SOUDNÍ INŽENÝRSTVÍ

Ročník 35 • *01/2024*

Doprava • *Traffic and Transport*

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

Analýza vybraných diagnostických protokolů se zaměřením na manipulace s digitálním tachografem

Analysis of selected diagnostic protocols with a focus on digital tachograph manipulations

Ondřej Koutník*,[1], Robert Kledus[1]

[1] *Ústav soudního inženýrství, VUT v Brně*

Rozšířený abstrakt

Za účelem zvýšení bezpečnosti silniční nákladní dopravy, sociálních podmínek řidičů a spravedlivé hospodářské soutěže jsou Evropskou unií stanovena pravidla pro provozování silniční dopravy, která se týkají zejména omezení maximální doby řízení a minimální doby přestávek a odpočinku řidičů. Dodržování těchto pravidel je předmětem silničních kontrol, přičemž se využívají zejména výstupy z povinně instalovaného záznamového zařízení, tzv. tachografu.

Z toho vyplývá, že útok na systém tachografu by mohl přinést řidičům a potažmo i dopravcům, značnou výhodu v podobě možnosti řízení bez provedení náležitého záznamu o době jízdy. Metody manipulace tachografů se vyvíjely společně s jejich technickým vývojem a v současnosti se jedná o profesionální postupy, které cílí nejen na fyzické prvky systému tachografu, ale i na softwarovou úroveň.

Pro účely silničních kontrol, ale i pro znalecké zkoumání systému tachografu, je zásadní mít znalosti a dovednosti v oblasti diagnostiky řídících jednotek vozidel a technice nákladních vozidel. Specifikem zejména silničních kontrol je časový limit dostupný pro kontrolu vozidla a variabilita kontrolované techniky.

V této práci se autoři zaměřili na analýzu využití vybraných diagnostických protokolů ISO 14229 a SAE J1939 s cílem ověřit jejich obecnou použitelnost pro analýzu systému tachografu. Předmětem zkoumání v této práci budou tachografy výhradně digitální, nikoliv analogové. Autoři pro analýzu využili profesionálních softwarových nástrojů i hardware Vector Informatik GmbH, a tachograf výrobce Continental. Byl sestaven testbed s tachografem, CAN komunikačním kanálem a notebookem, který sloužil jako tester k odesílání příkazů a vyhodnocení odpovědí.

Na základě výzkumu byly identifikovány prvky norem aplikované v systému tachografu, avšak bez znalosti proprietárních specifikací systému a efektivní orientaci v normách je uvedená metoda pro analýzu tachografu použitelná jen velice omezeně. Principy reverzního inženýrství a Hardware in the Loop testování, podpořené znalostmi norem a architektury vozidla mohou pozitivně podpořit analýzu soustavy tachografu a detekci odchylek, resp. nestandardních stavů. V případech, kdy software řídících jednotek vozidla má implementované relevantní zprávy, lze je přes dotazování podle protokolu SAE J1939 využit k určení pravděpodobné přítomnosti manipulace ve vozidle. Toto je však limitované variabilitou jednotlivých výrobců vozidel.

Budoucí výzkum je tak vhodné zaměřit na úroveň embedded a software designu a identifikaci potencionálních metod vhodných pro analýzu tachografu. Současně je důležité sledovat prostřednictvím kontrolních složek nebo znalců v dopravě aktuální trendy v oblasti manipulací a tomuto přizpůsobovat i zaměření výzkumu. Nelze přitom vynechat ani nejnovější verze tachografů a nové modely nákladních vozidel. Pro snížení výskytu manipulací tachografu ve vozidlech je žádoucí i budoucí analýza právních předpisů upravující pravomoci kontrolních pracovníků a způsoby postihu (výše pokut v kombinaci dalších druhů postihu).

Klíčová slova: diagnostika, J1939, nákladní doprava, tachograf, UDS

Citace:
KOUTNÍK, Ondřej a KLEDUS, Robert. Analýza vybraných diagnostických protokolů se zaměřením na manipulace s digitálním tachografem. Online. *Soudní inženýrství*. 2024, roč. 35, č. 01, s. 30-39. ISSN 2788-2764. Dostupné z: https://doi.org/10.13164/SI.2024.1.30

DOI:
doi.org/10.13164/SI.2024.1.30

Korespondenční adresa autora:
ondrej.koutnik@vutbr.cz

Přijato do redakce:
04.03.2024
Recenzní řízení:
28.06.2024
Publikováno:
26.07.2024

Extended abstract

In order to improve the safety of road freight transport, the social conditions of drivers and fair competition, the European Union has laid down rules for the operation of road transport, in particular limiting maximum driving times and minimum breaks and rest periods for drivers. Compliance with these rules is the subject of roadside checks, using in particular the output of a compulsorily installed recording device, the tachograph.

It follows that an attack on the tachograph system could give drivers, and hence hauliers, a significant advantage in terms of being able to drive without a proper record of driving time. Methods of tampering with tachographs have evolved together with their technical development and they are now on a professional level, which focus not only the physical elements of the tachograph system but also the software level.

For the purposes of roadside inspections, but also for expert investigation of the tachograph system, it is essential to have knowledge and skills in vehicle control unit diagnostics and vehicular technology. A particular feature of roadside inspections is the time limit available for vehicle inspection and the variability of the technology inspected.

In this work, the authors have focused on the analysis of the use of selected diagnostic protocols ISO 14229 and SAE J1939 in order to verify their general applicability for tachograph system analysis. The subject of investigation in this article will be exclusively digital tachographs, not analogue ones. For the analysis, the authors used professional software tools and hardware from Vector Informatik GmbH, and a tachograph from the manufacturer Continental. A testbed with a tachograph, CAN communication channel and a laptop was built to serve as a tester to send commands (requests) and evaluate the responses.

Based on the research, the elements of the standards applied in the tachograph system were identified, but without knowledge of the proprietary system specifications and effective orientation in the standards, the above method is of very limited use for tachograph analysis. The principles of reverse engineering and Hardware in the Loop testing, supported by knowledge of standards and vehicle architecture, can positively support the analysis of the tachograph system and the detection of deviations or non-standard conditions. In cases where the vehicle control unit software has implemented relevant messages, these can be used to determine the likely presence of tampering in the vehicle using SAE J1939 protocol. However, this is limited by the variability of individual vehicle manufacturers.

Thus, future research should be focused at the embedded and software design level to identify potential methods suitable for tachograph analysis. At the same time, it is important to monitor current trends in the field of manipulation through inspection units or transport experts and to adapt the research focus accordingly. The latest versions of tachographs and new truck models should not be overlooked. To reduce the incidence of tachograph manipulation in vehicles, it is also desirable to analyse future legislation governing the powers of control officers and the methods of punishment (the level of fines in combination with other types of punishment).

Keywords: cargo transport, diagnostics, J1939, tachograph, UDS

Citation:
KOUTNÍK, Ondřej a KLEDUS, Robert. Analýza vybraných diagnostických protokolů se zaměřením na manipulace s digitálním tachografem. Online. *Soudní inženýrství*. 2024, roč. 35, č. 01, s. 30-39. ISSN 2788-2764. Dostupné z: https://doi.org/10.13164/SI.2024.1.30

DOI:
doi.org/10.13164/SI.2024.1.30

****Author's correspondence address:***
ondrej.koutnik@vutbr.cz

Accepted for editing:
March 04, 2024
Review proceedings:
June 28, 2024
Published:
July 26, 2024

1 ÚVOD

Na základě právních předpisů Evropské unie (EU) jsou digitální tachografy zařízení, která jsou instalována do vozidel uvedených poprvé do provozu na území EU od 1. května 2006 a která jsou buď určena pro více než 9 cestujících (včetně řidiče), nebo jsou určena pro komerční nákladní dopravu s celkovou přípustnou hmotností nad 3500 kg.

Systém tachografu zaznamenává dobu jízdy, dobu přestávek a odpočinku, začátek a konec pracovní doby, a u některých typů i čas a místo překročení hranic a typ přepravy (osobní/nákladní). Záznamy se personalizují pomocí digitální karty tachografu. Účelem tachografu je zaznamenávat uvedené údaje a tím umožnit kontrolu dodržování stanovených právních předpisů. Z toho tedy vyplývá, že vyřazení funkcí tachografu z provozu může být negativně ovlivněna jak únava řidičů související s vyšší pravděpodobnosti dopravní nehody, ale také lze identifikovat negativní vliv na dopravní trh a sociální podmínky řidičů.

Z praxe kontrolních složek v dopravě jsou známy případy nezákonných útoků (nebo-li manipulací) s cílem vyřadit z provozu funkci záznamu pohybu vozidla. Účelem kontroly systému tachografu při silniční kontrole, nebo při analýze dopravní nehody je ověřit, zda se v systému vyskytuje prvek jehož funkce může ovlivňovat funkci tachografu. Specifika této procedury vyžadují vysoce odborné znalosti a postupy zaměřené na potřeby kontrolních složek v dopravě.

2 POPIS SYSTÉMU TACHOGRAFU

Systém tachografu se skládá ze snímače pohybu, kabeláže a jednotky ve vozidle. Tento celek je specifikovaný předpisy EU a disponuje bezpečnostním certifikátem úrovně EAL4+. V tuzemsku jsou jeho kontroly a provoz dále upraveny předpisy z oblasti metrologie a silniční nákladní dopravy. Ve vozidlové komunikační síti funguje tachograf jako řídící jednotka, která komunikuje s okolními prvky prostřednictvím komunikačních sběrnic. Hlavní jednotka je umístěna v kabině řidiče a disponuje rozhraními:

- CAN sběrnice,
- K-line,
- Hallův snímač pohybu,
- specializované rozhraní na předním panelu založené na protokolech RS232 a ISO 14230,
- Bluetooth (tachograf 2. generace),
- Komunikace DSRC,
- Komunikace GNSS,
- Rozhraní digitální karty (autentizace, paměťové médium, určení provozního režimu).

V závislosti na uživateli jsou rozlišovány následující druhy karet tachografu:

- karta řidiče,
- karta podniku,
- karta dílny,
- kontrolní karta.

Podle druhu karty jsou na kartě nahrány vybrané kryptografické klíče, jejichž rozpoznání tachografem určuje jeho režim provozu (např. provozní, kalibrační, kontrolní…), v odborné terminologii někdy označované jako tzv. „ECU mode“.

Standardní funkce systému spočívá v tom, že tachograf pravidelně vyhodnocuje příchozí informace z externích zdrojů pohybu (druhy zdrojů jsou závislé na generaci tachografu) a na základě získaných dat zaznamenává činnosti řidiče. Varianty digitálních tachografů výrobců VDO Continental a Stoneridge jsou shrnuty, viz tabulka 1.

DOI: https://doi.org/10.13164/SI.2024.1.30

Tabulka 1 *Varianty digitálního tachografu (vybraní výrobci) [autor]*

Table 1 *Variants of digital tachograph (selected manufacturers) [author]*

Druh a verze tachografu	1. generace			2. generace	
	DIGITÁLNÍ TACHOGRAF 1.verze	**DIGITÁLNÍ TACHOGRAF 2.verze**	**DIGITÁLNÍ TACHOGRAF 3.verze**	**INTELIGENTNÍ TACHOGRAF 1.verze**	**INTELIGENTNÍ TACHOGRAF 2.verze**
Specifikující přepis	příloha IB nařízení (EHS) č. 3821/85 platné do 30.9. 2011	příloha IB nařízení (EHS) č. 3821/85 platné od 1.10. 2011 (vč. 1. změny dle nař.(EU) č. 1266/2009	Příloha IB nařízení (EHS) č. 3821/85 platné od 1.10. 2012 (vč. 2 změny dle nař.(EU) č. 1266/2009	Příloha IC nařízení (EU) 2016/799 platná od 15.6.2019	Příloha IC nařízení (EU) 2016/799 v aktuálním znění
VDO CONTINENTAL (verze)	DTCO 1381	DTCO 1381	DTCO 1381	DTCO	DTCO
	1.0 -1.3U	1.4 - 1.4b	od 2.0	4.0,4.0e	4.1
STONERIDGE (revize)	Stoneridge SE5000	Stoneridge SE5000	Stoneridge Exakt Duo SE5000	Stoneridge SE5000 Exakt Duo²	Stoneridge SE5000 Exakt Duo²
	Rel. 5 - 7.2	Rel. 7.3	od Rel. 7.4	Rel 8.0	Rel 8.1

V případě rychlosti vyšší než nula se automaticky zaznamená činnost „jízda/řízení“. V ostatních případech může být činnost zvolena řidičem na základě předpisů (odpočinek/přestávka, jiná činnost). Obecně jsou vnější zdroje pohybu identifikovány následovně:

- Hallův snímač pohybu v převodovce,
- nezávislý signál pohybu (IMS) - obvykle brzdový systém nebo GNSS (závisí na konkrétním vozidle a verzi tachografu).

Základní myšlenkou manipulace senzoru, komunikačního kanálu nebo některé z připojených jednotek je upravit všechny zdroje s informacemi o pohybu vozidla tak, aby jednotka tachografu získala ze všech zdrojů nulovou rychlost. To znamená, že pro úspěšnou manipulaci musí být při tomto způsobu manipulace napaden:

- v případě 1. generace tachografu Hallův snímač pohybu a komunikační sběrnice CAN (v případě povinné přítomnosti nezávislého signálu pohybu),
- v případě 2. generace 1. verze tachografu Hallův snímač pohybu, systém GNSS,
- v případě 2. generace, 2. verze tachografu, Hallův snímač pohybu, systém GNSS a vnitřní snímač v jednotce tachografu.

Podle místa útoku (manipulace) lze rozlišit dva typy útoku:

- ve snímačích, v komunikačních kanálech nebo připojených jednotkách,
- ve firmwaru tachografu.

V případě útoku na firmware se snímače a komunikační kanály nemodifikují. Místo toho je napaden mikrokontroler tachografu a pomocí zásahu do firmwaru tachografu potlačeny funkce záznamu pohybu.

V počátcích digitálních tachografů používali útočníci magnety instalované v těsné blízkosti Hallova snímače pohybu. Jak se snímače zdokonalovaly (stávaly se odolnými vůči magnetickému působení) a zavedl se druhý zdroj informací o pohybu vozidla (IMS), útoky byly více směřovány do elektronických prvků tachografu.

DOI: https://doi.org/10.13164/SI.2024.1.30

Na aplikační úrovni je implementován standardní diagnostický protokol (UDS) a protokol SAE J1939. Protokol UDS je popsán v normě ISO 14229 a poskytuje široké spektrum funkcí, jako je čtení dat z řídící jednotky (tzv. datových identifikátorů DID), čtení závad, kódování parametrů jednotky, bezpečnostní přístup k omezeným funkcím, flashování softwaru, diagnostické testy a některé další. Bližší specifikace protokolu pro systémy tachografu jsou uvedeny v normě ISO 16844-2.

3 REŠERŠE

Bezpečnost ve vozidlech je aktuálním tématem, protože ve vozidlech jsou rozšířena elektronická zařízení a existuje velká skupina odborníků s odbornými znalostmi v oblasti embedded systémů. Existuje velké množství prací zaměřených na bezpečnost vozidlové komunikace. Obvykle lze rozpoznat dva cíle útočníků. Prvním cílem je vyřadit systém z provozu a způsobit finanční ztráty, škody nebo zranění. Druhý cíl poukazuje na modifikaci funkcí systému, únik dat nebo narušení soukromí [1].

Obecný přístup je popsán v [2], kde jsou ukazatele manipulace CAN sběrnice popsány v osmi třídách (formálnost, umístění, rozsah, frekvence, korelace, protokol, věrohodnost, konzistence). Některé z nich jsou použitelné i v praxi tachografů s přihlédnutím k reálným podmínkám v nákladním vozidle, principům tachografu a manipulačních zařízení. Systémy detekce manipulací jsou založeny na identifikaci anomálií. Anomálie jsou chápány jako podobnost chování s existujícím útokem, nebo jako odchylka od normálních stavů v komunikaci. Používané metody jsou například strojové učení [3], nebo neuronové sítě [4]. Práce zaměřené na útoky s využitím protokolů UDS jsou např. v pracích [5] nebo [6], které však cílí na jiné systémy a na tachografy nejsou aplikovatelné.

Odborné znalosti jsou rovněž v působnosti kontrolních složek v dopravě v Evropské unii, ale je zde úzká vazba na komerční sektor. V tomto případě mohou existovat hranice v podobě finančního rozpočtu na výzkum na straně státních institucí a omezení v přístupu k chráněným informacím na straně komerčních společností. Know-how veřejných složek není veřejně dostupné a je v podobě interních technických poznámek a postupů.

4 HYPOTÉZY

V současné době neexistuje účinný obecně použitelný způsob, jak ověřit přítomnost manipulace (tzn. dodatečně přidaného zařízení, nebo úpravy ve stávajícím zařízení) v systému tachografu. Toto je nezbytné jak pro kontrolní činnost v oblasti dopravy, tak i pro znaleckou činnost v této oblasti. Některé manipulace lze diagnostikovat prostřednictvím kapacit výrobce tachografu, avšak tento proces je destruktivní, nákladný a časové náročným, což neodpovídá potřebám praxe silničních kontrol.

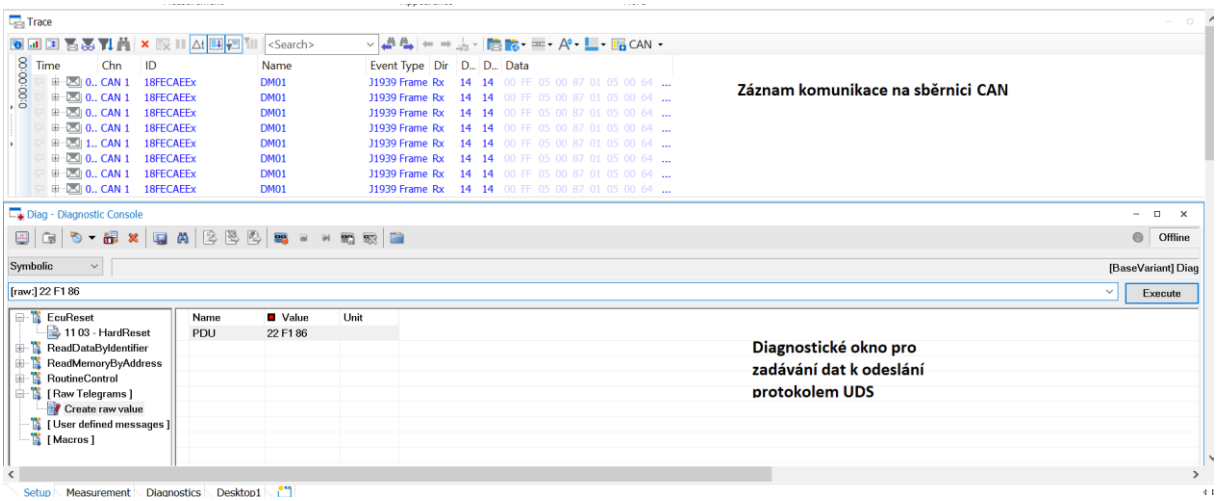
Současné manipulace jsou již na technické úrovni, kdy již často nelze jejich přítomnost odvodit pouze ze záznamu o době řízení, přestávek a odpočinku řidiče, a pro nalezení dalších indicií manipulace je nezbytné analyzovat i další systémy vozidla. Autoři se v této práci proto zaměřili na analýzu využitelnosti funkcí protokolů pro specifickou kontrolu systému tachografu a identifikaci ovlivnění tachografu ve vozidle. Využití protokolů předpokládá nedestruktivní postupy. Práce se zaměřuje na následující cíle:

1. Ověření hypotézy, že protokol UDS je obecně použitelný pro analýzu systému tachografu s ohledem na jeho nelegální manipulaci.
2. Ověření hypotézy, že protokol SAE J1939 je obecně použitelný pro analýzu systému tachografu s ohledem na jeho nelegální manipulaci.

5 OVĚŘENÍ HYPOTÉZ

Pro analýzu systému tachografu autoři využili rozhraní firmy Vector VN1610 s 2x CAN rozhraním a software CANoe PRO s funkcemi interpretace protokolů UDS i SAE J1939 i implementovaným protokolem ISO TP, náhled viz obrázek 1.

DOI: https://doi.org/10.13164/SI.2024.1.30



Obrázek 1 *Prostředí programu Vector CANoe (s popisem autorů) [autor]*

Figure 1 *Environment of software Vector CANoe (description by authors) [author]*

Testovaným tachografem byl model 1381 1 generace, 3. verze od výrobce Continental, parametrizovaný na vozidla výrobce Scania. Pro testovací účely bylo vytvořeno propojení mezi 8 pinovým rozhraním tachografu a rozhraním DB-9, kterým disponuje kabeláž rozhraní VN 1610.

Tabulka 2 *Příklad požadavku a odpovědi UDS protokolu [autor]*

Table 2 *Example of request and response according UDS protocol [author]*

	Servis [hex]	**Datový identifikátor* [hex]**
Požadavek	22	F1 91 (číslo hardwaru)
Odpověď	62	F1 91+ (číslo hardwaru)

* Využita délka jen 2 byty [bajty]; vícenásobný datový identifikátor nebyl brán v potaz

S využitím protokolu UDS byla otestována implementace servisů, jejichž stručný popis i implementace v jednotce, viz tabulka 2 výše a následující tabulka 3. Kromě servisu 10 testy probíhaly v provozním režimu tachografu. Pro servis 10 byl využit kalibrační režim. Existence implementace servisu je pro další i budoucí analýzy nezbytnou základní informací.

Tabulka 3 *Identifikované implementované servisy [autor]*

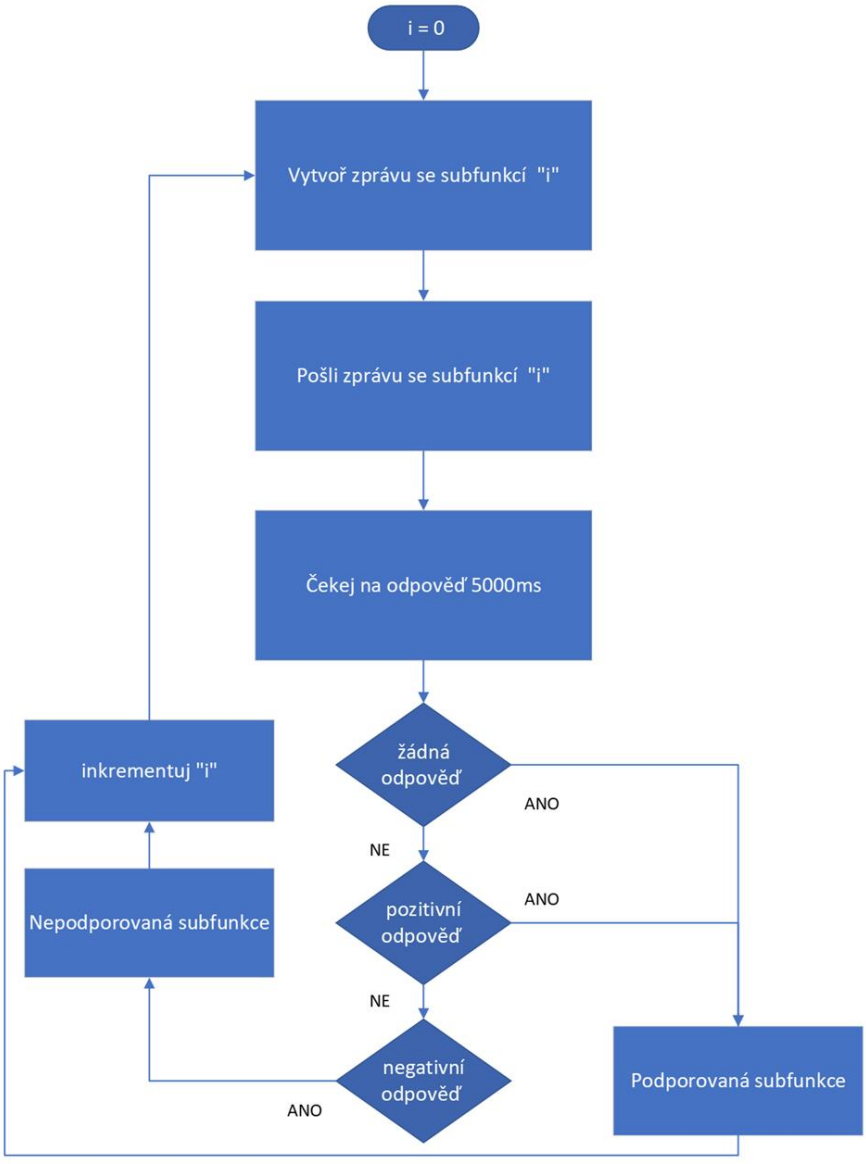
Table 3 *Identified implemented services [author]*

Servis (hexadecimální vyjádření)	**Implementace v tachografu**	**Popis**
10 – vstup do diagnostického módu	Ano	Umožňuje volbu módu pro spouštění dalších funkcí.
11 – reset jednotky	Ano	Umožňuje vyvolat výrobcem specifikované druhy resetu.
14 – mazání diagnostických chyb	Ne	Maže chybovou paměť.
19 – čtení diagnostických chyb	Ano	Vyčítá chybovou paměť ve zvolených režimech dle subfunkce
22 – čtení dat z datového identifikátoru	Ano	Vyčítá datové identifikátory.
23 – čtení dat podle adresy paměti	Ne	Vyčítá obsah paměťi dle adresy.
27- zabezpečený přístup	Ne	Odemyká jednotku pro použití zabezpečených funkcí.
28 – řízení komunikace	Ano	Umožňuje ovládat posílání některých zpráv na sběrnici.

DOI: https://doi.org/10.13164/SI.2024.1.30

Servis (hexadecimální vyjádření)	Implementace v tachografu	Popis
85 řízení záznamu chyb	Ne	Umožňuje ovládat záznam chyb do paměti.
2E – záznam dat do datového identifikátoru	Ne	Umožňuje zápis do datového identifikátoru.
3E – přítomnost testovacího zařízení	Ano	Indikuje přítomnost testovacího zařízení pro setrvání ve vybraném diagnostickém módu.

Nejprve byly otestovány datové identifikátory udávané normou UDS a ISO 16844, přičemž se ukázalo, že standardizovaná data poskytují informace většinou informativního charakteru bez aplikovatelnosti na manipulace s tachografem. Dále se testovala funkčnost definovaných subservisů a parametrů. Pro testování dostupných diagnostických módů nad rámec norem bylo využito testování hrubou silou, kdy se pro servis 0x10 procházely možnosti pro subfunkci a sledovala se odezva. Díky rozsahu pouze 1 byte (rozsah 0x00 až 0xFF v hexadecimální soustavě) se jednalo o 255 možností. Automatický algoritmus byl vytvořen ve skriptovacím jazyku CAPL, který je zahrnut v nástrojích Vector, návrh algoritmu, viz obrázek 2.



Obrázek 2 *Testovací algoritmus [autor]*

Figure 2 *Test algorithm [author]*

DOI: https://doi.org/10.13164/SI.2024.1.30

Výstupem bylo tedy zjištění dostupných módů: 0x01, 0x03, 0x02, 0x81, 0x85, a 0x87. Přičemž úrovně 0x85 a 0x87 jsou k dispozici pouze v kalibračním režimu. U dalších servisů bylo také využito pokusů s analýzou hrubou silou, nicméně s rostoucí délkou parametrů zprávy, přičemž tyto parametry jsou neveřejné, se jeví analýza hrubou silou jako velice časově náročná až téměř nemožná. Testování bylo prováděno v délce 72 hodin bez pozitivních výsledků.

Dále se autoři zaměřili na detekci dostupných rutin v tachografu, které mohou sloužit pro spuštění interních testů např. tlačítek, kontrolního součtu kódu, tiskárny, nebo pro vyvolání vstupu do bootloaderu jednotky. Výrobce však implementoval i do standardizovaných rutin nad rámec standardu dodatečné byty, proto jednotka vrací negativní odpověď s informací o nesprávné délce zprávy, a to jak v provozním tak i v kalibračním režimu. Testováno bylo i s využitím nedefaultního diagnostického módu. Pro další využití se jeví protokol UDS jako velice obtížně využitelný bez dalších znalostí specifikací systému. Tyto specifikace lze částečně zjistit metodami reverzního inženýrství, které však vyžadují další znalosti z oblasti diagnostiky na úrovni protokolu a samotný proces je náročný na čas a další zdroje.

Dále se autoři zaměřili na softwarové manipulace, kde se vycházelo z faktu, že zmanipulovaný tachograf a originální tachograf budou vykazovat v odpovědích na tyto standardizované UDS požadavky diference. Autoři měli možnost otestovat hypotézu na softwarově zmanipulovaném tachografu, proto dále využili komparativní metodu, a došlo ke srovnávání odpovědí UDS požadavků nicméně nedošlo k pozorování rozdílů a proto lze konstatovat, že softwarová manipulace v aktuálním odhaleném provedení nemá vliv na UDS komunikaci.

U druhé hypotézy došlo k analýze protokolu SAE J1939, který je implementován v nákladních vozidlech v aplikační úrovni CAN protokolu. Nad rámec testování výčtu dostupných parametrů (jako tomu bylo u UDS protokolu v první hypotéze) se pracovalo s upravenou hypotézou, která vycházela z faktu, že u vozidel s digitálním tachografem první generace dochází při manipulaci s tachografem k záznamu rozdílného počtu ujetých kilometrů do různých řídících jednotek. Ověření plausibility dat z různých zdrojů tedy může dle provedených měření sloužit pro detekci podezřelých stavů tachografu. Byly využity standardizované dotazovací zprávy s využitím dalších specifik v části J1939 Digital Annex, které obsahují zprávy o ujeté vzdálenosti a průměrné spotřebě paliva na ujetý kilometr, viz tabulka 4.

Tabulka 4 *Struktura zpráv dle SAE J1939 [autor]*

Table 4 *Message structure according SAE J1939 [author]*

Priorita zprávy	Požadavek	Identifikátor cílové jednotky	Adresa testovacího zařízení	Dotaz			Zjišťovaný signál
18	EA	00 (jednotka motoru)	F9	E0	FE	00	Celková ujetá vzdálenost vozidla
18	EA	FF	F9	BC	FE	00	Celková ujetá vzdálenost brzdového systému

V rámci testovacího pokusu byly tyto dotazovací zprávy zaslány po CAN sběrnici vozidla DAX XF, modelový rok 2018. Zjištěným pokusem byly zjištěny informace, viz tabulka 5.

Tabulka 5 *Zjištěné hodnoty [autor]*

Table 5 *Measured values [author]*

Ujetá vzdálenost dle tachografu	832 251 km
Ujetá vzdálenost dle řídící jednotky brzd	980 022 km
Rozdíl absolutní	147 771 km
Rozdíl procentuální (zaokrouhleně)	17,75 %

U předmětného vozidla došlo při kontrole k podezření na nelegální manipulaci s tachografem, neboť řídící jednotka brzd vykazovala větší ujetou vzdálenost než tachograf, a to o 17,75 %. Za běžnou lze považovat odchylku, která vzniká při získávání veličiny rychlosti odlišnými senzory a jejím následným zpracováním, a jedná se o odchylku přibližně do 5 %, přičemž tato hodnota se bude budoucím výzkumem dále upřesňovat. Nelegální

DOI: https://doi.org/10.13164/SI.2024.1.30

manipulace se následně potvrdila i hloubkovou kontrolou systému tachografu. Byla nalezena dodatečně instalovaná elektronika na principu CAN brány, která simuluje jednotku tachografu, viz obrázek 3.

Obrázek 3 *Snímač pohybu a manipulační zařízení v černém pouzdru [autor]*

Figure 3 *Motion sensor and manipulation device in the black case [author]*

Uvedená metoda byla dále zkoušena na vozidlech zn. Scania, a Volvo, avšak bez pozitivní odezvy. Pro další rozšíření metody do praxe by bylo potřeba ještě další zkoumání na větší sérii vozidel různých parametrů, což je však nad rámec této práce. Nutno také konstatovat, že v případě výměny jednotky brzd, lze touto metodou dojit k falešně pozitivnímu výsledku, a proto je nutné i přes nižší výskyt této situace v praxi, brát toto omezení při praxi v potaz.

6 DALŠÍ VÝZKUM

Na základě této práce se otevírají další témata pro budoucí výzkum, kterými jsou zejména nalezení dalších znaků značící nelegální manipulaci s tachografem a jejich unifikované vyčtení přes diagnostické protokoly, vstup do dalších částí paměti tachografu a standardizace procesů pro většinově zastoupená vozidla na trhu vozidel pro nákladní dopravu. Budoucí výzkum si tak pravděpodobně bude žádat využití dalších profesionálních nástrojů pro vývoj embedded systémů a rozšíření dalších znalostí na nižších úrovních mikrokontroleru. Otevřena je také oblast právních předpisů v problematice tachografů, kde lze najít problémy pro řešení.

7 ZÁVĚR

Autoři v práci analyzovali obecné možnosti protokolu UDS a SAE J1939 pro nedestruktivní analýzu systému tachografu se zaměřením na jeho nelegální manipulace. I přes rozsáhlé možnosti protokolů je identifikovatelná aplikovaná pouze vybraná menší část, neboť většina specifikací jednotky je proprietární a veřejnosti nepřístupná. V některých případech lze tyto specifikace zjistit reverzním inženýrstvím (např. analýza hrubou silou), avšak toto v mnoha případech nelze obecně aplikovat z důvodu značné náročnosti na čas i další zdroje (znalosti, hardware, software). U aplikovatelných funkcionalit protokolů je potřeba mít na zřeteli velkou provozní variabilitu, a to jak mezi jednotlivými výrobci vozidel, tak někdy i mezi modelovými roky jednotlivých typů vozidla. Na místě by byla pro lepší detekci manipulací s tachografem větší součinnost výrobců jak tachografů, tak i vozidel.

8 PODĚKOVÁNÍ

Článek byl podpořen v rámci specifického výzkumu na ÚSI VUT 2023 pod projektem ÚSI-J-23-8313.

9 Reference

[1] FAKHFAKH, Faten; TOUNSI, Mohamed a MOSBAH, Mohamed. Cybersecurity attacks on CAN bus based vehicles: a review and open challenges. Online. *Library Hi Tech*. 2022, roč. 40, č. 5, s. 1179-1203. ISSN 0737-8831. Dostupné z: https://doi.org/10.1108/LHT-01-2021-0013. [cit. 2024-03-24].

[2] MUTER, Michael; GROLL, Andre a FREILING, Felix C. A structured approach to anomaly detection for in-vehicle networks. Online. In: *2010 Sixth International Conference on Information Assurance and Security*. IEEE, 2010, s. 92-98. ISBN 978-1-4244-7407-3. Dostupné z: https://doi.org/10.1109/ISIAS.2010.5604050. [cit. 2024-03-24].

[3] LOUKAS, George; VUONG, Tuan; HEARTFIELD, Ryan; SAKELLARI, Georgia; YOON, Yongpil et al. Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning. Online. *IEEE Access*. 2018, roč. 6, s. 3491-3508. ISSN 2169-3536. Dostupné z: https://doi.org/10.1109/ACCESS.2017.2782159. [cit. 2024-03-24].

[4] PAUL, Avishek a ISLAM, Md Rabiul. An Artificial Neural Network Based Anomaly Detection Method in CAN Bus Messages in Vehicles. Online. In: *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*. IEEE, 2021, s. 1-5. ISBN 978-1-6654-3843-8. Dostupné z: https://doi.org/10.1109/ACMI53878.2021.9528201. [cit. 2024-03-24].

[5] RING, Martin, Tobias RENSEN a Reiner KRIESTEN. Evaluation of Vehicle Diagnostics Security – Implementation of a Reproducible Security Access [online]. Lisbon: IARIA, 2014 [cit. 2024-01-20]. ISBN 978-1-61208-376-6. ISSN ISSN: 2162-2116. Dostupné z: https://www.researchgate.net/publication/275463281_SECURWARE_2014_-_The_Eighth_International_Conference_on_Emerging_Security_Information_Systems_and_Technologies

[6] VALASEK, Chris a MILLER, Charlie. Adventures in Automotive Networks and Control Units. Online. 2014, s. 1-99. Dostupné z: https://ioactive.com/car-hacking-content/. [cit. 2024-03-27].

DOI: https://doi.org/10.13164/SI.2024.1.30