jest magazynowanie niezbędnych pakietów danych. Zastosowanie buzera umożliwia wykrycie nieprawidłowego podłączenia zasilania. Komunikacja z podzespołami samochodów odbywa się przez złącze DB25 lub bezpośrednio przez wejście OBD II. Na złącze D-SUB wyprowadzono sygnały CANL i CANLH, K-line, L-line, 3 × wyjście +12 V z przekaźnika (przekaźnik sterowany masą wejścia DB25). Sterowanie urządzeniem odbywa się za pomocą przycisku umieszczonego w lewym górnym rogu. Smart Connect został zabezpieczony przez weryfikację klucza produktu. Klucz składa się z zaszyfrowanej informacji, która zawiera m.in. numer seryjny urządzenia. Dodatkowo zastosowano zabezpieczenia wbudowane w mikrokontroler. Całość umożliwia zabezpieczenie przed niepowołanym dostępem do oprogramowania. Urządzenie zostało zamknięte w poręcznej metalowej obudowie w kształcie prostopadłościanu.

Ryc. 3. Smart Connect skonstruowany i wykonany przez TOMSAD.

Easy Dump służy do odczytu danych ukrytych w pamięci podzespołów takich jak numer VIN, wersji oprogramowania itp., uruchamiania urządzeń na stole warsztatowym lub bezpośrednio w pojeździe oraz sterowania nimi. Analizator wyposażony jest w transceiver CAN w standardzie 2.0A i 2.0B oraz transceiver protokołu ISO 9141 (K-line BUS). Dzięki zastosowaniu karty pamięci micro-SD możliwe jest magazynowanie niezbędnych danych. Ponadto analizator został wyposażony w złącze micro USB do komunikacji z komputerem. Dzięki zastosowaniu buzera możliwe jest dźwiękowe sygnalizowanie błędów ukończenia operacji. Komunikacja analizatora z podzespołami odbywa się przez złącze DB15. Na złącze wyprowadzono sygnały CANL i CANH, K-line i L-line, USART RX i TX, 3 × sygnał wejściowy, 2 × sygnał wyjściowy, wyjściowe +12 V sterowane procesorem oraz zasilanie. Sterowanie urządzeniem odbywa się za pomocą

Ryc. 4. Easy Dump skonstruowany i wykonany przez TOMSAD.

rezystancyjnego panelu dotykowego. Zgodnie z założeniami oprogramowanie przyjmuje postać katalogów z podziałem na marki pojazdów, a następnie rodzaje podzespołów. Całe urządzenie działa pod kontrolą systemu czasu rzeczywistego FreeRTOS. Zapewnia to minimalny czas wykonywania zadań. Easy Dump został zabezpieczony przez weryfikację ID procesora, zabezpieczenia wbudowanego w mikrokontroler oraz autorskie rozwiązania zespołu projektowego TOMSAD. Umożliwia to ochronę przed niepowołanym dostępem do oprogramowania. Całość została zamknięta w poręcznej plastikowej obudowie w kształcie prostopadłościanu.

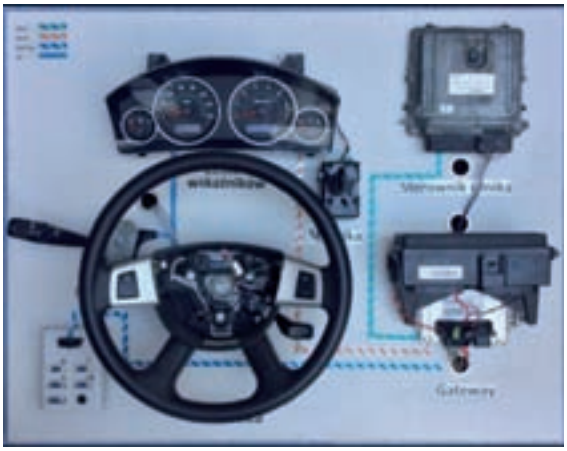
Poza ww. urządzeniami na Wydziale SiMR PW oraz w CLKP zbudowano cztery symulatory szkoleniowe na bazie samochodów marki Chrysler, Audi A6, BMW i Ford. Symulatory te pozwalają na obserwację kanałów przesyłu informacji podczas wymiany danych pomiędzy poszczególnymi sterownikami oraz urządzeniem diagnostycznym i daną grupą sterowników lub sterownikiem.

Do budowy stanowisk wybrano podstawowe sterowniki występujące w odtwarzanych pojazdach, takie jak:

- sterownik silnika,
- kierownicę wielofunkcyjną,
- gateway,
- manetkę przełącznika świateł,
- stacyjkę,
- zespół przekaźników,
- zestaw wskaźników.

Symulatory (ryc. 5–8) są przydatne m.in. w przypadku badania urządzeń służących do kradzieży samochodów. Podłączenie do symulatora elektronicznego urządzenia służącego do kradzieży samochodów oraz wpięcie do instalacji urządzenia zbudowanego przez TOMSAD w ramach przedmiotowego projektu pozwala na odczyt danych z pamięci sterownika silnika, immobilizera lub elektronicznej stacyjki. Na podstawie odczytanych informacji można ustalić przeznaczenie urządzenia zabezpieczonego do badań jako narzędzie służące do kradzieży samochodów, a tym samym poznać zasady działania badanego urządzenia. Zebrane informacje oraz zmiana kodów poleceń pozwolą zaś przygotować elektroniczne zabezpieczenie przeciwkradzieżowe.

W ramach CLKP przeprowadzono weryfikację oraz opracowano metodykę badań elektronicznych podzespołów samochodowych. Na podstawie uzyskanych



Ryc. 5. Symulator sieci informatycznych w pojeździe Chrysler (PW SiMR).

Ryc. 6. Symulator sieci informatycznych dla pojazdu Audi A6 (PW SiMR).

Ryc. 7. Symulator sieci informatycznych dla pojazdów grupy BMW (CLKP).

Ryc. 8. Symulator sieci informatycznych dla pojazdów grupy Ford (CLKP).

Ryc. 9. Mobilne stanowisko badawcze.

Ryc. 10. Mobilne stanowisko badawcze.

Ryc. 11. Mobilne stanowisko badawcze.

Ryc. 12. Mobilne stanowisko badawcze.

wyników oraz doświadczeń zbudowano mobilne stanowisko badawcze (ryc. 9–14) oparte na zabudowie samochodu dostawczego. Do projektowania oraz prototypowej budowy wykorzystano zakupione w ramach konsorcjum meble, urządzenia diagnostyczne i inne materiały. Tak przygotowany prototyp pozwolił na wytypowanie przestrzeni roboczej, przetestowanie funkcjonalności oraz ułożenia urządzeń diagnostycznych i sprzętu laboratoryjnego. Po dokonaniu testów sporządzono szkice robocze, na podstawie których można było skonstruować właściwe stanowisko pozwalające na zachowanie zarówno funkcyjności wewnątrz, jak i odpowiednich parametrów jezdnych. Na podstawie opracowanych założeń wykonano właściwe mobilne stanowisko badawcze.

Mobilne stanowisko zostało wyposażone w niezbędne narzędzia, urządzenia diagnostyczne, aparaturę badawczą, mikroskop stereoskopowy. Zasilanie urządzeń odbywa się za pomocą zespołu akumulatorów, przetwornic napięcia oraz agregatu prądotwórczego. W kontenerze zamontowane zostały trzy zespoły gniazdek sieciowych, do których można podłączyć komputer, drukarkę oraz monitor. Zostało również wyprowadzone zasilanie 12 V do podłączenia badanych elektronicznych podzespołów samochodowych.

Sterowanie urządzeniami umieszczonymi w kontenerze odbywa się przez komputer pokładowy wyposażony w pulpit dotykowy, za którego pośrednictwem operator wybiera odpowiednie nastawy, takie jak:

Ryc. 13. Mobilne stanowisko badawcze.

Ryc. 14. Mobilne stanowisko badawcze.

– temperatura wewnątrz kontenera (ogrzewanie i chłodzenie, wentylacja),
– oświetlenie wewnątrz i na zewnątrz (zespół lamp umieszczonych w suficie kontenera barwy białej oraz niebieskiej, dwie lampki oświetlające miejsce pracy, sześć lamp zewnętrznych po dwie na stronę),
– rodzaj zasilania (z sieci, z agregatu lub silnika samochodu),
– układ zabezpieczenia przed przeciążeniem.

Firma TOMSAD wyprodukowała w ramach projektu po 23 komplety urządzeń Easy Dump i Smart Connect, które zostały przekazane po jednym komplecie do wszystkich laboratoriów kryminalistycznych KWP/KSP oraz wybranych placówek Straży Granicznej, których funkcjonariusze zajmują się zwalczaniem przestępczości samochodowej.

Zbudowane symulatory szkoleniowe są wykorzystywane do badań, ale przede wszystkim do szkolenia kandydatów na biegłych z zakresu badań mechanoskopijnych odbywających praktyki zawodowe w Zakładzie Broni i Mechanoskopii CLKP.

Mobilne stanowisko badawcze jest wykorzystywane przez biegłych z Zakładu Broni i Mechanoskopii CLKP do realizacji bieżących badań identyfikacyjnych pojazdów, szkoleń kandydatów na biegłych oraz udziału w różnego rodzaju akcjach międzynarodowych związanych ze zwalczaniem przestępczości samochodowej, takich jak np. działania zorganizowane przez Europol na granicy zewnętrznej Unii Europejskiej, w których trakcie biegli z CLKP zabezpieczali przejście graniczne między Słowacją i Ukrainą.

Najważniejszym efektem projektu jest wdrożenie i ugruntowanie badań podzespołów elektronicznych pojazdów do praktyki w laboratoriach kryminalistycznych Policji i Straży Granicznej.

Źródła rycin: *autorzy*

Projekt nr DOBR-BIO4/037/13175/2013 pt. „Pozyskiwanie do celów procesowych informacji zakodowanych w podzespołach elektronicznych pojazdów i maszyn roboczych" finansowany przez Narodowe Centrum Badań i Rozwoju w ramach konkursu nr 4/2013 na rzecz bezpieczeństwa i obronności państwa.

Narodowe Centrum Badań i Rozwoju