VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2020 Bc. Vojtěch Matoušek

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY
DEPARTMENT OF CONTROL AND INSTRUMENTATION

VZDÁLENÉ ZÍSKÁVÁNÍ DAT Z DIGITÁLNÍHO TACHOGRAFU
REMOTE DATA DOWNLOADING FROM AUTOMOTIVE DIGITAL TACHOGRAPH

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Vojtěch Matoušek

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Petyovský, Ph.D.

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Kybernetika, automatizace a měření**

Ústav automatizace a měřicí techniky

Student: Bc. Vojtěch Matoušek ***ID:*** 186539
Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Vzdálené získávání dat z digitálního tachografu

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je navrhnout a realizovat firmware pro komunikační zařízení umožňující vzdálené získávání dat z digitálního tachografu motorových vozidel.

1. Seznamte se s problematikou využívání a legislativou digitálních tachografů pro motorová vozidla. Nastudujte vlastnosti otevřeného komunikačního protokolu určenému k získávání dat z digitálních tachografů.
2. Nastudujte vlastnosti a funkce sběrnic využívaných ke komunikaci s digitálními tachografy ve vozidle. Popište formát dat poskytovaný digitálními tachografy. Pořiďte testovací množiny s těmito daty.
3. Popište infrastrukturu a funkcionality pro komunikaci s nadřazeným serverem. Navrhněte koncepci celého řešení a popište jeho jednotlivé komponenty.
4. Definujte požadavky na vlastní firmware pro existující komunikační zařízení obsahující GSM modul. Doplňte další požadavky s ohledem na vzdálené ukládání dat na nadřazený server.
5. Realizujte firmware pro komunikační zařízení.
6. Vytvořte uživatelský SW na PC pro konfiguraci firmware komunikačního zařízení.
7. Funkčnost celého zařízení demonstrujte na praktickém příkladu.
8. Zhodnoťte nové funkce celého zařízení, navrhněte další možná vylepšení.

DOPORUČENÁ LITERATURA:

[1] PŘIBYL, P., SVÍTEK, M.: Inteligentní dopravní systémy, 1. vydání, BEN 2002, ISBN 9788073000295.

[2] Heavy Truck Electronic Interfaces Working Group.: Digital Tachograph Specification for remote company card authentication and remote data downloading [online]. 2018 [cit. 22.8.2019]. Dostupné z URL: <http://www.fms-standard.com/Truck/down_load/User_Guide_Version_02.01_181209.pdf>.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 1.6.2020

Vedoucí práce: Ing. Petr Petyovský, Ph.D.
Konzultant: Ing. Jan Němec (NAM system, a.s.)

doc. Ing. Václav Jirsík, CSc.
předseda oborové rady

ABSTRAKT

Tato diplomová práce se zabývá návrhem firmwaru zařízení umístěného v nákladním vozidle, které zajišťuje vzdálený přístup k datům digitálního tachografu vozidla dle požadavků legislativy EU. Výsledkem této práce je systém, který stáhne data z digitálního tachografu a uloží je na vzdálený server. Systém pro vzdálené stahování dat z digitálního tachografu se skládá ze třech druhů aplikací: aplikace serveru, aplikace uživatele a firmwaru pro komunikační zařízení. Komunikace mezi aplikacemi probíhá pomocí šifrovaného TCP spojení a speciálně vytvořených zpráv.

KLÍČOVÁ SLOVA

digitální tachograf, tachografové karty, autentifikace, CAN, ESM, telematické systémy, vzdálený přístup, klient - server, ISO 15765-2

ABSTRACT

Thesis deals with device firmware design located in lorry, which provides remote access to vehicle digital tachograph data according to valid EU legislation. The result of this work is a system, which downloads digital data from digital tachograph and save them on remote server. The system for remote data downloading from automotive digital tachograph consists of three kinds of applications: server application, user application and firmware for communication device. Communication between applications uses encrypted TCP connection and own special designed messages.

KEYWORDS

digital tachograph, tachograph cards, authentication, CAN, ESM, telematic systems, remote access, client - server, ISO 15765-2

MATOUŠEK, Vojtěch. *Vzdálené získávání dat z digitálního tachografu*. Brno, 2020, 77 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav automatizace a měřicí techniky. Vedoucí práce: Ing. Petr Petyovský, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Vzdálené získávání dat z digitálního tachografu“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno 1. 6. 2020 .....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Petru Petyovskému, Ph.D. a konzultantovi panu Ing. Janu Němcovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. V poslední řadě bych rád poděkoval společnosti NAM system a.s. za dodání veškerého vybavení potřebného k úspěšnému zvládnutí diplomové práce.

Brno 1. 6. 2020 .....

podpis autora

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

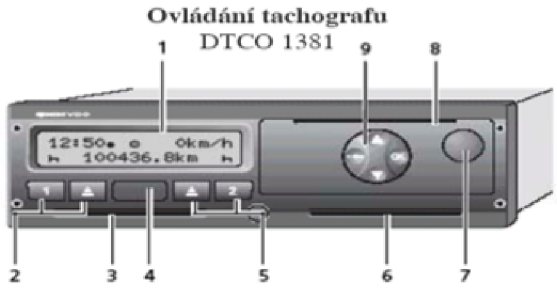
Digitální tachograf je záznamové zařízení montované do nákladních automobilů a autobusů za účelem sledování informací o řidiči, voze a jízdě, v podobě digitálních dat. Každý dopravce je povinen podle platné legislativy EU [6] umístit digitální tachograf do každého nákladního automobilu, zaznamenávaná data stahovat a také archivovat.

V případě obsáhlého vozového parku dopravce je značně obtížné realizovat stahování dat z každého digitálního tachografu nákladního vozidla. Proto dopravci v této době přecházejí ke vzdálenému stahování dat, čímž se zabývá i tato diplomová práce. Systém vzdáleného stahování dat spadá pod tzv. dopravní telematické systémy [1]. Což je technologický obor, zabývající se kombinací přenosu a zpracování dat se zobrazovacími a jinými sdělovacími prostředky, používaný v dopravě.

Tato práce obsahuje stručný popis problematiky digitálních tachografů, jejich legislativy, popis používaných sběrnic v digitálním tachografu a formát dat poskytovaných digitálním tachografem. V rámci této diplomové práce navrhnu také koncepci celého řešení vzdáleného stahování dat. Pro správnou funkci celého systému vzdáleného stahování dat z digitálního tachografu navrhnu aplikaci pro server, aplikaci klienta pro uživatelské funkce na ovládání systému vzdáleného stahování dat a firmware pro komunikační zařízení, které bude data z digitálního tachografu stahovat. Na konci této diplomové práce lze také najít demonstraci funkčnosti celého systému vzdáleného stahování dat z digitálního tachografu, zhodnocení všech funkcí celého systému a navržení případných vylepšení aplikací pro vzdálené stahování dat z digitálního tachografu.

2 Digitální tachograf

Jak už bylo řečeno v úvodu, digitální tachograf je záznamové zařízení montované do nákladních automobilů a autobusů. Data (např.: informace o řidiči, voze, kontrolách atd.), která zaznamenává digitální tachograf, se ukládají do vnitřní paměti tachografu nebo na čipové paměťové karty, které slouží jako přenosné záznamové medium. Vzhled a uspořádání tlačítek digitálních tachografů se může mírně lišit v závislosti na verzi či výrobci digitálních tachografů. Na obrázku 2.1 lze vidět vzhled digitálního tachografu VDO DTCO 1381 od výrobce Siemens [4].



Obr. 2.1: Vzhled digitálního tachografu Siemens VDO DTCO 1381 [4]

(1) Displej
(2) Tlačítka řidiče 1
(3) Vstup na kartu 1
(4) RS232 rozhraní pro stahování dat
(5) Tlačítka řidiče 2
(6) Vstup na kartu 2
(7) Tlačítko pro otevření zásuvky tiskárny
(8) Trhací hrana tiskárny
(9) Tlačítka menu

Do digitálního tachografu lze najednou vložit maximálně dvě paměťové karty. Data z karet a digitálního tachografu lze kromě stažení přes RS232 nebo CAN sběrnici vytisknout pomocí integrované tiskárny.

2.1 Paměťové karty digitálního tachografu

Paměťová karta digitálního tachografu je čipová karta, která dovoluje zjistit identitu držitele karty. Umožňuje přenos dat a ukládání dat, která se týkají činností uživatelů záznamového zařízení. Uživatelem záznamového zařízení jsou řidiči, dopravní

podniky, dílny pro opravu tachografu a kontrolní orgány. Každý z těchto uživatelů má speciální typ čipové karty s jinými právy použití [4].

- **Karta řidiče** slouží k identifikaci řidiče a ukládání dat o řidiči. Tato karta má bílou barvu [7].

- **Karta podniku** slouží k identifikaci podniku digitálního tachografu a k povolení stažení dat z digitálního tachografu pro účely podniku. Karta podniku má žlutou barvu [7].

- **Karta dílny** slouží k identifikaci dílny, která provádí servis digitálních tachografů a má červenou barvu [7].

- **Kartu kontroly** používá kontrolní orgán za účelem zjišťování dodržování předpisů o používání digitálních tachografů a má modrou barvu [7].

Struktura dat na paměťových kartách tachografu je rozdělena do stromové struktury. Hlavní soubor se nazývá master file (MF), který se člení na soubory dedicated file (DF) a elementary file (EF). DF obsahuje jiné soubory EF nebo DF. EF je elementární soubor dat (obsahuje různé typy informací, certifikáty atd.). Ukázka struktury dat na jednotlivých paměťových kartách tachografu je v příloze B.

2.1.1 Komunikace s paměťovými kartami

Paměťové karty digitálního tachografu se řídí souborem mezinárodních norem ISO/IEC 7816. Tento soubor norem popisuje umístění kontaktů, elektrické rozhraní, protokoly přenosu, bezpečnost, příkazy pro správu karet atd.

Pro komunikační rozhraní čipové karty jsou definovány dva přenosové protokoly: T=0 a T=1. Rozdíly mezi protokoly jsou popsány v dokumentu: Nařízení komise (ES) č. 1360/2002 na straně 380, viz [7]. Pro komunikaci s kartami se používá čtečka paměťových karet. Před samotnou komunikací s kartou je potřeba zjistit informace o kartě (typ karty, jaký používá protokol, výrobce karty atd.). K tomuto účelu se používá událost RESET, jejíž součástí je generování bloku dat nazývaného jako odpověď na reset, který je označován zkratkou ATR (Answer-to-Reset). Po odpovědi na reset je hlavní soubor MF implicitně vybrán a stává se aktuálním adresářem. Komunikace s čipovou kartou probíhá pomocí tzv. APDU příkazů (Application Protocol Data Unit) [7]. Typy jednotlivých APDU popisuje tabulka 2.1.

Tab. 2.1: Typy APDU příkazů [7]

APDU příkaz	**Význam**
SELECT FILE	Vybere soubor ve struktuře dat čipové karty.
READ BINARY	Používá se ke čtení EF.
UPDATE BINARY	Aktualizuje bity v EF.
GET CHALLENGE	Vyžaduje vydání výzvy (např. náhodné číslo) pro použití v proceduře související se zabezpečením (např. příkaz EXTERNAL AUTHENTICATE). Výzva je platná pouze pro příští příkaz.
VERIFY	Ověření správnosti PINu dat.
GET RESPONSE	Použití pro přenos připravených dat z karty do zařízení rozhraní (čtečky čipové karty).
VERIFY CERTIFICATE	Příkaz používá čipová karta k získání veřejného klíče a ke kontrole jeho platnosti.
INTERNAL AUTHENTICATE	Použitím příkazu může IFD (interface device - zařízení rozhraní) ověřit pravost karty.
EXTERNAL AUTHENTICATE	Tímto příkazem může karta prokázat totožnost IFD.

Po každém příkazu APDU následuje odpověď od čipové karty, která obsahuje vždy dva stavové bajty SW1, SW2. Dále odpověď může obsahovat také data v závislosti odpovědi na konkretní APDU. Stavové bajty označují zpracování příkazů APDU v čipové kartě viz. tabulka 2.2.

Tab. 2.2: Ukázka typů značení stavových bajtů [7]

SW1 [hex]	**SW2 [hex]**	**Význam**
90	00	Normální zpracování.
61	XX	Normální zpracování. XX = počet platných bajtů odezvy.
62	81	Zpracování výstrahy. Část vrácených dat může být poškozená.
63	CX	Chybný PIN. Čítač zbývajících pokusů X.
64	00	Chyba provedení - stav stálé paměti nezměněn. Chyba integrity.
65	00	Chyba provedení - stav stálé paměti změněn.
65	81	Chyba provedení - stav stálé paměti změněn - porucha paměti.
66	88	Chyba bezpečnosti.
67	00	Chybná délka.

SW1 [hex]	SW2 [hex]	Význam
69	00	Zakázáný příkaz.
69	82	Status bezpečnosti nesplněn.
69	83	Metoda ověřování pravosti zablokována.
69	85	Podmínky použití nesplněny.
69	86	Nedovolený příkaz (není vybráno žádné aktuální EF).
69	87	Očekávané datové objekty bezpečného zpracování zpráv chybí.
69	88	Nesprávné datové objekty bezpečného zpracování zpráv.
6A	82	Datové soubory nenalezeny.
6A	86	Chybné parametry.
6A	88	Referenční data nenalezena.
6B	00	Chybné parametry (offset mimo EF).
6C	XX	Chybná délka, SW2 udává přesnou délku. Žadné datové pole není vráceno.
6D	00	Kód příkazu není podporován, nebo je neplatný.
6E	00	Třída příkazu není podporována.
6F	00	Jiné kontrolní chyby.

Detailní popis jednotlivých APDU a odpovědí lze zhlédnout v [7] na str. 383-393.

2.2 Data zaznamenávaná digitálním tachografem

Digitální tachograf ukládá a zaznamenává data do svojí vnitřní paměti a na paměťovou kartu řidiče. Následně tato data lze z digitálního tachografu stáhnout. Stažená data se poté uchovávají pomocí souboru ESM (External Storage Media) s příponou `ddd`.

2.2.1 Záznam a uložení dat do vnitřní paměti tachografu

Paměť digitálního tachografu je schopna uchovat data nejméně 365 kalendářních dní průměrné činnosti řidiče ve vozidle. Po vyčerpání paměťové kapacity jsou nejstarší data uložená v paměti přepisována nejnovějšími daty. Průměrnou činností řidiče za jeden den ve vozidle se rozumí činnost nejméně šesti řidičů nebo druhých řidičů, 6 cyklů vložení a vyjmutí karty a 256 změn činností denně. Při tomto vytížení se připíše denně na tachografovou kartu cca 3 kB nových dat. Digitální tachograf zaznamenává a ukládá do vnitřní paměti následující údaje [7]:

1. **Údaje identifikující zařízení:**
   - **Identifikační údaje digitálního tachografu ve vozidle:** jméno výrobce, adresa výrobce, číslo typu zařízení, výrobní číslo, rok výroby zařízení, číslo schválení typu.
   - **Identifikační data snímače pohybu:** jméno výrobce, adresa výrobce, číslo typu snímače, výrobní číslo a číslo schválení typu.

2. **Bezpečnostní prvky:** evropský veřejný klíč, certifikát členského státu, certifikát zařízení a soukromý klíč zařízení.

3. **Data související s vložením a vyjmutím karty řidiče:** jméno a příjmení držitele karty, číslo karty, členský stát vydávající kartu, datum platnosti karty, hodnotu údaje na měřiči ujeté vzdálenosti v době vložení a vyjmutí karty, slot, do kterého byla karta vložena, datum a čas vložení a vyjmutí karty.

4. **Data o činnosti řidiče:** stav řízení vozidla (posádka, samotný řidič), otvor pro vkládání karet (řidič, druhý řidič), stav karty v příslušném otvoru pro vkládání karet (vložená, nevložená), činnost (jízda, pohotovost, práce, přestávka/odpočinek), datum a čas změny.

5. **Údaje měřiče ujeté vzdálenosti:** počet ujetých kilometrů vozidla.

6. **Podrobná data o rychlosti:** záznam aktuální rychlosti vozidla každou sekundu. Tento záznam se každých 24 hodin přemazává novými údaji.

7. **Údaje o událostech:** rozpor karet (tato událost nastane, jestliže se vložením dvou platných karet do digitálního tachografu dosáhne nedovolené kombinace, viz tabulka v příloze C), jízda bez náležité karty, vložení karty v průběhu jízdy, nesprávně ukončené poslední vložení karty, překročení povolené rychlosti, přerušení elektrického napájení, chybné údaje o pohybu vozidla a pokus o narušení bezpečnosti systému.

8. **Údaje o závadách:** závada karty a závada digitálního tachografu.

9. **Kalibrační údaje:** známé kalibrační parametry (obvod pneumatiky, charakteristický koeficient vozidla, konstanta záznamového zařízení a rozměr pneumatiky) v okamžiku aktivace, první kalibrace po aktivaci, první kalibrace v současném vozidle a pět posledních kalibrací.

10. **Data o nastavení času:** čas posledního nastavení času.

11. **Data o kontrolní činnosti:** datum a čas kontroly, číslo kontrolní karty, členský stát vydávající kartu, typ kontroly (zobrazování, tisk nebo stahování dat z digitálního tachografu nebo z karty).

12. **Data o zámcích podniku:** datum a čas uzamčení, datum a čas odemknutí, číslo karty podniku a členský stát vydávající kartu, jméno a adresa podniku.

13. **Údaje o stahování dat:** datum a čas stahování dat, číslo karty podniku nebo karty dílny a členský stát vydávající kartu, jméno podniku nebo dílny.

14. **Údaje o specifických podmínkách:** datum a čas vkládání specifických podmínek, druh specifických podmínek (mimo působnost, převoz lodí/vlakem).

2.2.2 Záznam a uložení dat na paměťovou kartu řidiče

Digitální tachograf na paměťovou kartu řidiče ukládá údaje o použitých vozidlech. Dále aktualizuje a ukládá data, která jsou uvedena v kapitole 2.2.1: data o činnosti řidiče, údaje o událostech, údaje o závadách, data o kontrolní činnosti, údaje o stahování dat a údaje o specifických podmínkách [7].

2.3 Legislativa digitálních tachografů

V této kapitole popíšu dle platné legislativy povinnost užívání digitálních tachografů a povinnosti dopravců při používání digitálních tachografů.

2.3.1 Povinnost použití digitálních tachografů

Podle nařízení (ES) 561/2006 [6] musí být digitálním tachografem vybavena motorová vozidla pro přepravu:

a) zboží, jejichž maximální přípustná hmotnost včetně návěsu nebo přívesu překračuje 3,5 tuny.

b) cestujících vozidly, která jsou svou konstrukcí nebo trvalou úpravou určena pro přepravu více než devíti osob včetně řidiče.

Toto nařízení se nevztahuje na silniční dopravu:

a) vozidly používanými pro přepravu cestujících v linkové dopravě, jestliže délka tratě této linky nepřesahuje 50 km.

b) vozidly, jejichž nejvyšší dovolená rychlost nepřesahuje 40 kilometrů v hodině.

c) vozidly, která jsou ve vlastnictví ozbrojených sil, sil civilní obrany, požárních sborů a sil odpovědných za udržování veřejného pořádku nebo jsou jimi najata bez řidiče, uskutečňuje-li se přeprava v rámci jim svěřených úkolů a je-li pod jejich kontrolou.

d) vozidly, včetně vozidel používaných při neobchodní přepravě humanitární pomoci, používanými za mimořádných okolností nebo při záchranných akcích.

e) specializovanými vozidly používanými pro lékařské účely.

f) speciálními havarijními vozidly, operují-li v okruhu do 100 km od místa obvyklého odstavení vozidla.

g) vozidly používanými při silničních jízdních zkouškách pro účely vývoje, opravy nebo údržby, a novými nebo přestavěnými vozidly, která ještě nebyla uvedena do provozu.

h) vozidly nebo jejich kombinacemi, jejichž maximální přípustná hmotnost nepřesahuje 7,5 tuny a která se používají k neobchodní přepravě zboží.

i) obchodními vozidly, která jsou podle právních předpisů členského státu, ve kterém se používají, považována za historická vozidla a používají se k neobchodní přepravě cestujících nebo zboží.

2.3.2 Povinnost dopravce stahovat data z digitálního tachografu

Nařízení (ES) č. 561/2006 stanoví v čl. 10 odst. 5, aby dopravce, který používá vozidla vybavená digitálním tachografem, zajistil, aby se veškeré údaje z přístroje ve vozidle a karty řidiče pravidelně stahovaly [6].

V souladu s čl. 10 odst. 5 písm. c) nařízení 561/2006 bylo přijato nařízení č. 581/2010 o stanovení maximálních časových úseků pro stahování příslušných údajů z přístroje ve vozidle a z karty řidiče, přičemž stanovené maximální časové úseky nesmí přesáhnout dobu [5]:

a) 90 dnů v případě údajů ze záznamového zařízení ve vozidle,

b) 28 dnů v případě údajů z karty řidiče.

Podle nařízení (ES) č. 561/2006 čl. 10 odst. 5 písm. a) bodě ii) je dopravce povinen, zajistit aby veškeré údaje stažené z přístroje vozidla a z karty řidiče byly uchovávány po dobu nejméně 12 měsíců po jejich zaznamenání a na žádost kontrolora byly tyto údaje dostupné z provozovny dopravce, přímo, nebo dálkově [6].

3 Sběrnice pro komunikaci s digitálním tachografem

Digitální tachograf používá ke komunikaci dvě sběrnice: RS232 a CAN. Konektor pro sběrnici RS232 se nachází v přední části digitálního tachografu a je používán hlavně ke stahování dat silniční kontrolou či k přímému stažení dat z digitálního tachografu. Konektory sběrnice CAN jsou umístěny na zadní části digitálního tachografu viz. obrázek 3.1. Digitální tachograf obsahuje čtyři konektory CAN sběrnice označené: A, B, C a D. Konektor A slouží k připojení CAN sběrnice vozidla k digitálnímu tachografu, ke konektoru B se připojuje přídavné čidlo rychlosti vozidla, konektor C slouží k připojení zařízení pro vzdálené stahování dat a konektor D se může využít pro online vizualizaci dat z digitálního tachografu.

Obr. 3.1: Zadní strana digitálního tachografu

3.1 Sběrnice RS232

Komunikace s digitálním tachografem pomocí sběrnice RS232 probíhá pomocí zpráv, jejichž struktura je znázorněna v tabulce 3.1.

Tab. 3.1: Formát komunikační zprávy poslané přes sběrnici RS232 [7]

Hlavička zprávy				**Datové pole**					**Kontrolní součet**
FMT	TGT	SRC	LEN	SID	TRTP	...	...	...	CS
4 bajty				Max 255 bajtů					1 bajt

Hlavička zprávy obsahuje formátový bajt (FMT), cílový bajt (TGT), zdrojový bajt (SRC) a bajt délky dat (LEN). Bajt FMT identifikuje příchod zprávy na sběrnici RS232. Bajty TGT a SRC zastupují fyzickou adresu příjemce a odesílatele zprávy. Digitální tachograf vysílá na adrese EE_H a zařízení, které stahuje data pomocí sběrnice RS232, musí vysílat na adrese $F0_H$. Bajty SID a TRTP identifikují typ zprávy a mají přesně stanovenou hodnotu podle obsahu zprávy. Následuje 253 bajtů dat zprávy. Jednotlivé typy zpráv a jejich podrobný obsah lze zhlédnout v dokumentu: Nařízení komise (ES) č. 1360/2002 dodatek 7: Protokoly stahování dat [7].

V případě, že data, která mají být přenesena zprávou jsou větší než 253 bajtů, je zpráva poslána v několika částech. Struktura dílčí zprávy je znázorněna v tabulce 3.2.

Tab. 3.2: Formát dílčí zprávy poslané přes sběrnici RS232 [7]

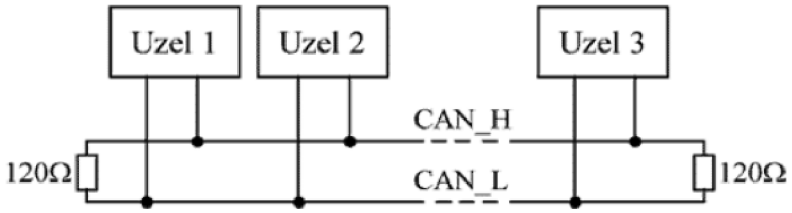
Hlavička zprávy	**SID**	**TRTP**	**C1**	**C2**	**Dílčí zpráva**	**Kontrolní součet**
4 bajty	255 bajtů					1 bajt

Hlavička a bajty SID a TRTP dílčí zprávy jsou stejné jako v případě zprávy menší než 255 bajtů. Bajty C1 a C2 jsou čítače zpráv. Čítač C1 začíná na 0 a čítač C2 začíná na 1. Čítač C2 se inkrementuje s každou dílčí zprávou. V případě přetečení čítače C2 se inkrementuje čítač C1 a čítač C2 se nastaví na 0. V případě přetečení čítače C1 se jeho hodnota nastaví na 1. Poslední dílčí zpráva obsahuje méně než 255 bajtů dat.

3.2 Sběrnice CAN

CAN (Controller Area Network) je sběrnice vyvinutá firmou Bosch pro vnitřní komunikační sít senzorů a funkčních jednotek v automobilu. Z této aplikační oblasti se CAN rychle rozšířil také do sféry průmyslové automatizace. Důvodem je především nízká cena, snadné nasazení, spolehlivost, vysoká přenosová rychlost a snadná rozšiřitelnost [11].

CAN je sériový komunikační protokol typu multi-master, kde každý uzel sběrnice může být master a řídit tak chování jiných uzlů na sběrnici. Dva uzly mezi sebou komunikují prostřednictvím datové zprávy a zprávy s charakterem žádost o data. Fyzická vrstva sběrnice je tvořena dvouvodičovým vedením, jehož signálové vodiče jsou označeny CAN_H a CAN_L a zakončeny rezistory 120 Ω [9].



Obr. 3.2: Fyzické uspořádání sítě CAN [9]

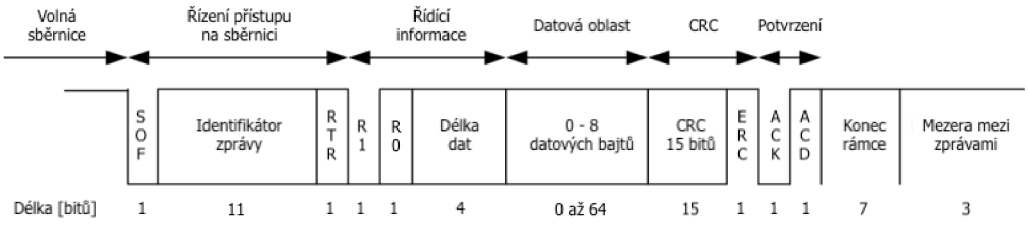
Sběrnicí se přenášejí dva logické stavy [9]:

- aktivní (dominantní) stav:
  - představuje logickou 0
  - je reprezentován nenulovým rozdílem napětí mezi vodiči CAN_H a CAN_L
- pasivní (recesivní) stav:
  - představuje logickou 1
  - je reprezentován nulovým rozdílem napětí mezi vodič CAN_H a CAN_L

3.2.1 Komunikace po sběrnici CAN

Uzly připojené na sběrnici CAN mezi sebou komunikují pomocí zpráv. CAN protokol definuje čtyři typy zpráv: datovou zprávu, žádost o data, zprávu o chybě a zprávu o přetížení [10].

Datová zpráva tvoří základ komunikace a umožňuje poslat zprávu dlouhou až 8 bajtů. CAN protokol používá dva typy datových zpráv. První typ je definován specifikací 2.0A a je označován jako standardní formát, zatímco specifikace 2.0B definuje i tzv. rozšířený formát. Rozdíl mezi oběma formáty je v délce identifikátoru zprávy, který je 11 bitů pro standardní formát a 29 bitů pro rozšířený formát. Strukturu datové zprávy podle specifikace 2.0A ilustruje obrázek 3.3.

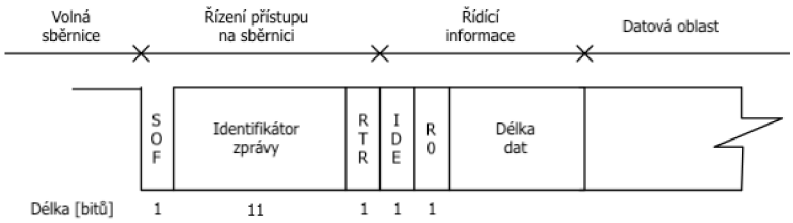


Obr. 3.3: Standardní formát datové zprávy podle specifikace CAN 2.0A [10]

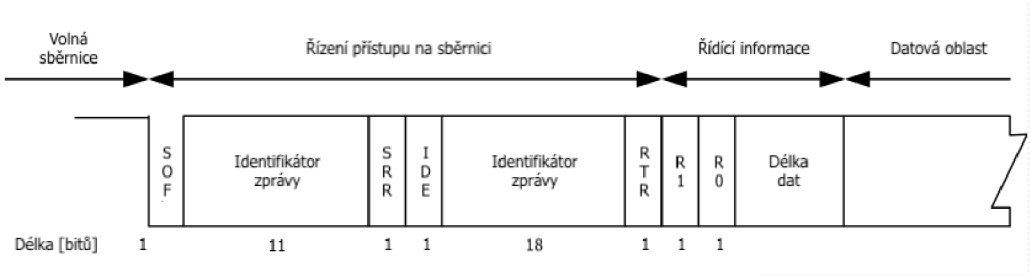
Význam jednotlivých částí datové zprávy:

- SOF (Start of Frame): začátek zprávy
- Identifikátor zprávy: určuje prioritu zprávy a význam přenášené zprávy
- RTR (Remote Request): určuje, jestli jde o zprávu datovou, nebo o žádost o data
- R1 a R0: rezervované bity
- CRC: zabezpečovací kód
- ACK, ACD: potvrzení přijetí zprávy
- Konec zprávy: 7 ukončovacích bitů zprávy

Specifikace CAN 2.0B definuje dva formáty datové zprávy: standardní a rozšířený. U specifikace 2.0B se standardní formát datové zprávy liší jen jedním bitem IDE (Identifier Extended), který označuje, zda se jedná o standardní nebo rozšířený formát datové zprávy. Rozšířený formát obsahuje navíc bit SRR (Substitute Remote Request), který má v rozšířeném formátu vždy hodnotu logickou jedničku. Tento bit zajišťuje, aby při vzájemné kolizi standardního a rozšířeného formátu zprávy na jedné sběrnici se stejným 11 bitovým identifikátorem získal přednost standardní formát zprávy. Obrázek 3.4 ilustruje standardní formát datové zprávy a obrázek 3.5 ilustruje rozšířený formát datové zprávy pro specifikaci 2.0B.



Obr. 3.4: Standardní formát datové zprávy podle specifikace CAN 2.0B [10]



Obr. 3.5: Rozšířený formát datové zprávy podle specifikace CAN 2.0B [10]

Formát **žádosti o data** je podobný jako formát datové zprávy. Pouze bit RTR je nastaven na logickou jedničku. Pokud nějaký uzel žádá o zaslání dat, nastaví takový identifikátor zprávy, jako má datová zpráva, jejíž zaslání požaduje [10].

Zpráva o chybě slouží k signalizaci chyb na sběrnici CAN. Jakmile uzel na sběrnici detekuje v přenášené zprávě chybu, vygeneruje ihned na sběrnici chybový rámec [10].

Zpráva o přetížení slouží k oddálení vyslání datové zprávy nebo žádosti o data, když je zařízení zaneprázdněno a nezvládá komunikovat [10].

3.2.2 Protokol pro komunikaci s digitálním tachografem po CAN sběrnici

Digitální tachograf komunikuje pomocí výměny datových zpráv jednotky síťového protokolu (N_PDU - Protocol Data Unit), definovaného v normě ISO 15765-2 [3]. Norma ISO 15765-2 definuje čtyři typy: N_PDU - Single Frame (SF N_PDU), First Frame (FF N_PDU), Consecutive Frame (CF N_PDU) a Flow Control (FC N_PDU). Formát N_PDU je vyznačený v tabulce 3.3.

Tab. 3.3: Formát N_PDU [3]

Adresní informace	Řídicí informace protokolu	Data
N_AI	N_PCI	N_Data

Adresní informace (N_AI) identifikují vysílací uzel a určují adresu přijímacího uzlu [3].

Řídicí informace protokolu (N_PCI) definují typ N_PDU a další speciální řídicí parametry [3].

Data (N_Data) obsahují obsah odeslané zprávy [3].

Tabulka 3.4 ukazuje mapování jednotlivých N_PDU do rámce datové zprávy CAN protokolu.

Tab. 3.4: Mapování N_PDU do rámce datové zprávy CAN sběrnice [3]

Typ N_PDU	**CAN ID** 29 bitů	**CAN Data [Byte]**							
		1	2	3	4	5	6	7	8
Single Frame (SF)	N_AI	N_PCI	N_Data						
First Frame (FF)	N_AI	N_PCI		N_Data					
Consecutive Frame (CF)	N_AI	N_PCI	N_Data						
Flow Control (FC)	N_AI	N_PCI				N/A			

Protokol pro komunikaci s digitálním tachografem využívá rozšířený formát datové zprávy sběrnice CAN. Tabulka 3.5 ukazuje mapování N_AI do identifikátoru datové zprávy CAN protokolu. Tabulka 3.6 ukazuje formát jednotlivých N_PCI bajtů pro jednotlivé N_PDU.

Tab. 3.5: Mapování N_AI do ID datové zprávy CAN sběrnice [3]

Bitová pozice	28 ... 26	25	24	23 ... 16	15 ... 8	7 ... 0
CAN ID	6	0	0	218	N_TA	N_SA

Pro mapování N_AI datové zprávy využívá digitální tachograf tzv. normální pevné adresování, což znamená, že k mapování N_AI se využívá pouze rozšířeného identifikátoru datové zprávy CAN protokolu. Tuto skutečnost oznamují bity 23-16, což je číslo 218 v dekadické soustavě. První tři bity označují prioritu zprávy, která je nastavena standardně na 6 v dekadické soustavě. N_AI používá k identifikaci zprávy dvou parametrů: N_TA a N_SA. N_TA (Target Address) identifikuje adresu cíle a N_SA (Source Address) identifikuje adresu zdroje zprávy. Adresa záznamové jednotky digitálního tachografu je pevně stanovena na 238 dekadicky [3].

SF N_PDU se používá k odeslání kratších zpráv, dlouhých maximálně sedm bajtů. SF N_PDU obsahuje parametr SF_DL (Single Frame Data Length), který slouží k definování velikosti vyslané zprávy. Parametr SF_DL je dlouhý maximálně 4 bity a nesmí obsahovat číslo větší než sedm dekadicky. Posledních sedm bajtů

Tab. 3.6: Formát N_PCI bajtů pro jednotlivé druhy N_PDU [3]

Typ N_PDU	**N_PCI bajty**			
	Byte #1		Byte #2	Byte #3
	Bity 7 - 4	Bity 3 - 0		
Single Frame (SF)	N_PCItype = 0	SF_DL	N/A	N/A
First Frame (FF)	N_PCItype = 1	FF_DL		N/A
Consecutive Frame (CF)	N_PCItype = 2	SN	N/A	N/A
Flow Control (FC)	N_PCItype = 3	FS	BS	STmin

SF_NPDU obsahuje data zprávy [3].

FF N_PDU se odesílá jako první zpráva při odesílání zprávy delší než sedm bajtů. FF N_PDU obsahuje parametr FF_DL (First Frame Data Length), který slouží k definování velikosti vyslané zprávy. Parametr FF_DL je dlouhý maximálně 12 bitů a může obsahovat čísla v rozmezí 8_H - $0FFF_H$. Dále zpráva obsahuje 6 datových bajtů zprávy [3].

CF N_PDU se odesílá po FF N_PDU a obsahuje data delší zprávy, které jsou rozděleny do zpráv CF N_PDU po sedmi bajtech. CF N_PDU obsahuje parametr SN (Sequence Number), který označuje sekvenční číslo zprávy. Je dlouhý maximálně 4 bity a může obsahovat číslice 0_H - F_H hexa podle tabulky 3.7.

Tab. 3.7: Definice hodnot parametru SN [3]

N_PDU	1. CF	2. CF	...	14. CF	15. CF	16. CF	17. CF	...
SN (hex)	1	2	...	E	F	0	1	...

FC N_PDU slouží k řízení toku zpráv. FC N_PDU odesílá uzel, který zprávy přijímá a posílá je vysílacímu uzlu. Obsahuje tři parametry: FS, BS a STmin. Hodnoty parametru FS (Flow Status) jsou uvedeny v tabulce 3.8. Parametr BS (Block Size) obsahuje velikost odeslaného bloku, viz tabulka 3.9. Parametr STmin (Separation Time min.) obsahuje minimální čas pro odeslání dvou po sobě jdoucích zpráv CF N_PDU. Jednotlivé hodnoty STmin jsou popsány v tabulce 3.10. Komunikace pomocí zpráv FF, CF a FC N_PDU je zaznamenána na obrázku 3.6.

Tab. 3.8: Definice hodnot parametru FS [3]

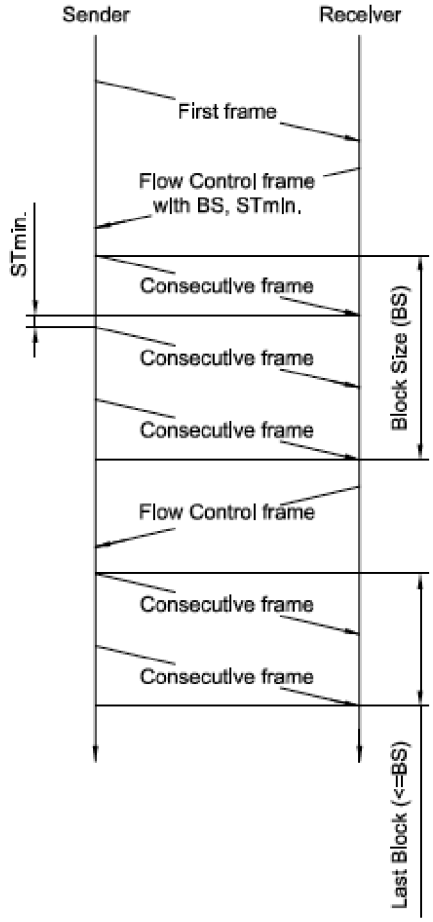
Hodnota hex	**Popis**
0	**ContinueToSend (CTS)**: Tento parametr znamená, že příjemce je schopen přijmout maximum zpráv CF N_PDU uvedených v parametru BS viz. tabulka 3.2.2.
1	**Wait (WT)**: Odesílatel musí počkat na nové FC N_PDU. Do té doby nesmí nic vysílat.
2	**Overflow (OVFLW)**: Odesílatel musí zrušit všechny odesílané CF N_PDU. Tento parametr se posílá po FF N_PDU, když je parametr, který značí velikost dat větší než velikost bufferu příjemce.
3 - F	**Rezervováno**.

Tab. 3.9: Definice hodnot parametru BS [3]

Hodnota hex	**Popis**
00	Hodnota parametru 0 značí, že příjemce během přenosu CF N_PDU nebude odesílat další FC N_PDU. Odesílatel může poslat všechny části zprávy.
01 - FF	V případě hodnoty v tomto rozsahu, odesílatel může poslat maximálně tolik částí zprávy, které udává tato hodnota. Následně příjemce musí odeslat novou zprávu FC N_PDU s novými parametry.

Tab. 3.10: Definice hodnot parametru STmin [3]

Hodnota hex	**Popis**
00 - 7F	**Minimální čas mezi zprávami**: 0 ms - 127 ms.
80 - F0	**Rezervováno**.
F1 - F9	Minimální čas mezi zprávami: 100 μs - 900 μs.
FA - FF	**Rezervováno**.



Obr. 3.6: Princip komunikace po CAN sběrnici [3].

Obrázek 3.6 značí princip komunikace po CAN sběrnici, když je velikost celkové zprávy větší než sedm bajtů. Odesílatel nejprve musí odeslat zprávu FF N_PDU s parametrem celkové délky dat zprávy. Následně příjemce odpoví zprávou FC N_PDU, kde definuje parametry FS, BS a STmin. Následně odesílatel může odeslat tolik zpráv CF N_PDU, kolik příjemce požaduje pomocí parametru BS (Block Size). Pokud po odeslání povolených CF N_PDU nebyla odeslána celá zpráva, příjemce odešle novou zprávu FC N_PDU s novými parametry.

4 Specifikace pro vzdálené stahování dat z digitálního tachografu

V následující kapitole popíšu princip vzdáleného stahování dat a komunikace s digitálním tachografem.

Pro stažení dat z digitálního tachografu je nejprve potřeba provést autentifikaci oprávnění ke stažení dat. Autentifikaci provádí společnost vlastnící digitální tachograf pomocí tachografové karty společnosti. Tuto kartu je nutné vložit do čtečky čipových karet. Digitální tachograf následně s tachografovou kartou komunikuje pomocí zpráv, viz tabulka 4.1. Když je autentifikace úspěšná, lze pomocí zprávy požádat digitální tachograf o data.

V tabulce 4.1 je v prvním sloupci vyznačen směr posílání zpráv (-> DT znamená posílání zpráv do digitálního tachografu, DT -> znamená posílání zpráv z digitálního tachografu). Digitální tachograf při autentifikaci může také odpovědět negativní zprávou indikující chyby, viz tabulka 4.2.

Tab. 4.1: Zprávy potřebné pro úspěšnou autentifikaci tachografové karty společnosti [2]

Směr	**Jméno zprávy**	**Popis zprávy**	**Data zprávy**
-> DT	RemoteCompanyCardReady	Tato zpráva signalizuje DT, že karta společnosti je vložená ve čtečce čipových karet a je připravena na proces autentifikace.	Answer to reset (ATR).
DT ->	DTReady	DT je připraven zahájit proces autentifikace.	Žádné.
-> DT	CompanyCardToDTData	Poslání APDU příkazu do DT z karty společnosti.	Žádné, nebo APDU tachografové karty.
-> DT	DTToCompanyCardData	Poslání APDU příkazu z DT do karty společnosti.	APDU tachografové karty.

Směr	Jméno zprávy	Popis zprávy	Data zprávy
		Pokračování výměny APDU mezi DT a kartou společnosti do té doby než přijde zpráva RemoteAuthenticationSucceeded.	
DT ->	RemoteAuthenticationSucceeded	Autentifikace byla úspěšně dokončena.	Žádné.
-> DT	RemoteDownloadDataRequest	Poslání seznamu žádostí o stažení dat z DT.	Seznam žádostí o stažení.
DT ->	RemoteDownloadAccessGranted	DT signalizuje povolení stažení dat z DT ze seznamu žádostí.	Žádné.
-> DT	CloseRemoteAuthentication	Ukončení autentifikace karty podniku.	Žádné.

Tab. 4.2: Možné chybové zprávy při autentifikaci karty společnosti [2]

Směr	Jméno zprávy	Popis zprávy
DT ->	RemoteAuthenticationClosed	Tato zpráva signalizuje ukončení procesu autentifikace.
DT ->	APDUError	Tato zpráva signalizuje, že bylo vysláno třikrát po sobě špatné APDU.
DT ->	AuthenticationError	Tato zpráva signalizuje, že autentifikace karty společnosti selhala.
DT ->	TooManyAuthenticationError	Tato zpráva signalizuje, že během autentifikace bylo způsobeno více než pět chyb.

V tabulce 4.3 je přehled zpráv potřebných pro vzdálené stažení dat z digitálního tachografu.

Tab. 4.3: Zprávy potřebné pro vzdálené stažení dat z DT [2]

Směr	Jméno zprávy	Popis zprávy
-> DT	RequestUpload	Tato zpráva signalizuje DT, že už bylo úspěšně požádáno o povolení vzdáleného stažení dat.
-> DT	TransferData	Tato zpráva slouží k požádání konkrétních dat z DT.

Data, která zaznamenává digitální tachograf (viz kapitola 2.2.1), jsou rozdělena do datových bloků. Při požadavku ke stažení dat z digitálního tachografu pomocí zprávy TransferData se jako parametr uvede konkrétní blok dat ke stažení (při jednom požadavku na stažení dat lze uvést najednou více bloků dat). Digitální tachograf definuje 6 datových bloků:

1. **Přehled** - údaje identifikující zařízení (tento blok dat je povinný při každém požadavku na stažení dat).

2. **Aktivity** - obsahuje činnosti řidiče (lze vybrat činnosti řidiče v konkrétním čase).

3. **Události a chyby** - údaje o vložení a vyjmutí karty řidiče, údaje o kontrolách, stahování dat, kalibracích a závadách digitálního tachografu.

4. **Podrobná data o rychlosti** - údaje o zaznamenání rychlosti každou sekundu jízdy za posledních 24 hodin.

5. **Technická data o vozidle** - kalibrační data.

6. **Data z karty řidiče** - blok dat obsahující všechna data z karty řidiče vložené v digitálním tachografu.

Podrobný obsah jednotlivých zpráv potřebných pro autentifikaci a stahování dat je možné zhlédnout v dokumentu: specifikace pro vzdálenou autentifikaci karty společnosti a vzdálené stahování dat z digitálního tachografu [2].

Pro povolení používání všech zpráv a správnou funkci vzdáleného stahování dat je nutné v digitálním tachografu aktivovat specifickou diagnostickou relaci (remoteSession). Aktivace se provede posláním specifické zprávy. Pro udržení digitálního tachografu v režimu remoteSession je nutné každých 5 sekund tuto zprávu vyslat znovu [2]. Názorný výpis posloupnosti zpráv pro úspěšné stažení dat z digitálního tachografu lze zhlédnout v příloze D.

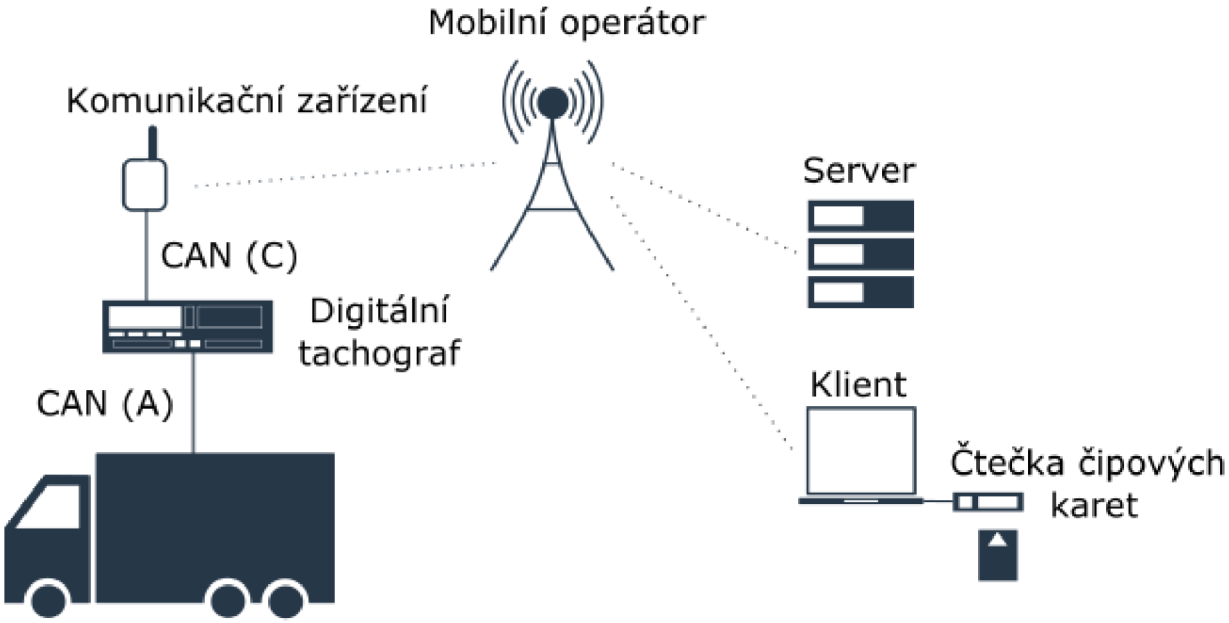
4.1 Omezení při stahování dat z digitálního tachografu

Při stahování dat z digitálního tachografu existují jistá omezení, která je nutné dodržet. První podmínkou je, že při vypnutém zapalování vozidla, ve kterém je umístěn digitální tachograf, je umožněno stahovat data pouze do 24 hodin od vypnutí zapalování. Druhou podmínkou pro úspěšné stažení dat je, že stahování dat nesmí být přerušeno vypnutím, nebo zapnutím zapalování vozidla během stahování dat. Z důvodu těchto omezení je nejvhodnější data z digitálního tachografu stahovat při zapnutém zapalování vozidla a nezačínat stahování dat hned na začátku zapnutí zapalování nebo po velmi dlouhé době zapnutého zapalování vozidla. Při dodržení těchto pravidel je nejpravděpodobnější, že data budou z digitálního tachografu v pořádku stažená [2].

Tato omezení při vzdáleném stahování dat existují z důvodu úspory baterie vozidla v případě nečinnosti digitálního tachografu. Další podmínka přerušení stahování dat z digitálního tachografu při vypnutí nebo zapnutí zapalování je z důvodu, že digitální tachograf musí zapsat do paměti plno údajů a nemůže se zatěžovat jinými událostmi [2].

5 Návrh koncepce řešení vzdáleného stahování dat z digitálního tachografu

Na obrázku 5.1 můžeme vidět princip navrženého řešení pro vzdálené stahování dat z digitálního tachografu.



Obr. 5.1: Návrh koncepce pro vzdálené stahování dat z digitálního tachografu

Jak už bylo řečeno v kapitole 3, digitální tachograf se v nákladním automobilu připojuje ke CAN sběrnici pomocí konektoru A a komunikační zařízení pro vzdálené stahování dat z digitálního tachografu je připojeno k digitálnímu tachografu pomocí konektoru C. Komunikační zařízení komunikuje pomocí GSM modulu se vzdáleným serverem, který ukládá stažená data z digitálního tachografu. Ke vzdálenému serveru se také může připojit klient, který si může stažená data z digitálního tachografu ze vzdáleného serveru stáhnout, ovládat komunikační zařízení manuálně, případně vydat konkrétní pokyn pro komunikační zařízení ke stažení dat z digitálního tachografu. Pro správnou funkci systému vzdáleného stahování dat z digitálního tachografu je nutné k aplikaci klienta připojit čtečku čipových karet, do které se vloží tachografová karta společnosti, která slouží ke vzdálené autentifikaci tachografové karty společnosti. Až po úspěšné autentifikaci tachografové karty společnosti je možné stáhnout data z digitálního tachografu, viz kapitola 4.

5.1 Komunikace s nadřazeným serverem

V následující kapitole uvedu navržený princip komunikace aplikace klienta a komunikačního zařízení se vzdáleným serverem.

Komunikace aplikace klienta a komunikačního zařízení se vzdáleným serverem na internetu je realizováno pomocí protokolu TCP (Transport Control Protocol). Což je spolehlivá transportní služba, která zaručí spolehlivé doručení dat. Pro bezpečný přenos dat internetem využívá komunikace protokol TLS (Transport Layer Security) verze 1.2. Protokol TLS slouží k šifrování přenášených dat pomocí kryptografických metod a k autentizaci koncových bodů připojovaných ke vzdálenému serveru.

Komunikace s nadřazeným serverem probíhá pomocí vlastních navržených zpráv s identifikátorem $D4_H$ na úrovni aplikační vrstvy ISO/OSI modelu. Formát D4 zprávy lze zhlédnout na obrázku 5.2.

<table>
<tr><td>ID zprávy
(8 bitů)</td><td>Verze
(8 bitů)</td><td>Délka hlavičky zprávy
(16 bitů)</td></tr>
<tr><td colspan="2">ID typ zařízení
(16 bitů)</td><td>Typ zařízení
(16 bitů)</td></tr>
<tr><td colspan="2">ID adresa zdroje
(16 bitů)</td><td>Adresa zdroje
(16 bitů)</td></tr>
<tr><td colspan="2">ID adresa cíle
(16 bitů)</td><td>Adresa cíle
(16 bitů)</td></tr>
<tr><td colspan="2">ID typ zprávy
(16 bitů)</td><td>Typ zprávy
(16 bitů)</td></tr>
<tr><td colspan="3">Kontrolní součet hlavičky zprávy
(32 bitů)</td></tr>
<tr><td colspan="2">Data ID
(16 bitů)</td><td>Délka dat
(16 bitů)</td></tr>
<tr><td colspan="3">Data zprávy
(0 - 65535 bajtů)</td></tr>
<tr><td colspan="3">Kontrolní součet dat zprávy
(32 bitů)</td></tr>
</table>

Obr. 5.2: Formát $D4_H$ komunikačních zpráv

Popis jednotlivých buněk z obrázku 5.2:

ID zprávy: jedná se o identifikátor zprávy, který obsahuje číslo $D4_H$.
Verze: značí verzi komunikační zprávy. Hodnota aktuální verze $D4_H$ zprávy je nastavená na číslo 1_H.
Délka hlavičky zprávy: označuje délku hlavičky v bajtech.
ID typ zařízení: identifikuje následující blok, typ zařízení. Hodnota této položky hlavičky je nastavená na číslo $F801_H$.
Typ zařízení: identifikace, zda zprávu vyslal server (0001_H), klient (0002_H), nebo komunikační zařízení (0003_H).
ID adresa zdroje: identifikuje následující blok, adresa zdroje. Hodnota této položky hlavičky je nastavená na číslo $F802_H$.
Adresa zdroje: tento blok označuje adresu odesílatele zprávy. Tato verze zprávy počítá s 16 bitovými adresami.
ID adresa cíle: identifikuje následující blok, adresa cíle. Hodnota této položky hlavičky je nastavená na číslo $F803_H$.
Adresa cíle: tento blok označuje adresu příjemce zprávy. Tato verze zprávy počítá s 16 bitovými adresami.
ID typ zprávy: identifikuje následující blok, typ zprávy. Hodnota této položky hlavičky je nastavená na číslo $F804_H$.
Typ zprávy: označuje obsah D4 zprávy nebo akci, kterou má příjemce provést.
Kontrolní součet hlavičky: 32 bitový kontrolní součet podle algoritmu Adler32 [12]. Kontrolní součet se určuje od buňky ID zprávy po typ zprávy.
Data ID: identifikace začátku bloku dat. Hodnota této položky hlavičky je nastavená na číslo $F900_H$.
Délka dat: velikost dat v bajtech. Maximální velikost dat je 65535 bajtů.
Data zprávy: Data $D4_H$ zprávy.
Kontrolní součet dat zprávy: 32 bitový kontrolní součet podle algoritmu Adler32 [12]. Kontrolní součet se určuje od buňky ID data až po konec dat.

Každý specifický blok hlavičky zprávy má svůj vlastní 16 bitový identifikátor, který definuje obsah dat v následujících 16-ti bitech zprávy. Pro lepší modifikaci v budoucích rozšíření navrženého formátu $D4_H$ zpráv, je možné také přidávat verze formátu zpráv. V případě modifikace formátu zprávy stačí, když všechny verze zpráv bude znát pouze server a ve starších komunikačních zařízení se s každou verzí nemusí aktualizovat firmware. V tom případě bude komunikační zařízení komunikovat se serverem pomocí nejnovějšího formátu zpráv, který podporuje.

Pomocí bloku typ zprávy se identifikuje typ dat, která D4 zpráva obsahuje nebo případně označuje povel pro příjemce, který na danou zprávu bez dat může reagovat odpovědí v závislosti na typu zprávy. Typ zprávy identifikuje 16 bitové číslo v bloku typ zprávy. Každý typ $D4_H$ zprávy je definovaný názvem, který začíná značkou CMD. Jednotlivé možné typy $D4_H$ zpráv v první verzi formátu D4 zprávy jsou vyznačeny v tabulce 5.1.

Tab. 5.1: Typy $D4_H$ zpráv

Typ zprávy	**Popis zprávy**	**Data zprávy**
CMD_CONNECT_CLIENT	Zprávu posílá klient po připojení k serveru.	Komunikační zařízení: ID, aplikace klienta: přihlašovací jméno společnosti.
CMD_CONNECT_SERVER	Zprávu odesílá server jako odpověď na zprávu CMD_CONNECT_CLIENT.	Žádná.
CMD_CLIENT	Zprávu odesílá aplikace klienta. Tato zpráva požaduje odeslání všech adres komunikačních zařízení, dostupných pro přihlášenou společnost, připojených k serveru.	Jméno a adresa komunikačního zařízení.
CMD_DEVICES	Odpověď na zprávu CMD_CLIENT.	Jména a adresy všech dostupných komunikačních zařízeních připojených k serveru.
CMD_READY	Příkaz posílá klient a značí, že tachografová karta společnosti je připravena, nebo v případě komunikačního zařízení, že tachograf je připravený na autentifikaci tachografové karty.	Žádná.
CMD_START_AUTHENTIFICATION	Signalizace serveru z aplikace klienta, že autentifikace tachografové karty společnosti začala.	Adresa komunikačního zařízení, s kterým začala autentifikace tachografové karty společnosti.
CMD_AUTHENTIFICATION	Zpráva, která se předává mezi aplikací klienta a komunikačním zařízením. Zpráva slouží k předání zpráv z tachografové karty společnosti k tachografu.	APDU příkaz pro tachografovou kartu společnosti nebo tachograf.

Typ zprávy	Popis zprávy	Data zprávy
CMD_END_AUTHENTIFICATION	Signalizace serveru z aplikace klienta, že autentifikace tachografové karty společnosti úspěšně skončila.	Adresa komunikačního zařízení, s kterým se úspěšně ukončila autentifikace tachografové karty společnosti.
CMD_REQUEST_UPLOAD	Odeslání požadavku komunikačnímu zařízení na stažení konkrétních dat.	Specifikace požadavku na stažení konkrétních dat.
CMD_START_DOWNLOAD	Zpráva dává signalizaci, že komunikační zařízení může začít stahování dat z digitálního tachografu.	Žádná.
CMD_DOWNLOAD_PERIOD_CARD	Signalizace, že časovač pro automatické stažení dat z karty řidiče doběhl a může začít stahování dat.	Adresa komunikačního zařízení, které vyslalo tuto zprávu.
CMD_DOWNLOAD_PERIOD_TACHO	Signalizace, že časovač pro automatické stažení dat z digitálního tachografu doběhl a může začít stahování dat.	Adresa komunikačního zařízení, které vyslalo tuto zprávu.
CMD_DATA	Zpráva, která obsahuje stažená data z digitálního tachografu.	Data stažená z digitálního tachografu.
CMD_DATA_END	Signalizace serveru z komunikačního zařízení, že požadovaná data byla z digitálního tachografu stažena a poslána na server.	Adresa aplikace klienta, která vznesla požadavek na stažení dat z digitálního tachografu.
CMD_DOWNLOAD_END	Signalizace aplikaci klienta ze serveru, že data byla z digitálního tachografu stažena a jsou dostupná na serveru.	Žádná.
CMD_FILE_END	Signalizace aplikaci klienta ze serveru, že požadavek na stažení souboru ze serveru byl dokončen.	Žádná.
CMD_VIEW_FILES	Zprávu posílá aplikace klienta a žádá server o poslání dostupných souborů ke stažení ze serveru.	Žádná.
CMD_FILES	Odpověď na zprávu CMD_VIEW_FILES.	Jména dostupných souborů na serveru.
CMD_DOWNLOAD_FILE	Požadavek klienta na stažení souboru.	Jméno souboru ke stažení ze serveru.
CMD_SEND_FILE	Odpověď na zprávu CMD_DOWNLOAD_FILE.	Data stahovaného souboru ze serveru.

Typ zprávy	Popis zprávy	Data zprávy
CMD_STOP	Ukončí autentifikaci tachografové karty.	Žádná.
CMD_DISCONNECT	Odpojení klientů ze serveru.	Čas možného opětovného připojení k serveru v sekundách.
CMD_ERROR	Odpověď příjemce odesílateli v případě chyby.	8 bitový kód chyby.

Přesné hexadecimální hodnoty jednotlivých definic lze shlédnout v dokumentaci kódu jednotlivých aplikací, vytvořené pomocí nástroje Doxygen, přiložené v elektronické příloze této diplomové práce.

V tabulce 5.2 jsou vyznačeny definice chybových kódů zprávy CMD_ERROR.

Princip navázání a ukončení spojení mezi komunikačním zařízením a serverem pomocí D4 zpráv je znázorněn na obrázku 5.3. Vlevo na obrázku je znázorněno zahájení spojení mezi serverem a komunikačním zařízením s ukončením spojení z důvodu výpadku signálu komunikačního zařízení. Vpravo je znázorněno zahájení spojení mezi serverem a komunikačním zařízením s ukončením spojení ze strany serveru. Na obrázku 5.4 je znázorněno odmítnutí zahájení spojení ze strany serveru. U D4 zpráv, znázorněných na obrázcích 5.3 a 5.4, je v závorkách vyznačen obsah dat dané D4 zprávy.

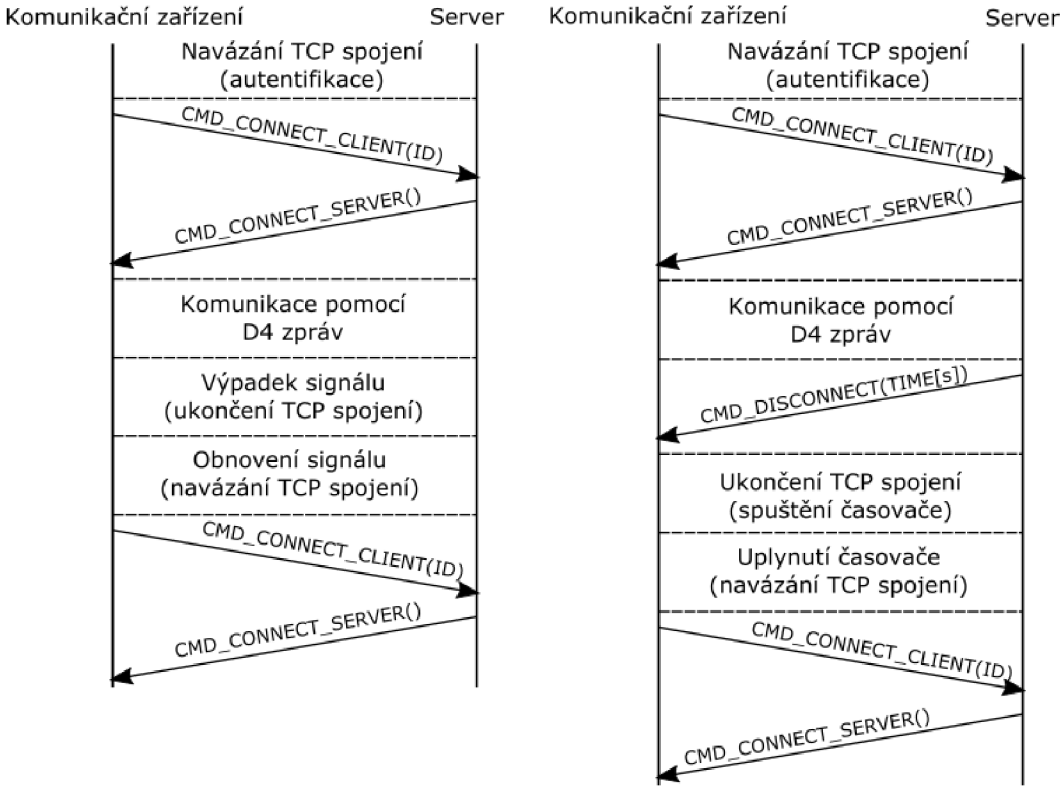
Každé komunikační zařízení komunikuje se serverem pomocí GSM modulu s vlastní SIM kartou, která má statickou IP adresu. Komunikační zařízení má také své vlastní jedinečné ID, které identifikuje komunikační zařízení a instituci, které komunikační zařízení patří. Při komunikaci mezi komunikačním zařízením a serverem zahajuje TCP spojení vždy komunikační zařízení a autentifikuje se pomocí vlastního vygenerovaného certifikátu pomocí OpenSSL frameworku. Při zahájení spojení mezi serverem a komunikačním zařízením vyšle komunikační zařízení zprávu CMD_CONNECT_CLIENT společně se svým jedinečným ID. Server si ID uloží a odpoví zprávou CMD_CONNECT_SERVER. Z hlavičky zprávy (blok adresa cíle) zjistí komunikační zařízení svou přidělenou 16 bitovou adresu, pod kterou bude komunikační zařízení se serverem komunikovat. V případě, že komunikační zařízení vyšle ID, které server nezná, server odpoví zprávou CMD_ERROR s chybou ERR_CONNECT_CLIENT a komunikační zařízení ukončí TCP spojení, viz obrázek 5.4. TCP spojení mezi komunikačním zařízením a serverem se udržuje vždy

Tab. 5.2: Typy definic chybových kódů zprávy CMD_ERROR

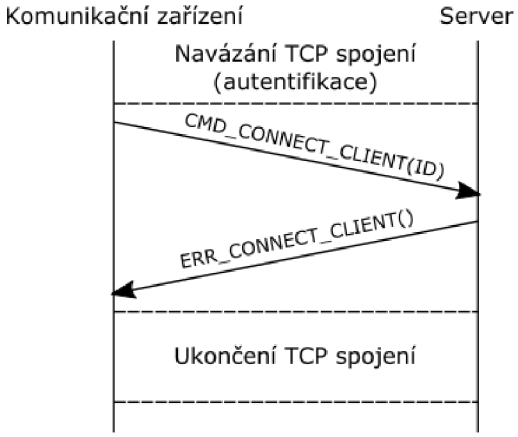
Typ chyby	**Popis chyby**
ERR_CLIENT_DISCONNECT	Klient s adresou cíle není připojený k serveru.
ERR_DEVICES	Odpověď serveru aplikaci klienta (není žádné dostupné komunikační zařízení).
ERR_CONECT_CLIENT	Špatné ID komunikačního zařízení, nebo jméno společnosti.
ERR_MESSAGE_TYPE	Příjemce nezná požadovaný typ zprávy.
ERR_MESSAGE	Chyba v přijaté zprávě (špatný kontrolní součet, neznámý typ bloku atd.).
ERR_VERSION	Neznámá verze zprávy.
ERR_DOWNLOAD_PERIOD_CARD	K serveru není připojena aplikace klienta s přihlášenou společností, které patří komunikační zařízení, které poslalo zprávu CMD_DOWNLOAD_PERIOD_CARD
ERR_DOWNLOAD_PERIOD_TACHO	K serveru není připojena aplikace klienta s přihlášenou společností, které patří komunikační zařízení, které poslalo zprávu CMD_DOWNLOAD_PERIOD_TACHO
ERR_AUTHENTIFICATION	Chyba v autentifikaci tachografové karty společnosti.
ERR_DOWNLOAD	Chyba ve stahování dat z digitálního tachografu.
ERR_FILE_NAME	Chyba při požadavku na stažení dat ze serveru. Jméno požadovaného souboru ke stažení není správné.
ERR_FILE	Odpověď na zprávu CMD_VIEW_FILES. Na serveru nejsou uloženy žádné dostupné soubory ke stažení.

tak dlouho, dokud má GSM modul signál. V případě výpadku signálu GSM modulu se opakuje připojení k serveru, až dojde k obnovení signálu GSM modulu. Když je potřeba komunikační zařízení odpojit ze serveru (např: správa serveru, modifikace kódu serveru atd.), vyšle server zprávu CMD_DISCONNECT všem komunikačním zařízením, která obsahuje čas opětovného spuštění serveru. Po uplynutí doby pro opětovné spuštění serveru, aby nedošlo k přetížení a zahlcení serveru, každé komunikační zařízení náhodně počká od 0 do 10 minut a až tehdy se připojí k serveru.

Na obrázku 5.5 je znázorněn princip zahájení a ukončení spojení pomocí D4 zpráv mezi aplikací klienta a serverem. Vlevo je znázorněno zahájení spojení mezi serverem a aplikací klienta s ukončením spojení ze strany aplikace klienta. V pravo je znázorněno zahájení spojení mezi aplikací klienta a serverem s ukončením spojením ze strany serveru.

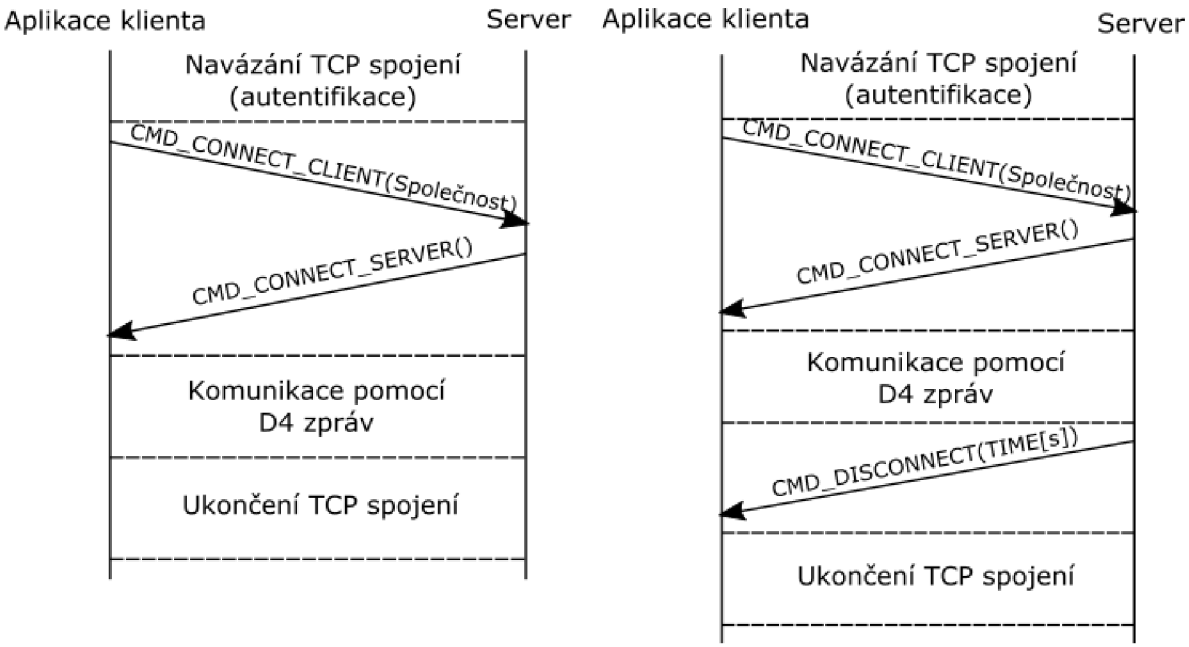


Obr. 5.3: Princip zahájení a ukončení spojení pomocí D4 zpráv mezi serverem a komunikačním zařízením



Obr. 5.4: Odmítnutí spojení mezi komunikačním zařízením a serverem

Aplikace klienta nemá své vlastní ID. Aplikace klienta při spuštění naváže TCP spojení se serverem a pošle zprávu CMD_CONNECT_CLIENT obsahující jméno společnosti, která se chce k serveru přihlásit. V případě, že server danou společnost zná, odpoví zprávou CMD_CONNECT_SERVER, kde aplikace klienta získá svou

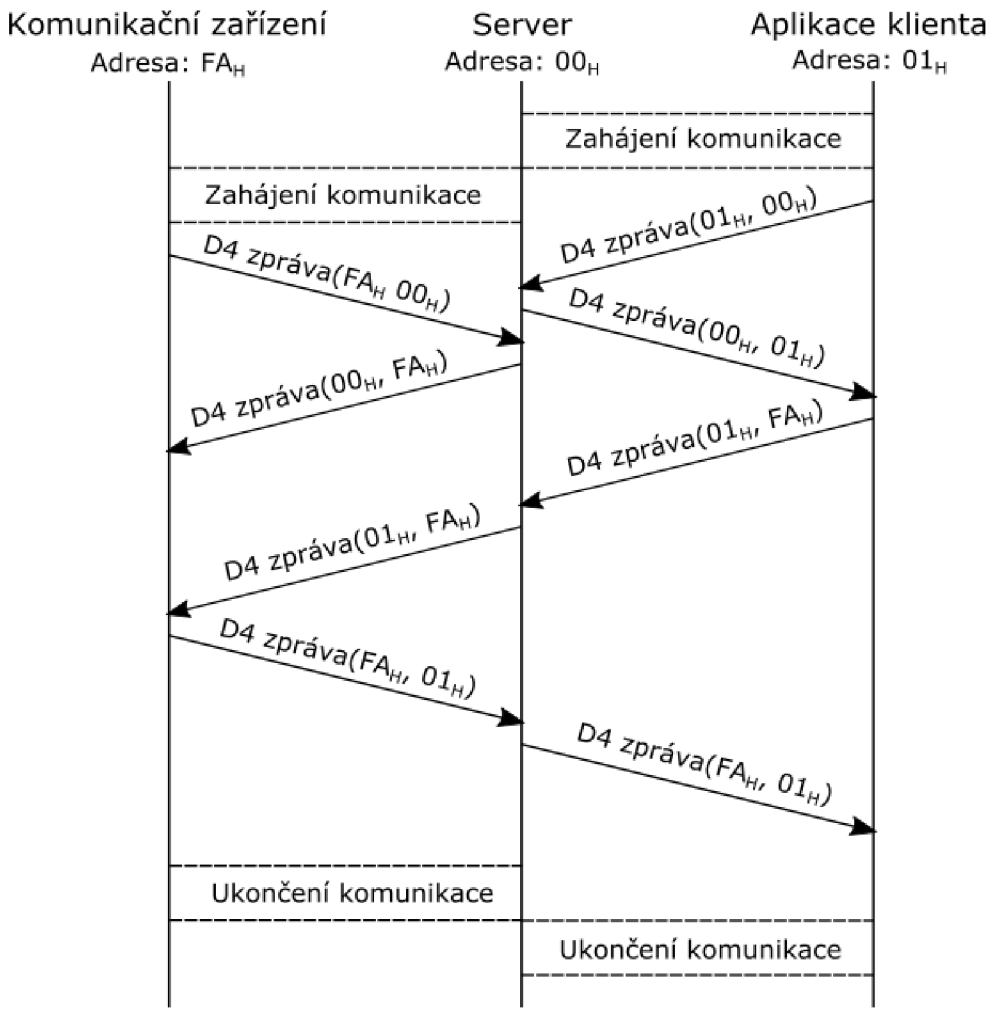


Obr. 5.5: Princip zahájení a ukončení spojení pomocí D4 zpráv mezi serverem a aplikací klienta

přidělenou 16 bitovou adresu z hlavičky zprávy (blok adresa cíle). V následující komunikaci bude aplikace klienta se serverem komunikovat s touto přidělenou adresou. Když server jméno společnosti odeslané ve zprávě CMD_CONNECT_CLIENT nezná, odpoví zprávou CMD_ERROR s chybovým kódem ERR_CONNECT_CLIENT. V tomto případě není dovoleno aplikaci klienta se připojit k serveru. V případě odpojení spojení ze strany serveru (např: správa serveru, modifikace kódu serveru atd.) pošle server zprávu CMD_DISCONNECT, která obsahuje opětovný čas spuštění serveru a tento čas se klientovi pouze v aplikaci zobrazí. Po uplynutí doby nedojde k opětovnému navázání spojení aplikace klienta se serverem, ale pouze je umožněno klientovi se opětovně přihlásit k serveru.

Po navázání spojení aplikace klienta a komunikačního zařízení se serverem probíhá komunikace adresování D4 zpráv podle obrázku 5.6. U znázornění D4 zpráv na obrázku je v závorce umístěná jako první hexadecimální adresa zdroje a druhým parametrem v závorce je adresa cíle D4 zprávy.

Adresování zpráv mezi aplikací klienta, komunikačním zařízením a serverem probíhá pomocí 16 bitových adres přidělených ze strany serveru při navázání spojení, viz obrázek 5.3 a 5.5. Ukázku adresování D4 zpráv uvádí obrázek 5.6. V ukázce má aplikace klienta adresu 01_H a komunikační zařízení FA_H. Server má vždy adresu



Obr. 5.6: Princip komunikace a adresování D4 zpráv mezi aplikací klienta, komunikačním zařízením a serverem

00_H. V případě komunikace klientů pouze se serverem uvádí klient adresu serveru, tedy 00_H. Když chce komunikovat klient s komunikačním zařízením pomocí aplikace klienta, pošle prvně na server zprávu CMD_CLIENT a server odpoví zprávou CMD_DEVICES, která obsahuje jména a adresy dostupných komunikačních zařízení pro daného klienta. Klient si vybere zařízení, se kterým chce komunikovat a další zprávy posílá na adresu vybraného zařízení. Když dojde na server zpráva s nenulovou adresou, přepošle server zprávu na konkrétní zařízení s danou adresou. Komunikační zařízení nemůže kontaktovat aplikaci klienta jako první, pouze může reagovat na přijaté zprávy z aplikace klienta. V případě, že není dostupné žádné komunikační zařízení pro daného klienta, server na zprávu CMD_CLIENT odpoví zprávou CMD_ERROR s chybovým kódem ERR_DEVICES.

Při automatickém stahování dat z digitálního tachografu nebo karty řidiče vyšle komunikační zařízení zprávu CMD_DOWNLOAD_PERIOD_TACHO (při stažení dat z digitálního tachografu) nebo CMD_DOWNLOAD_PERIOD_CARD (při stažení dat z karty řidiče). Tyto zprávy obsahují také adresu komunikačního zařízení, které danou zprávu vyslalo. Při kontaktování komunikačního zařízení touto zprávou server vyhledá připojenou aplikaci klienta s přihlášenou společností, které patří komunikační zařízení, které odeslalo tuto zprávu. V případě, že server najde takovou aplikaci klienta, předá ji tyto zprávy obsahující adresu komunikačního zařízení, které žádá o stažení dat. Následně dojde ke komunikaci aplikaci klienta a komunikačního zařízení a stažení dat z digitálního tachografu. V případě, že server nenalezne připojenou aplikaci klienta s přihlášenou společností, které patří komunikační zařízení, odpoví komunikačnímu zařízení zprávou CMD_ERROR s chybovým kódem ERR_DOWNLOAD_PERIOD_TACHO (při odpovědi na požadavek stažení dat z digitálního tachografu), nebo ERR_DOWNLOAD_PERIOD_CARD (při odpovědi na požadavek stažení dat z karty řidiče). V tomto případě odloží komunikační zařízení stahování dat o 24 hodin, kdy opětovně vyšle požadavek na stažení dat z digitálního tachografu nebo z karty řidiče.

6 Požadavky na aplikace vzdáleného stahování dat z digitálního tachografu

V následující kapitole jsou definovány požadavky na firmware komunikačního zařízení a na ukládání dat na vzdálený server:

1. Možnost vzdáleného ovládání komunikačního zařízení přes počítačovou aplikaci.

2. Připojení alespoň dvou komunikačních zařízení, připojených k digitálnímu tachografu, ke vzdálenému serveru.

3. Připojení alespoň dvou aplikací klienta ke vzdálenému serveru.

4. Možnost manuálního stažení dat z digitálního tachografu za zvolené časové období.

5. Možnost manuálního stažení dat z karty řidiče.

6. Stažení konkrétního bloku dat (např. technická data, detailní rychlost atd.) z digitálního tachografu, který můžeme manuálně zvolit v aplikaci klienta.

7. Automatické stažení dat z karty řidiče každých 28 dnů a uložení dat na vzdálený server.

8. Automatické stažení dat z digitálního tachografu každých 90 dnů a uložení dat na vzdálený server.

9. Umožnění stažení dat ze serveru do PC pomocí aplikace klienta.

10. Správa připojených klientů k serveru pomocí jednoduché databáze.

11. Schopnost komunikačního zařízení obnovit TCP spojení při výpadku signálu.

7 Software pro vzdálené stahování dat z digitálního tachografu

Pro správnou funkčnost vzdáleného stahování dat z digitálního tachografu podle požadavků z kapitoly 6 jsem navrhl aplikaci pro server, klienta a komunikační zařízení. Ke každé aplikaci je sepsána dokumentace pomocí nástroje doxygen. Zdrojové soubory dokumentace jsou k dispozici v elektronické příloze diplomové práce.

7.1 Aplikace serveru

Aplikace pro vzdálený server je naprogramována v programovacím jazyku C++. Jedná se o konzolovou aplikaci a pro programování jsem využil prostředí Apple XCode. Jak bylo řečeno v předchozích kapitolách, vzdálený server slouží především ke komunikaci s komunikačním zařízením a aplikací klienta. Uchovává stažené soubory z digitálního tachografu a spravuje databázi připojených klientů.

Aplikace využívá dynamické alokování paměti a pro správnou kontrolu uvolňování paměti používá knihovnu check, viz [13]. Aplikace typu server pro plnění své funkce obsahuje tři C++ třídy, které se jmenují: `server`, `klient` a `database`.

Třída server slouží k realizaci serveru pomocí knihovny POSIX socket a následně k realizaci šifrovaného spojení a autentizaci klientů připojovaných k serveru pomocí knihovny OpenSSL. Šifrování komunikace probíhá, jak bylo řečeno v kapitole 5, pomocí protokolu TLS verze 1.2.

Třída klient uchovává data o jednotlivých klientech. Data, která se shromažďují o klientech jsou: adresa zařízení (přidělená adresa v $D4_H$ zprávě), typ zařízení (zařízení, které se připojilo k serveru), instituce (instituce, které patří dané zařízení), číslo socketu, SSL strukturu (struktura uchovává informace o TLS spojení klienta a serveru), file stream (práce se soubory daného klienta) a stav klienta (zobrazuje aktuální provozovanou akci klienta).

Třída database slouží k ukládání klientů třídy klient do databáze. Databáze je realizována pomocí C++ kontejneru, pomocí knihovny std::map. Třída database obsahuje například metody ke vkládaní, mazání nebo k hledání klientů podle adresy v C++ kontejneru.

Aplikace pro vzdálený server běží na dvou hlavních vláknech. Jedno vlákno slouží k obsluze klávesnice, kde lze pomocí předem určené klávesy ze serveru odhlásit všechny připojené klienty nebo zvolit konkrétního klienta, který se ze serveru odhlásí. Druhé vlákno slouží ke zpracování příchozích dat na konkrétním portu, navázání TCP spojení a následně každému připojenému klientovi vytvoří vlákno, ve kterém probíhá obsluha konkrétního klienta. Po ukončení TCP spojení s klientem je dané vlákno ukončeno. Po vytvoření vlákna, ve kterém probíhá obsluha daného klienta, čeká server na příjem zprávy od klienta. Po příjmu zprávy se v první řadě zkontroluje správnost formátu a verze D4 zprávy. V případě chyby ve formátu nebo typu D4 zprávy odpoví server chybovou zprávou, viz kapitola 5.1. Když je D4 zpráva v pořádku, tak ji server zpracuje a odpoví na příslušnou adresu podle typu zprávy. Vložení dat o klientovi do databáze probíhá po příjmu první zprávy CMD_CONNECT_CLIENT.

Pro přehlednost připojených klientů k serveru se na konzolu aplikace vypisují informace o připojených klientech k serveru, viz obrázek 7.1.

```
********************************************************************************************
********************************** APLIKACE SERVER *****************************************
********************************************************************************************
Pocet klientu pripojenych k serveru: 3
================================================

Klient 1
Spolecnost: NAM SYSTEM
Aplikace: Klient
Stav: Klient byl pripojen k serveru

Klient 2
Spolecnost: NAM SYSTEM
Aplikace: Komunikacni zarizeni
Jmeno zarizeni: NAM1
Stav: Klient byl pripojen k serveru

Klient 3
Spolecnost: COMPANY
Aplikace: Klient
Stav: Klient byl pripojen k serveru
```

Obr. 7.1: Výpis informací o připojených klientech ke vzdálenému serveru

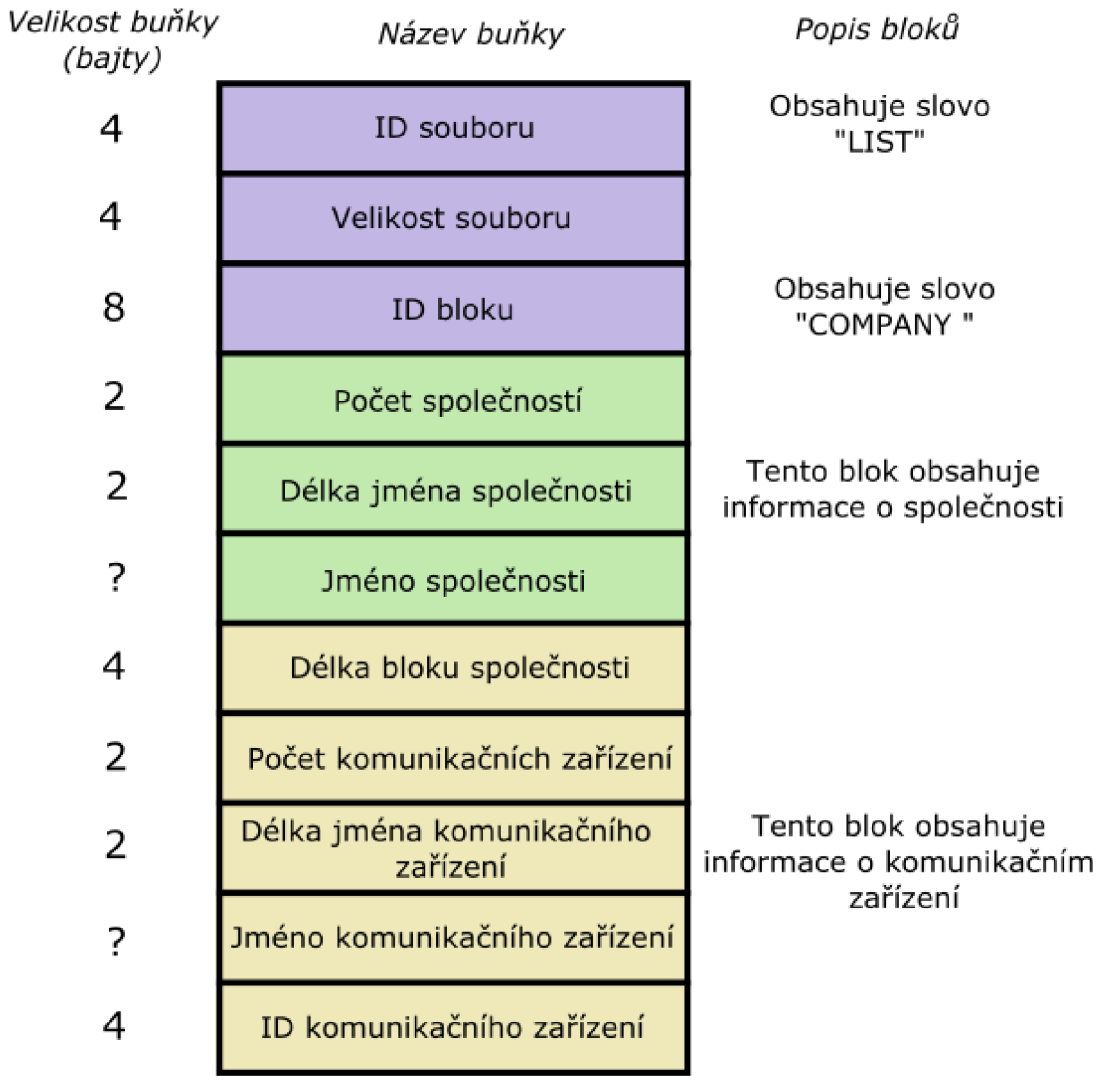
U výpisu klientů z databáze na serveru se vypisuje společnost, ke které daný klient patří, zda se jedná o připojenou aplikaci klienta, nebo komunikační zařízení a stav, který slouží k indikaci právě prováděného úkolu klienta. U připojených klientů jako komunikační zařízení se ve výpisu navíc zobrazuje jméno daného komunikačního zařízení.

Jak bylo řečeno v kapitole 5.1, při přihlášení klienta a příjmu první zprávy CMD_CONNECT_CLIENT server ověří, zda přihlašované jméno společnosti nebo

ID komunikačního zařízení je správné. K tomuto účelu slouží vytvořený binární soubor `device.list`, který je umístěný na serveru. V tomto souboru jsou uložena jména všech společností a jejich komunikačních zařízení s přiřazeným ID, které používají tento systém vzdáleného stahování dat z digitálního tachografu. Když komunikační zařízení odešle zprávu CMD_CONNECT_CLIENT, server ověří v tomto souboru jeho ID, které odeslal ve zprávě. U konkrétního ID se v souboru nachází také jméno komunikačního zařízení, které si uloží server do své databáze. Když dané ID v souboru nenajde, odpoví server chybovou zprávou. V případě, že zprávu CMD_CONNECT_CLIENT odešle aplikace klienta, server ověří, zda se v souboru nachází jméno společnosti odeslané ve zpravě. Poté je aplikaci klienta dovoleno komunikovat se vzdáleným serverem nebo s komunikačním zařízením patřící pod tuto přihlášenou společnost. Ukázku formátu binárního souboru `device.list` lze zhlédnout na obrázku 7.2.

Popis jednotlivých buněk z obrázku 7.2:

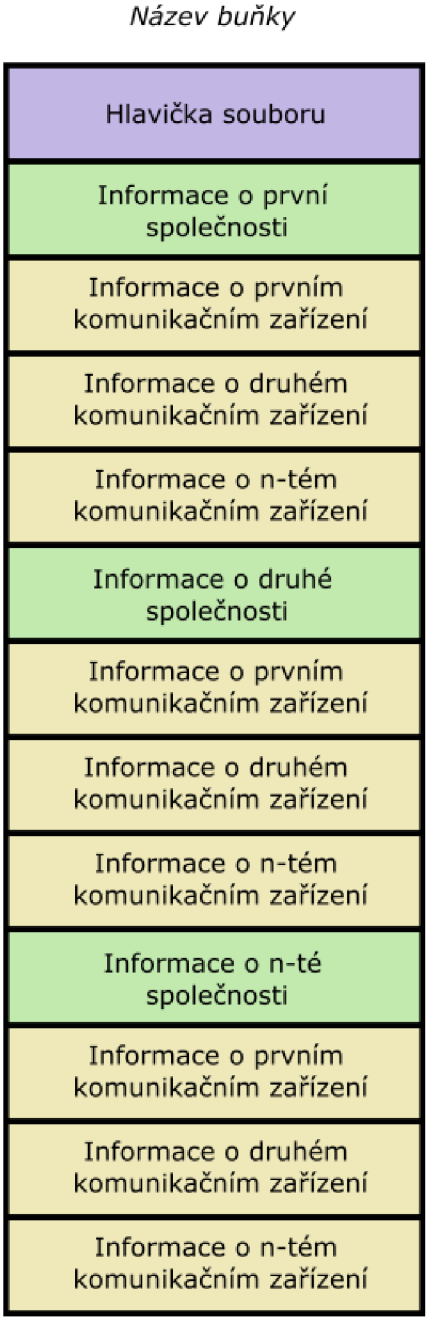
ID souboru: identifikuje začátek binárního souboru device.list. Obsahuje slovo „LIST“ v ASCII formátu ($4C495354_H$).
Velikost souboru: obsahuje velikost souboru v bajtech bez buňky ID souboru a velikost souboru.
ID bloku COMPANY: značí začátek bloku COMPANY. Obsahuje slovo „COMPANY“ v ASCII formátu ($434F4D50414E5920_H$).
Počet společností: značí počet společností, které obsahuje blok COMPANY. Maximální počet společností, které soubor může obsahovat je 65535.
Délka jména společnosti: značí počet písmen jména společnosti v následující buňce.
Jméno společnosti: obsahuje jméno společnosti v ASCII formátu.
Velikost bloku společnosti: značí velikost bloku společnosti v bajtech. Velikost se počítá od buňky počet komunikačních zařízení po další záznam o společnosti v souboru device.list.
Počet komunikačních zařízení: značí počet záznamů o komunikačních zařízení v bloku společnosti.
Délka jména komunikačního zařízení: značí počet písmen jména komunikačního zařízení v následující buňce.
Jméno komunikačního zařízení: obsahuje jméno komunikačního zařízení v ASCII formátu.
ID komunikačního zařízení: obsahuje ID komunikačního zařízení.



Obr. 7.2: Formát binárního souboru device.list

Buňku ID souboru, Velikost souboru a ID bloku COMPANY musí vždy soubor device.list obsahovat. Následně blok COMPANY obsahuje volitelný počet bloků společností a blok společnosti obsahuje volitelný počet komunikačních zařízení. Bloky označené tedy zelenou a žlutou barvou v obrázku 7.2 lze opakovat, ale pořadí bloků je neměnné. Pořadí jednotlivých bloků pro lepší názornost lze zhlédnout na obrázku 7.3.

Hlavička označená fialovou barvou na obrázcích 7.2 a 7.3 se nachází vždy na začátku souboru. Poté následují informace o první společnosti, uložené v souboru device.list, označené zelenou barvou. Každý blok společnosti obsahuje také volitelný počet informací o komunikačních zařízení. Po ukončení bloku první společnosti následuje začátek bloku druhé společnosti, která obsahuje také volitelný počet informací



Obr. 7.3: Pořadí bloků v souboru device.list

o komunikačních zařízeních. Počet společností takto uložených v souboru může být až 65535.

Pro lepší správu souboru device.list jsem navrhl aplikaci pro ukládání a načítaní dat ze souboru device.list, viz kapitola 8.4.

7.2 Aplikace klienta

Aplikace klienta je naprogramována v programovacím jazyku C++ v prostředí Microsoft Visual Studio. Aplikace slouží k manuálnímu vzdálenému ovládání firmwaru komunikačního zařízení. Ve fázi ladění firmwaru komunikačního zařízení sloužila aplikace klienta také k analýzám chybových stavů GSM modulu komunikačního zařízení, případně chybových stavů digitálního tachografu. K analýze chybových stavů pomocí aplikace jsem používal sběrnici RS232. Aplikace typu klient také obstarává obsluhu čtečky čipových karet, kde je umístěna tachografová karta společnosti.

Aplikace, tak jako v případě serveru, využívá dynamické alokování paměti a knihovnu check [13]. Aplikace obsahuje čtyři C++ třídy: `d4`, `client`, `smartcard` a `usart`.

Třída d4 slouží k sestavení D4 zpráv.

Třída client slouží k realizaci TCP připojení klienta k serveru. Pro realizaci TCP připojení k serveru využívá knihovnu Windows Socket (winsock). Šifrování dat a autentizace klienta pomocí protokolu TLS verze 1.2 je realizována, jako v případě serveru, knihovnou OpenSSL.

Třída smartcard realizuje obsluhu čtečky čipových karet a komunikaci s tachografovou kartou společnosti. Pro komunikaci s tachografovou kartou využívá knihovnu Windows Smart Card (winscard).

Třída serial slouží k obsluze sériové linky, která byla použita při ladění firmwaru komunikačního zařízení.

Aplikace klienta běží na dvou vláknech. Jedno vlákno slouží k příjmu zpráv odeslaných ze serveru. Druhé vlákno obsluhuje klávesnici. Při spuštění aplikace je nutno nejprve přihlásit společnost, které patří komunikační zařízení, které chceme ovládat. Ovládání aplikace je prováděno přes určité klavesy, viz menu aplikace na obrázku 7.4.

Klávesou 1 lze PC manuálně připojit k serveru, klávesou 2 můžeme PC odpojit ze serveru. Klávesa 3 slouží ke stažení všech zaznamenaných dat z digitálního tachografu v konkrétním zadaném intervalu. Klávesou 4 stáhneme všechna data z karty prvního nebo druhého řidiče. Klávesou 5 lze stáhnout konkrétní vybraná data z digitálního tachografu. Klávesa 6 zobrazí dostupné soubory společnosti na serveru

```
Menu aplikace:
[1] - Pripojit PC k serveru manualne
[2] - Odpojit PC ze serveru manualne
[3] - Stazeni dat z digitalniho tachografu za urcity interval
[4] - Stazeni dat z karty ridice
[5] - Nastaveni dat ke stazeni z digitalniho tachografu
[6] - Stazeni souboru ze serveru
[ESC] - konec programu
```

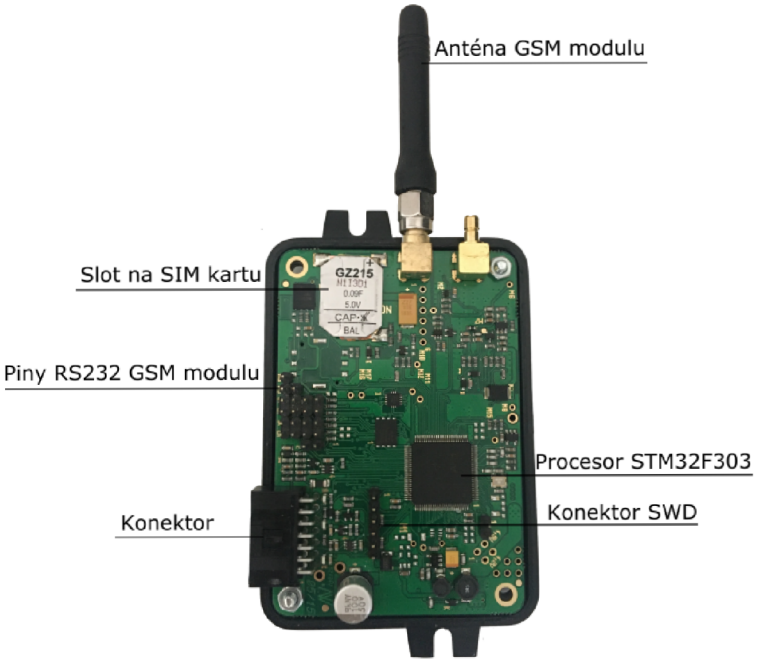
Obr. 7.4: Menu aplikace klienta

a následně lze stáhnout konkrétní vybraný soubor. Klávesou escape odhlásíme PC s aplikací klienta ze serveru a ukončíme aplikaci.

7.3 Firmware komunikačního zařízení

Komunikační zařízení komunikuje s digitálním tachografem a stažená data z digitálního tachografu posílá na vzdálený server.

Na obrázku 7.5 můžeme vidět hardware komunikačního zařízení, který dodala firma NAM system a.s.

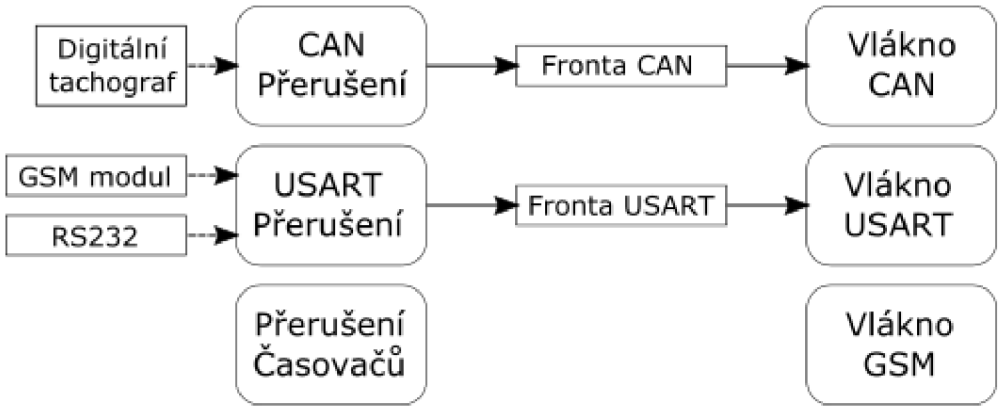


Obr. 7.5: Hardware komunikačního zařízení

Firmware komunikačního zařízení je realizován v programovacím jazyku C na procesoru STM32F303. Programování mikroprocesoru probíhalo pomocí desky STM32 Nucleo pomocí spojení konektoru SWD (Serial wire debug) na komunikačním zařízení a desky STM32 Nucleo. Projekt firmwaru komunikačního zařízení je napsaný v programovacím prostředí AC6 STM32 System Workbench. Pro vygenerování základního nastavení všech použitých periferií procesoru, jsem využil grafickou aplikaci STM32Cube. Při programování byly použity knihovny HAL (High Abstraction Layer) pro programování obsluhy jednotlivých periferií a knihovny CMSIS (Cortex Microcontroller Software Interface Standard) pro práci s obsluhou vláken mikroprocesoru a předáváním informací mezi vláknem a přerušením. Dále knihovna CMSIS sloužila pro práci s dynamicky alokovanou pamětí. Spojení se serverem je realizováno pomocí GSM modulu M95 od firmy quectel. Komunikace mezi GSM modulem a procesorem probíhá pomocí sběrnice RS232. Procesor řídí GSM modul pomocí tzv. AT příkazů. Pomocí vývodů pinů sběrnice RS232 GSM modulu na komunikačním zařízením lze GSM modul ovládat také přes sériovou linku z PC. GSM modul podporuje také protokol TLS, kterým je pomocí GSM modulu realizováno šifrované spojení se vzdáleným serverem. Autentifikace komunikačního zařízení při připojení k serveru probíhá pomocí vlastního vygenerovaného certifikátu. Pro uložení certifikátu v komunikačním zařízení jsem použil nevolatilní paměť GSM modulu. Firmware procesoru také realizuje obsluhu CAN sběrnice, která je připojena k digitálnímu tachografu. Vývod CAN sběrnice na komunikačním zařízení je realizován pomocí konektoru se 14 piny, viz obrázek 7.5. Konektor slouží společně také pro napájení komunikačního zařízení a vývod sběrnice RS232, kterou jsem využil při ladění komunikačního zařízení.

O běh komunikačního zařízení se stará operační systém reálného času FreeRTOS se třemi vlákny. První vlákno se stará o zpracování přijaté zprávy na CAN sběrnici, druhé vlákno se stárá o zpracování přijaté zprávy ze sběrnice RS232 GSM modulu a sběrnice RS232 připojené k PC. Poslední vlákno udržuje spojení komunikačního zařízení se serverem a odesílá požadavky na automatické stahování dat z digitálního tachografu serveru. V případě výpadku signálu GSM modulu vlákno zablokuje komunikaci po CAN sběrnici do té doby, než se podaří znovu obnovit signál GSM modulu. Na obrázku 7.6 lze zhlédnout realizaci obsluhy jednotlivých použitých periférií.

Obsluha jednotlivých periférií je realizována pomocí přerušení. Když dojde k přerušení inicializované sběrnicí CAN nebo RS232, tak se zpráva předá do FIFO (First In First Out) fronty, kde si ji převezme jedno vlákno, které zprávu podle obsahu zpracuje. Vlákno GSM čeká pouze na signál výpadku signálu GSM modulu, nebo



Obr. 7.6: Blokové schéma funkčnosti firmwaru komunikačního zařízení

na signál automatického stažení dat z digitálního tachografu. Když dojde k výpadku signálu, vlákno GSM se snaží navázat opětovné spojení se vzdáleným serverem. V případě vypršení časovačů pro automatické stažení dat z digitálního tachografu vyšle vlákno zprávu na požadavek stažení dat vzdálenému serveru. Komunikační zařízení využívá také čtyři časovače. První časovač udržuje diagnostickou relaci (remoteSession) s digitálním tachografem při nečinnosti na CAN sběrnici, viz kapitola 4. Další časovač slouží k odpočtu času při odhlášení komunikačního zařízení ze serveru inicializovaného serverem, viz kapitola 5.1. Poslední dva časovače zajišťují splnění legislativy digitálních tachografů o povinném stahování dat z digitálního tachografu a tachografové karty řidiče [5], viz kapitola 2.3. Inicializují tedy stahování dat z digitálního tachografu každých 90 dní a z karty řidiče každých 28 dní.

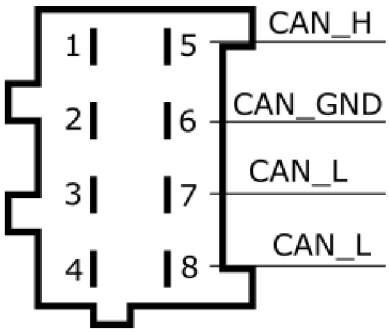
8 Demonstrace funkčnosti zařízení pro vzdálené stahování dat z digitálního tachografu

V této kapitole bude demonstrována funkčnost zařízení pro vzdálené stahování dat z digitálního tachografu. Funkčnost je demonstrována také ve videosouboru, který je součástí přílohy této diplomové práce. Vzdálené stahování dat je realizováno univerzálně a dokáže pracovat a stahovat data z několika digitálních tachografů. V této demonstraci funkčnosti budeme pracovat pouze s jedním komunikačním zařízením a jedním digitálním tachografem z důvodu vysokých pořizovacích nákladů digitálního tachografu pro tuto diplomovou práci.

Soubory stažené z digitálního tachografu se vždy budou uchovávat na vzdáleném serveru. Pomocí aplikace klienta lze tyto data ze vzdáleného serveru stáhnout a uložit na PC uživatele.

8.1 Připojení komunikačního zařízení k digitálnímu tachografu

Pro správnou funkci vzdáleného stahování dat z digitálního tachografu musíme připojit CAN sběrnici komunikačního zařízení k digitálnímu tachografu. CAN sběrnici připojujeme do konektoru C na zadní straně digitálního tachografu, viz obrázek 3.1. Zapojení jednotlivých pinů v konektoru C lze zhlédnout na obrázku 8.1.



Obr. 8.1: Zapojení pinů konektoru C digitálního tachografu

Vodič CAN sběrnice CAN_H připojíme na pin číslo 5 konektoru C digitálního tachografu. Vodič CAN_GND připojíme na pin 6 a vodič CAN_L připojíme na pin 7 a 8. Ostatní piny ponecháme nezapojené.

8.2 Vzdálené stahování dat z digitálního tachografu

Vzdáleně lze z digitálního tachografu stahovat data dvojím způsobem. První způsob je manuální stažení dat z digitálního tachografu pomocí aplikace klienta. Druhým způsobem je automatické stažení dat z digitálního tachografu na základě platné legislativy, kdy je dopravce povinen stahovat data z karty řidiče každých 28 dní a z digitálního tachografu každých 90 dní, viz kapitola 2.3.2.

Pro vzdálené stahování dat z digitálního tachografu musí být zajištěno, aby komunikační zařízení bylo v době požadavku na stažení dat připojeno ke vzdálenému serveru. Což je zajištěno tak, jak bylo řečeno v kapitolách 7 a 5, že se každé dostupné komunikační zařízení připojuje ke vzdálenému serveru automaticky. Spojení mezi serverem a komunikačním zařízením se udržuje, dokud má komunikační zařízení dostatečný signál na spojení se vzdáleným serverem. V případě výpadku signálu komunikačního zařízení dojde k přerušení spojení mezi vzdáleným serverem a komunikačním zařízením, které se obnoví při obnovení signálu komunikačního zařízení.

Při stahování dat z digitálního tachografu existují jistá omezení. Jak bylo řečeno v kapitole 4.1, stahování dat z digitálního tachografu se přeruší v okamžiku zapnutí nebo vypnutí zapalování vozidla. Proto je ideální stahovat data z digitálního tachografu při zapnutém zapalování nákladního automobilu. K přerušení stahování dat z digitálního tachografu dochází také při vypnutí nebo zapnutí zapalování vozidla. V tom případě komunikační zařízení informuje aplikaci klienta o přerušeném stahování dat z digitálního tachografu.

Pro manuální stahování dat je nutné spustit aplikaci klienta. Před spuštěním aplikace klienta se musíme ujistit, zda je k PC klienta připojena čtečka čipových karet, ve které je vložená tachografová karta společnosti. Když tachografová karta nebude do PC klienta vložena, aplikace klienta na tuto skutečnost upozorní. Aplikaci klienta je také nutné umístit do adresáře společně se složkou `Download`, do které se budou ukládat stažené soubory ze serveru a složkou `Certificates`, ve které budou uloženy certifikáty pro autentifikaci při navázání spojení se vzdáleným serverem.

Při spuštění aplikace klienta budeme dotázáni na přihlašovací jméno společnosti. Po zadání jména společnosti, server ověří pomocí binárního souboru device.list umístěného na serveru (viz kapitola 7.1), zda danou společnost zná. V případě, že přihlašovací jméno společnosti je v pořádku, server aplikaci klienta přihlásí k serveru a uloží si informace o klientovi do databáze. Po přihlášení aplikace ke vzdálenému serveru se zobrazí menu aplikace a hlášení, že přihlášení ke vzdálenému serveru pro-

běhlo v pořádku, viz obrázek 8.2. Jak už bylo řečeno v kapitole 7.2, aplikace klienta se ovládá stiskem ovládacích kláves. Klávesy pro ovládání jsou popsány v hranatých závorkách v menu aplikace. Nad menu aplikace lze také vidět jméno přihlašené společnosti. V případě nesprávného přihlašovacího jména společnosti dojde k odmítnutí připojení aplikace ze strany serveru a lze zadat nové přihlašovací jméno společnosti.

```
********************************************************************************************
************* Aplikace klienta pro stahovani dat z digitalniho tachografu *************
********************************************************************************************
Prihlasena spolecnost: NAM SYSTEM

Menu aplikace:
[1] - Pripojit PC k serveru manualne
[2] - Odpojit PC ze serveru manualne
[3] - Stazeni dat z digitalniho tachografu za urcity interval
[4] - Stazeni dat z karty ridice
[5] - Nastaveni dat ke stazeni z digitalniho tachografu
[6] - Stazeni souboru ze serveru
[ESC] - konec programu


Pripojeni k serveru probehlo uspesne
```

Obr. 8.2: Úvodní obrazovka aplikace klienta

Volbu pro stažení dat z digitálního tachografu můžeme zvolit pomocí klávesy čísla 3. Tato volba stáhne všechna data z digitálního tachografu (přehled, aktivity, události a chyby, podrobná data o rychlosti a technická data o vozidle) za stanovený časový interval, který můžeme stanovit po zvolení této volby, viz obrázek 8.3.

```
Zadejte cas od ve formatu dd-mm-YYYY
12-09-2019
Zadejte cas do ve formatu dd-mm-YYYY
04-04-2020
```

Obr. 8.3: Stanovení časového intervalu pro stažení dat z digitálního tachografu

Pokud uživatel zadá datum časového intervalu, který ještě nenastal, bude na tuto skutečnost upozorněn a může datum upravit.

Po zadání intervalu pro stažení dat z digitálního tachografu bude uživatel dotázán na výběr dostupného komunikačního zařízení, které stáhne data z určitého digitálního tachografu, viz obrázek 8.4.

```
[1] NAM1

Zadejte cislo komunikacniho zarizeni se kterym chcete komunikovat:
```

Obr. 8.4: Výběr komunikačního zařízení pro stažení dat z digitálního tachografu

Výběr dostupného komunikačního zařízení pro přihlášenou společnost je zobrazen formou seznamu. Komunikační zařízení lze vybrat číselnou volbou, která je zobrazena v hranatých zavorkách vedle jména daného komunikačního zařízení. V případě více dostupných komunikačních zařízeních pro danou společnost budou v seznamu zobrazena všechna komunikační zařízení. V případě, že pro danou přihlášenou společnost nebude dostupné komunikační zařízení, budeme o tomto v aplikaci informováni a stahování dat z digitálního tachografu se neuskuteční.

Po zvolení komunikačního zařízení začne autentifikace tachografové karty společnosti a po ukončení autentifikace tachografové karty začne stahování dat z digitálního tachografu a poslání a uložení těchto dat na vzdáleném serveru. Průběh autentifikace tachografové karty společnosti a průběh stahování dat je zobrazován jak v aplikaci klienta, tak ve výpisu aplikace serveru v položce stav daného klienta, viz obrázek 7.1.

Volba klávesy čísla 4 z menu aplikace (obrázek 8.2) slouží ke stažení dat z tachografové karty řidiče, umístěné ve slotu digitálního tachografu. Digitální tachograf má 2 sloty pro umístění karty řidiče. Proto při této volbě se menu aplikace klienta rozšíří o volbu, zda chceme stáhnout data z karty řidiče v prvním, či druhém slotu, viz obrázek 8.5.

```
Menu aplikace:
[1] - Pripojit PC k serveru manualne
[2] - Odpojit PC ze serveru manualne
[3] - Stazeni dat z digitalniho tachografu za urcity interval
[4] - Stazeni dat z karty ridice
  [1] - Stazeni dat z karty prvniho ridice
  [2] - Stazeni dat z karty druheho ridice
[5] - Nastaveni dat ke stazeni z digitalniho tachografu
[6] - Stazeni souboru ze serveru
[ESC] - konec programu
```

Obr. 8.5: Rozšíření menu klienta při volbě stažení dat z karty řidiče

Po zvolení tachografové karty řidiče, ze které budeme data stahovat, musíme zvolit dostupné komunikační zařízení (obrázek 8.4). Následně proběhne autentifikace tachografové karty společnosti a začne stahování dat z karty řidiče a uložení dat na vzdálený server.

Volbou klávesy číslo 5 můžeme přesně specifikovat, jaká data z digitálního tachografu chceme stáhnout. Při této volbě se menu aplikace klienta rozšíří o specifikaci dat ke stažení z digitálního tachografu (přehled, aktivity, události a chyby, podrobná data o rychlosti, technická data o vozidle a data z karty řidiče), viz obrázek 8.6. Obsah těchto specifických dat pro stažení z digitálního tachografu je popsán v kapitole 4.

```
Menu aplikace:
[1] - Pripojit PC k serveru manualne
[2] - Odpojit PC ze serveru manualne
[3] - Stazeni dat z digitalniho tachografu za urcity interval
[4] - Stazeni dat z karty ridice
[5] - Nastaveni dat ke stazeni z digitalniho tachografu
  [1] - Prehled
  [2] - Aktivity
  [3] - Udalosti a chyby
  [4] - Podrobna data o rychlosti
  [5] - Technicke data o vozidle
  [6] - Data z karty ridice
  [7] - Zacit proces stahovani
[6] - Stazeni souboru ze serveru
[ESC] - konec programu
```

Obr. 8.6: Rozšíření menu klienta při volbě nastavení dat ke stažení

Stisknutím čísla umístěného v hranaté závorce vybereme postupně volby, pomocí kterých chceme data z digitálního tachografu stáhnout. Volba přehled je povinná pro každé stáhnutí dat z digitálního tachografu a bez této volby bude uživatel upozorněn, že pro úspěšné stažení dat tuto volbu musí doplnit. Pod menu aplikace se zobrazuje přehled aktuálně zvolených dat ke stažení z digitálního tachografu (obrázek 8.7).

```
Pozadavek na stazeni dat:
Prehled
Aktivity
Udalosti a chyby
Podrobna data o rychlosti
Technicke data o vozidle
Data z karty ridice
```

Obr. 8.7: Zobrazení zvolených dat ke stažení z digitálního tachografu

Při volbě aktivity bude uživatel ještě vyzván k upřesnění dnů pro stažení aktivit z digitálního tachografu (obrázek 8.8).

```
[2] - Aktivity
  [1] - Specifikace intervalu pro stazeni dat
  [2] - Specifikace konkretniho dnu pro stazeni dat
  [3] - Ukonceni specifikace dnu pro stazeni dat
```

Obr. 8.8: Volba aktivity při nastavování dat ke stažení

Uživatel může specifikovat dny ke stažení aktivit pomocí intervalu (volba číslo 1), nebo stáhnout aktivity z konkrétního dnu (volba číslo 2). Tyto dvě volby můžeme mezi sebou kombinovat, tedy můžeme specifikovat dny pro stažení dat najednou pomocí intervalu i konkrétních dnů. Pro ukončení specifikace dnů pro stažení zvolíme volbu čísla 3. Následně se vratíme do menu pro nastavení dat ke stažení z digitálního tachografu a volbou klávesy čísla 7 můžeme začít proces stahování dat z digitálního tachografu.

8.3 Stažení dat ze serveru do aplikace klienta

Stažená data z digitálního tachografu lze také ze serveru stáhnout a uložit je pomocí aplikace klienta na PC uživatele.

Stažení dat ze serveru na PC uživatele se provede v aplikaci kliienta volbou číslo 6 z menu aplikace. Následně se zobrazí seznam dostupných souborů pro přihlášenou společnost (obrázek 8.9). Názvy uložených souborů na serveru začínají písmenem C, když se jedná o soubory stažené z karty řidiče, nebo T, data stažená z digitálního tachografu. Poté je v názvu souboru umístěná časová značka v okamžiku vytvoření daného souboru. Stažený soubor stáhneme ze serveru zadáním čísla daného souboru,

které je v hranaté závorce před názvem souboru. Stažený soubor se uloží do složky `Download`, umístěné ve stejném adresáři jako aplikace klienta.

```
[1] C_2020-03-16_11:42:37.ddd
[2] C_2020-03-16_11:45:47.ddd
[3] C_2020-03-16_11:49:48.ddd
[4] C_2020-04-04_13:37:05.ddd
[5] C_2020-04-06_11:31:21.ddd
[6] C_2020-04-06_12:54:33.ddd
[7] C_2020-04-08_10:34:21.ddd
[8] C_2020-04-08_13:17:01.ddd
[9] C_2020-04-14_11:30:04.ddd
[10] C_2020-04-14_11:46:34.ddd
[11] T_2020-04-03_15:37:52.ddd
[12] T_2020-04-04_13:16:53.ddd
[13] T_2020-04-04_13:34:32.ddd
[14] T_2020-04-06_11:28:31.ddd
[15] T_2020-04-06_12:51:06.ddd
[16] T_2020-04-06_13:13:51.ddd
[17] T_2020-04-08_10:31:47.ddd
[18] T_2020-04-08_13:07:39.ddd
[19] T_2020-04-08_13:14:26.ddd
[20] T_2020-04-08_13:19:15.ddd
[21] T_2020-04-13_16:30:29.ddd

Zadejte cislo souboru ktery chcete stahnout:
```

Obr. 8.9: Volba stažení souboru ze serveru

Volbou klávesy číslo 1 z hlavního menu můžeme aplikaci klienta manuálně přihlásit k serveru a volbou klávesy číslo 2 můžeme aplikaci klienta odhlásit ze serveru.

Zařízení pro vzdálené stahování dat z digitálního tachografu umožňuje také automatické stahování dat z digitálního tachografu. Výchozí interval automatického stahování dat z digitálního tachografu je 28 dní u dat z karty řidiče a 90 dní u stahování dat z digitálního tachografu. Tento interval lze změnit pouze změnou firmwaru komunikačního zařízení. Při automatickém stahování dat z digitálního tachografu se stažený soubor uloží na vzdáleném serveru. Pro správnou funkci automatického stahování dat z digitálního tachografu je nutné mít spuštěnou také aplikaci klienta a mít zapojenou čtečku čipových karet s vloženou tachografovou kartou společnosti, aby se mohla provést autentifikace.

8.4 Ovládání aplikace pro správu souboru device.list

Jak bylo řečeno v kapitole 7.1, soubor device.list je binární soubor, který uchovává informace o společnostech a komunikačních zařízeních, které využívají tento systém vzdáleného stahování dat z digitálního tachografu. Pro lepší správu tohoto souboru jsem navrhl aplikaci, která s tímto souborem pracuje a dokáže ho různě modifikovat.

Aplikace pro úpravu souboru device.list je navržená pomocí programovacího prostředí Apple XCode. Ovládání aplikace se provadí výběrem volby písmene nebo čísla z menu aplikace. Volba se při výpisu menu v aplikaci nachází v hranaté závorce, viz. obrázek 8.10.

```
********************************************************************************
********************** Aplikace pro upravu souboru device.list ***********************
********************************************************************************

Menu aplikace:
[1] Pridani komunikacniho zarizeni ke konkretni spolecnosti
[2] Pridani nove spolecnosti do seznamu
[3] Upraveni jmena komunikacniho zarizeni v seznamu
[4] Upraveni jmena spolecnosti v seznamu
[5] Smazani spolecnosti ze seznamu
[6] Smazani komunikacniho zarizeni ze seznamu
[7] Zobrazit cely seznam komunikacnich zarizeni
[8] Zobrazit komunikacni zarizeni jen od konkretni spolecnosti
[9] Zobrazit pouze informace o konkretnim komunikacnim zarizeni
[k] Ukonceni uprav seznamu

Zadejte volbu z menu a potvrdte entrem:
```

Obr. 8.10: Menu aplikace pro správu souboru device.list

Následně příslušnou volbou z menu můžeme doplnit údaje o společnosti nebo komunikačním zařízení. Příslušné údaje můžeme také mazat, upravovat, přidávat nebo vypisovat. Aplikace také kontroluje správnost zapsaných informací. Jedná se například o kontrolu, zda v seznamu nejsou dvě stejné společnosti nebo dvě komunikační zařízení se stejným ID. Aplikace kontroluje také, zda nejsou v seznamu u jedné společnosti dvě komunikační zařízení se stejným jménem.

8.5 Kontrola stažených dat z digitálního tachografu

Stažená data z digitálního tachografu lze zobrazit a kontrolovat pomocí speciálních aplikací. V této diplomové práci jsem k tomuto účelu použil aplikaci Tachograph

File Viewer a aplikaci ReadESM.

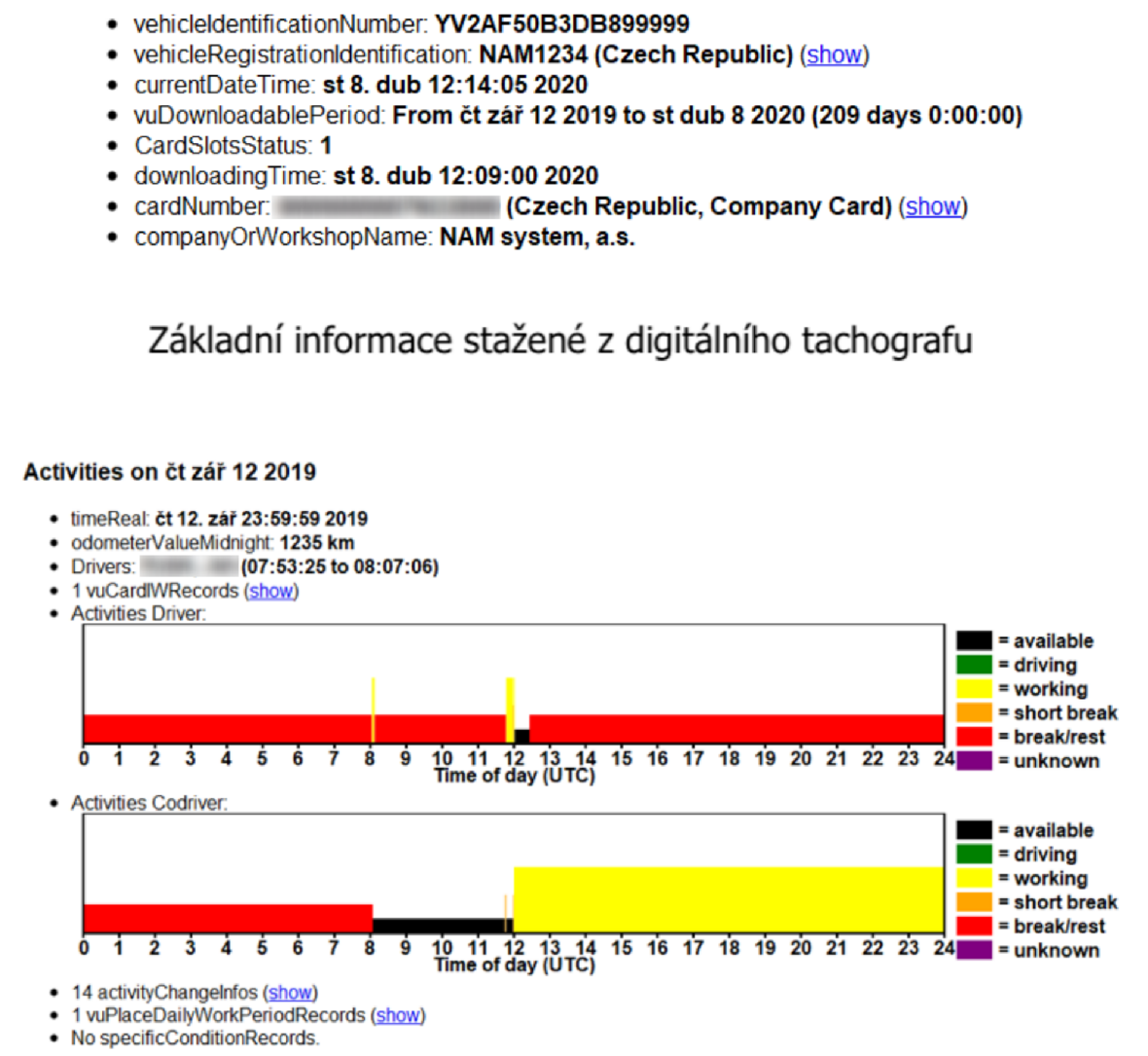
Tachograph File Viewer je placená aplikace a zdarma je dostupná pouze zkušební verze. Ve zkušební verzi aplikace lze zobrazit z dat digitálního tachografu pouze přehled, tedy základní data o digitálním tachografu a vozidle, kde je digitální tachograf umístěn. V případě dat z karty řidiče lze zobrazit pouze základní informace o držiteli tachografové karty. V případě neúplného a nesprávného formátu souboru, aplikace soubor nedokáže otevřít a upozorní uživatele o chybě v souboru. Ukázku zobrazení základních dat ze souboru z digitálního tachografu a karty řidiče v aplikaci Tachograph File Viewer lze zhlédnout na obrázku 8.11.

Obr. 8.11: Ukázka aplikace Tachograph File Viewer

Vlevo na obrázku 8.11 lze zhlédnout zobrazení dat z digitálního tachografu a vpravo se nachází zobrazení dat z karty řidiče. U souboru staženého z digitálního tachografu zobrazuje aplikace registrační značku vozidla a VIN kód vozidla, ve kterém je digitální tachograf umístěn. Dalším zobrazeným údajem je, za jaký časový interval jsou zaznamenaná data ve staženém souboru. Poslední základní údaj souboru je o výrobci daného typu digitálního tachografu. Údaje o registrační značce a VIN kódu na obrázku 8.11 jsou smyšlené a neobsahují reálné údaje. V případě zobrazení souboru staženého z karty řidiče v aplikaci jsou zobrazeny pouze základní údaje o řidiči (jméno, datum narození atd.). Z důvodu, že údaje na obrázku z karty řidiče obsahují reálné údaje, jsou rozmazány.

ReadESM je volně dostupná aplikace. Grafika této aplikace, v porovnání s apli-

kací Tachograph File Viewer, není tak vyspělá. Aplikace zobrazuje textový výpis informací, obsažených v souboru digitálního tachografu nebo karty řidiče, případně jednoduché grafy činností řidiče. Ukázku aplikace ReadEsm lze zhlédnout na obrázku 8.12.



Obr. 8.12: Ukázka aplikace ReadESM

V horní části obrázku 8.12 můžeme vidět zobrazení základních informací o vozidle jako VIN kód, registrační značku. Základní informace zobrazené pomocí aplikace

ReadESM obsahují také časový interval stahovaných dat nebo společnost, které patří tento digitální tachograf. Ve spodní části obrázku je ukázka zobrazení aktivit prvního i druhého řidiče pomocí jednoduchého grafu.

8.6 Funkce pro ovládání a správu vzdáleného serveru

Pro lepší správu, ovládání a možnosti modifikací kódu vzdáleného serveru jsou na serveru implementovány následující podpůrné funkce:

- Možnost manuálně vyvolat výpis všech klientů z databáze. Tato funkce se aktivuje zadáním písmene *p* do konzole aplikace serveru a potvrdí se klávesou ENTER.

- Možnost odhlášení konkrétního klienta. Tato funkce se aktivuje zadáním písmene *d* do konzole aplikace serveru a potvrdí se klávesou ENTER. Následně správce serveru musí zadat index klienta z databáze, viz výpis klientů na serveru (obrázek 7.1).

- Možnost odhlášení všech klientů ze serveru a ukončení aplikace serveru. Tato funkce se aktivuje zadáním písmene *k* do konzole aplikace serveru a potvrdí se klávesou ENTER. Následně správce serveru musí nastavit dobu nečinnosti serveru v sekundách. Poté se ze serveru odhlásí všichni klienti (komunikační zařízení i aplikace klienta), kteří jsou připojení ke vzdálenému serveru. Po uplynutí nečinnosti serveru se jednotlivá komunikační zařízení opětovně přihlásí. Přihlašování komunikačních zařízení ke vzdálenému serveru neprobíhá pro všechna zařízení ve stejnou dobu, aby nedošlo k přetížení serveru. Každé komunikační zařízení si ke zvolené době nečinnosti serveru náhodně přičte od 0 do 10 minut a poté se k serveru přihlásí.

9 Zhodnocení funkce celého zařízení pro vzdálené stahování dat z digitálního tachografu

V této kapitole bude popsán stručný souhrn všech funkcí celého zařízení pro vzdálené stahování dat z digitálního tachografu:

- Komunikace mezi komunikačním zařízením, aplikací klienta a serverem probíhá pomocí autorem navržených a definovaných zpráv. Komunikace je zašifrována pomocí protokolu TLS verze 1.2 a autorizace klientů při připojení k serveru probíhá pomocí certifikátu.

- Server podporuje správu a komunikaci teoreticky až s 65535 komunikačními zařízeními a 65535 aplikacemi klienta připojenými k serveru najednou. Server je limitován pouze svojí výkonností zvládnout všechny tyto klienty obsloužit (v rámci této diplomové práce bylo testováno připojení ke vzdálenému serveru 1 komunikační zařízení a 10 aplikací klienta).

- Server obsahuje podpůrné funkce pro správu a ovládání. Mezi podpůrné funkce patří odhlášení všech klientů najednou ze serveru, odhlášení konkrétního klienta ze serveru, nebo výpis informací o všech klientech připojených k serveru.

- Systém vzdáleného stahování dat podporuje správu jednotlivých komunikačních zařízení pod konkrétní společností. Což znamená, že jednotlivé společnosti mohou přistupovat k souborům a ukládat požadavky ke stažení dat z digitálního tachografu pouze komunikačním zařízením, které patří společnosti, která vznesla tento požadavek.

- Komunikační zařízení umožňuje automatické stažení dat z digitálního tachografu každých 90 dní a z karty řidiče každých 28 dní.

- Možnost manuálního stažení dat z digitálního tachografu pomocí aplikace klienta. Aplikace klienta podporuje stažení dat z digitálního tachografu za předem stanovený interval. Je možné také stáhnout data pouze z karty řidiče, vložené ve slotu digitálního tachografu. V aplikaci klienta můžeme i předem stanovit, která data chceme z digitálního tachografu stáhnout.

- Aplikace klienta umožňuje stažení konkrétního souboru ze vzdáleného serveru na PC klienta.

- Manuální přihlašení a odhlášení aplikace klienta ke vzdálenému serveru.

- Podpora obnovení TCP spojení komunikačního zařízení se vzdáleným serverem při výpadku signálu.

9.1 Návrh možných vylepšení pro vzdálené stahování dat z digitálního tachografu

V této kapitole jsou popsány návrhy dalších možných vylepšení pro vzdálené stahování dat z digitálního tachografu.

1. Přihlašování společnosti v aplikaci klienta pomocí jména a hesla společnosti. V dosavadním návrhu aplikace klienta se společnost přihlašuje pouze prostřednictvím jména společnosti (viz kapitola 8.2), kdy server pouze zkontroluje, zda je název společnosti v pořádku. Vylepšení by spočívalo v přidání hesla k přihlašovacímu jménu společnosti a tedy znemožnění neoprávněného stažení souboru dané společnosti ze serveru.

2. Umístění čtečky čipových karet s tachografovou kartou společnosti na vzdáleném serveru. Dosavadní návrh systému vzdáleného stahování dat z digitálního tachografu počítá s umístěním tachografových karet u PC klienta (viz obrázek 5.1). Z důvodu, že systém vzdáleného stahování dat z digitálního tachografu umožňuje automatické stahování, je nutné, aby při každém stažení dat byla zapnutá aplikace klienta s připojenou čtečkou čipových karet a vloženou tachografovou kartou společnosti. Při každém i automatickém stažení dat z digitálního tachografu je totiž nutné provést autentifikaci tachografové karty společnosti. Při umístění tachografových karet společnosti na serveru by odpadla nutnost mít zapnutou aplikaci klienta při stahování dat z digitálního tachografu.

3. Změna intervalu automatického stahování dat z digitálního tachografu z aplikace klienta. V aktuálním stavu systému stahuje komunikační zařízení automaticky každých 28 dní data z karty řidiče a každých 90 dní data z digitálního tachografu. Změnu tohoto intervalu pro automatické stahování lze provést pouze změnou firmwaru komunikačního zařízení. Vylepšení by umožnilo tento interval změnit také v aplikaci klienta.

4. Detekce zapnutého zapalování vozidla pomocí komunikačního zařízení. Při stahování dat z digitálního tachografu se vyskytují jistá omezení, která souvisí se zapnutím nebo vypnutím zapalování vozidla (viz kapitola 4.1). Z důvodu těchto omezení je nejvhodnější stahovat data z digitálního tachografu, když má vozidlo zapnuté zapalování a není v provozu příliš krátkou či dlouhou dobu. Kvůli velké pravděpodobnosti, že nedojde k přerušení stahování dat z digitálního tachografu v důsledku vypnutí nebo zapnutí zapalování.

Závěr

Výsledkem této diplomové práce je navržení funkčního systému vzdáleného stahování dat z digitálního tachografu (DT). V rámci této práce jsem navrhl koncepci celého řešení vzdáleného stahování dat. Dále jsem vyhotovil aplikaci pro server, aplikaci pro klienta a firmware komunikačního zařízení. Navrhl jsem vlastní komunikační zprávy pro komunikaci mezi aplikacemi a celá komunikace probíhá v zašifrované formě pomocí protokolu TLS. Obsahem diplomové práce je také videosoubor popisující funkčnost celého systému, přiložený v příloze této diplomové práce. Pro lepší orientaci v kódu vytvořených aplikací jsem zhotovil dokumentaci pomocí nástroje Doxygen, která je taktéž dostupná v příloze této diplomové práce.

V kapitole 2 se práce věnuje problematice DT a jejich právní legislativou. Mimo jiné obsahuje tato kapitola také popis formátu dat poskytovaných DT nebo popis komunikace s tachografovými kartami.

Kapitola 3 se věnuje sběrnicím používaných v DT ke stahování dat. DT používá ke stahování dat sběrnici RS232, viz kapitola 3.1 a sběrnici CAN, viz kapitola 3.2. V rámci této kapitoly je popsán také komunikační standard pro komunikaci s DT podle normy ISO 15765-2.

V kapitole 4 je uvedena specifikace pro vzdálené stahování dat z DT. Tato kapitola také obsahuje popis omezení při stahování dat. Prvním omezením je, že při vypnutém zapalování vozidla, ve kterém je umístěn DT, je umožněno stahovat data pouze do 24 hodin od vypnutí zapalování. Druhým omezením pro úspěšné stažení dat je, že stahování dat nesmí byt přerušeno vypnutím nebo zapnutím zapalování vozidla během stahování dat.

Kapitola 5 popisuje návrh a funkcionalitu řešení vzdáleného stahování dat z DT. Obsahem této kapitoly je také popis struktury vytvořených zpráv pro komunikaci se vzdáleným serverem včetně popisu komunikace mezi aplikacemi pomocí těchto zpráv.

V kapitole 6 jsou uvedeny požadavky na firmware komunikačního zařízení a na proces vzdáleného stahování dat na nadřazený server. Mezi požadavky na firmware a vzdálený server patří připojení alespoň dvou komunikačních zařízení a dvou aplikací klienta k serveru, možnost manuálního i automatického stažení dat z karty řidiče a DT, umožnění stažení dat ze serveru na PC klienta, správa připojených klientů k serveru pomocí databáze nebo schopnost komunikačního zařízení obnovit TCP

spojení při výpadku signálu.

Kapitola 7 se věnuje popisu vytvořené aplikace pro klienta, server a firmwaru komunikačního zařízení.

Popis postupu stahování dat, pomocí navržených aplikací, z DT se nachází v kapitole 8. V rámci této diplomové práce jsem zhotovil také krátké video, které demonstruje základní funkce navrženého systému vzdáleného stahování dat z DT. Vytvořené video je uloženo na přiloženém CD, viz příloha A.

Poslední kapitola 9 se věnuje zhodnocení všech funkcí navrženého systému vzdáleného stahování dat z DT a také lze zde najít návrhy na vylepšení celého systému. Mezi navrhovaná vylepšení patří například přihlašování společnosti v aplikaci klienta pomocí jména a hesla společnosti, umístění čteček čipových karet s tachografovou kartou společnosti na vzdáleném serveru, změnu intervalu automatického stahování dat z DT z aplikace klienta nebo detekci zapnutého zapalování vozidla pomocí komunikačního zařízení.

Celý systém je navržený tak, že všechny jeho součásti (aplikace klienta, aplikace serveru a komunikační zařízení) komunikují na internetu pomocí veřejných IP adres. Na začátku řešení systému bylo tedy nutné zařídit u poskytovatele internetu veřejnou IP adresu pro zařízení, na kterém bude spuštěna aplikace serveru. Z důvodu, že stažené soubory obsahují citlivé údaje uživatelů, bylo nutné také zajistit šifrovaný přenos těchto dat, což jsem zajistil implementací protokolu TLS.

Následující systém najde uplatnění u společností s větším vozovým parkem nákladních automobilů. Systém umožňuje automatické dodržení legislativy o povinném stahování dat z DT a karty řidiče [5]. Uživateli tedy nehrozí žádné postihy za nedodržení legislativy. V případě potřeby si uživatel může jakékoliv data vzdáleně stáhnout pomocí aplikace klienta.

Literatura

[1] PŘIBYL, Pavel a SVÍTEK, Miroslav. *Inteligentní dopravní systémy.* Praha: BEN - technická literatura, 2001. ISBN 978-807-3000-295.

[2] Heavy Truck Electronic Interfaces Working Group. *Digital Tachograph Specification for remote company card authentication and remote data downloading* [online]. 2018 [cit. 22 .8 .2019]. Dostupné z URL: <http://www.fms-standard.com/Truck/down_load/User_Guide_Version_02.01_181209.pdf>

[3] ISO 15765-2. *Road vehicles — Diagnostics on Controller Area Networks (CAN) — Part 2: Network layer services.* Ženeva (Švýcarsko): ISO copyright office, 2004, 44s.

[4] SYSTEMCONSULT. *Digitální tachograf* [online]. Pardubice 2009 [cit. 5 .11 .2019]. Dostupné z URL: <https://www.nehody.net/wp-content/uploads/2012/03/Digitáln%C3%AD-tachograf.-Př%C3%ADručka-na-CD.pdf>

[5] NAŘÍZENÍ KOMISE (EU) č. 581/2010: *o stanovení maximálních časových úseků pro stahování příslušných údajů z přístroje ve vozidle a z karty řidiče.* In:. Brusel: BARROSO, 2010, 581/2010.

[6] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (ES) č. 561/2006: *o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy, o změně nařízení Rady (EHS) č. 3821/85 a (ES) č. 2135/98 a o zrušení nařízení Rady (EHS) č. 3820/85.* In:. Štrasburk: FONTELLES, 2006, 561/2006.

[7] NAŘÍZENÍ KOMISE (ES) č. 1360/2002: *kterým se posedmé přizpůsobuje technickému pokroku nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě.* In:. Brusel: PALACIO, 2002, 1360/2002.

[8] PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2016/799: *kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí.* In:. Evropská komise, 2016, 2016/799.

[9] MERTLÍK, Daniel: *Průmyslové komunikační sítě pro automatizaci* [online]. Brno 2010 [cit. 3 .12 .2019]. Dostupné z URL: <https://core.ac.uk/download/pdf/30291496.pdf>. Bakalářská práce. Vysoké učení technické v Brně, Fakulta strojního inženírství, Ústav automatizace a informatiky. Vedoucí práce Zdeněk Němec.

[10] POLÁK, Karel: *Sběrnice CAN* [online]. Brno 2003 [cit. 3 .12 .2019]. Dostupné z URL: <http://www.elektrorevue.cz/clanky/03021/index.html>

[11] Přispěvatelé Wikipedie: *CAN bus* [online]. 2020 [cit. 27 .05 .2020]. Dostupné z URL: <https://cs.wikipedia.org/w/index.php?title=CAN_bus&oldid=18369931>

[12] Wikipedia contributors: *Adler-32* [online]. 2020 [cit. 27 .05 .2020]. Dostupné z URL: <https://en.wikipedia.org/wiki/Adler-32>

[13] ŠABATKA, Pavel: *Tvorba úloh pro výuku předmětu: Praktické programování v C++*. Brno 2008. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Petr Petyovský.

Seznam symbolů, veličin a zkratek

APDU	Application Protocol Data Unit (str. 12)
ATR	Answer The Reset (str. 12)
BS	Block Size (str. 25)
CAN	Controller Area Network (str. 20)
CF	Consecutive Frame (str. 23)
DF	Dedicated File (str. 12)
DT	Digitální Tachograf (str. 28)
EF	Elementary File (str. 12)
ESM	External Storage Media (str. 14)
FC	Flow Control (str. 23)
FF	First Frame (str. 23)
FF_DL	First Frame Data length (str. 25)
FIFO	First In First Out (str. 51)
FS	Flow Status (str. 25)
HAL	High Abstraction Layer (str. 51)
CMSIS	Cortex Microcontroller Software Interface (str. 51)
MF	Master File (str. 12)
N_AI	Address Information (str. 23)
N_PCI	Protocol Control Information (str. 23)
N_PDU	Protocol Data Unit (str. 23)
N_TA	Target address (str. 24)
N_SA	Source Address (str. 24)
SF	Single Frame (str. 23)
SF_DL	Single Frame Data length (str. 24)
SN	Sequence Number (str. 25)
SSL	Secure Sockets Layer (str. 38)
STmin	Separation Time min. (str. 25)
SWD	Serial Wire Debug (str. 51)
TCP	Transmition control protocol (str. 33)
TLS	Transport Layer Security (str. 33)

Seznam příloh

A Obsah přiloženého CD

- `/` ..... kořenový adresář přiloženého CD
  - `Documentation` .... adresář obsahující dokumentaci vytvořených aplikací, která je vytvořena pomocí nástroje Doxygen
  - `SourceCode` ..... adresář obsahující zdrojové kódy vytvořených aplikací
    - `klient` ..... C++ zdrojové kódy aplikace klienta
    - `server` ..... C++ zdrojové kódy aplikace serveru
    - `firmware` ..... C zdrojové kódy firmwaru komunikačního zařízení
    - `device_list` ..... C++ zdrojové kódy aplikace pro správu souboru device.list
  - `Application` ..... adresář obsahující spustitelné aplikace
    - `app_klient` ..... adresář obsahující spustitelnou aplikaci klienta
    - `app_server` ..... adresář obsahující spustitelnou aplikaci serveru
    - `app_device_list` . adresář obsahující spustitelnou aplikaci pro správu souboru device.list
  - `ThesisCode` ..... adresář obsahující zdrojové texty diplomové práce v LaTeX
  - `Thesis` ..... elektronická verze textu a prezentace k obhajobě diplomové práce
    - `xmatou28-prace.pdf` ..... elektronická verze textu diplomové práce
    - `xmatou28-obhaj.pdf` ..... elektronická verze prezentace k obhajobě diplomové práce
  - `Video` ..... adresář obsahující video přiložené k diplomové práci
    - `xmatou28.mp4` ..... video demonstrující funkčnost diplomové práce
  - `readme.txt` ..... soubor s návodem pro práci s přílohami na přiloženém CD

B Struktury dat na tachografových kartách

Tab. B.1: Struktura dat na kartě řidiče

Soubor/prvek dat	Popis souboru dat
MF	Master file.
├─EF ICC	Informace týkající se označení karty.
├─EF IC	Informace týkající se čipu karty.
└─DF Tachograph	Soubor tachograf.
├─EF Application_Identification	Informace týkající se identifikace žádosti o kartu.
├─EF Card_Certificate	Certifikát karty.
├─EF CA_Certificate	Certifikát členského státu vydávajícího kartu.
├─EF Identification	Informace o čipové kartě a jeho držiteli.
├─EF Card_Download	Informace o posledním stažením dat.
├─EF Driving_Licence_Info	Informace o řidičském oprávnění držitele.
├─EF Events_Data	Zaznamenání událostí na kartě.
├─EF Faults_Data	Zaznamenání chybových stavů karty.
├─EF Driver_Activity_Data	Záznam aktivit řidiče.
├─EF Vehicles_Used	Informace o použitých vozidlech.
├─EF Places	Místa, kde byla karta použita.
├─EF Current_Usage	Data aktuálního využití karty.
├─EF Control_Activity_Data	Informace o kontrolách řidiče.
└─EF Specific_Conditions	Údaje o specifických podmínkách.

Tab. B.2: Struktura dat na kartě podniku

Soubor/prvek dat	Popis souboru dat
MF	Master file.
├─EF ICC	Informace týkající se označení karty.
├─EF IC	Informace týkající se čipu karty.
└─DF Tachograph	Soubor tachograf.
├─EF Application_Identification	Informace týkající se identifikace žádosti o kartu.
├─EF Card_Certificate	Certifikát karty.
├─EF CA_Certificate	Certifikát členského státu vydávajícího kartu.
├─EF Identification	Informace o čipové kartě a jeho držiteli.
└─EF Company_Activity_Data	Informace o aktivitách podniku.

Tab. B.3: Struktura dat na kartě dílny

Soubor/prvek dat	Popis souboru dat
MF	Master file.
├─EF ICC	Informace týkající se označení karty.
├─EF IC	Informace týkající se čipu karty.
└─DF Tachograph	Soubor tachograf.
├─EF Application_Identification	Informace týkající se identifikace žádosti o kartu.
├─EF Card_Certificate	Certifikát karty.
├─EF CA_Certificate	Certifikát členského státu vydávajícího kartu.
├─EF Identification	Informace o čipové kartě a jeho držiteli.
├─EF Card_Download	Informace o posledním stažením dat.
├─EF Calibration	Záznamy o provedených kalibracích DT.
├─EF Sensor_Installation_Data	Záznamy o instalacích senzorů.
├─EF Events_Data	Záznamy o událostech.
├─EF Faults_Data	Záznamy o chybových stavech karty.
├─EF Driver_Activity_Data	Záznamy o aktivitách řidiče.
├─EF Vehicles_Used	Záznamy o použitých vozidlech.
├─EF Places	Místa, kde byla karta použita.
├─EF Current_Usage	Data aktuálního využití karty.
├─EF Control_Activity_Data	Informace o kontrolách.
└─EF Specific_Condtions	Údaje o specifických podmínkách.

Tab. B.4: Struktura dat na kartě kontroly

Soubor/prvek dat	Popis souboru dat
MF	Master file.
├─EF ICC	Informace týkající se označení karty.
├─EF IC	Informace týkající se čipu karty.
└─DF Tachograph	Soubor tachograf.
├─EF Application_Identification	Informace týkající se identifikace žádosti o kartu.
├─EF Card_Certificate	Certifikát karty.
├─EF CA_Certificate	Certifikát členského státu vydávajícího kartu.
├─EF Identification	Informace o čipové kartě a jeho držiteli.
└─EF Controller_Activity_Data	Záznamy o provedených kontrolách.

C Rozpor karet

Tato událost nastane, jestliže se vložením platných karet, do slotů digitálního tachografu, dosáhne kombinace označené v tabulce písmenem X.

Tab. C.1: Rozpor karet [7]

Vložení neodpovídající karty		**Otvor pro vložení karty prvního řidiče**			
		Karta řidiče	Karta kontroly	Karta dílny	Karta podniku
Otvor pro vložení karty druhého řidiče	Karta řidiče			X	
	Karta kontroly		X	X	X
	Karta dílny	X	X	X	X
	Karta podniku		X	X	X

D Posloupnost zpráv pro úspěšné stažení dat z digitálního tachografu

Tab. D.1: Posloupnost zpráv pro úspěšné stažení dat z digitálního tachografu [2]

Komunikační zařízení	**Směr**	**Digitální tachograf**	**Poznámky**
StartDiagnosticSession(remoteSession)	-> <-	Pozitivní odpověď StartDiagnosticSession	V případě, že vzdálená relace v DT není aktivní.
RemoteCompanyCardReady(ATR)	-> <-	DTReady	
CompanyCardToDTData(NoData)	-> <-	DTToCompanyCardData(APDU)	
CompanyCardToDTData(APDU)	-> <-	DTToCompanyCardData(APDU)	
Výměna CompanyCardToDTData a DTToCompanyCardData do té doby, než bude autentifikace karty hotová.			
CompanyCardToDTData(APDU)	-> <-	RemoteAuthenticationSucceeded	
RemoteDownloadDataRequest(RequestList)	-> <-	RemoteDownloadAccessGranted	
RequestUpload	-> <-	Pozitivní odpověď RequestUpload	
TransferData (wrapAround/blockSequence = 0x00/0x01, typ dat overview)	-> <-	TransferData (wrapAround/blockSequence = 0x00/0x01, Data)	Při stahování dat z DT musí být staženy prvně data typu overview.
TransferData (wrapAround/blockSequence = 0x00/0x02, typ dat overview)	-> <-	TransferData (wrapAround/blockSequence = 0x00/0x02, Data)	
Posílání TransferData, dokud přenos dat typu overview nebude dokončeno.			
TransferData (wrapAround/blockSequence, typ dat overview)	-> <-	TransferData (wrapAround/blockSequence, Data)	Poslední blok dat typu overview.
TransferData (wrapAround/blockSequence = 0x00/0x01, další typ dat)	-> <-	TransferData (wrapAround/blockSequence = 0x00/0x01, Data)	Další požadovaný typ dat.
TransferData (wrapAround/blockSequence = 0x00/0x02, další typ dat)	-> <-	TransferData (wrapAround/blockSequence = 0x00/0x02, Data)	
Posílání TransferData dokud přenos dat nebude dokončeno.			
TransferData (wrapAround/blockSequence, typ dat overview)	-> <-	TransferData (wrapAround/blockSequence, Data)	Poslední blok dat