

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA STROJNÍHO INŽENÝRSTVÍ

ÚSTAV AUTOMATIZACE A INFORMATIKY

FACULTY OF MECHANICAL ENGINEERING

INSTITUTE OF AUTOMATION AND COMPUTER SCIENCE

PŘÍSTUPOVÝ BEZPEČNOSTNÍ SYSTÉM MOBILNÍHO ZAŘÍZENÍ NA PRINCIPU
RFID

TITLE

ACCESS SECURITY SYSTÉM OF MOBILE DAVICE ON RFID PRINCIPLE

DIPLOMOVÁ PRÁCE

THESES THESIS

AUTOR PRÁCE

AUTHOR

BC. MAREK PETRUŠEK

VEDOUcí PRÁCE

SUPERVISOR

ING. DANIEL ZUTH, PH.D.

BRNO 2013

Abstrakt

Tato diplomová práce se zabývá, model bezpečnostního přístupu s využitím mikrokontroléru a RFID čtečky. Model je navržen pro využití v automobilu, kde bude mít vlastnosti imobilizéru a také ukládání času a ID použitého čipu. Pro použití v automobilu je řešena minimalizace spotřeby mobilního zařízení. Práce je součástí řešení projektu IGA VUT Brno, FSI-S-11-31, APLIKACE METOD UMĚLÉ INTELIGENCE.

Abstract

This thesis discusses the model of security access with the use of microcontroller and RFID reader. The model is designed for utilization in automobiles, in which it will have the properties of an immobilizer and also the function of saving the time and ID of the chip in use. For application in automobiles the minimalization of consumption of the mobile device is also described. This thesis is a part of project IGA VUT Brno, FSI-S-11-31, Application of artificial intelligence methods.

Klíčová slova

Atmel, RFID čtečka, imobilizér, ATmega128L, mikrokontrolér,

Keywords

Atmel, RFID modul, immobilizer, ATmega128L, microcontroller,

PROHLÁŠENÍ O ORIGINALITĚ

Prohlašuji, že jsem diplomovou práci vypracoval samostatně dle pokynů vedoucího diplomové práce Ing. Daniela Zutha Ph.D. a s použitím uvedené literatury.

BIBLIOGRAFICKÁ CITACE

PETRUŠEK, M. *Přístupový bezpečnostní systém mobilního zařízení na principu RFID*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2013. 65 s. Vedoucí diplomové práce Ing. Daniel Zuth, Ph.D..

PODĚKOVÁNÍ

Za odbornou pomoc při řešení problémů, získání cenných informací a zkušeností děkuji vedoucímu diplomové práce Ing. Danielu Zuthovi Ph.D.

Obsah:

1.	ÚVOD	9
1.1.	Cíl práce	9
2.	ZABEZPEČENÍ MOBILNÍCH ZAŘÍZENÍ [1]	10
2.1.	Všeobecně o zabezpečení motorových vozidel [1]	10
2.2.	Princip zabezpečení [1]	10
2.2.1.	Mechanické zábranné prostředky [1]	10
2.2.2.	Elektronické zábranné prostředky [1]	10
2.2.3.	Vyhledávací systémy [1]	12
2.2.4.	Identifikační systémy [1]	12
3.	SYSTÉM RFID [2]	13
3.1.	Princip RFID [2]	13
3.2.	Zabezpečení dat [2]	14
4.	PROCESORY ATMEGA	15
4.1.	Procesory obecně [3]	15
4.2.	Vlastnosti [3]	15
4.3.	Využití procesorů [3]	17
5.	UKLÁDÁNÍ DAT [5]	19
5.1.	Historie programovatelných obvodů [5]	19
5.2.	EPROM, EEPROM, FLASH [5]	19
5.3.	Ukládání přijatých dat na FLASH paměť [5]	20
5.4.	Napájení [5]	21

6.	RTC SPECIALIZOVANÉ OBVODY [6].....	22
7.	FUNKČNÍ MODEL V KITU A SOFTWARE.....	23
7.1.	Vývojový kit EvB 4.3 v4 obecně [7]	23
7.2.	Popis vývojového kitu a jeho periférií [7]	24
7.3.	Funkční model kitu EvB 4.3 v4 a RFID modul EM – 18	26
7.4.	Použitý Software.....	28
7.4.1.	AVR studio 4.....	28
7.5.	Vytvořený Software	29
7.5.1.	Úvodní stav.....	29
7.5.2.	Kontrola a přístup do systému Master a Slave	30
7.5.3.	Ukládání na EEPROM.....	31
7.5.4.	Změna oprávnění přístupu Mastra	33
7.5.5.	Přístup do paměti EEPROM.....	35
7.5.6.	Nastavení data a času a RTC obvod	36
7.5.7.	Vymazání paměti EEPROM.....	37
8.	ŘEŠENÍ STUDIE	40
8.1.	Navržení komponentů pro montáž do vozidla	40
8.2.	Blokové schéma a popis navrženého obvodu	40
8.3.	Ovládané části automobilu.....	41
8.3.1.	Imobilizér [9].....	41
8.3.2.	Zapalování motoru [10].....	42
8.3.3.	Odemykání a zamykání auta [12].....	46
8.4.	Pořizovací náklady.....	48
8.5.	Ovládání jednotky pro účely firem	48
8.5.1.	Řízená kontrola užívání vozidel	48
8.5.2.	Řízené garanční prohlídky.....	50

8.6.	Spotřeba zařízení.....	50
8.6.1.	Jak ovlivnit spotřebu zařízení [6]	50
8.6.2.	Parametry a spotřeba RFID čtečky EM-18 [8]	51
8.7.	Zápis mikrokontroléru ATmega128L na SD kartu.....	52
8.7.1.	Propojení mikrokontroléru a SD karty pomocí SPI [14]	52
8.7.2.	Komunikace pomocí SD protokolu [14].....	53
8.7.3.	Ochrana dat při přenosu po sběrnici	54
8.7.4.	Rozdělení paměťových částí [14].....	54
8.7.5.	Čtení dat [14]	55
8.7.6.	Zápis dat [14].....	56
8.7.7.	Komunikace mezi SD a mikrokontrolerem ATmega128L [14].....	56
8.8.	Bezdrátový přenos dat z modulu mobilního zařízení.....	57
8.9.	GPS moduly	57
8.9.1.	Navržený GPS modul [15].....	58
8.9.2.	Spotřeba a technické parametry GPS modul M10264 [15]	58
9.	PŘÍSTUP K SYSTÉMU	60
9.1.	Přiložení karty	60
9.1.1.	Načtení data, času a GPS polohy	60
9.1.2.	Kontrola k oprávnění služební cesty.....	60
9.1.3.	Aktivace knihy jízd.....	60
10.	ZÁVĚR.....	61
11.	POUŽITÁ LITERATURA A ZDROJE	62
12.	SEZNAM POUŽITÝCH OBRÁZKŮ.....	64
13.	SEZNAM POUŽITÝCH TABULEK.....	65

1. ÚVOD

1.1. Cíl práce

V současnosti je už velice běžná identifikaci osob, nejrůznějších předmětů, zboží, nebo zvířat. Cílem této práce je seznámit se s implementováním přístupového bezpečnostního systému mobilního zařízení na principu RFID.

V devadesátých letech nastali podmínky pro využití RFID v mezinárodním měřítku. Nové technologie přišly s vývojem bezdrátových sítí. V počáteční fázi šlo o jednoduché aplikace v oblasti bezpečnosti. RFID technologie se využívá také v oblasti sportu, kde se používá nejen pro uživatele lyžařských vleků, ale i pro měření času závodníků podle čipu upevněného na jejich výstroji, ale hlavně jako bezdotykové čipové karty na kontrolu vstupu do objektů.

Tato práce se, ale zabývá přístupovým bezpečnostním systémem mobilního zařízení na principu RFID s implementací do automobilů. RFID nabízí vyšší rychlost snímání a podstatně jednoduší je aplikace v automatizovaných systémech jako při využití čárových kódů na identifikaci. Začátek komerčního využití RFID je přibližně od druhé poloviny 90. let a začátek 21. Století přináší standardy a rozvoje čipů. Technologie RFID je známá už několik desítek let. Toto miniaturní zařízení bez potřeby vlastního napájení je schopné v blízkosti snímacího zařízení poskytnout údaje, které uchovává. V této diplomové práci bylo cílem ukázat přístupový bezpečnostní systém na principu RFID.

2. ZABEZPEČENÍ MOBILNÍCH ZAŘÍZENÍ [1]

2.1. Všeobecně o zabezpečení motorových vozidel [1]

Zabezpečení motorových vozidel představují technické systémy, které chrání motorová vozidla zejména proti krádeži, případně i proti jiným poškozením.

Mezi tyto prostředky patří například:

- Mechanické zámky dveří vozidel
- Centrálního zamykání, které zahrnuje řídicí jednotku a dveřní ovladače
- Imobilizér
- Poplašné zařízení s detektory otevření dveří, otřesů a náklonů
- Družicový systém (GPS zabezpečení vozidel), které umožňuje sledovat polohu odcizeného vozidla

2.2. Princip zabezpečení [1]

Zabezpečení vozidel se zabývají všechny světoznámé značky výrobců automobilů, ať už se jedná o mechanické zabezpečení, elektronické zábranné prostředky, vyhledávací systémy a identifikační systémy. Zabezpečení vozidel jednotlivých stupňů ochrany je nedílnou součástí každého automobilu.

2.2.1. Mechanické zábranné prostředky [1]

Základním stupněm ochrany vozidla je instalace mechanických zábranných prostředků, které mají za úkol především výrazně prodloužit dobu nutnou k odcizení vozidla a tím toto znemožnit. Pro řidiče je jejich obsluha jednoduchá a rychlá. Nejúčinnější z této skupiny je mechanické uzamykání systému řazení vozidla. Skutečně účinnou ochranu vozu zajišťují pouze zařízení pevně spojená s karoserií vozu, případně kombinující současné blokování řazení a blokování otevírání kapoty motoru.

2.2.2. Elektronické zábranné prostředky [1]

Další možností zabezpečení a ochrany vozidla je instalace imobilizérů a autoalarmů. Imobilizér je zařízení, které blokuje možnost neoprávněného nastartování vozidla. Elektronické autoarmy jsou aktivním zabezpečovacím zařízením a slouží ke střežení narušení vozu nebo manipulaci s ním. V případě napadení vozidla odrazují

zloděje pomocí sirény a upozorní okolí vozu na narušení. Kromě signalizace sirény může být použit i přenos poplachové informace na mobilní telefon uživatele vozu.

Autoalarmy jsou vhodným doplňkem pro kombinaci s např. mechanickým zabezpečením, jelikož aktivně upozorňují okolí vozu na neoprávněnou manipulaci. Na rozdíl od imobilizérů jsou aktivním zabezpečovacím zařízením. Autoalarm se skládá z těchto dílů:

Řídící jednotka - slouží k vyhodnocení signálů z jednotlivých detektorů a v případě, že signál vyhodnotí jako poplachový, dochází k akustickému a optickému poplachu. Může být vybavena i komunikátorem pro vzdálený přenos informací.

Detektory - slouží k snímání podnětů, které by mohly být vyhodnoceny jako napadení vozidla. Mohou doplnit základní funkce střežení vniknutí do vozidla dveřmi, kapotou, kufrem o např. střežení vnitřního prostoru nebo manipulaci s vozidlem i pokus o krádež kol.

Siréna - slouží k akustické signalizaci v případě poplachu. Upozorní okolí vozu na neoprávněnou manipulaci a odrazuje zloděje od „práce“, při které je na něj upozorňováno.

Kvalitní autoalarmy mají zpravidla integrovaný imobilizér. Autoalarmy pro základní zabezpečení zajišťují lokální signalizaci. Autoalarmy vyšších kategorií obsahují komunikátory pro přenos poplachové zprávy k uživateli. Nejčastěji se k tomuto využívá komunikace na mobilní telefon, který je běžnou součástí našeho života. Výhodou telefonu je i zpětná komunikace s vozidlem například pro ověření stavu uzamčení vozidla nebo blokování vozidla proti zneužití. Kvalitní autoalarmy s GSM komunikací jsou vybaveny GPS přijímačem pro přesné určení polohy vozidla. To lze využít samozřejmě při poplachu, ale také při kontrole zaměstnanců, kde se právě nachází.

Imobilizér je zařízení, které pasivním způsobem blokuje možnost neoprávněného nastartování vozidla. Imobilizér, podle typu, přerušuje důležité elektrické a palivové obvody vozu. V zemích Evropské unie jsou imobilizéry povinnou výbavou u nově vyráběných vozů. Každopádně rozšíření sériového a doplňkového imobilizéru v kombinaci s autoalarmem je výrazným zvýšením ochrany vozidla.

2.2.3. Vyhledávací systémy [1]

Zde se jedná již o tzv. pokrádežové systémy zaručující zvýšení objasňenosti krádeží, případné zadržení pachatele a hlavně nalezení odcizeného vozidla. Jedná se o vyhledávací, monitorovací a lokalizační systémy odcizených vozidel. Tyto systémy umožňují v okamžiku spáchání útoku na vozidlo přenos informace v reálném čase případně určení směru pohybu a konkrétního místa, kde se vozidlo pohybuje nebo stojí. Tím vytvářejí dobré výchozí podmínky pro rychlé zadržení pachatele a zajištění vozidla.

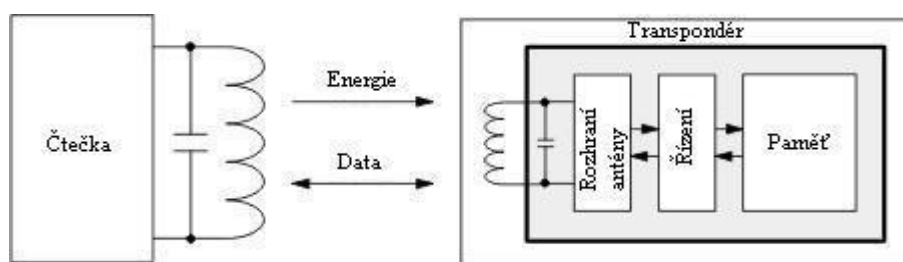
2.2.4. Identifikační systémy [1]

Jedná se o neodstranitelné označování vozidel speciálními prostředky, které buď viditelně, nebo skrytě označují vozidlo nebo části automobilu a tím znemožňují změnu identity vozidla a jeho další prodej. Mezi identifikační systémy patří například neodstranitelné značení skel (tzv. pískování), u kterého se na skla automobilu vyznačí VIN kód vozidla nebo speciální alfanumerický kód. Dalším identifikačním systémem jsou unikátní mikrotečky, kterými se značí nosné díly karoserie vozidla. Tyto systémy patří mezi vysoce účinné a zároveň finančně nenáročné prostředky, které chrání vozidlo před odcizením.

3. SYSTÉM RFID [2]

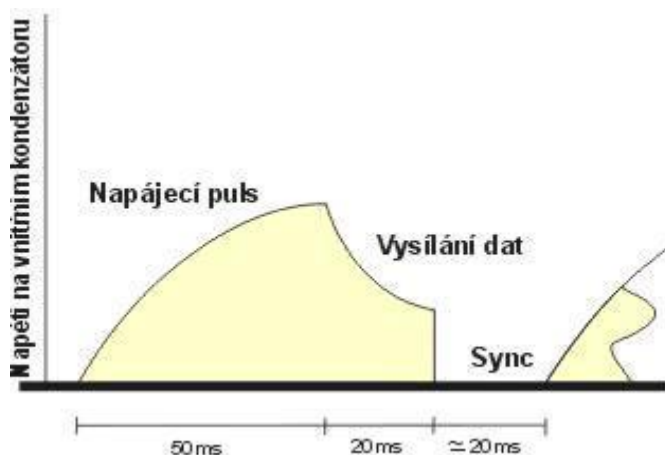
3.1.Princip RFID [2]

Systém RFID se skládá z antény, vysílače s dekodérem a transponderem pro označení sledovaného předmětu nebo osoby. Princip činnosti RFID spočítá v tom, že čtečka periodicky vysílá pulzy prostřednictvím antény do okolí. Objeví-li se v dosahu antény transponder (TAG), přes jeho vlastní anténu přijme signál a ten využije k nabití svého kondenzátoru energií, která je dostatečná k jeho aktivaci a následné odpovědi zpět snímači. Ten signál od transponderu přijme a po jeho vyhodnocení jej předá k dalšímu zpracování. Data mohou být předána ihned počítači ke zpracování, nebo mohou být uložena v paměti přenosných čteček a později nahraná do počítače.



Obr. 1 Blokové schéma RFID (převzato z [2]).

Čtečka vysílá napájecí impuls o délce asi 50ms - obr. 2. Impuls je přijat anténou transponderu, která je naladěna na stejnou frekvenci. Tato přijatá energie je usměrněna a vzniklým napětím je nabit interní kondenzátor. Po ukončení vysílaného pulsu transpondér okamžitě vyšle zpět svá data. K napájení transponderu během jeho vysílání slouží právě toto napětí nastřádané na vnitřním



Obr. 2 Princip přenosu dat (převzato z [2]).

Délka přenášených dat je 128 bitů včetně zabezpečovacího kódu a přenos trvá přibližně 20 ms. Tato data jsou zachycena anténou přijímače (čtečky) a dekodována. Poté je nabíjecí kondenzátor transpondéru vybit a očekává se další nabití a čtení. Perioda mezi dvěma cykly je mezi 20 ms až 50 ms a je závislá na nastavení systému – obrázek 2.

3.2. Zabezpečení dat [2]

K zabezpečení přenosu dat užívá systém TIRIS 16 bitový CRC algoritmus (CRC-CCITT), který zajišťuje, že budou přenášena jen platná data. V případech, že intenzita elektromagnetického pole není dost silná ke spolehlivému přenosu dat, čtečka odpovídá řídicímu počítači příznaky NO READ nebo INVALID.

4. PROCESORY ATMEGA

4.1. Procesory obecně [3]

Zakladateli této technologie jsou dva studenti z Norského technického institutu - Alf-Egil Bogen a Vegard Wollan. Podle jejich jmen vznikla právě zkratka AVR, oficiálně ale znamená Advanced Virtual RISC.

AVR procesory jsou RISC procesory postavené na Harvardské architektuře (mají oddělenou paměť pro program a data). Skládají se z třiceti dvou stejných 8bitových registrů, které mohou obsahovat jak data, tak i adresy. Jsou přímo propojeny s aritmeticko-logickou jednotkou, proto je ALU schopna provést jednu operaci v jednom hodinovém cyklu. Posledních 6 registrů je možno také po párech využít jako ukazatele pro nepřímé adresování do paměti.

4.2. Vlastnosti [3]

Hlavní vlastností RISC procesorů:

- redukováná sada instrukcí
- obsahuje převážně jednoduché instrukce
- délka provádění jedné instrukce je vždy jeden cyklus
- délka (počet bitů) všech instrukcí je stejná
- mikroinstrukce jsou hardwarově implementovány na procesoru
- využívá se zde techniky řetězení instrukcí

Většina instrukcí z instrukčního souboru je jednoslovných (16 bitových), pouze 4 instrukce jsou dvouslovné (32 bitové). To umožňuje rychlejší vykonávání instrukcí a také dovoluje jednodušší strukturu mikroprocesorového řadiče. Většina instrukcí umožňuje přímý jedno-cyklový přístup do všech registrů.

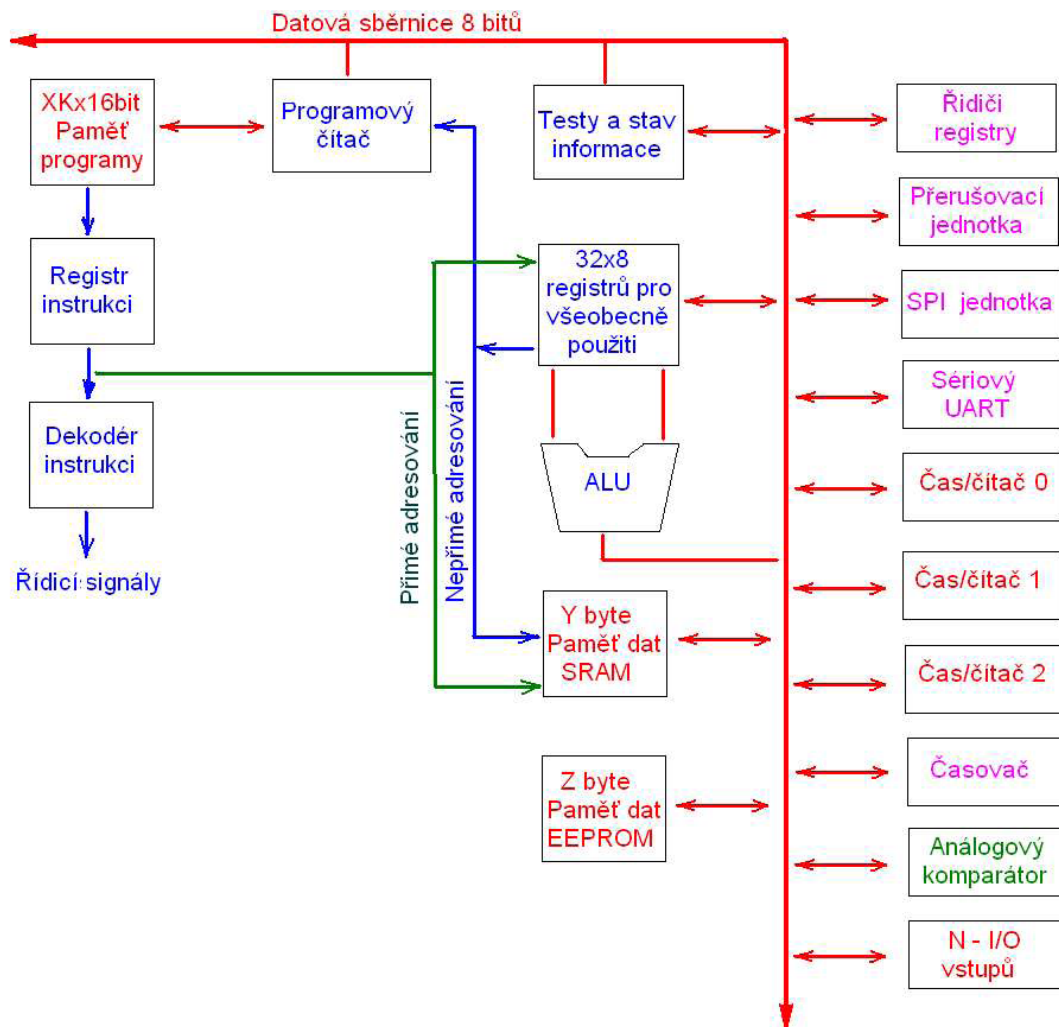
Zpracování operandů probíhá následovně: Oba operandy se během taktu převedou z pracovních registrů, uskuteční se operace a výsledek se uloží do registru. Vždy se jedná o operace registr-registr, na kterých je AVR technologie založena.

Toto má ale i několik záporů. Pouze některé instrukce umožňují pracovat s přímými datovými typy a to pouze s omezeným počtem registrů. Ostatní instrukce

mohou pracovat pouze s registry. Výkon těchto mikropočítačů se blíží k 1 miliónu instrukcí za sekundu na 1 MHz, což je způsobeno vykonáváním jedné instrukce v jednom hodinovém cyklu.

Architektura AVR obrázek 7, umožňuje 5 adresovacích módů:

- přímé adresování
- nepřímé adresování s 6ti-bitovým posunem
- nepřímé adresování
- nepřímé adresování s dekrementací ukazatele před zpracováním instrukce
- nepřímé adresování s dekrementací ukazatele po zpracování instrukce



Obr. 3 Základní architektura mikroprocesorů AVR (převzato z [4]).

4.3. Využití procesorů [3]

AVR se využívá v různých bezpečnostních, ochranných a zábavních systémech. Atmel vydal publikaci „Atmel Automotive Compilation“, aby pomohl vývojářům při vývoji těchto aplikací. Využívají je firmy jako BMW, Daimler-chrysler nebo TRW.

Vývojový kit Arduino, který se stává stále oblíbenějším, je založen na mikrokontroléru ATmega328 (u starších verzí je to ATmega 168 nebo ATmega 8). Na rozvoji Arduino Mega platformě se také podílel čip ATmega 1280, který má na rozdíl od svých předchůdců více pinů a větší paměť. Desky Arduino se programují pomocí jejich vlastního jazyka nebo s pomocí více konvenčních programovacích prostředí jako C, Asembler, jak je obvyklé na AVR platformách.

AVR založené na USB jsou využívány např. v Microsoft Xbox řadiči, kde se USB rozhraní používá pro propojení XBoxu a řadiče.

Několik společností vyrábí mikrokontroléry založené na AVR pro konstruktéry robotů, vývojáře drobných experimentálních systémů jako Cubloc, BasicX, Oak Micros nebo ZX Microkontrollers.

Pro vývoj motoru M3000 a Motion Control Chip využila firma Systém Semikonduktor, Inc. jádro Atmel AVR a Advanced Motion Controller pro užití v mnoha pohybových aplikacích.

V roce 2006 Atmel vydal mikrokontroléry založené na nové, 32ti-bitové, AVR32 architektuře. Ty obsahují SIMD instrukce, DSP instrukce a další funkce pro zpracovávání zvuku a videa. Tato 32ti-bitová rodina procesorů je určena ke konkurování procesorům založených na ARM. Instrukční sada je podobná jiným RISC jádrům, ale není kompatibilní s originální AVR ani s žádným z mnoha ARM jader.

5. UKLÁDÁNÍ DAT [5]

5.1. Historie programovatelných obvodů [5]

První integrovaný obvod zkonstruoval Jack St. Clair Kilby z firmy Texas Instruments již v roce 1958. Kilbyho integrovaný obvod byl na základní desce z germania o velikosti $11 \times 1,6$ mm a obsahoval jediný tranzistor s několika pasivními součástkami.

Tento vynález si nechal patentovat v roce 1964. V témže roce si také připsal konstrukci první kapesní kalkulačky založené na integrovaném obvodu zpracovávající jednoduché matematické operace.

V roce 2000 byl oceněn Nobelovu cenu za fyziku. První integrovaný obvod zkonstruoval Jack St. Clair Kilby z firmy Texas Instruments již v roce 1958. Kilbyho integrovaný obvod byl na základní desce z germania o velikosti $11 \times 1,6$ mm a obsahoval jediný tranzistor s několika pasivními součástkami. Tento vynález si nechal patentovat v roce 1964.

V témže roce si také připsal konstrukci první kapesní kalkulačky založené na integrovaném obvodu zpracovávající jednoduché matematické operace. V roce 2000 byl oceněn Nobelovu cenu za fyziku.

5.2. EPROM, EEPROM, FLASH [5]

EPROM (Erasable Programmable Read-Only Memory). Jedná se o paměť typu ROMRAM, jejíž obsah je mazatelný ultrafialovým zářením. Pokud chceme paměť nově programovat je nutné paměť nejdříve kompletně smazat. K programování se používá většinou několikanásobně vyšší napětí než ke čtení (typ. 12 V nebo 25 V proti 5 V napájecího napětí). Paměť se používá k uložení dat (např. firmware), často u malosériové výroby, kde není vyžadována možnost měnit obsah paměti v již zabudovaném zařízení.

EEPROM (Electrically Erasable Programmable Read-Only Memory). Jedná se o elektricky mazatelnou paměť typu ROM-RAM. Paměť má umožňuje menší počet zápisů než paměť typu flash. Před novým naprogramováním musíme pomocí elektrického signálu smazat celý její obsah. (Výhoda oproti EPROM, pro smazání bylo

nutné použití ultrafialového světla) Využití této paměti je jako úložiště (např. firmware) u zařízení, kde nedochází často k přepisům paměti. Nyní se již od použití této paměti upouští a využívá se paměti typu flash.

FLASH je nevolatilní elektricky programovatelná paměť s libovolným přístupem. Vnitřní organizace paměti je v blocích na rozdíl od pamětí typu EEPROM, lze programovat každý blok samostatně (nedochází k přepisu ostatních bloků).

Paměť se používá jako paměť typu ROM např. pro uložení firmware (např. ve vestavěných zařízeních). Výhodou této paměti je, že ji lze znovu naprogramovat (např. přeprogramování novější verzí firmware) bez vyjmutí ze zařízení s použitím minima pomocných obvodů. Flash paměť se používá jako výměnné datové médium ve formě paměťových karet. Flash paměť se používá i v discích Solid State SSD jako vestavěná paměť, kde ji označujeme jako paměťové technologické zařízení Memory Technology Device.

5.3.Ukládání přijatých dat na FLASH paměť [5]

Data jsou ukládána v poli tranzistorů (plovoucí brány), zvaných „buňky“, každá z nich obvykle uchovává 1 bit informace. Jedna brána je kontrolní brána (CG-control gate) druhá je plovoucí brána (FG-floating gate) navzájem izolované vrstvou oxidu.

Protože je FG izolovaný jeho izolační vrstvou oxidu, každé elektrony na něj přivedené jsou „uvězněny“ a tím pádem je uložena informace. Když jsou na FG nějaké elektrony, tak modifikují (částečně ruší) elektrické pole přicházející z CG, což modifikuje prahové napětí (V_t) buňky.

Buňka je čtená umístěním specifického elektrického napětí na CG, elektrický proud pak buď teče, nebo neteče, a to v závislosti na V_t buňky, které je závislé na počtu elektronů na FG. Tato přítomnost nebo nepřítomnost elektrického proudu je přeložena na 1 a 0, představující uložená data.

Flash buňka je naprogramovaná (nastavená na specifickou hodnotu) spuštěním toku elektronů ze zdroje do odvodu. Přivedení velkého napětí na CG pak poskytne dostatečně silné elektrické pole pro jejich vysátí na FG. Pro vymazání flash buňky je velký napěťový rozdíl přiveden mezi CG a zdroj, což odvede elektrony pryč skrz kvantový tunel. Současné flash paměti jsou rozdělené do vymazatelných částí

nazývaných buď bloky, nebo sektory. Všechny paměťové buňky v rámci jednoho bloku musí být vymazány současně.

5.4.Napájení [5]

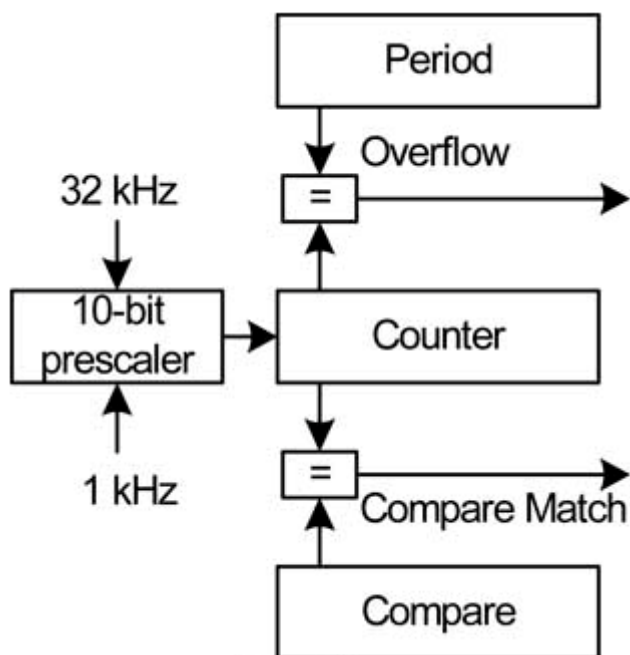
Data flash pamětí mají velikou výhodu, jelikož jsou uchovávána i bez přítomnosti napájecího napětí.

6. RTC SPECIALIZOVANÉ OBVODY [6]

Se stále častějším požadavkem aby aplikace běžela v „reálném“ čase se zvyšuje nutnost implementace vhodného obvodu zaručujícího generování „reálného“ času. Tento požadavek je možné splnit buď pomocí externího specializovaného obvodu RTC nebo pomocí interního obvodu. V případě představovaného mikrokontroléru je to ten druhý způsob, takže ve vnitřní struktuře najdeme úplně ten nejzákladnější hardware, který nám implementaci reálného času umožní. Blokové schéma je vidět na obr. 4.

Jedná se o 16ti-bitový čítač se dvěma jednotkami compare z nichž jedna je určena pro definování periody, druhá je klasická jednotka compare. Zdroji kmitočtu pro 16ti bitový čítač může být buď nízkopříkonový oscilátor s externím krystalem 32768Hz nebo kalibrovaný interní 32kHz RC oscilátor.

Vstupem může být též frekvence 1kHz odvozená od interního „ultra low power“ 32kHz RC oscilátoru. Pro dosažení delších intervalů přerušení generovaného tímto obvodem RTC lze vydělit jmenované kmitočty pomocí předděličky 2, 8, 16, 64, 256 či 1024. Při největším rozlišení, které je 30,5 μ s, je nejdelší perioda rovna 2sec. Při nejpomalejším časování je nejdelší perioda mezi přerušeními větší než 18hodin.



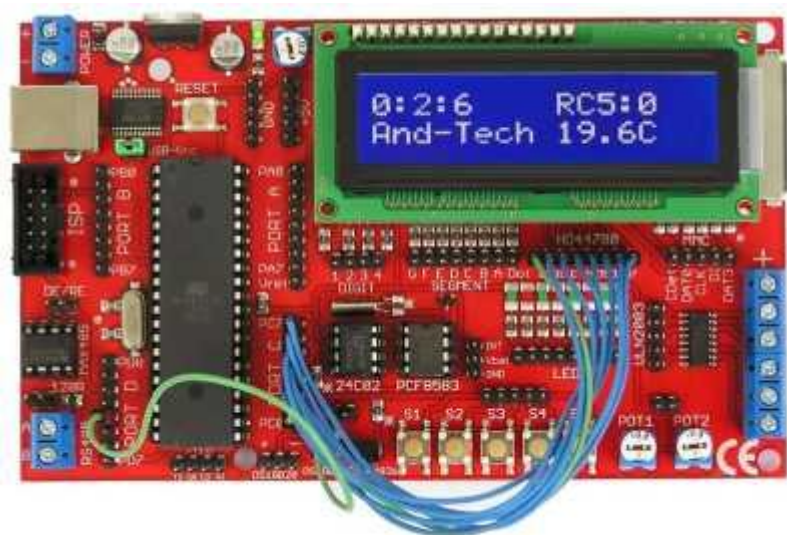
Obr. 4 Blokové schéma RTC odvodu (převzato z [6]).

7. FUNKČNÍ MODEL V KITU A SOFTWARE

7.1. Vývojový kit EvB 4.3 v4 obecně [7]

Konstrukce celého kitu umožňuje velice flexibilní zapojení a konstrukci na obr.5. Veškeré periferie jsou sice součástí desky, ale využívají většinou pouze napájecí větve spojů. Jejich vstupy nebo výstupy jsou vyvedeny na samostatné piny, stejně jako nevyužité brány mikroprocesoru, takže zůstává zcela na libovůli konstruktéra, kam periferie připojí.

Mikrokontrolér má pevně připojený pouze krystalový oscilátor 16MHz, tlačítko RESET a Pull-Up rezistory pro I2C sběrnici o velikosti 10k Ω a napájení. Ostatní volné porty jsou volně dostupné na propojovacích pinech. To umožňuje, že i LCD display si lze připojit takovým způsobem, na který je konstruktér zvyklý.



Obr. 5 Vývojový kit EvB 4.3 v4 (převzato z [7]).

Osazení kitu EvB 4.3 v 4:

- Procesor AVR ATmega32, krystal 16MHz
- Obvod reálného času PCF8583
- Paměť EEPROM AT24C02
- Infračervený přijímač TSOP4836
- Teplotní čidlo DS18B20
- Převodník sběrnic RS485/RS232 - SN75176BP
- Patice pro kartu MMC/SD
- 5 tlačítek
- 8 indikačních LED diod
- 2 potenciometry pro nastavení napětí
- 4 x sedmisegmentový LED zobrazovač
- 5 x výkonový výstup s otevřeným kolektorem ULN2003
- podsvětlený displej LCD 2x16 znaků (modrý)
- USB konektor
- ISP programovací konektor

7.2. Popis vývojového kitu a jeho periferií [7]

Vlastní jádro vývojového kitu tvoří mikrokontrolér ATmega 32, interní EEPROM a SRAM paměti. Mikrokontrolér je napevno taktován krystalem 16MHz, můžeme však využít interního RC oscilátoru 8MHz, popřípadě vestavěné děličky pro snížení tohoto hodinového kmitočtu. Mikrokontrolér je umístěn v patici DIL40, lze tedy volit z libovolných typů, splňujících umístění napájení, signálu reset a připojení krystalu.

Použití sběrnice I2C může být demonstrováno na dvou obvodech s tímto rozhraním – paměť AT24C02 a obvodu hodin RTC PCF8583. V části mikrokontroléru jsou k signálům SDA a SCL připojeny Pull-Up rezistory, není tedy nutno připojovat externí rezistory. Tyto signály jsou také připojeny „natvrdo“, není možné použít například simulaci I2C na libovolném pinu pro spojení s těmito obvody. Pro připojení

externích obvodů přes I2C použijeme piny SDA a SCL na portu C tak, jak je určil výrobce.

Pro měření teploty je použit známý senzor od Maxim - Dallas digitálním výstupem – DS18B20, který má svůj digitální výstup na společném konektoru s výstupem od přijímače infračerveného signálu TSOP4836, pracujícím na standardu IR vysílání 36 kHz. Lze však použít dálková ovládání pracující na 38 i 40kHz, výsledkem bude snížená citlivost přijímače, pro ověření funkce vysílače však postačí.

Pro interakci s okolím je kit vybaven pěti tlačítky a pěti výkonovými výstupy. Tlačítka se zapojují přímo na vstupy mikroprocesoru, neboť v režimu „input“ mají zapojeny Pull-Up rezistory a tlačítko tak lze připojit mezi vstupní pin a zem. Proto jsou všechna tlačítka automaticky spojena se zemí. Výkonové výstupy jsou realizovány přes šroubovací svorkovnici obvodem ULN2003, u kterého se využívá pět kanálů. Šestá svorka je spojena přímo s kladnou napájecí svorkou, tedy ještě před stabilizátorem, je na ní plné napájecí napětí – slouží k připojení zátěží.

Pro zobrazení stavů můžeme využít tři typy optických indikátorů. Vždy je k dispozici osmice zeleno-červených samostatných LED připojených přes rezistory pevně k +5VDC, spínají se tedy vůči zemi, nebo LCD displej s možností řízení jasu vestavěným trimrem a řízením LED podsvětlení buď automaticky procesorem nebo přímým spojením pinu BL(1)s +5VDC. Použití LCD se předpokládá ve 4bitovém režimu. Poslední možností zobrazení údajů je sedmisegmentový displej se 4 pozicemi. Tento displej je poněkud složitější na ovládání, je třeba použít multiplex pro přepínání číslic – interface je vybaven spínacími tranzistory Q1, 3, 4 a 5, stačí tedy pouze správně propojit s mikroprocesorem.

Uchování údajů a naměřených hodnot můžeme na desce dvojím způsobem. Buď pomocí I2C paměti, nebo uložením na MMC/SD kartu, slot je umístěn pod LCD displejem. Odporové děliče zajišťují kompatibilitu s napěťovými úrovněmi signálů – karta využívá 3.3V logiku. Analogová část vývojové desky – dva potenciometry, mohou být připojeny k analogovým převodníkům.

Předposlední částí desky jsou obvody pro připojení vývojového kitu k dalším perifériím pomocí sběrnic, neboli obvody zajišťující komunikaci. Obsahuje rozhraní RS485, realizované budičem SN75176BP a USB rozhraní s notoricky známým čipem

FT232RL, který se chová jako virtuální sériový port na PC. Pomocí tohoto rozhraní lze jednak na PC využívat sériovou linku RS232 a při použití bootloaderu v mikroprocesoru ho také programovat pomocí speciálního software. Pro klasické využití RS232 rozhraní, je třeba se napojit přímo na piny PD0 a PD1 portu D. Pak je třeba použít externí převodník napěťových úrovní. Rozhraní RS485 je na desce vybaveno volitelným rezistorem 120Ω jako zakončení sběrnice a volitelně lze připojit k mikrokontroléru signál DE/RE pro řízení toku dat (port D, signál PD2).

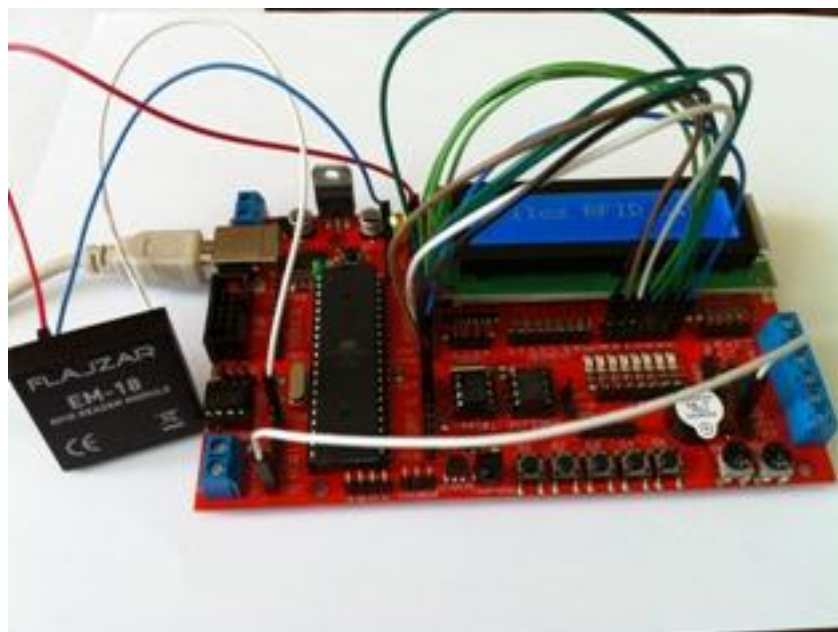
Celá deska je napájena napětím min. +9VDC, které se je stabilizováno obvodem 7805 na +5VDC. Hrubé napájecí napětí je přítomné pouze na svorkovnici pro výkonový výstup, na celé desce je použito napětí +5VDC, které je spolu s GND vyvedeno na speciální pomocné piny pro potřeby aplikace a kde jej může konstruktér využít dle libosti. Protože je vývojový kit většinou propojen s PC pomocí USB sběrnice, lze přepínačem (jumperem) USB-Vcc připojit za stabilizátor napětí +5VDC ze sběrnice USB a eliminovat tak použití externího napájecího zdroje. V tomto případě ale nemůžeme použít kladnou napájecí svorku na terminálu výkonových výstupů.

7.3.Funkční model kitu EvB 4.3 v4 a RFID modul EM – 18

Funkční model kitu obr. 6 byl navržen tak, aby byl demonstrován model bezpečnostního přístupového systému mobilního zařízení na principu RFID.

Z vývojového kitu byly využity tyto periferie:

- Procesor AVR ATmega32, krystal 16MHz
- podsvětlený displej LCD 2x16 znaků
- Paměť EEPROM AT24C02
- Obvod reálného času PCF8583
- USB port pro sériovou komunikaci



Obr. 6 Funkční model vývojového kitu.

Další periferie, které nebyly z nedostatku času využity, jsou patice pro kartu MMC/SD a patice pro záložní zdroj, kterou je baterie. Tato baterie nám může sloužit k uchování důležitých a velmi potřebných údajů data a času a také GPS polohy (není součástí kitu). Kit je napájen pomocí USB rozhraní, kde probíhá také sériová komunikace pro nahrání vytvořeného software. Bez potřebného napájení a záložního zdroje (baterie) dojde ke ztrátě tolik potřebných údajů jako je datum a čas a popřípadě GPS polohy.

K vývojovému kitu obr. 7 je pomocí jedno pinových kabelů připojen RFID modul EM -18 obr. 4. Pro ověření a přihlášení uživatele do systému slouží tagy. Pro funkční model používáme dva typy těchto tagů obr. 7 a to ve formě přístupové plastové karty a tagů ve formě přívěšků, aby byla demonstrována jednoduchost, velikost a také cenová dostupnost těchto důležitých periférií.

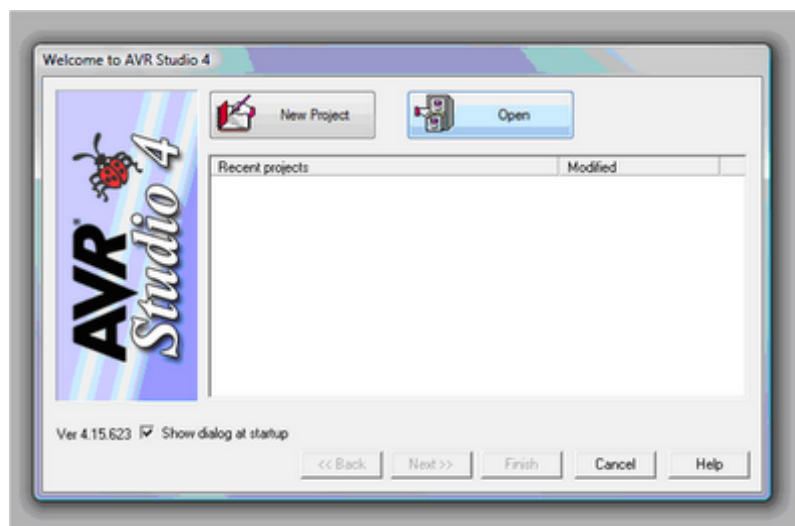


Obr. 7 Tagy a přístupová karta pro přihlášení do systému.

7.4. Použitý Software

7.4.1. AVR studio 4

Pro tuto práci bylo použito vývojové prostředí AVR studio 4 obrázek 8. Samotné vývojové prostředí je vyvinuto firmou Atmel pro programování mikroprocesorů, které sami vyrábí. Při programování v AVR studiu 4 máme na výběr, jestli využijeme pro psaní kódu jazyk C nebo assembler. Součástí vývojového prostředí je kompilátor, který nám kompiluje kód napsaný v jazyce C. AVR studio 4 a kompilátor nejsou nijak zpoplatněny a každý si je může stáhnout na internetových stránkách výrobce.



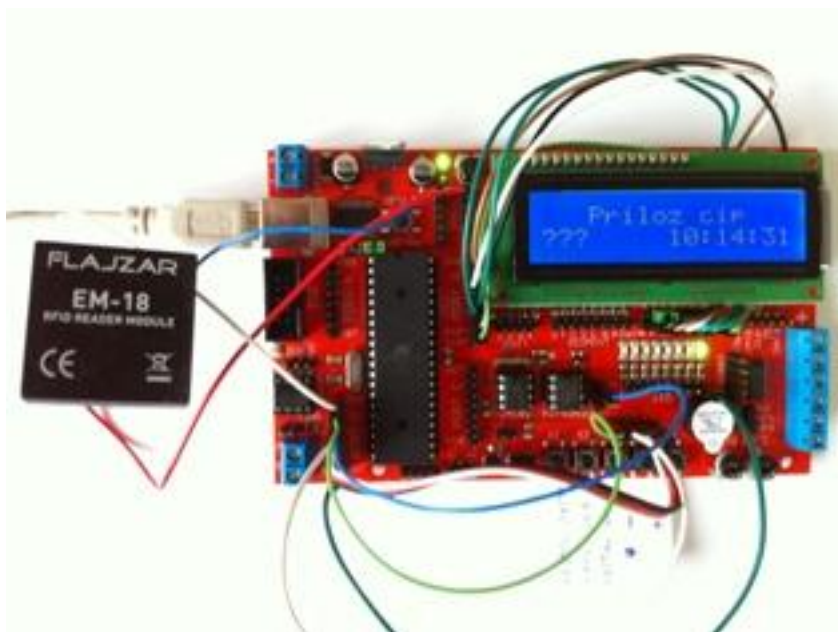
Obr. 8 AVR vývojové studio 4 (převzato z [13]).

7.5. Vytvořený Software

Vytvořený software na vývojovém kitu EvB 4.3 v4 demonstruje funkci bezpečnostního přístupového modelu mobilního zařízení na principu RFID. Jednotlivé části vytvořeného softwaru ukazují, jak se přistupuje do systému v jednoduchých částech programu s využitím pěti tlačítek.

7.5.1. Úvodní stav

Úvodní stav se zobrazí po připojení napájecího napětí pomocí USB kabelu, kde nás systém vyzve pomocí displeje k přiložení čipu a zároveň zobrazí aktuální čas. Na displeji jsou vidět tři otazníky, které znázorňují poslední přihlášení uživatele.

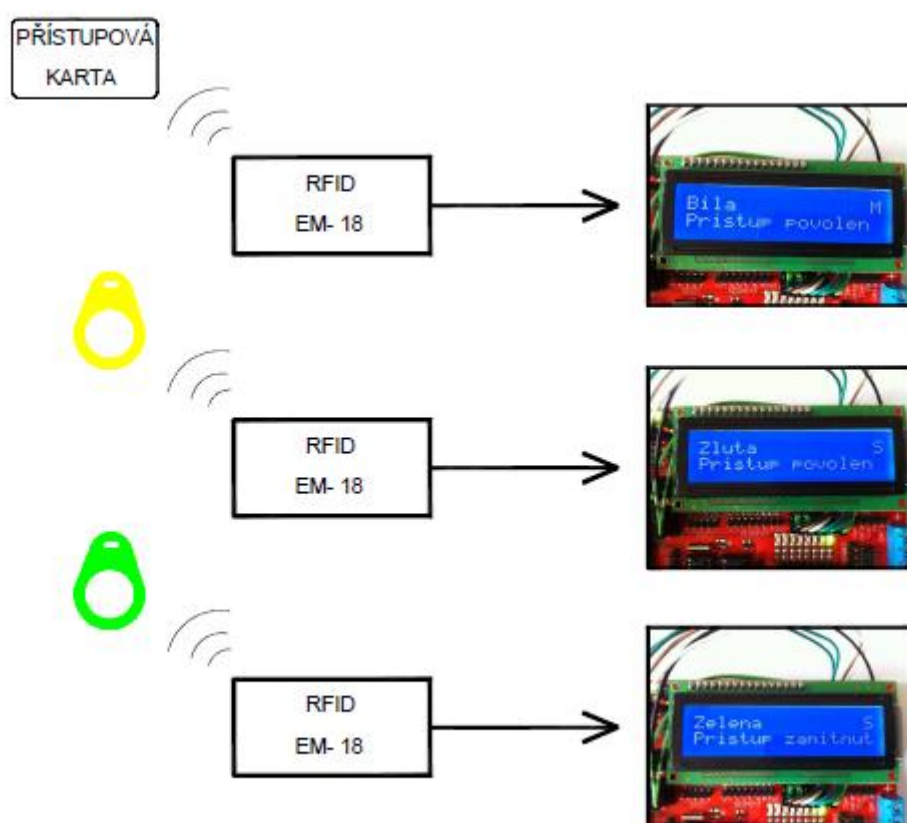


Obr. 9 Úvodní stav kitu EvB 4.3 v4.

7.5.2. Kontrola a přístup do systému Master a Slave

Pro přístup do systému je použita bílá přístupová karta (Master) a dva přívěškové tagy žlutý (slave) a zelený (slave) obrázek 7 (viz. kapitola 7.3). Přihlášením do systému nám ať už kartou nebo tagy nastanou tyto stavy.

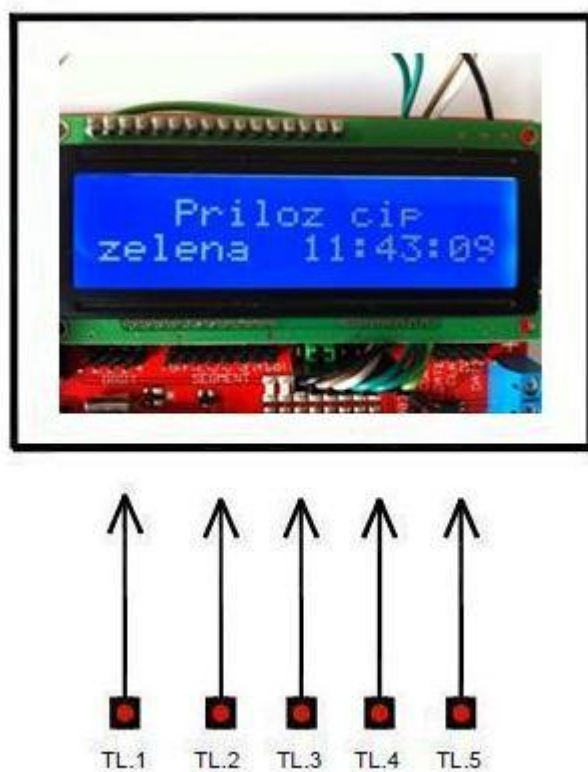
přístupové karty nebo tagy displej zobrazí barvu karty oprávnění uživatel (master, slave) a povolení nebo zamítnutí přístupu do systému a zazní zvukový signál doprovázen bliknutím diody. Pro uživatele s povolením přístupu je to dlouhý tón a bliknutí žluté diody. Pro uživatele s odmítnutím přístupem tři krátké tóny a rozsvítí se červená dioda. Jednotlivá přihlášení jsou znázorněny blokově na obrázku 10.



Obr. 10 Blokové schéma přihlášení uživatele Master a Slave.

7.5.3. Ukládání na EEPROM

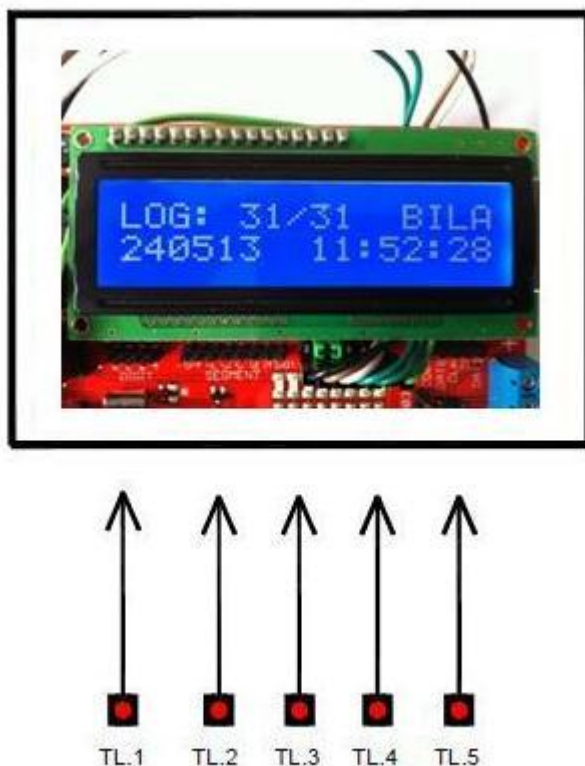
Všechna přihlášení do systému jsou ukládána na EEPROM. Poslední přihlášení uživatele je zobrazeno na displeji ve formě barvy přístupového média (bílá karta, žlutý a zelený tag) obrázek 11.



Obr. 11 Blokové schéma posledního načteného uživatele.

Na EEPROM se ukládají údaje, které si můžeme zobrazit na displeji kitu obrázek 12:

- Počtu přihlášení do systému
- Jaký uživatel byl přihlášen
- Aktuální datum
- Aktuální čas

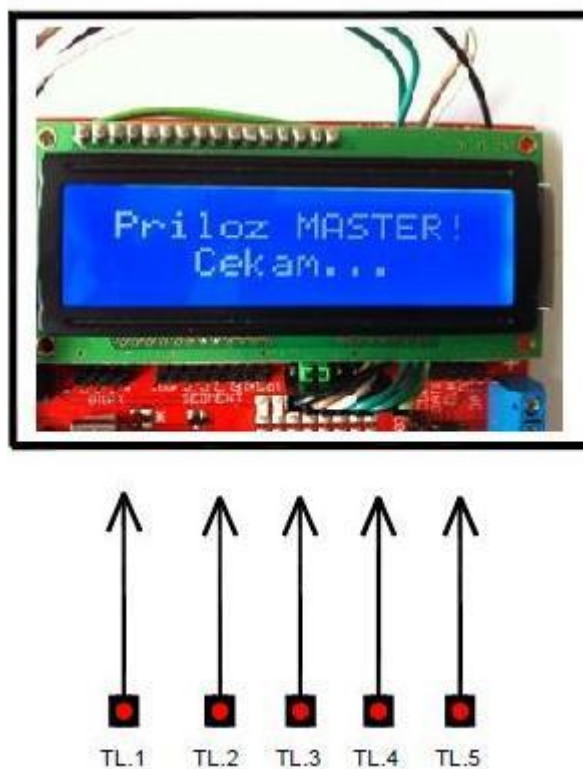


Obr. 12 Blokové schéma zobrazení údajů o LOGU uložené na EEPROM.

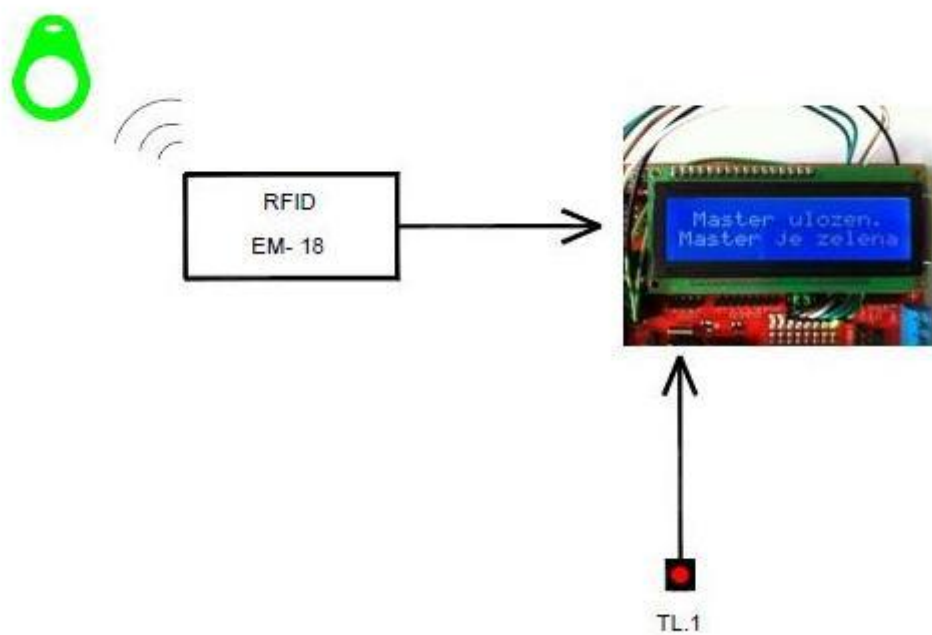
7.5.4. Změna oprávnění přístupu Mastra

Už mnohokrát se stalo, zaměstnanci ztratí nebo jim je přístupová karta (tag) ukradena a v neposledním případě příchod, odchod nového zaměstnance. Je proto software naprogramovaný tak, aby byla možnost kdykoliv změnit Mastra obrázek 13.

Pro změnu Mastra nejdříve zmáčkne tlačítko TL. 1 a přiložíme k RFID EM - 18 čteče novou kartu nebo tag obrázek. 14 a systém automaticky uloží nového Mastra.



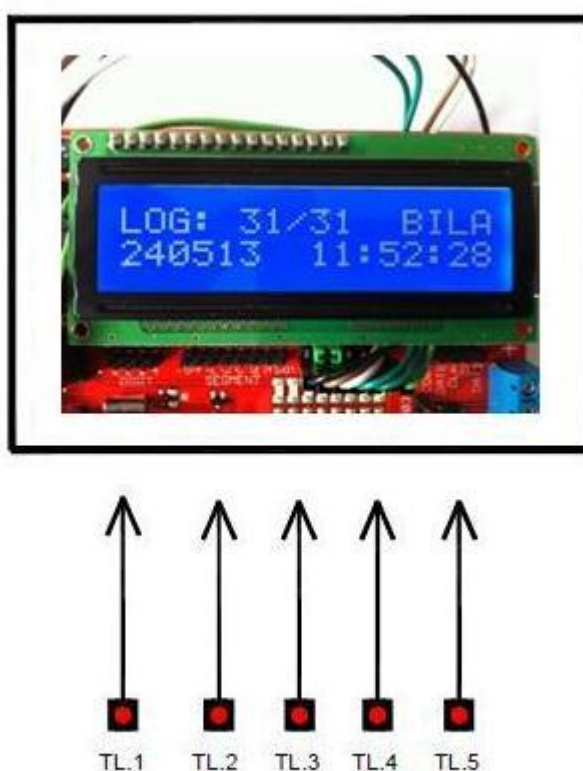
Obr. 13 Blokové schéma změny Mastera.



Obr. 14 Blokové schéma načtení a uložení nového Mastera.

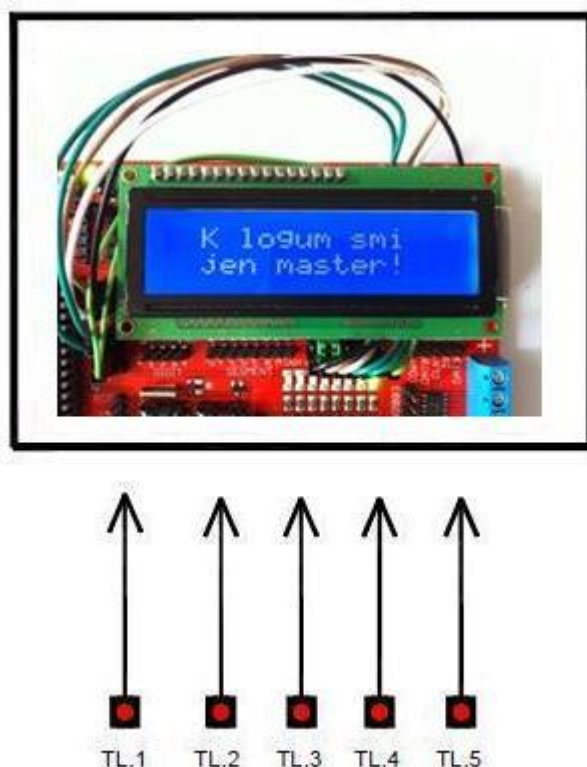
7.5.5. Přístup do paměti EEPROM

Do paměti EEPROM má přístup pouze uživatel s oprávněním Master. Pro přístup do paměti EEPROM se uživatel s oprávněním Master musí nejdříve přihlásit do systému (viz. kapitola 7.5.2.) a následně stlačit tlačítko TL.2. Na displeji se mu zobrazí, LOG: počet přístupů, uživatel, datum a čas přihlášení obrázek 15. Pro pohyb v menu paměti EEPROM slouží tlačítka TL.4 a TL.5.



Obr. 15 Blokové schéma pro menu EEPROM.

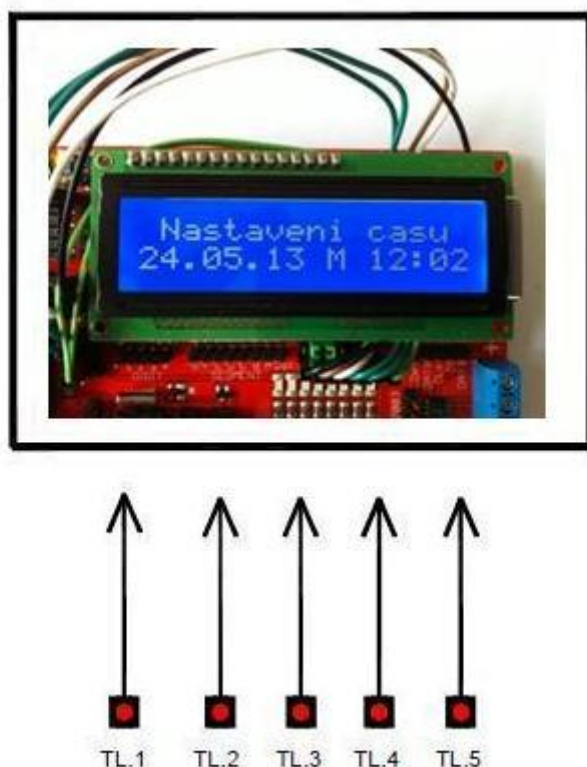
Pokud uživatel nemá oprávnění Master a i přesto se chce dostat do menu pomocí tlačítka TL.2 na EEPROM, vytvořený software odepře uživateli přístup obrázek 16.



Obr. 16 Blokové schéma odepření přístupu.

7.5.6. Nastavení data a času a RTC obvod

Pro nastavení data a času použijme tlačítka na kitu EvB 4.3 v4. Pro vstup na do na stavení použijme tlačítko TL.3. Nastavit můžeme, den, měsíc, rok, hodiny, minuty a vteřiny. Jednotlivé periferie navolíme pomocí tlačítek TL.2 a TL.3 a tlačítka TL.4 a TL.5 navolíme požadovanou hodnotu nastavení obrázek 17.

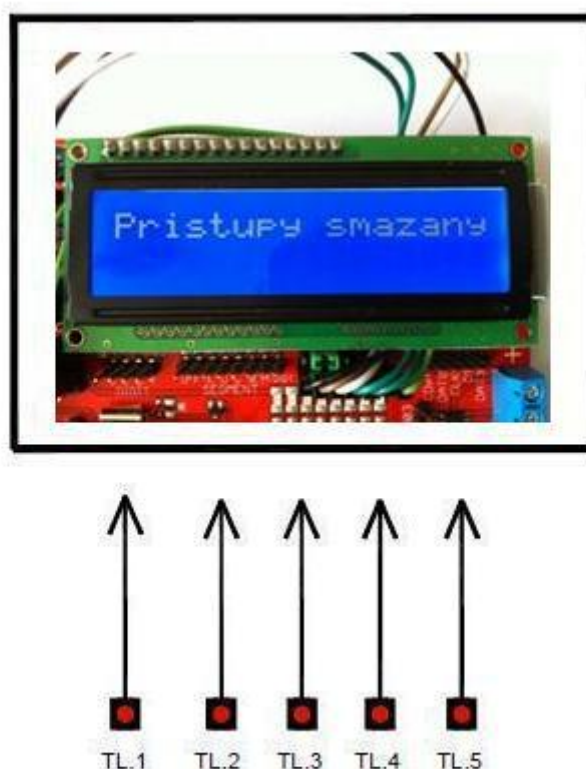


Obr. 17 Blokové schéma nastavení data a času.

O aktuální čas ve vytvořeném softwaru zajišťuje RTC obvodu PCF8583 (viz. kapitola 6). Tento obvod je napájen vlastní externí baterií CR 1616. Proto po odpojení napájení nedojde ke ztrátě aktuálního času a spotřeba zařízení je téměř nulová.

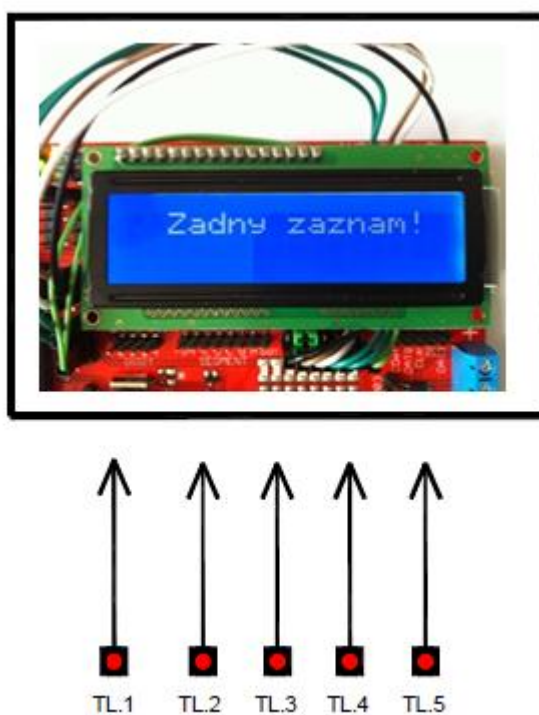
7.5.7. Vymazání paměti EEPROM

Kvůli možnému střídání zaměstnanců vytvořený software umožňuje vymazání záznamů všech dosud uložených uživatelů. Pro vymazání paměti EEPROM zmáčkne současně tlačítka TL.4 a TL.5 a provede se vymazání všech uložených záznamů obrázek 18.



Obr. 18 Blokové schéma vymazání paměti EEPROM.

Pokud by chtěl majitel vozového parku kontrolu, že je paměť EEPROM zcela smazána a posledním přihlášeným uživatel je Master zmáčkne tlačítko TL.2. Displej nám zobrazí hlášku „přístupy smazány“ obrázek 19.



Obr. 19 Blokové schéma obrázku pro kontrolu smazání EEPROM.

8. ŘEŠENÍ STUDIE

8.1. Navržení komponentů pro montáž do vozidla

Pro přístupový bezpečnostní systém mobilního zařízení na principu RFID do automobilů navrhují komponenty, které jsou vhodné pro použití do automobilů.

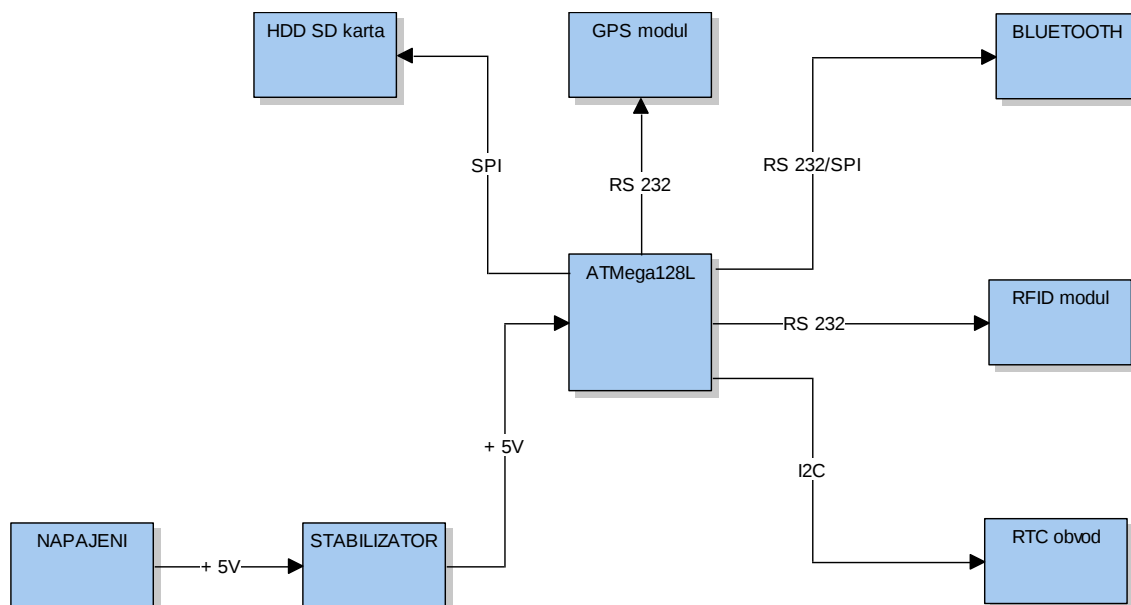
Navržené komponenty:

- RFID reader module EM-18
- Mikroprocesor ATmega128L-8MHz:
 - Krystalový oscilátor 16MHz
 - 2x Kondenzátor
 - Lineární stabilizátor 7805-STM
 - Který pro svou funkci potřebuje:
 - 2x Kondenzátor
- Napájecí zdroj +5V
- RTC specializovaný obvod PCF8583T SMD
- Slot na SD kartu
- GPS modul
- Bluetooth 3.0

Rozvržení navržených součástek je znázorněno a popsáno v kapitole 8.2. .

8.2. Blokové schéma a popis navrženého obvodu

Blokové schéma je na obrázku 20. Hlavním mikrokontrolérem navrhují ATmega128, který zajišťuje komunikaci s pevným diskem, RFID modulem, GPS modulem, Bluetooth a RTC obvodem.



Obr. 20 Blokové schéma navrženého obvodu.

Mikrokontrolér ATmega128L s taktovací frekvencí 8MHz řídí všechny navržené periferie obvodu. Součástky jsou navrženy tak aby splňovaly požadavky jak výrobců automobilů tak samozřejmě i spotřebitelů. Funkční model kitu kapitola 5.2 má mikroprocesor ATmega32L, který je z finančních důvodů dostatečný pro ukázkou navrhovaného obvodu. Pro navrhovaný obvod, ale navrhuji mikroprocesor ATmega128L na který připojíme GPS modul, externí paměťové medium pro SD karty a bluetooth pro bezdrátové posílání veškerých načtených a uložených dat.

Ke čtení tagů v obvodu volím RFID modul EM – 18, který načítá tagy, které mají nebo nemají oprávnění k užívání automobilu. Součástí návrhu je RTC specializovaný obvod PCF8583T SMD pro počítání aktuálního času. Pro kompletní obvod je také navržen zdroj napájení +5V a lineární stabilizátor 7805-STM.

8.3.Ovládané části automobilu

8.3.1. Imobilizér [9]

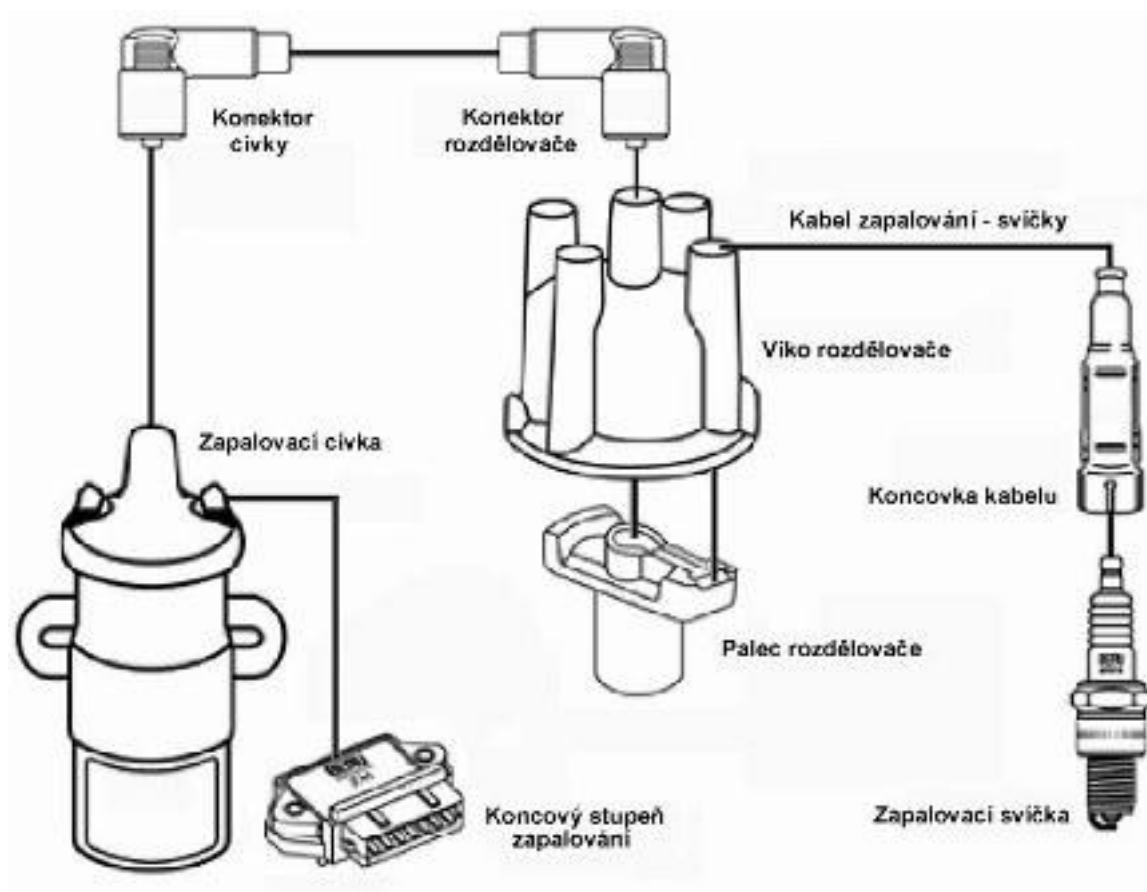
Starší modely imobilizérů využívaly statický (neměnný) kód uložený v čipu v klíči. Tento kód rozpozná RFID čtečka umístěná v zámku a je porovnáván elektronickou řídicí jednotkou automobilu (ECU). Pokud ECU nerozpozná správný kód, uzavře průtok paliva do motoru a tím zabrání nastartování. Novější imobilizéry

používají proměnlivé kódy nebo vyspělejší šifrovací metody pro to, aby zabránili možnému zkopírování kódu z klíče nebo ECU.

Na podobném principu bude pracovat i navrhovaný obvod mobilního zařízení. Po přiložení tagu k RFID čtečce pod startovacím tlačítkem, se ověří ID uživatele, uloží se datum, čas a GPS poloha na SD kartu v textovém souboru (.txt).

8.3.2. Zapalování motoru [10]

Podíváme-li se na zapalování jako systém obrázek 21, tak se dá rozdělit na několik částí. První částí je snímač polohy klikové hřídele. Tento snímač je vstupní veličinou a spouští celý proces zapálení jiskry. Další prvek může být řízení okamžiku zážehu. U kontaktních zapalování čtyřdobých motorů býval tento systém na mechanickém principu a byl řízen okamžik zážehu v závislosti na otáčkách a zatížení motoru. U elektronických zapalování bývá řízení předstihu děláno elektronicky. U dvoudobých motorů většinou řízení předstihu nebylo potřeba. Dalším prvkem je spínač. U kontaktních zapalování byl spínač zároveň snímačem okamžiku zážehu, u elektronických zapalování je spínač polovodič (tranzistor, tyristor). Předposledním prvkem je indukční cívka transformující napětí na primární straně na vysoké napětí na sekundární straně. Posledním prvkem (pomineme-li kabeláž) je zapalovací cívka neboli jiskřiště, kde probíhá inicializace zážehu směsi.



Obr. 21 Schéma zapalování motoru (převzato z [11]).

8.3.2.1. Druhy zapalování [10]

Druhy zapalování se dají rozdělit podle několika kritérií ovšem zapalování jako celek se vždy skládá ze zdroje energie, spínače a indukční cívky transformující energii na vysoké napětí. Podle toho jaké konkrétní prvky jsou použity, se nazývají jednotlivé druhy zapalování.

Konkrétně lze vyjmenovat například:

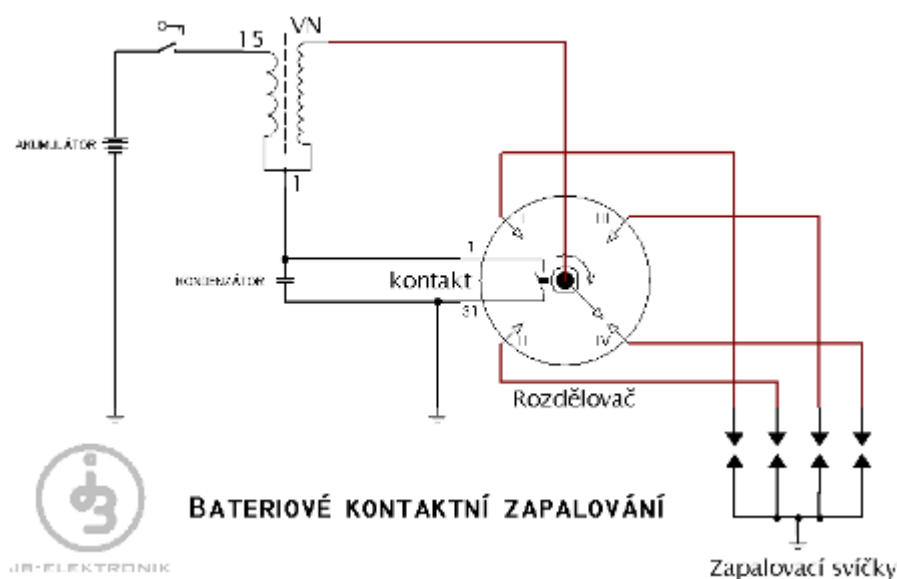
- magnetové kontaktní zapalování
- bateriové kontaktní zapalování
- bateriové bezkontaktní tranzistorové zapalování
- bateriové bezkontaktní tyristorové zapalování
- kapacitní bezkontaktní zapalování

8.3.2.2.Magnetové kontaktní zapalování [10]

Jedno z prvních elektrických zapalování zážehových motorů bylo magnetové kontaktní zapalování. Jak již z názvu vyplývá, tak zdrojem energie byl permanentní magnet (rotor) rotující okolo pevné cívky (stator) poháněný z klikové hřídele. Součástí byl také mechanický kontakt (přerušovač) a v případě víceválcových motorů i rozdělovač. Podle druhu statorové cívky byl vyveden vysokonapěťový kabel přímo z ní nebo byla ještě připojena indukční cívky (zde ve funkci transformátoru) a až teprve z ní byl vyveden vysokonapěťový kabel přímo na zapalovací svíčku nebo přes rozdělovač na jednotlivé zapalovací svíčky. Tento systém se vyznačuje nezávislostí na vnějším zdroji energie. Pracuje zcela bez akumulátoru a krom občasného seřízení kapky oleje na mazací plst' u vačky nevyžaduje další údržbu.

8.3.2.3.Bateriové kontaktní zapalování [10]

Dalším vývojovým stupněm bylo bateriové kontaktní zapalování obrázek 22, které využívalo energii z akumulátoru. Po sepnutí kontaktu se začala energie akumulovat v indukční cívce do doby okamžiku zápalu. V tuto chvíli se rozpojil kontakt a změna proudu na primární části indukční cívky vyvolala indukci napětí a toto indukované napětí bylo vedeno přímo nebo přes rozdělovač na zapalovací svíčku. Obvod se uzavírá zpět do sekundárního vinutí přes kostru motoru a akumulátor.



Obr. 22 Schéma Bateriového Kontaktního Zapalování (převzato z [10]).

8.3.2.4. Bezkontaktní bateriové tranzistorové zapalování [10]

Hlavním problémem u kontaktních zapalování byl právě mechanický spínací prvek. Byly na něj kladeny velké nároky na poměrně velký spínací proud (v řádu jednotek ampér), dobré izolační vlastnosti (odolnost proti průrazu a přeskočení jiskry na kontaktu), odolnost proti opalování kontaktů. Proto dalším vývojovým stupněm byla náhrada mechanického spínače (kladívka) polovodičem. Takto vzniklo bateriové tranzistorové zapalování (označované jako TCI). Vstupním signálem tohoto druhu zapalování může být jakýkoli bezkontaktní snímač (indukční, Hallův snímač, optická závora) nebo původní mechanický kontakt. Tímto systémem jsou eliminovány problémy s opalováním kontaktů na kladívku, ale při použití původního mechanického spínače jako snímače otáček může nastat další problém s nečistotou kontaktních ploch. Při původní funkci kladívka se kontaktní plocha vlastně sama čistila průchodem vyššího proudu a přeskočení drobných jisker, ovšem spíná-li stejný mechanický kontakt mnohonásobně menší proud a nedochází k přeskočení jisker na kontaktu, tak i drobná nečistota (mastnota, prach) může zabránit dokonalému kontaktu.

V současné době je právě používán tento druh zapalování. O vše se stará řídicí jednotka motoru (zapalování i příprava směsi naráz). Vstupní veličinou pro zapalování je snímač polohy klikové hřídele nebo snímač polohy vačkové hřídele nebo kombinace

obojího. Pro určení doby zážehu a doby syčení cívky (energie jiskry) se dále využívá signál zátěže a otáček motoru. Výstup z řídicí jednotky může být přímo silový pro spínání indukčních cívek nebo signálový pro spínání zesilovače (zapalovacích modulu obsahující el. spínače).

8.3.2.5. Bezkontaktní kondenzátorové zapalování [10]

Kondenzátorové zapalování (označované CDI - capacitor discharge ignition) jak již z názvu vyplývá, používá pro svou funkci energii akumulovanou v kondenzátoru. Zdrojem energie je zde obdobně jako u magnetového zapalování statorová cívka. Vícepólový rotor s permanentními magnety vytvoří během jedné otáčky klikové hřídele několik period a statorová cívka vinutá mnoha závity slabšího drátu nabíjí přes usměrňovač akumulací kondenzátor. Takto nabitý kondenzátor na napětí několika stovek voltů se následně ve správný okamžik vybije přes spínací prvek (většinou tyristor) do indukční cívky (zde ve funkci impulsního transformátoru) a následně je vysoké napětí vedeno na zapalovací svíčku (nebo dvě svíčky zapojeny sériově), kde dojde k přeskoku jiskry. Spouštěcím impulsem je buď přímo indukční snímač umístěný na statorové části zapalování, nebo přes řídicí jednotku zapalování, která řídí okamžik zápalu v závislosti na provozních podmínkách motoru. V základu je CDI zapalování jedno z nejjednodušších a nejspolehlivějších zapalování. Výhoda je v nezávislosti na jakémkoli přídavném zdroji energie, elektronika může být umístěna přímo v obalu indukční cívky (tzv. vysokonapěťový spínač). Vypínání zapalování CDI se provádí pomocí vnějšího vybití kondenzátoru.

Zapalování typu CDI se v drtivé většině používá u motocyklů a malých pracovních strojů (sekačky, motorové pily, atd.). Výhodou je, že se celá elektronika včetně indukční cívky dá zabudovat do jednoho modulu (tzv. VN spínač). Indukční cívka jako taková může být podstatně menších rozměrů, protože se energie před okamžikem zážehu neakumuluje do magnetického obvodu cívky, ale do kondenzátoru.

8.3.3. Odemykání a zamykání auta [12]

Centrální zamykání a odemykání automobilu umožňuje zamknout nebo odemknout všechny dveře vozidla klíčem, stisknutím tlačítka nebo přepnutím přepínače. Centrální zamykání bylo poprvé použito u luxusního vozu Scripps-Booth v roce 1914, ale nebylo běžné, dokud ho znovu nezavedl Packard v

roce 1956. Dnes se téměř u všech modelů automobilů nabízí přinejmenším jako doplňková výbava.

Zpočátku systémy centrálního zamykání a odemykání ovládaly pouze dveře. Mnoho vozů má dnes systémy, které ovládají také víko zavazadlového prostoru nebo dvířka plnicího otvoru palivové nádrže.

U moderních automobilů je také běžné, že se zámky automaticky aktivují, když se zařadí rychlostní stupeň nebo vozidlo dosáhne určité rychlosti. U takových systémů se obvykle dveře odemknou při zaparkování.

8.3.3.1. Dálkové a bezobslužné zamykání a odemykání [12]

Dnes má mnoho vozů centrálním zamykáním obr. 23 nebo také dálkový bezklíčový systém, který umožňuje odemknout vozidlo stiskem tlačítka na dálkovém ovladači nebo vložení číselné kombinace přes klávesnici. Tyto systémy potvrzují úspěšné odemčení/zamčení pomocí světelného nebo zvukového signálu a obvykle nabízejí možnost mezi oběma variantami přepínat. Obě poskytují tutéž funkcionalitu, avšak světelný signál je diskrétnější, kdežto zvukový může být nepříjemný v obytných oblastech nebo všude jinde, kde se často parkuje (např. na krátkodobých parkovištích).

Jiná vozidla mají bezobslužný systém založený na vzdálenosti. Je spouštěn tím, že je jeho vysílač v určité vzdálenosti od vozidla. Některé systémy obsahují navíc ještě funkci pro otevírání garážových vrat.



Obr. 23 Dálkové centrální zamykání a odemykání (převzato z [12]).

8.4. Pořizovací náklady

Se stále se zvyšujícími nároky automobilek na ceny jednotlivých součástí jsou pořizovací náklady na mobilní zařízení tabulka 1: mikroprocesor ATMega128L – 260,-, RFID modul EM-18 – 353,- Kč, SD Karta 8GB – 232,-Kč, GPS modul – 920,-Kč, ostatní součástky cca 100,-Kč, všechny ceny jsou v korunách a uvedeny s 21% DHP.

Tab. 1 Tabulka pořizovacích nákladů jednotlivých součástí

Navržené součástky	Cena vč. 21% DPH
ATMega128L	260,-
RFID modul EM - 18	353,-
SD karta 8GB	232,-
GPS modul	920,-
Ostatní součástky	cca 100,-
Celkem:	1865,-

8.5. Ovládání jednotky pro účely firem

8.5.1. Řízená kontrola užívání vozidel

Se stále se zvyšujícími se požadavky majitelů firem na šetření nákladů a neustálou kontrolou nad tím, který zaměstnanec, kdy odjel se služebním vozidlem a jestli nedošlo k zneužití služební vozidla pro soukromé účely nebo pro vlastní obohacování.

S přiděleným tagem (kartou nebo čipem), zamezíme zneužívání služebních vozidel. Tag (kartu/čip), dostane zaměstnanec který má oprávnění k používání vozidla.

Otevírá se nám totiž prostor k tomu, aby jedno vozidlo, bylo přiděleno více zaměstnancům. Systém spočívá v tom, že každý má přiděleno své vlastní ID (Identifikační číslo), pod kterým se ukrývá čas a den kdy má přidělené vozidlo pro služební cestu. Díky vestavěnému GPS modul odpadá zapisování ujetých kilometrů do knihy jízd, jelikož jsou tyto údaje ukládány na pevný disk (SD kartu), v textovém formátu txt. Pro pohodlné stahování dat veškerých údajů o jízdě v textovém souboru je

součástí mobilního zařízení navržena technologie Bluetooth, která na funkčním modelu ukázána není z nedostatku času.

8.5.1.1.Ověření uživatele k povolení k jízdě

K ověření zda má či nemá, zaměstnanec povolení k jízdě slouží, přidělené ID (identifikační číslo), které má každý uživatel nezaměnitelné a to rodné číslo plus první písmeno ze svého jména a příjmení.

Nedojde-li ke správnému načtení uživatele, dojde stejně jako u imobilizéru popsaného v kapitole 8.3.1. dojde k uzavření průtoku paliva do motoru a tím nedojde k nastartování automobilu. Eliminujeme tak případné zneužití služebního vozidla k soukromým účelům.

8.5.1.2.Načtení a uložení všech údajů o jízdě

Po správném ověření uživatele (viz. kapitola 8.5.1.1), procesor ATMega128L pošle všechny údaje k uložení v textovém souboru na pevný disk (SD kartu). Díky načtení a uložení všech údajů včetně GPS modulu, odpadá nutnost vypisování všech ujetých kilometrů, startu a cíli cesty. Vše za nás obstará GPS modul, který nám počítá nejen ujeté kilometry, ale také souřadnice o poloze, pomocí kterých zjistíme přesnou trasu pohybu vozidla v době služební cesty a také čas strávený na místě.

Kartou Master, popřípadě administrátorskou kartou zjistíme veškeré údaje o všech Slave kartách a v případě potřeby zablokovat odcizenou či ztracenou kartou.

8.5.1.3.Úplné zablokování vozidla při neoprávněném přístupu

Pokud by zaměstnanci chtěli zneužít vozidlo ať už k soukromým účelům nebo vlastnímu obohacení, dojde k jeho úplnému zablokování. Jednak se aktivuje imobilizér stejně jako v kapitole 8.5.1, ale také ke spuštění alarmu, samozřejmě pokud je jím automobil vybaven (viz. kapitola 2.2.2.). Porušením pravidel o užívání vozidla dojde také k úplnému zablokování tagu (karty). Takto zablokováný tag (karta) nedovolí použití jakéhokoliv jiného vozu.

8.5.2. Řízené garanční prohlídky

Velké náklady vynaloží zaměstnavatel na garanční prohlídky svého vozového parku. Údaje o intervalech garančních prohlídek ukládá administrátor do systému mobilního zařízení a sám hlídá počet ujetých kilometrů a informace o průběhu jednotlivých prohlídek a použitého materiálu. Tím zabráníme zneužívání náhradních dílu určené pro služební vozový park.

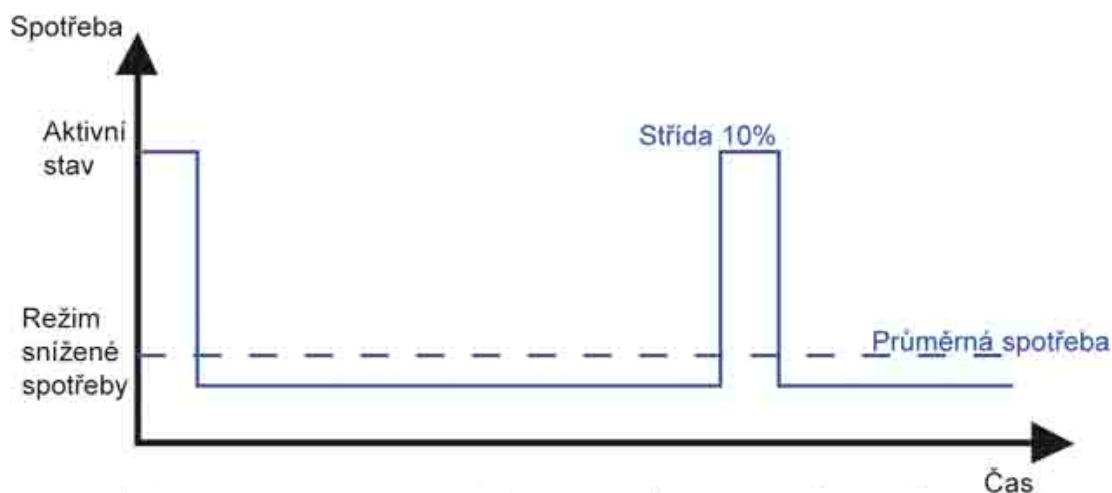
8.6. Spotřeba zařízení

8.6.1. Jak ovlivnit spotřebu zařízení [6]

Spotřebu zařízení můžeme ovlivnit pomocí mikroprocesoru ATmega128L taktován na frekvenci 8MHz dvěma způsoby, v prvním se probouzí každou 1s a kontroluje, zda někdo nechce číst, neboli bude sám aktivovat napájení čtečky. Druhý způsob řešení ovlivnění spotřeby zařízení spočívá v tom, že RFID čtečka EM – 18 bude napájena stálým napětím +5V a procesor ATmega128L se probudí od přijatého znaku.

Spotřebu, především ovlivníme frekvencí řídicího signálu (hodinový kmitočet). Tady platí, že čím vyšší je kmitočet, tím stoupá i příkon mikrokontroléru. Pokud tedy chceme snížit spotřebu, tak používáme mikrokontrolér s co nejnižším taktovacím kmitočtem 8Mhz. Dalším faktorem ovlivňujícím příkon mikrokontroléru je pak velikost napájecího napětí. Jelikož je příkon dán součinem napětí a proudu, dosáhneme snížení napětí a klesne i celkový příkon. Snižování napájecího napětí následně vede k dalšímu snižování proudového odběru, takže příkon klesá rychleji než by odpovídalo pouhému snížení napájecího napětí. Tento fakt je právě jedním z hlavních důvodů pro přechod z 5V napájecího napětí na 3,3V, který má mikrokontrolér ATmega128L.

Ovlivnění spotřeby vhodnými režimy snížené spotřeby je ukázáno na obr. 24, kde můžeme vidět, jak významně klesne spotřeba (průměrná spotřeba), využijeme-li vhodně režimů se sníženou spotřebou. V případě bateriově napájených modulů to bude znamenat prodloužení života baterií např. na 5ti násobek.



Obr. 24 Graf úsporných režimů (převzato z [6]).

8.6.2. Parametry a spotřeba RFID čtečky EM-18 [8]

Modul čtečky RFID EM-18 do navrhovaného mobilního zařízení. Parametry modulu popsány podle výrobce. RFID modul EM-18 je na obr. 25.

Technické parametry:

- Formát: EM 4001 nebo kompatibilní
- Frekvence: 125kHz
- Čtecí vzdálenost: 10 cm
- Rozměry: 32x32x8mm
- Kódování: Manchester 64 bit
- Formát dat: ASCII nebo Wiegand26
- Výstup: TTL
- Napájení: 5V DC/50mA

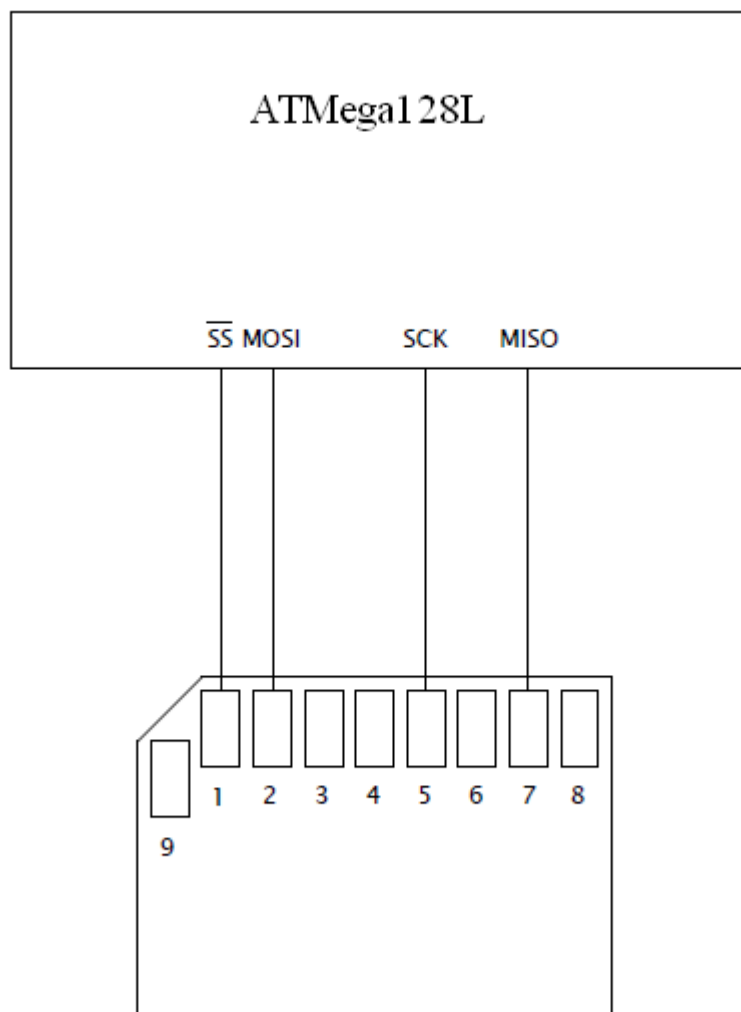


Obr. 25 Modul čtečky RFID EM-18 (převzato z [8]).

8.7. Zápis mikrokontroléru ATmega128L na SD kartu

8.7.1. Propojení mikrokontroléru a SD karty pomocí SPI [14]

Systém propojení Master-Slave (uživatel a SD karta) se skládá ze dvou posuvných registrů a generátoru hodinových pulzů. Master začíná komunikovat po nastavení pinu SS (slave select) na nulu (u SD karty pin CS). Slave připraví data k odeslání pomocí svého posuvného registru a Master generuje hodinové pulzy na lince SCK (CLK na SD kartě). Data jsou vždy odeslána od zařízení pracující jako „master“ k „slave“ pomocí pinu MOSI (master out, slave in) a od zařízení „slave“ k „master“ pomocí pinu MISO (master in, slave out). Propojení je znázorněno na obrázku obr. 26. Po každém datovém paketu zařízení „master“ synchronizuje „slave“ nastavením pinu SS (slave select) na úroveň high.



Obr. 26 Schéma propojení SD karty s mikrokontrolérem ATmega128L (převzato z [14]).

8.7.2. Komunikace pomocí SD protokolu [14]

Komunikace probíhá pomocí command-response protokolu. Příkazy jsou posílány od uživatele, na které karta odpovídá pomocí odpovědních tokenů. Podle typu příkazu karta odpovídá pomocí tokenů R1, R2, R3 nebo datovými tokeny „token star block“, „stop tran“, případně chybovým tokenem „data error“. SD příkazy jsou posílány ve formě „CMDXX“ nebo „ACMDXX“, kde „CMD“ a „ACMD“ značí obecně příkaz a „XX“ dvoumístné číslo jednotlivého příkazu. Příkazy jsou posílány pomocí příkazového rámce délky 6 bytů přes rozhraní SPI. Rámec vždy začíná sekvencí „01“ následovanou šesti bity označující číslo příkazu. Další čtyři byty je argument příkazu (první je poslán MSB). V posledním bytu je vyhrazeno 7 bitů pro kontrolní součet CRC a konečný stop bit „1“ je poslán jako poslední. Všechny byty jsou poslány uživatelem

na port MOSI (DataIn). MSB se posílá jako první. V režimu SPI, je kontrola CRC primárně vypnuta.

8.7.3. Ochrana dat při přenosu po sběrnici

Každý příkaz posílaný hostem na sběrnici je chráněn kontrolním součtem CRC. Při přepnutí do režimu SPI, je tato kontrola primárně vypnuta a na kontrolní součet není brán zřetel. Ovšem při přepínání, do režimu SPI pomocí příkazu CMD0 je stále kontrolní součet vyžadován, protože karta je v režimu SD. V režimu SPI, se kontrolní součet CRC stále posílá, u vyžadovaných rámců, ale není na něj brán zřetel a je ignorován při přijetí. Uživatel může kontrolní součet zapnut požitím příkazu CRC_ON_OFF (CMD59).

8.7.4. Rozdělení paměťových částí [14]

Základní jednotkou pro datový přenos je jeden byte. Každá datová operace definuje velikost bloku jako celočíselné násobky bytů. Pro blokově orientované příkazy se používají následující označení: Blok – jednotka, která se vztahuje k blokově orientovaným příkazům pro čtení a zápis. Její velikost je počet bytů, které se přenáší, když je uživatelem poslán příkaz pro práci s blokem. Velikost bloku je buď programovatelná, nebo pevně daná. Informace o povolené velikosti je uložena v registru CSD. U příkazů pro mazání není velikost jednotky stejná jako pro blokově orientované příkazy:

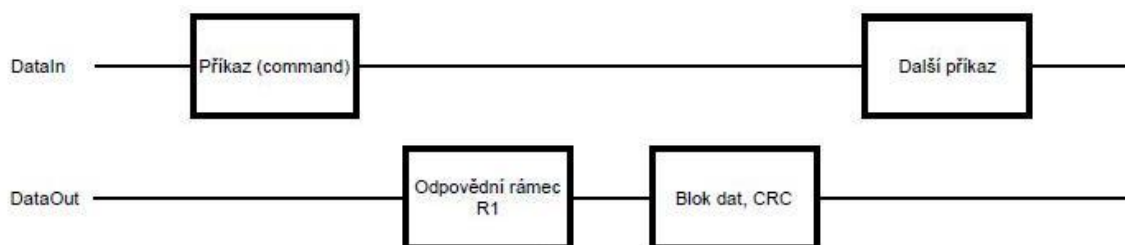
- Sektor – jednotka, která se vztahuje k příkazům pro mazání. Její velikost je počet bloků, které jsou vymazány v jedné dávce. Velikost sektoru je pevně dána pro každé zařízení. Informace o velikosti sektoru (počet bloků) je uložena v registru CSD.

U zařízení, která využívají ochranu proti zápisu, se používá následující označení:

- WP skupina – je jednotka, která může mít individuální ochranu proti zápisu. Její velikost je definována jako počet skupin, které budou chráněny proti zápisu nebo vymazání. Velikost WP skupiny je pevně dána pro každé zařízení. Informace o velikosti je uložena v registru CSD.

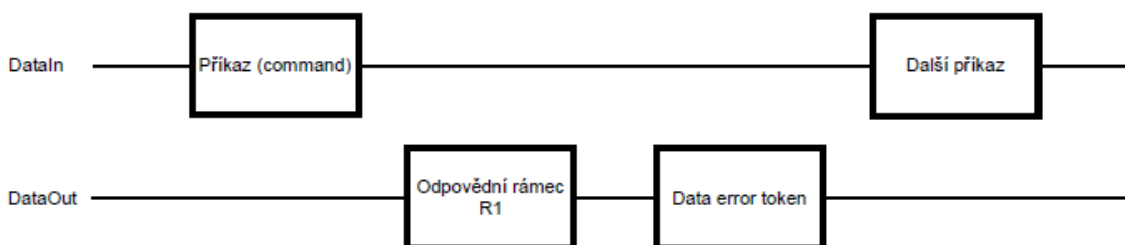
8.7.5. Čtení dat [14]

Režim SPI podporuje jak jednotlivé čtení, tak čtení po blocích. Pro čtení dat je určen příkaz CMD17 nebo CMD18. Po přijetí příkazu pro čtení karta odpoví tokenem, který je následován blokem dat obr. 27. Velikost jednoho bloku dat se definuje pomocí příkazu SET_BLOCKLEN (CMD16). Velikost bloku bývá standardně 512B. Maximální velikost bloku je uložena v registru CSD. Pro standardní kapacitu karet může být blok čten od jednotlivých bytů až po celý blok 512 B. U vysokokapacitních karet je možno pouze číst celé bloky 512 B.



Obr. 27 Schéma čtení bloku dat (převzato z [14]).

Adresa, odkud se mají číst data se posílá v příkazovém rámci. Je vždy nastavena na čtení začátku bloku. Není možné číst blok 512 B odkudkoliv. V případě, že se čtení dat nepovede, žádná data se nepřenáší a karta vyšle speciální chybové hlášení (token) na stranu hosta obr. 28.



Obr. 28 Schéma chyby při čtení dat (převzato z [14]).

8.7.6. Zápis dat [14]

Režim SPI umožňuje zápis jak po jednotlivých blocích, tak i po více blocích. Po přijetí příkazu pro zápis (příkaz CMD24, CMD25), karta odpoví a vyčká na blok dat poslaný od uživatele obr. 29.

Každý blok dat má vlastní předponu (prefix 0xFEh), který určuje začátek bloku dat. Po přijetí dat karta odpoví, zda data byla přijata v pořádku. Pokud byla data přijata bez chyb, začnou se zapisovat na kartu. Po celou dobu zápisu dat na kartu posílá karta informaci o tom, že je zaneprázdněná. Jakmile je zápis dokončen, je na hostu, aby tuto událost zkontroloval pomocí příkazu CMD13. Pokud při zápisu nastanou chyby (např.: zápis mimo paměť, ochrana proti zápisu) jsou odhaleny pouze při zápisu. Zatímco je karta zaneprázdněna zápisem dat, můžeme odpojit signál CS, což nebude mít efekt na právě zapisovaná data. Karta uvolní linku DataOut a pokračuje se zápisem. Pokud karta bude znovu vybrána před dokončením zápisu dat, nastaví se linka DataOut na nízkou úroveň a odmítne všechny přicházející příkazy. Pokud resetujeme kartu (příkazem CMD0), ukončí se probíhající zapisování dat. To může vést ke ztrátě dat na kartě. Je na uživateli, aby se tomuto vyvaroval.



Obr. 29 Schéma zápisu bloku dat (převzato z [14]).

8.7.7. Komunikace mezi SD a mikrokontrolerem ATmega128L [14]

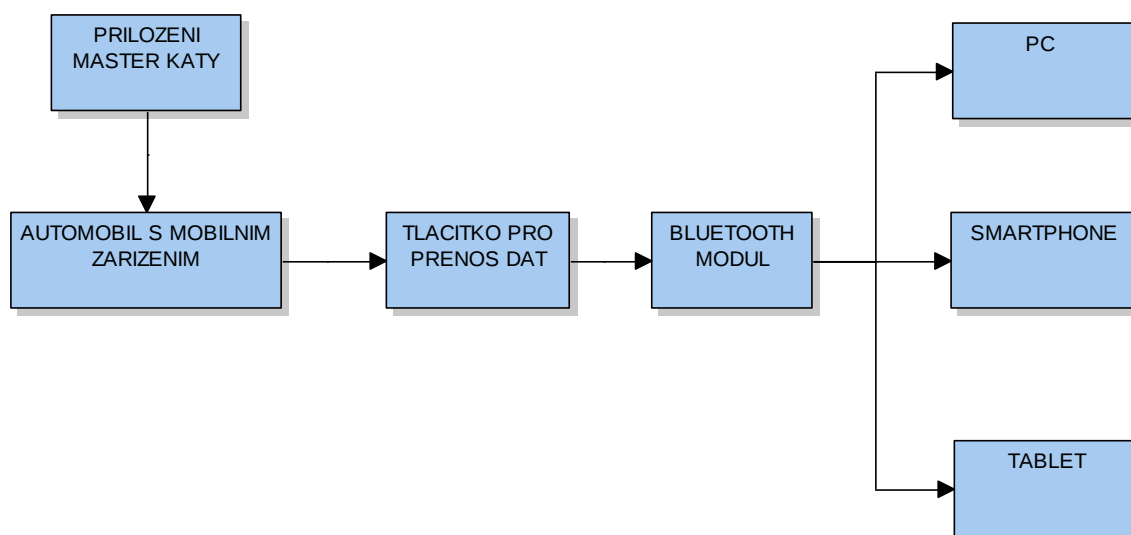
Komunikace mezi mikrokontrolérem ATmega128L a SD kartou probíhá po bytech. Data jsou posílána a přijímána datovým registrem. Dokud nejsou data přijata, nebo odeslána, probíhá cyklus, který bude testovat příznak ve stavovém registru. Jakmile je příznak nastaven, data jsou odeslána a program bude pokračovat dál. Funkci se předáváme paramter, který byte má být poslán.

8.8. Bezdrátový přenos dat z modulu mobilního zařízení

Pro bezdrátový přenos dat z mobilního zařízení umístěného v automobilu navrhuji, následující postup.

Pro přenos dat z bezpečnostního mobilního zařízení přiložíme Master kartu (s jinou kartou není přenos možný), zmačkneme tlačítko na palubní desce dojde k přenosu dat (Log, kniha jízd) pomocí Bluetooth modulu na zařízení, které máte zrovna k dispozici.

Těmito zařízeními může být PC, Smartphone nebo tablet. Díky bezdrátovému přenosu dat odpadá zbytečné připojení kabelů. Blokové schéma bezdrátového přenosu dat je ukázáno na obrázku 30.



Obr. 30 Blokové schéma bezdrátového přenosu dat.

8.9. GPS moduly

GPS je otevřený systém a možnosti jeho využití se neustále rozšiřují. Jako konkrétní příklad můžeme vzít implementaci do automobilů. Už dávno naše možnosti nekončí navigací na přístrojové desce.

Podnikatelé a správci vozového parku mohou využít GPS modul, který jim bude v reálném čase hlásit polohu vozidla na mapě, rychlost pohybu i spotřebu a především možnou krádež paliva. Online systém vše zaznamená a majitel vozového parku už

nikdy nemusí ztrácet čas s knihou jízd (viz. kapitola 9.1.3). Podnikatelům tak nevznikají zbytečné náklady spojené s neužitím služebního vozidla. Jako další z možných bezpečnostních prvků k ochraně firemních nákladů a investic navrhuji vůz na dálku znehybnit.

8.9.1. Navržený GPS modul [15]

Jako GPS modul navrhuji miniaturní model M10264 s integrovanou anténou od výrobce GPS RADIONOVA. GPS modul je kombinací kompletní GPS elektroniky a pasivní antény na jediné desce. Model M10264 je integrovaný modul pro pásmo L1 GPS s podporou A-GPS.

Modul je postaven na architektuře SiRFstarIIITM v kombinaci s výkonnou anténí technologií společnosti Antenova. Anténa je navržena s ohledem na optimální vyzařovací charakteristiku.

Jako interface pro host procesor je použitý 1,8V UART. Modul je také vybaven vstupem pro externí anténu s automatickým rozpoznáváním připojení antény.

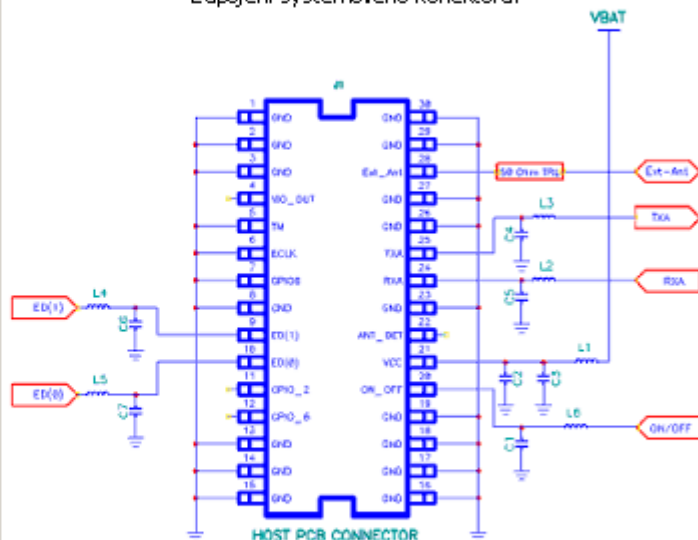
8.9.2. Spotřeba a technické parametry GPS modul M10264 [15]

Modul je napájen jediným napětím 3,6V a má nízkou spotřebu. Navíc jsou k dispozici režimy pro další úsporu energie. Je proto vhodný pro miniaturní zařízení napájené z baterií. Pro GPS modulu M10264 byly vybrány tyto parametry tabulka 2.

Tab. 2 Tabulka vybraných technických parametrů M10264 (převzato z [15]).

Frekvence:	1575 MHz
GPS Chipset:	SiRFstarIII™ GSC3LT
A-GPS:	ano
Kanály:	až 20
Možnost ext. antény:	ano
Napájecí napětí:	3,6V
Napájecí proud:	
Acquisition Mode:	50mA
Track Mode:	30mA
Sleep (Hibernate):	30uA
Výstup:	SiRF Binary / NMEA 0183
COM Interface:	UART (1,8V)
Teplotní rozsah:	-40°C až +85°C
Hot Start:	<1s
Warm Start:	<35s
Cold Start:	<35s
Konektor (protikus):	Hirose DF12 (4.0) -30DP0, 5V (86)

Zapojení systémového konektoru:



9. PŘÍSTUP K SYSTÉMU

9.1. Přiložení karty

9.1.1. Načtení data, času a GPS polohy

K přístupu do systému budou zaměstnanci firmy používat tagy a to buď plastové karty, nebo čipy ve formě přívěsku obrázek 7 v (kapitole 7.3.). Po přiložení karty k RFID modulu EM – 18 si navržené mobilní zařízení načte a uloží údaje ID uživatele, data, času a GPS polohy.

9.1.2. Kontrola k oprávnění služební cesty

Pro neustálou kontrolu užívání služebního vozidla slouží, kontrola jestli zaměstnanec má oprávnění služební cesty a konkrétního osobního automobilu. Pro majitele firem v tom vidím velkou výhodu, protože nemůže dojít k libovolnému používání jednotlivých služebních vozidel a tím se výrazně ušetří náklady spojené s provozem jednotlivých vozidel vozového parku dané firmy.

9.1.3. Aktivace knihy jízd

Po načtení všech potřebných údajů a kontrole k oprávnění služební cesty se automaticky aktivuje kniha jízd, kde odpadá neustálé vypisování papírových záznamů o jízdě. Díky GPS modulu je uživatel monitorován po celou dobu užívání služebního vozidla. Nemůže tak nastat situace, že dojde k zneužití počtu najetých kilometrů. Všechny údaje ukládá mikrokontrolér ATmega128L na SD kartu. Extrémní navýšení kilometrů si tak každý zaměstnanec zaplatí sám.

10. ZÁVĚR

Práce je členěna do dvou logických řazených částí. První část je pojata jako teoretická a obsahuje šest kapitol. První kapitola představuje úvod do celé problematiky, která byla řešena v rámci této závěrečné práce. Ve druhé kapitole je popsáno již známé zabezpečení automobilů. Následující kapitola podrobně popisuje problematiku RFID. V dalších třech kapitolách jsou popsány mikrokontroléry ATmega, ukládání dat a v šesté kapitole se práce věnuje RTC speciálním obvodům.

Druhá část této diplomové práce zahrnuje práci autora, viz. Kapitola 7, 8 a 9. Kapitola 7 se zabývá podrobným popisem vývojového kitu a popisem vytvořeného programu. Jedná se o popis vývojového kitu, viz kapitola 7.1, 7.2 a 7.3. V kapitole 7.5 je popsán vytvořený software pro funkční model demonstrováný na vývojovém kitu. V další kapitole se práce zabývá samotným návrhem mobilního zařízení pro implementaci do automobilů, (viz. kapitola 8).

Takto vytvořený software na základě požadavků umožňuje:

- Načítat uživatele
- Kontrolovat oprávnění uživatelů
- Ukládání dat o jednotlivých uživateli
- Přidělení práv užívání, Master, Slave
- Možnost zobrazení údajů pomocí Master karty

Z důvodu nedostatku času a velkého pracovního vytížení nebyly na vytvořeném software dokončeny části navrhované v kapitole 8. Pro další testování a zpracování funkčního modelu je důležité ukládat data na pevný disk (SD kartu) dokoupit GPS modul a zpracovat bezdrátové posílání uložených dat pomocí technologie Bluetooth.

11. POUŽITÁ LITERATURA A ZDROJE

- [1] Rok Zabezpečení Vozidla, internetový list. [Online] citováno 5. února 2013. Dostupné na WWW: <http://www.rokzabezpecenivozidel.cz/zabezpeceni-vozidel/>
- [2] RFID princip, internetový list. [Online] citováno 5. února 2013. Dostupné na WWW: <http://rfid.wz.cz/princip.htm>
- [3] Architektura mikroprocesoru AVR ATmega, Führer Ondřej, FUH002. Dostupné na WWW:
[http://wh.cs.vsb.cz/mil051/images/c/ca/PAP_Architektura_procesoru_AVR_ATmega_\(Ond%C5%99ej_F%C3%BChrer\).pdf](http://wh.cs.vsb.cz/mil051/images/c/ca/PAP_Architektura_procesoru_AVR_ATmega_(Ond%C5%99ej_F%C3%BChrer).pdf)
- [4] Mikrokontroléry od Amel, V.Kustail., internetový zdroj [Online] citováno 5. února 2013. Dostupné na WWW: <http://ojs.ujf.cas.cz/~kushpil/02EMBS/Lecture4.pdf>
- [5] Mikrokontroléry Atmel AVR, Jiří Volf, Bakalářská práce. [Online] citováno 5. února 2013. Dostupné na WWW:
http://theses.cz/id/ork9bj/downloadPraceContent_adipIdno_14258
- [6] FKtechnics s.r.o., ATmega, katalogový list. [Online] citováno 5. února 2013. Dostupné na WWW: http://www.fkt.cz/cz/clanky/soucastky/art_119/atmega48pa-atmega88pa-atmega168p.aspx
- [7] OnPa Design & Development, EvB 4.3 v4 katalogový list. [Online] citováno 5. února 2013. Dostupné na WWW: <http://shop.onpa.cz/?kit-evb-4.3,27>
- [8] Flajzar Electronics, katalogový list. [Online] citováno 5. února 2013. Dostupné na WWW: <http://www.flajzar.cz/pristupove-systemy-rfid/ctecka-cipu-rfid-modul-em-18.htm>
- [9] Wikipedie, internetový zdroj. [Online] citováno 16. dubna 2013. Dostupné na WWW: <http://cs.wikipedia.org/wiki/Imobiliz%C3%A9r>
- [10] JB-ELEKTRONIK. Internetový zdroj. [Online] citováno 2. května 2013. Dostupné na WWW: http://www.jb-elektronik.cz/diagnostika-druhy_zapalovani.php
- [11] Calibra., internetový zdroj. [Online] citováno 2. května 2013. Dostupné na WWW: <http://www.calibra.cz>

- [12] Wikipedia, Otevřená encyklopedie. Internetový zdroj. [Online] citováno 2. května 2013. Dostupné na WWW: http://cs.wikipedia.org/wiki/Centr%C3%A1ln%C3%AAD_zamyk%C3%A1n%C3%AD
- [13] Electronics and instrumentation engineering. Internetový zdroj. [Online] citováno 15. května 2013. Dostupné na WWW: <http://einstrumentation.blogspot.cz/2012/09/how-to-build-your-own-robot.html>
- [14] Implementace Čtení Záznamu Dat Na SD Kartu, Jaroslav Bašus. Bakalářská práce. Internetový zdroj. [Online] citováno 16. května 2013. Dostupné na WWW: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=42924
- [15] Spezial Electronic. Katalogový list. [Online] citováno 16. května 2013. Dostupné na WWW: <http://www.spezial.cz/antenna/gps-modul-antenna-radionova-m10264.html>

12. SEZNAM POUŽITÝCH OBRÁZKŮ

Obrázek 1 Blokové schéma RFID.....	13
Obrázek 2 Princip přenosu dat.....	14
Obrázek 3 Základní architektura mikroprocesorů AVR.....	17
Obrázek 4 Blokové schéma RTC odvodu.....	22
Obrázek 5 Vývojový kit EvB 4.3 v4	23
Obrázek 6 Funkční model vývojového kitu.....	27
Obrázek 7 Tagy a přístupová karta pro přihlášení do systém.....	28
Obrázek 8 AVR vývojové studio 4.....	29
Obrázek 9 Úvodní stav kitu EvB 4.3 v4.....	30
Obrázek 10 Blokové schéma přihlášení uživatele Master a Slave.....	31
Obrázek 11 Blokové schéma posledního načteného uživatele.....	32
Obrázek 12 Blokové schéma zobrazení údajů o LOGU uložené na EEPROM.....	33
Obrázek 13 Blokové schéma změny Mastera.....	34
Obrázek 14 Blokové schéma načtení a uložení nového Mastera.....	34
Obrázek 15 Blokové schéma pro menu EEPROM.....	35
Obrázek 16 Blokové schéma odepření přístupu.....	36
Obrázek 17 Blokové schéma nastavení data a času.....	37
Obrázek 18 Blokové schéma vymazání paměti EEPROM.....	38
Obrázek 19 Blokové schéma obrázku pro kontrolu smazání EEPROM.....	39
Obrázek 20 Blokové schéma navrženého obvodu.....	41
Obrázek 21 Schéma zapalování motoru.....	43
Obrázek 22 Schéma Bateriového Kontaktního Zapalování.....	45
Obrázek 23 Dálkové centrální zamykání a odemykání.....	47
Obrázek 24 Graf úsporných režimů.....	51
Obrázek 25 Modul čtečky RFID EM-18.....	52
Obrázek 26 Schéma propojení SD karty s mikrokontrolérem ATmega128L.....	53
Obrázek 27 Schéma čtení bloku dat.....	55
Obrázek 28 Schéma chyby při čtení dat.....	55
Obrázek 29 Schéma zápisu bloku dat.....	56
Obrázek 30 Blokové schéma bezdrátového přenosu dat.....	57

13. SEZNAM POUŽITÝCH TABULEK

Tabulka 1 Tabulka pořizovacích nákladů jednotlivých součástí.....	48
Tabulka 2 Tabulka vybraných technických parametrů M10264.....	59