

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV MIKROELEKTRONIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF MICROELECTRONICS

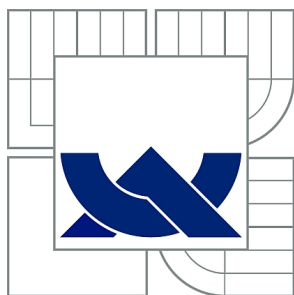
ZAŘÍZENÍ PRO OSOBNÍ IDENTIFIKACI A SDÍLENÍ DAT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

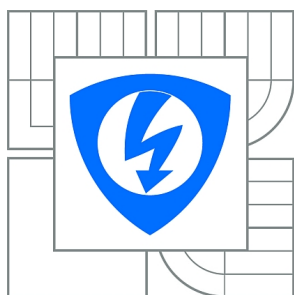
AUTOR PRÁCE
AUTHOR

Bc. PAVEL SEVERA

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNologiÍ
ÚSTAV MIKROELEKTRONIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF MICROELECTRONICS

ZAŘÍZENÍ PRO OSOBNÍ IDENTIFIKACI A SDÍLENÍ DAT

DEVICE FOR PERSONAL IDENTIFICATION AND DATA SHARING

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

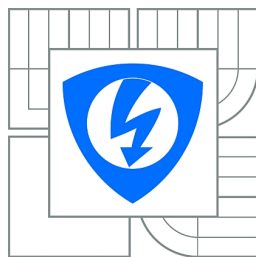
AUTOR PRÁCE
AUTHOR

Bc. PAVEL SEVERA

VEDOUcí PRÁCE
SUPERVISOR

Ing. MARTIN FRIEDL, Ph.D.

BRNO 2015



VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav mikroelektroniky

Diplomová práce

magisterský navazující studijní obor
Mikroelektronika

Student: Bc. Pavel Severa

ID: 140453

Ročník: 2

Akademický rok: 2014/2015

NÁZEV TÉMATU:

Zařízení pro osobní identifikaci a sdílení dat

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou uživatelské identifikace pomocí bezkontaktních čipů (NFC), smartphonů či tabletů. Dále prostudujte možnosti datových přenosů z externího do čtecího stacionárního zařízení a následné zpracování a odeslání dat na server. Na základě rešerše vyberte vhodné komponenty a navrhnete vlastní systém pro identifikaci, sdílení dat a vzdálenou synchronizaci dle požadavků zadavatele.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce

Termín zadání: 10.2.2015

Termín odevzdání: 28.5.2015

Vedoucí práce: Ing. Martin Friedl, Ph.D.

Konzultanti diplomové práce:

prof. Ing. Vladislav Musil, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Cílem práce je vytvořit zařízení pro zaznamenávání návštěvy turisty či hráče vytvořené hry. Po domluvě se zadávajícím Ing. Filipem Kovářem budou navrženy dvě zařízení, webová aplikace a protokol pro odesílání dat na server. První zařízení bude obsahovat grafický displej se vstupem HDMI, řídicí jednotkou Raspberry Pi, NFC čtecí zařízení, kamerou a GSM modulem. Druhé zařízení bude postaveno s mikrokontrolérem ATMEGA644, čtečkou NFC, může být osazen 2-4 řádkovým displejem a může být připojen GSM modul. Obě zařízení budou komunikovat pomocí GPRS se serverem. Server bude moci řídit jednotlivá zařízení a bude se starat o sběr dat.

KLÍČOVÁ SLOVA

ATmega644, Raspberry pi, NFC, GPRS, SIM, grafický displej, PN532, SIM900A

ABSTRACT

Result of my work is make device for logging visitors or game players. I arranged to make two devices, web pages and communication protocol between server and devices. Graphical device will have graphical display with HDMI input, Raspberry main board, NFC reader, camera and GSM module. Second device will have microcontroller ATMEGA644, NFC reader, 2-4 line text display and optional GSM module. Both device will communicate with server via GPRS. Server can change configuration of devices and collecting logs

KEYWORDS

ATmega644, Raspberry pi, NFC, GPRS, SIM, graphic display, PN532, SIM900A

PAVEL SEVERA, Bc. *Zařízení pro osobní identifikaci, sdílení dat a vzdálenou synchronizaci*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav mikroelektroniky, 2015. 51 s. Vedoucí práce byl Ing. Martin Friedl, Phd.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Zařízení pro osobní identifikaci, sdílení dat a vzdálenou synchronizaci“ 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

.....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu semestrální práce panu Ing. Martinu Friedlovi a Ing. Filipovi Kováři za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno

.....

(podpis autora)

OBSAH

1	Úvod	10
2	Varianta 1 - Informační kiosk	11
2.1	LCD pro Raspberry Pi	12
2.2	Raspberry Pi	13
2.3	NFC čtecí modul pro Raspberry Pi	14
2.4	GSM modul pro Raspberry Pi	15
3	Varianta 2 - Logger	16
3.1	NFC PN532 mini	17
3.2	Čtečka NFC RC522	17
3.3	Textový LCD displej	18
3.4	RTC obvod	19
3.5	Mikrokontrolér ATmega644	20
3.5.1	Bloková struktura	21
3.5.2	Vstupně/výstupní porty	22
3.5.3	Přerušení	22
3.5.4	Časovač/čítač	22
3.5.5	Sběrnice I ² C	22
3.5.6	Vývojové prostředí	23
4	Vývojový kit EvB 5.1	24
5	NFC karty	26
6	Postup vypracování	27
6.1	Odesílání SMS	32
6.2	Logický analyzátor	33
6.3	Internet – FTP	34
6.4	Čtečka NFC	35
6.5	Odesílání dat na server	38
6.6	Nahrávání SW do vývojového kitu	38
6.7	Program a knihovny	39
6.7.1	lcd.c	39
6.7.2	Shamir.c	39
6.7.3	aes256.c	40
6.7.4	pn532_spi.c	40
6.7.5	uart.c	40

6.7.6	sim900.c	41
7	Program - server	42
8	Závěr	44
	Literatura	45
	Seznam symbolů, veličin a zkratk	48
	Seznam příloh	50
A	Ukázka průběhu komunikace	51

SEZNAM OBRÁZKŮ

2.1	Blokové schéma	11
2.2	LCD displej 9" s řadičem a kabely	12
2.3	Raspberry Pi B+ [2]	13
2.4	NFC kit od firmy NXP [3]	14
2.5	SIM900 GSM [5]	15
3.1	Blokový diagram zapojení	16
3.2	čtečka karet PN532	17
3.3	Čtečka karet RC522	18
3.4	LCD 16x2 s modrým podsvícením [8]	18
3.5	Příklad zapojení LCD displeje s HD47780 [9]	19
3.6	Pohled na modul RTC s DS1307 [11]	20
3.7	Pouzdro TQFP44 ATmega644 s popisem vývodů a reálné foto [12] [13]	20
3.8	Blokové schéma ATmega644 [12]	21
3.9	Pracovní prostředí AtmelStudio, náhled programu	23
4.1	Vývojový kit EVB 5.1 [19]	25
5.1	Struktura uspořádání paměti karty Mifare classis 1K [24]	26
6.1	Komunikace s GSM modulem přes Hyperterminal	27
6.2	Napěťové úrovně komunikace RS232 a UART [25]	28
6.3	Připojení USB-RS232 převodníku k GSM modulu	28
6.4	Odhalena chyba ve schématu, prohozen řídicí signál s napětím pro pullup	29
6.5	Ovládání GSM modulu pomocí AT Command Tester	30
6.6	SIM900 Series download Tools Develop 1.9	31
6.7	Logický analyzátor Saleae a jeho klon [26] [27]	33
6.8	Vývojový kit, čtečka PN532, USBasp programátor, logický analyzátor	36
6.9	NFC čtečka ACR122, pokusné karty a čipy	36
6.10	Obslužný program pro NFC čtečku ACR122	37
6.11	Vývojový kit napájený z power bank, GSM modul, čtečka PN532	38
7.1	XAMPP ovládací okno	42
7.2	Ukázka záznamů načtených karet v PHPMyAdmin	43
A.1	Průběh celé komunikace TX, RX a detailnější pohled na průběh	51

SEZNAM TABULEK

3.1	Porovnání RC522 a PN532 [6]	17
6.1	Seznam zkoušených firmware pro SIM900A	30
6.2	Formát odeslání obsahu SMS do SIM900	32

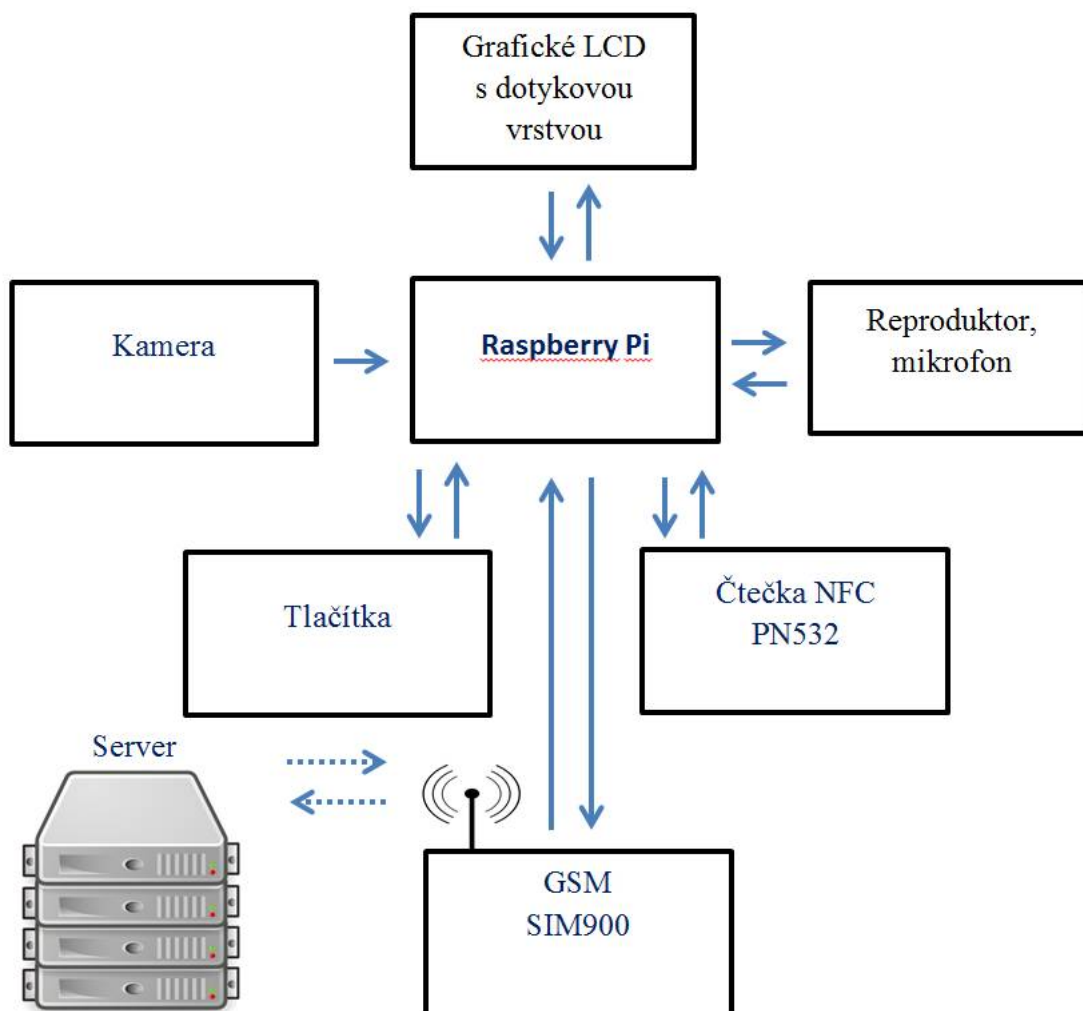
1 ÚVOD

Požadavkem zadavatele bylo navrhnout dvě zařízení pro osobní identifikaci a sdílení dat, včetně softwaru. První varianta, nazvaná jako informační kiosk obsahuje grafický displej s dotykovou vrstvou, čtečku NFC, komunikační GSM modul. Jako vhodné řešení se nabízí Raspberry Pi. Informační kiosk může disponovat podáním informací o dané lokalitě, o profilu spárovaného s kartou a dle projektu může obsahovat webovou kameru s mikrofonom a přídatným reproduktorem. Druhá varianta - logger, obsahuje čtecí zařízení pro NFC karty, signalizační diody nebo displej a GSM modul pro odesílání informací na server. Může být napájena ze solárního panelu. Logger slouží převážně k načtení karty, zobrazení informace, zda proběhlo vše v pořádku. Veškeré údaje se posílají na server.

Pro prvotní otestování systému byla vybrána varianta číslo dvě, jejíž konstrukce je popsána v kapitole 3. Zařízení najde využití ve městech pro poskytnutí informací o daném místě, při hrách či závodech, kde je zapotřebí zaznamenat dosažení daných kontrolních bodů (takzvaných "checkpointů"). Dále projekt může být dalším rozšířením známé celosvětové hry Geocaching. Kde nalezení cache, lidově kešky, může být online monitorované s možností pořízení fotografie nálezce.

2 VARIANTA 1 - INFORMAČNÍ KIOSEK

Tato varianta bude obsahovat grafický displej s dotykovou vrstvou. Kamerou pro možné vytvoření fotografie návštěvníka či soutěžícího. Řídící jednotkou bude mini-počítač Raspberry Pi. GSM a NFC modul bude stejný jako u levnější varianty.



Obr. 2.1: Blokové schéma

2.1 LCD pro Raspberry Pi

Raspberry Pi obsahuje HDMI konektor pro připojení LCD, což umožňuje připojení téměř jakéhokoliv monitoru. Pro naše využití bude dostačující LCD monitor o úhlopříčce 7-9", ale dle přání koncového zákazníka může být nahrazen za jiný. Například 7" monitor s dotykovou vrstvou se dá při aktuálním kurzu (25 Kč/USD) zakoupit za 1.620,-, napájení a data z dotykové vrstvy jsou přes USB.



Obr. 2.2: LCD displej 9" s řadičem a kabely

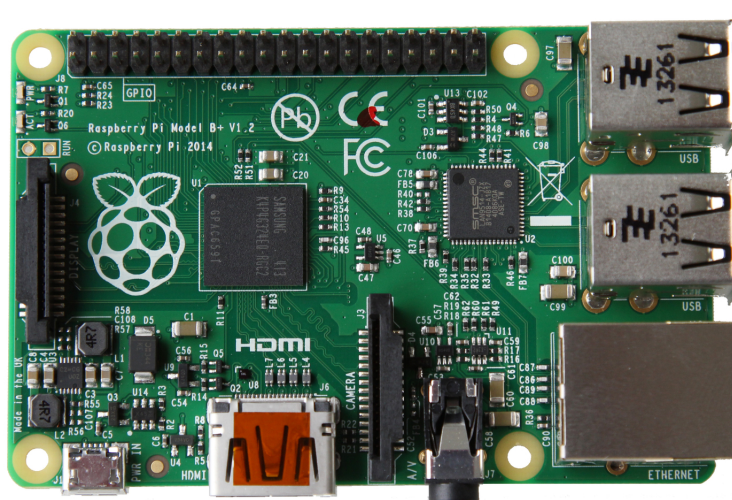
2.2 Raspberry Pi

Deska Raspberry Pi (Obr. 2.3) vynalezli ve Velké Británii, původem měla sloužit především za účelem zlepšení školní výuky programování na britských školách. Parametry jsou skvělé, rozměry 8,5 x 5,5 cm, svojí otevřeností vzniklo nemálo aplikací této desky a využívá se dokonce i pro řízení dronů. Poměr cena/výkon výborná. V současné době se prodává od 700,- do 1.200,- dle provedení. Vývoj trval bezmála 6 let, první kusy byly k dostání od 29. února 2012 ovšem pouze pro Velkou Británii. Do České republiky první desky Raspberry Pi dorazily zhruba o 2 měsíce později [1]

Vytvářet podobnou desku v tomto případě nepřipadá v úvahu, vyšlo by to drahé a s nejistými výsledky. Následující parametry platí pro novější verzi označenou A+ a B+, které vznikly až v roce 2014. Letos bude v prodeji již 3. generace desky.

Společné parametry:

- jednojádrový procesor Broadcom BCM2835 s mikrokontrolérem ARM1176JZF - z rodiny ARM11 taktovaný na 700 MHz
- HDMI výstup
- Audio část A/V jacku
- 40 GPIO
- slot na MicroSD kartu
- MPI CSI-2 konektor pro Raspberry Pi HD videokameru

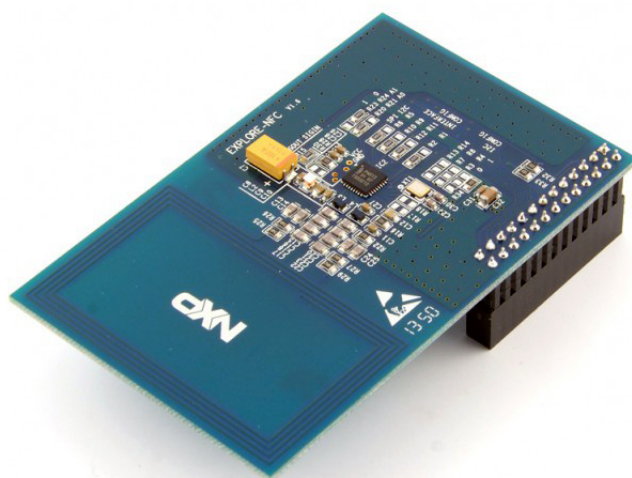


Obr. 2.3: Raspberry Pi B+ [2]

Raspberry Pi se vyrábí ve dvou variantách A a B. Od sebe se liší rozměry, počtem USB, LAN a velikostí paměti. Varianta A nemá LAN konektor, je osazena 256 MB a má 1x USB. Cena \$20. Varianta B obsahuje LAN konektor, je osazena 512 MB a má 4x USB. Cena \$35.

2.3 NFC čtecí modul pro Raspberry Pi

V dnešním světě se NFC používá jak v identifikačních kartách tak i v mobilních telefonech. Snahou je využít tyto prostředky i pro další aplikace. Díky této technologii můžeme i přenášet data, čehož se dá využít u informačních kiosků a nebo ukládat informace na karty. Komunikační anténu lze snadno navrhnout a vyrobit na DPS. Komunikační vzdálenost je závislá na kvalitě antény, při dobrém návrhu až do 70 mm. Komunikace vybraného obvodu PN532 od firmy NXP je pomocí I2C nebo SPI. [4]



Obr. 2.4: NFC kit od firmy NXP [3]

- rozhraní: SPI a I2C
- osazena čipem NXP PN532
- umožňuje 3 módy: Reader, P2P and Card Emulation
- čtecí vzdálenost 20 až 70 mm
- komunikační frekvence 13,56 MHz

2.4 GSM modul pro Raspberry Pi

Firma SIMCom Wireless Solutions (SIMCom) rozšířila svoji nabídku o dosud nejvýkonnější GSM modul s označením SIM900. Tento miniaturní modul s rozměry jen 24x24x3mm je postaven na procesoru s jádrem ARM923EJ-S a je zhruba dvakrát výkonnější než jeho předchůdce v modulech série SIM300. Mimo to, díky inovativnímu designu modulu je jeho spotřeba zredukována v sleep módu až o 40% v porovnání s průměrem u ostatních výrobců. [4]

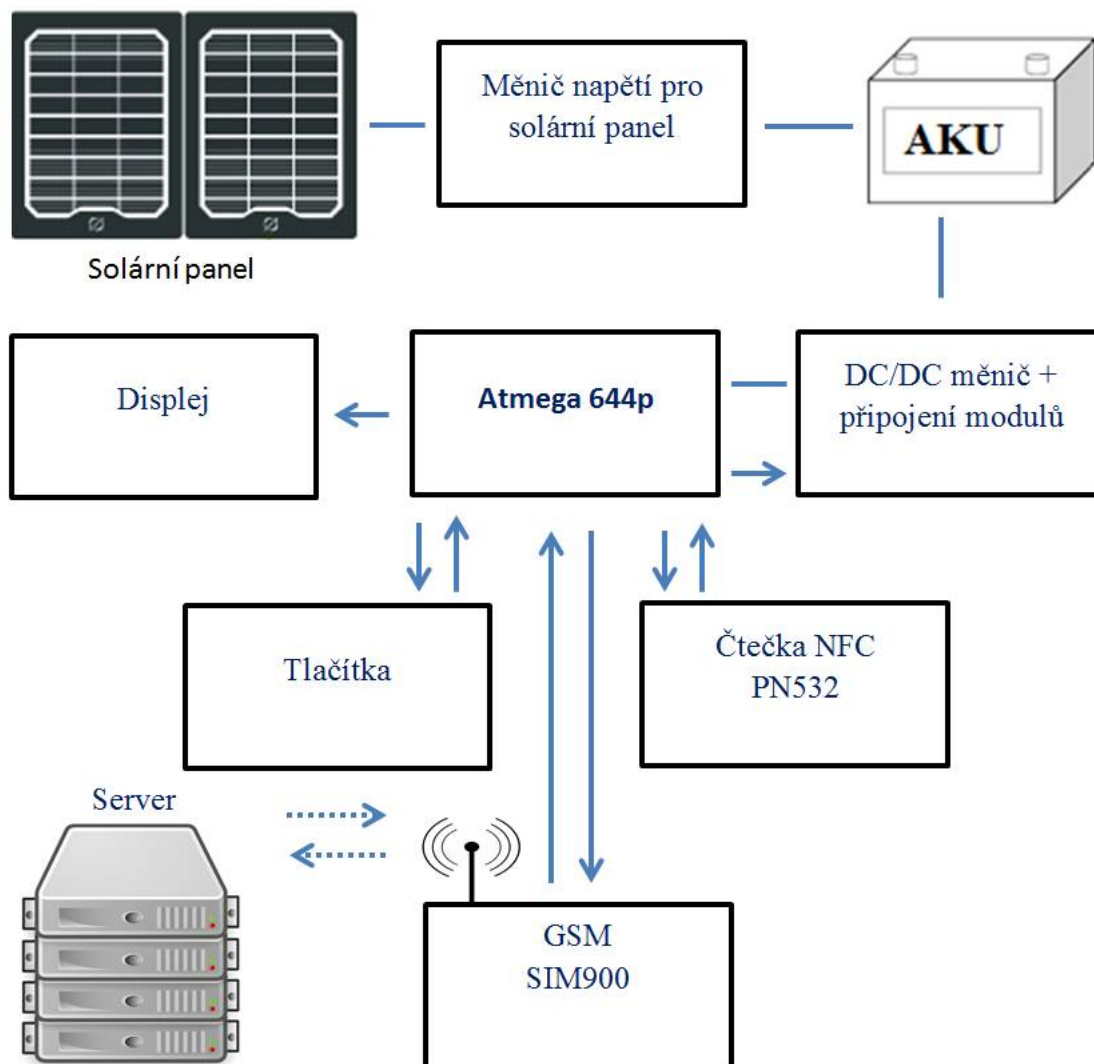


Obr. 2.5: SIM900 GSM [5]

- Quad-Band 850/ 900/ 1800/ 1900 MHz
- GPRS multi-slot class 10/8
- GPRS mobile station class B
- Napájecí napětí 3,4 ... 4,5 V
- nízká spotřeba ve sleep módu

3 VARIANTA 2 - LOGGER

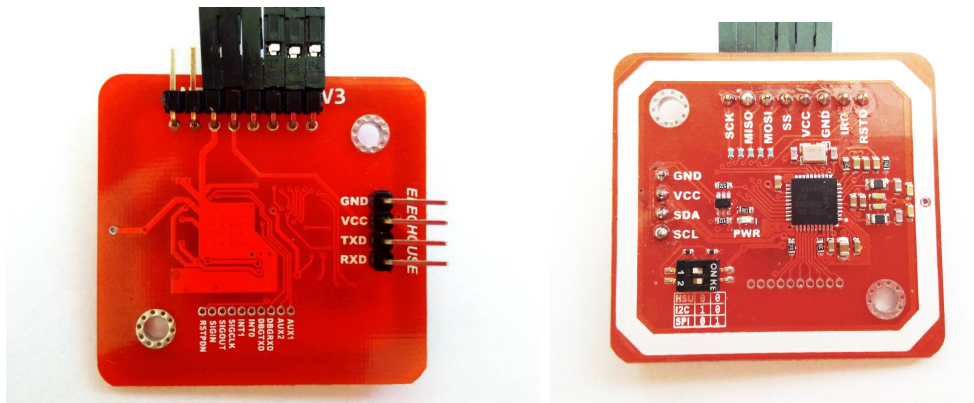
Tato varianta zařízení bude převážně napájena z akumulátoru a solární energie, proto je zapotřebí přizpůsobit spotřebu zařízení na minimum, ale zároveň obsáhnout všechny potřebné funkce. Pro zobrazení informací jsem vybral textový displej s řadičem HD44780, GSM modul, NFC čtečku a řídicí mikrokontrolér ATmega644.



Obr. 3.1: Blokový diagram zapojení

3.1 NFC PN532 mini

Menší verze čtečky karet podporuje i komunikaci UART. Ve své aplikaci jsem zvolil komunikaci SPI, aby každý modul měl svůj kanál. Na přepínači je nutné zvolit správnou kombinaci přepínačů, pro komunikaci SPI musí být nastaveno 01. Čtečka umí simulovat NFC čip a tak zpřístupnit data i pro jiná chytrá zařízení.



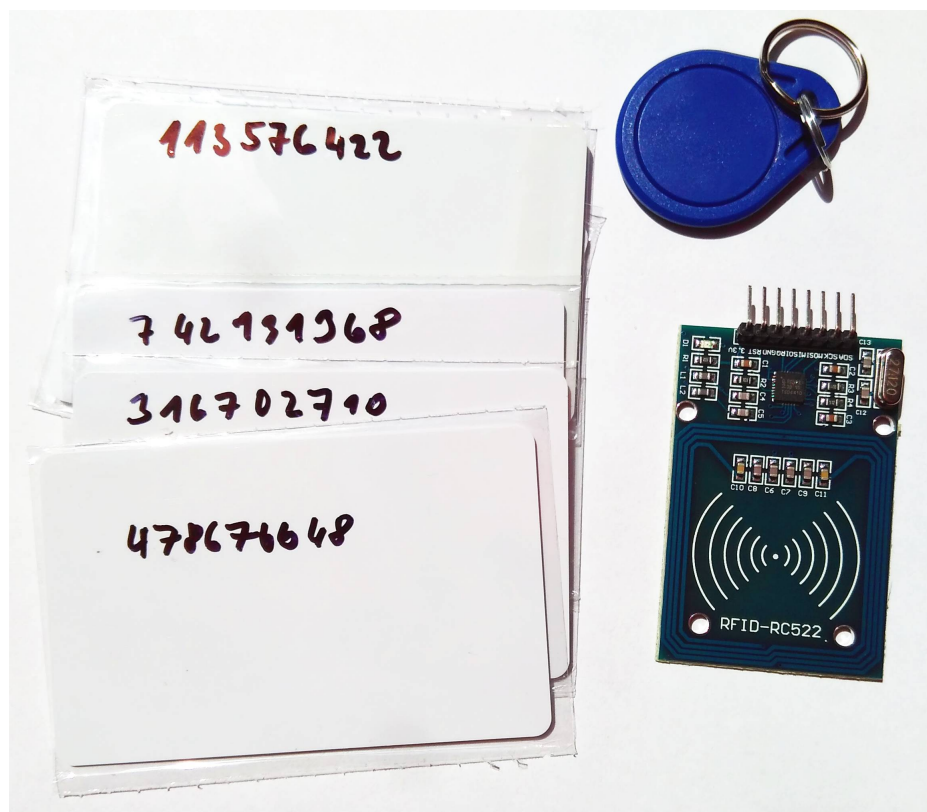
Obr. 3.2: čtečka karet PN532

3.2 Čtečka NFC RC522

Plánoval jsem přidat i možnost připojení čtečky NFC RC522. Komunikace je obdobná jako u PN532. Vzhledem k horším parametrům jsem pro ni zatím nepředělával knihovnu.

Tab. 3.1: Porovnání RC522 a PN532 [6]

	RC522	PN532
Komunikační rozhraní	SPI, I2C, RS232	SPI, I2C, RS232
Modulace	10% 100% ASK	neuvezeno
ISO 14443 A/B	ano/ne	ano/ano
NFC	ano	ano
MIFARE	ano	ano
FELICA	ne	ano
Spotřeba	30/13 mA	60/25 mA



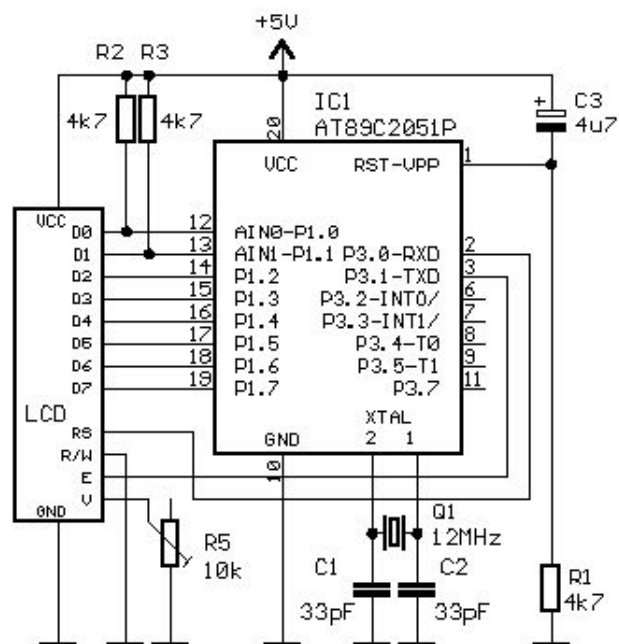
Obr. 3.3: Čtečka karet RC522

3.3 Textový LCD displej

S řadičem HD44780 pracuje naprostá většina znakových displejů. Vyrábějí se provedení od 1x8 znaků do 4x40 znaků. K propojení s jednočipem je třeba 4 nebo 8 datových vodičů, jeden na přepínání zápisu instrukcí / dat (RS) a další s hodinovým signálem (E). Pro případné čtení obsahu displeje je třeba připojit ještě jeden (R/W), jinak je trvale uzemněn. Základní znakovou sadu lze doplnit osmi vlastními znaky, které jsou pak dostupné pod kódy 0-15. [7]



Obr. 3.4: LCD 16x2 s modrým podsvícením [8]



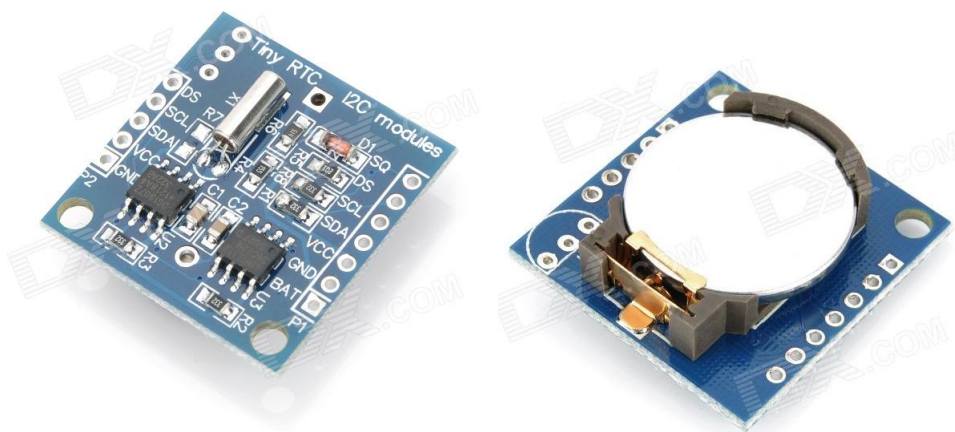
Obr. 3.5: Příklad zapojení LCD displeje s HD44780 [9]

3.4 RTC obvod

DS1307 je obvod reálného času (RTC, Real-Time Clock), který obsahuje 63 bajtů nevolatilní paměti (tedy po odpojení napájení se obsah paměti smaže) a je možné s ním komunikovat pomocí sběrnice I²C. Pokud je připojen k napájení, počítá impulzy z externího oscilátoru a ukládá aktuální hodnoty data a času. V tomto režimu, pokud je připojen pouze k baterii má spotřebu méně jak 500 nA.

Čtení a zápis dat z/do obvodu probíhá pomocí sběrnice I²C s hodinovým kmitočtem 100 kHz. DS1307 se chová jako slave s adresou 1101000 (+ LSB, který určuje směr komunikace — R/W, viz specifikace I²C). Zápis dat do paměti začíná adresou zařízení, počáteční adresou paměťové buňky a nakonec následují samotná data. Čtení dat začíná adresou zařízení a za ním následují příchozí data. Každý odeslaný bajt musí příjemce potvrdit bitem ACK. Celá komunikace přesně odpovídá standardu I²C. Další podrobnosti viz [10].

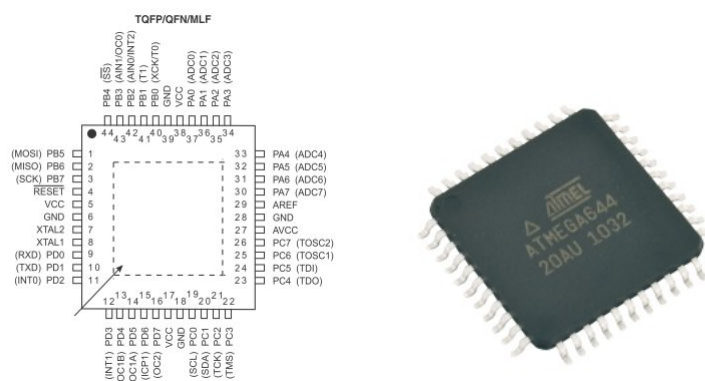
Využití RTC obvodu není v této aplikaci nutné, GSM modul v sobě RTC obvod má. Stačí po spuštění zařízení synchronizovat čas z GSM nebo internetu.



Obr. 3.6: Pohled na modul RTC s DS1307 [11]

3.5 Mikrokontrolér ATmega644

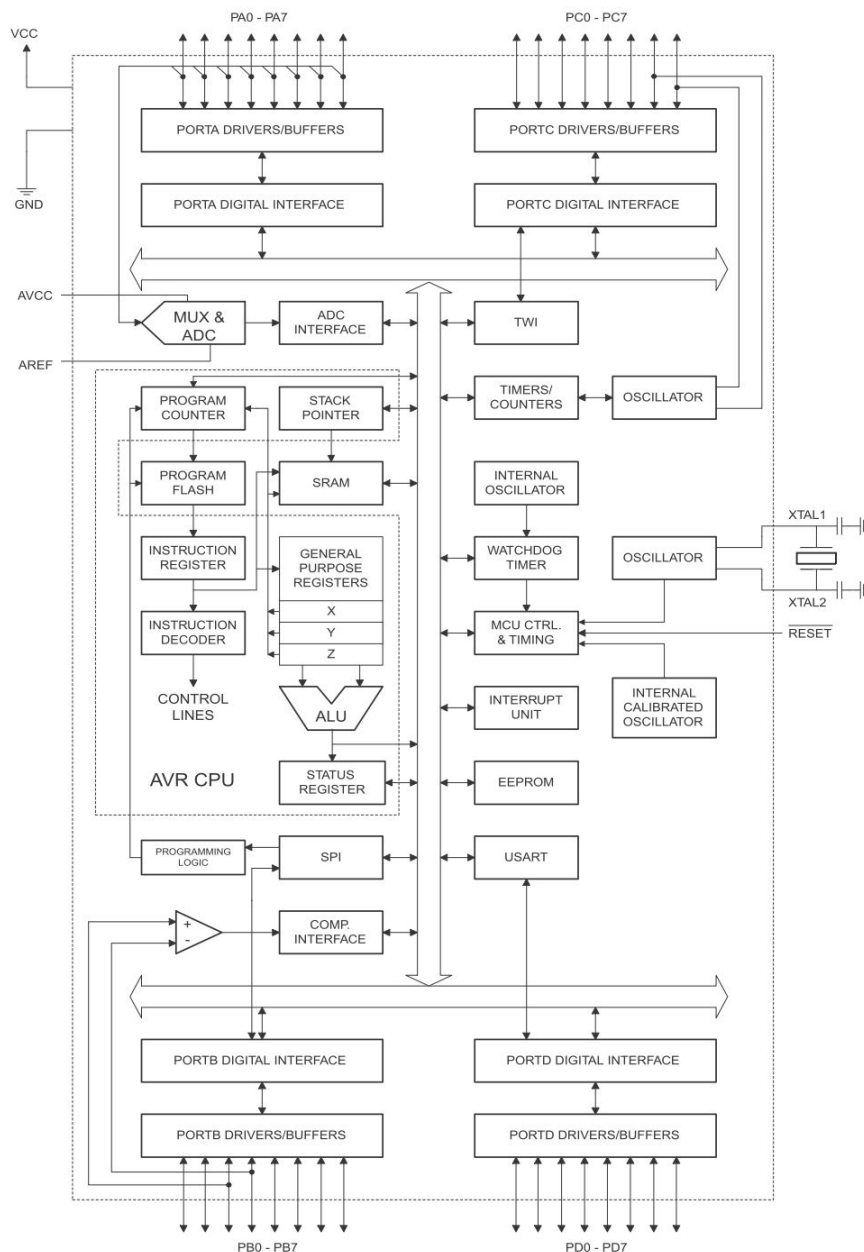
Jako řídicí jednotka byl vybrán od firmy Atmel mikrokontrolér ATmega644. Jedná se o 8 bitový mikrokontrolér s architekturou RISC (omezená instrukční sada, rychlé vykonávání instrukcí). Flash paměť programu je 64 kB, paměť pro výpočty SRAM 4 kB a paměť EEPROM 2 kBytů. Počet vstupních a výstupních pinů je 32 rozdělených do 4 portů označených písmeny A až D. Některé vývody jsou určeny pro speciální využití jako je A/D převodník, analogový komparátor, UART, čítač nebo časovač a přerušování (IRQ). Dále lze využít 16-bitový časovač/čítač a dva 8-bitové. Nabízí se využití vnitřního oscilátoru 1 MHz nebo externího oscilátoru/kryystalu do maximální velikosti 8 MHz při napájení 3,3 V.



Obr. 3.7: Pouzdro TQFP44 ATmega644 s popisem vývodů a reálné foto [12] [13]

3.5.1 Bloková struktura

Během návrhu připojení k periférii k mikrokontroléru ATmega644 se musíme podívat na vnitřní zapojení. Některé vývody mají speciální zaměření, příkladem může být port A, který lze využít pro A/D převodník.



Obr. 3.8: Blokové schéma ATmega644 [12]

3.5.2 Vstupně/výstupní porty

Porty mohou sloužit jako vstupní i jako výstupní. Jejich funkce se nastavuje registry. Každý registr obsluhující daný port nese jeho číselné označení. Jsou to: **DDRX** -> **DATA DIRECTION REGISTER** Určuje směr toku dat – vstup/výstup **PORTX** Datový registr – stav pinů portu odpovídá hodnotě zapsané do registru **PINX** Určen pouze pro čtení, odpovídá aktuální hodnotě na pinech

Porty jsou tedy obousměrné, pro každý směr využíváme jiného datového registru. Směr nastavujeme registrem DDRX, přičemž X značí číslo portu (1, 2, 3...). Log. 1 nastavuje port jako výstupní, log. 0 jako vstupní (tedy přesně obráceně, než je tomu u procesorů PIC) [14].

3.5.3 Přerušení

Přerušení je reakce procesoru na určitou vnitřní nebo vnější událost. Například přetečení čítače/časovače, přijmutí bajt sériovým kanálem, změna stavu na pinu procesoru a jiné. Umožňuje, aby se normální běh programu přerušil a pokračoval na jiném místě vykonáním obslužné rutiny. Po jejím vykonání se program vrátí zpět na místo, odkud byl přerušen [15].

3.5.4 Časovač/čítač

Procesory ATMEGA644 obsahují celkem tři čítače/časovače. Dva osmibitové, jeden šestnáctibitový. Vstupní signály mohou být vyděleny předřazenou předděličkou, a to v hodnotách 1;8;64;1024 [16].

Čítače časovače nastavujeme speciálními registry. Zde je jejich krátký výčet:

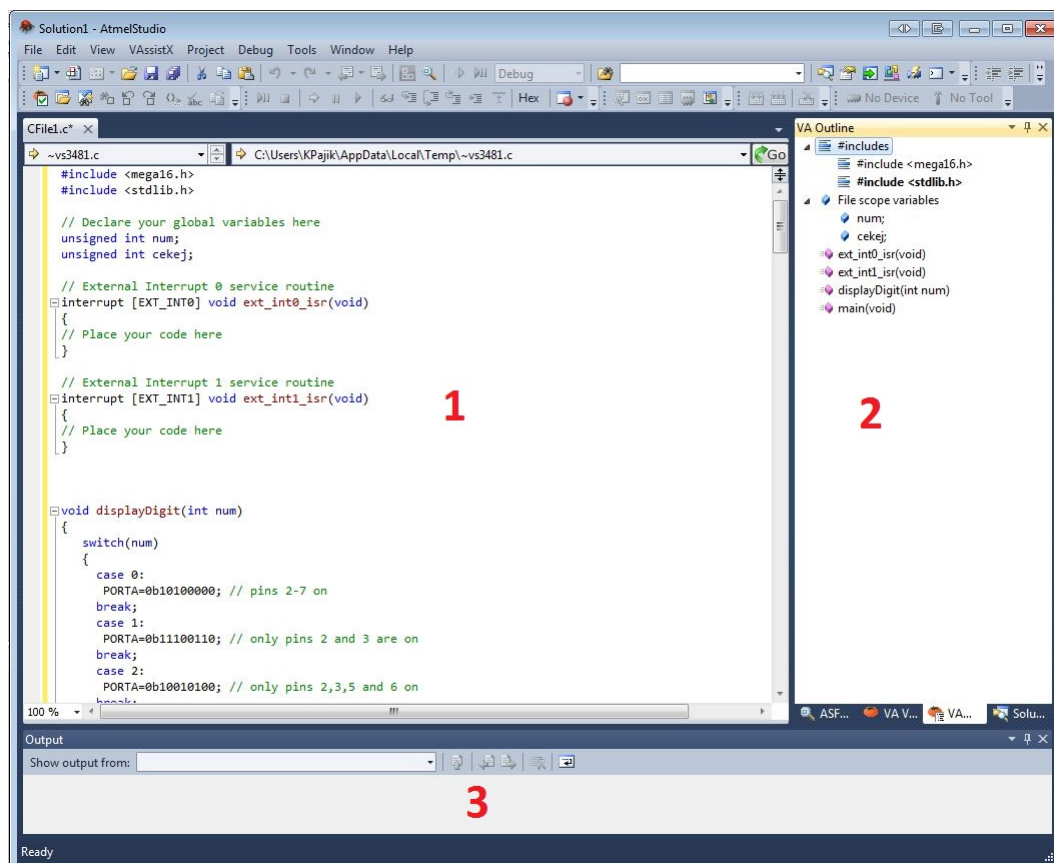
- TCNT(N) – obsahuje načítanou hodnotu
- OCR(N) – obsahuje hodnotu, s níž se TCNT(N) porovnává
- TCCR(N) – řídí funkce čítače/časovače
- TIMSK – masky přerušení

3.5.5 Sběrnice I²C

Sběrnice rozděluje připojená zařízení na řídicí (master – zahajuje a ukončuje komunikaci; generuje hodinový signál SCL) a řízené (slave – zařízení adresované masterem) [17]

3.5.6 Vývojové prostředí

Existuje mnoho vývojových prostředí pro mikrokontroléry programované v jazyce C. Ne mnoho jich je zdarma včetně kompilátoru. Zvolil jsem Atmel Studio¹, které je zdarma a je přímo od výrobce mikrokontroléru. Podporuje psaní v assembleru, C a C++.



Obr. 3.9: Pracovní prostředí AtmelStudio, náhled programu

Oblast zdrojového kódu (1) - zde je psán samotný kód programu

Průvodce projektu (2) - přehled importovaných souborů v projektu a metod otevřeného souboru

Výpis z kompilátoru (3) - výpis průběhu kompilátoru, varování a chyby v kódu.

¹odkaz ke stažení: http://www.atmel.com/microsite/atmel_studio6/

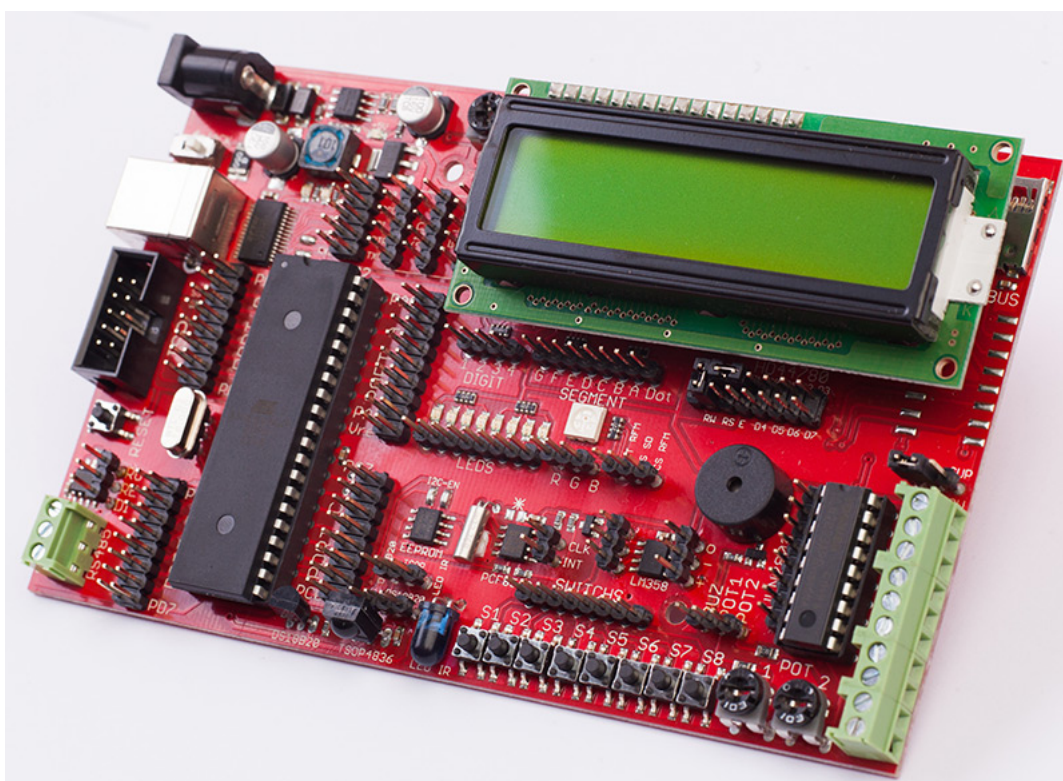
4 VÝVOJOVÝ KIT EVB 5.1

Během několika mých předchozích projektů se mi osvědčilo využívání vývojového kitu EvB 5.1, který má následující parametry: [18]

- Procesor AVR ATmega32 (nebo ATmega 644p)
- výměnný krystal pro mikrokontrolér, standardní dodávaný krystal 16MHz
- Obvod reálného času PCF8563
- Paměť EEPROM AT24C02
- Infračervený přijímač TSOP4836
- Infračervený vysílač LL-503IRT2E (LuckyLight)
- Teplotní čidlo DS18B20
- Převodník sběrnic RS485/RS232 - SN75176BP
- Patice (slot) pro kartu micro MMC/SD
- Patice pro RF modul RFM12B
- 8 tlačítek
- 8 indikačních LED diod
- 1 dioda RGB (Everlight 61-23RGBC/TR8)
- 2 potenciometry pro nastavení napětí
- 4 x sedmisegmentový LED zobrazovač
- 8 x výkonový výstup s otevřeným kolektorem ULN2803
- 1x operační zesilovač LM358
- podsvětlený displej LCD 2x16 znaků (zelený, modrý, černý)
- USB konektor
- ISP10 programovací konektor
- přepínač pro zdroj napájení – externí konektor / USB
- spínaný zdroj 5V
- lineární zdroj 3.3V

Pro mě je výhodou vyvedení veškerých pinů mikrokontroléru a možnost připojení periférií na kterýkoliv pin. Verze EVB 5.1 oproti starší verzi EVB 4.3 má dvě řady pinů. Toho jsem využil především při ladění programu a odposlouchávání komunikace. Logický analyzátor je popsán v kapitole 6.2 na straně 33.

Na vývojovém kitu jsem využil RS232, tlačítka, displej, AD převodník a komunikaci přes RS232, SPI a UART.



Obr. 4.1: Vývojový kit EVB 5.1 [19]

5 NFC KARTY

Bezkontaktní čipové karty MIFARE spadají do kategorie Proximity Integrated Circuit Card, což je obecný název pro bezkontaktní integrovaný obvod, který se používá například pro zabezpečený přístup, nebo platební systém. Na trhu se tyto karty poprvé objevily v roce 1994 a jejich jediným výrobcem je společnost NXP Semiconductors.[20]

Princip fungování MIFARE technologie je téměř stejný jako u RFID, nacházíme zde ale několik zásadních vylepšení. Mezi největší výhody patří zejména větší paměť a vyšší úroveň zabezpečení. Veškerá komunikace, která probíhá mezi kartou a čtečkou, je šifrovaná. Pro přístup k paměťovým blokům je nutné znát příslušný kryptografický klíč. [21]

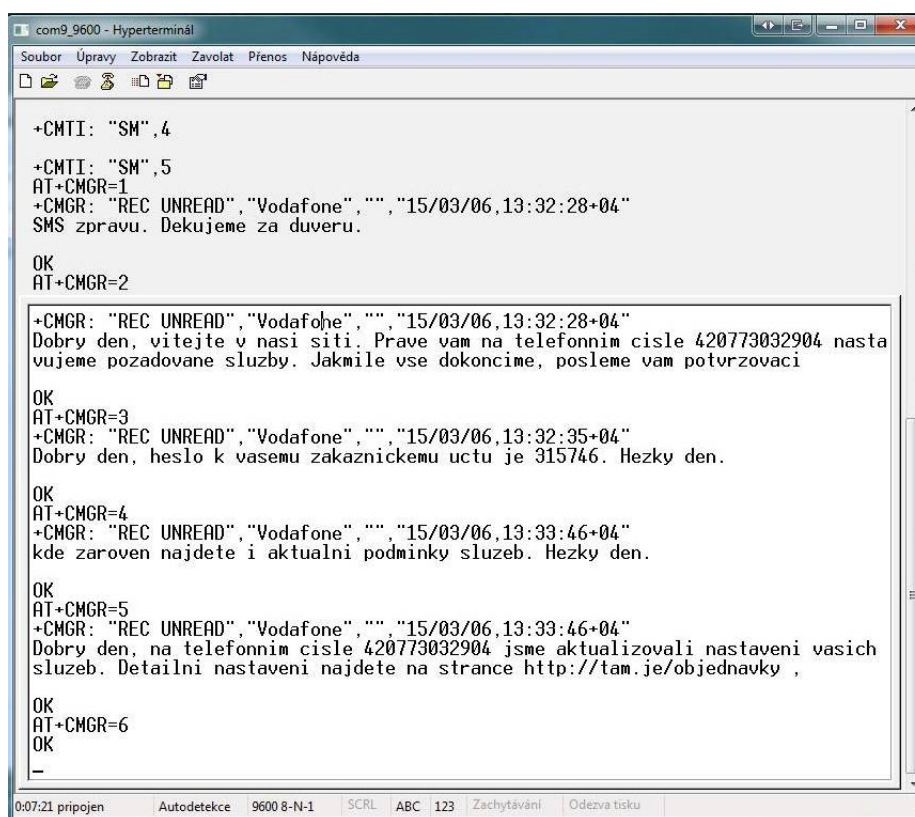
Stejně jako RFID, i MIFARE čipy používají identifikační číslo, které je ale jen 32bitové. Pracovní frekvence, na které probíhá veškerá komunikace je již stejná – 13,56 MHz. Základní komunikační rozhraní karet je kompatibilní se standardem ISO/IEC 14 443 A. V současnosti se můžeme setkat se dvěma nejobvyklejšími typy karet z hlediska kapacity. Jedná se o 1 kB a 4 kB. Tato dostupná paměť se dělí do bloků po 16 bajtech, které se poté sdružují do takzvaných sektorů [22] [23]

Číslo bytu		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Sektor 0	Blok 0	Seriové číslo				X	Tovární data										
	Blok 1																
	Blok 2																
	Blok 3	Klíč A					Bity přístupu					Klíč B (volitelný)					
Sektor 1	Blok 0																
	Blok 1																
	Blok 2																
	Blok 3	Klíč A					Bity přístupu					Klíč B (volitelný)					
⋮	⋮	⋮															
⋮	⋮	⋮															
⋮	⋮	⋮															
Sektor 15	Blok 0																
	Blok 1																
	Blok 2																
	Blok 3	Klíč A					Bity přístupu					Klíč B (volitelný)					

Obr. 5.1: Struktura uspořádání paměti karty Mifare classis 1K [24]

6 POSTUP VYPRACOVÁNÍ

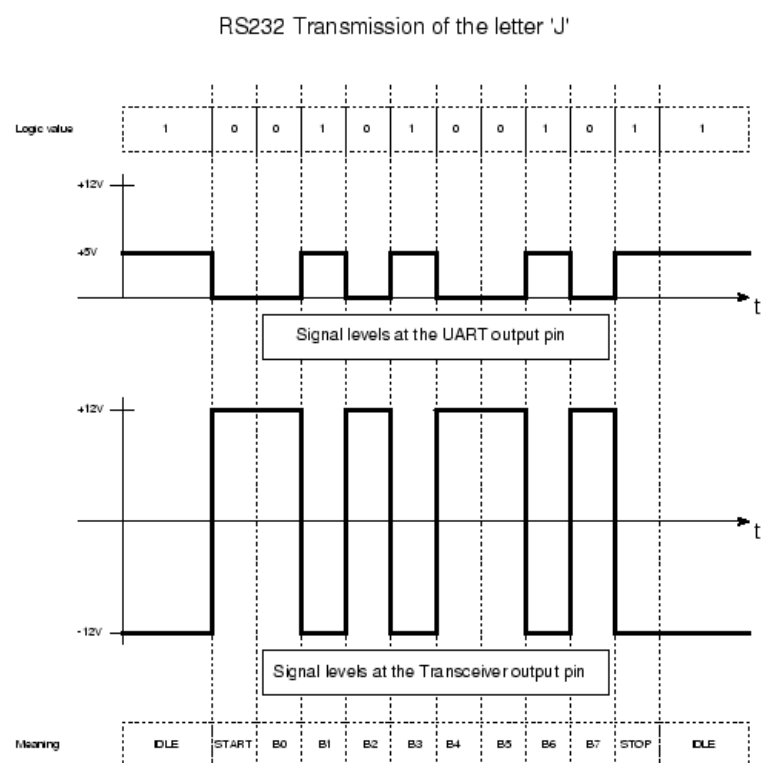
Veškeré komponenty byly kvůli ceně objednány z Číny, přes aukční server Ebay. Což mi na druhou stranu způsobilo velké oddálení začátku práce. Jakmile přišly zakoupené moduly, dal jsem se do psaní programu do kontroléru. Předpokládal jsem, že nejtěžší část programování bude ovládat modul SIM900 (dále jen GSM modul), samotný obvod umí většinu funkcí celého telefonu – přijímat a odesílat SMS i MMS, zavolat i přijmout hovor, ovládat vyzvánění, LCD displej, maticovou klávesnici a tak dále. I samotné nastavení se nejevilo v začátcích nejllehčí. GSM modul komunikuje po UARTu 3,3 V/5 V nebo přes RS232. Níže je graficky znázorněn rozdíl mezi UART 5 V a RS232.



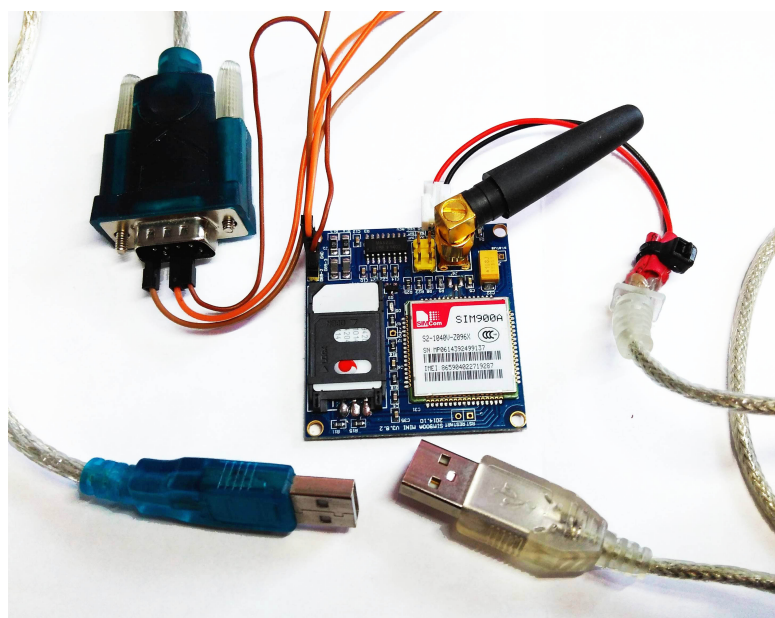
```
+CMTI: "SM",4
+CMTI: "SM",5
AT+CMGR=1
+CMGR: "REC UNREAD","Vodafone","", "15/03/06,13:32:28+04"
SMS zprávu. Dekujeme za duveru.
OK
AT+CMGR=2
+CMGR: "REC UNREAD","Vodafone","", "15/03/06,13:32:28+04"
Dobry den, vitezte v nasi siti. Prave vam na telefonnim cisle 420773032904 nastavujeme pozadovane sluzby. Jakmile vse dokoncime, posleme vam potvrzovací
OK
AT+CMGR=3
+CMGR: "REC UNREAD","Vodafone","", "15/03/06,13:32:35+04"
Dobry den, heslo k vasemu zakaznickemu uctu je 315746. Hezky den.
OK
AT+CMGR=4
+CMGR: "REC UNREAD","Vodafone","", "15/03/06,13:33:46+04"
kde zaroven najdete i aktualni podminky sluzeb. Hezky den.
OK
AT+CMGR=5
+CMGR: "REC UNREAD","Vodafone","", "15/03/06,13:33:46+04"
Dobry den, na telefonnim cisle 420773032904 jsme aktualizovali nastaveni vasich sluzeb. Detailni nastaveni najdete na strance http://tam.je/objednavky
OK
AT+CMGR=6
OK
-
```

Obr. 6.1: Komunikace s GSM modulem přes Hyperterminal

Komunikaci po RS232 jsem znal jen teoreticky, tedy nejprve jsem zkusil komunikaci z počítače: USB převodník na RS232, RS232 - UART - SIM900. Na odesílaný znak jsem neobdržel žádnou odpověď. Tím jsem musel udělat krok zpět a ověřit, zda počítač správně komunikuje přes RS232. Napsal jsem jednoduchý program do vývojového kitu pro vytváření ozvěny. Tedy co přijme, odešle zpět. Komunikace proběhla v pořádku.

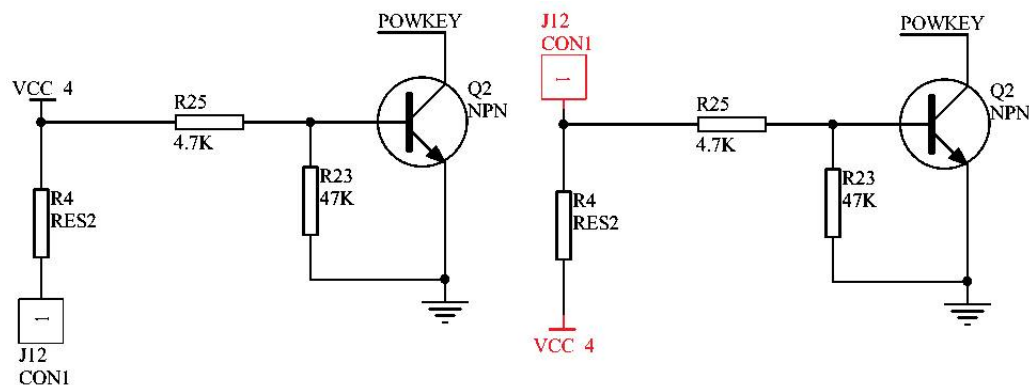


Obr. 6.2: Napětové úrovně komunikace RS232 a UART [25]



Obr. 6.3: Připojení USB-RS232 převodníku k GSM modulu

Chyba musela být na straně GSM modulu. Prostudoval jsem schéma GSM modulu a narazil na prohození konektoru pro připojení a napájení pullup rezistoru, naštěstí tato chyba byla jen ve schématu a na plošném spoji to bylo v pořádku. Dále jsem ze zkušeností zkusil přeletovat většinu spojů cesty mezi RS232 a SIM900A čipem, evidentně byl někde studený spoj nebo nedostatek pájky a problém s komunikací jsem vyřešil. Odpověď „OK“ na příkaz „AT“ byl pro mne již slibným začátkem. Následovalo zkoušení dalších a dalších příkazů.



Obr. 6.4: Odhalena chyba ve schématu, prohozen řídicí signál s napětím pro pullup

Stále zůstávala simkarta neaktivní a nebylo z ní možné odesílat ani přijímat hovory či SMS. PIN kód jsem telefonem vypnul, ale stále to nechodilo. Po delším pátrání jsem došel k možnosti problému evropského a čínského firmware.

Se seznámením příkazů pro GSM modul mi pomohla stránka M2MSupport¹. Prostředí je napsané v Javě a je dostupný v online i offline verzi. Na začátku stačí vybrat správný COM port a komunikační rychlost. Aplikace podporuje GSM moduly Simcom, Telit a Quectel. Před použitím je nutné jako u mobilního telefonu odblokovat SIM kartu zadáním PIN kódu. Slouží pro to příkaz "AT+CPIN=xxxx", kde xxxx je 4-6ti místný PIN kód.

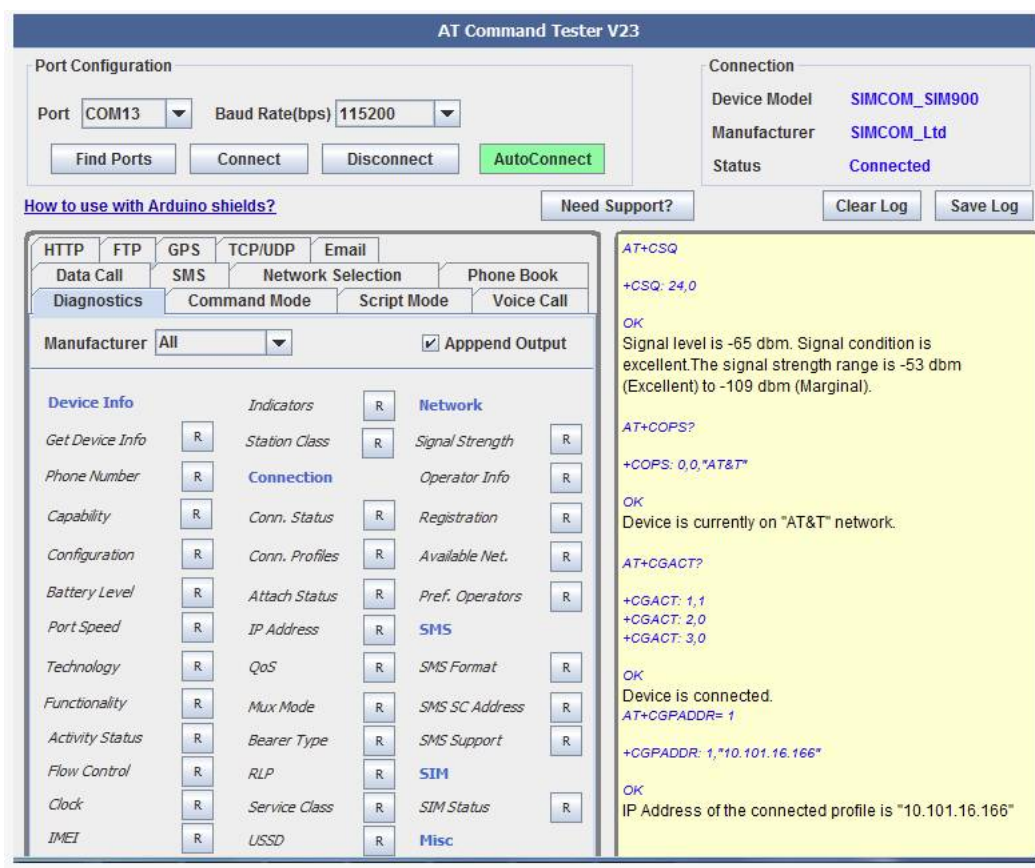
V tomto kroku jsem zkoušel možnosti GSM modulu a potřebné příkazy pro využití mobilního internetu. Ani po správném zadání PINu nedošlo k aktivaci SIM karty, nebylo možné přijímat SMS či hovory. Na internetu jsem dohledal možný problém ve firmware.

Při pročítání různých diskuzních fór jsem našel odkaz na blog², kde je možné stažení různých verzí firmware. Je zde v aktuální době dostupných 14 verzí firmware pro SIM900 a 6 verzí pro SIM900A. Dle článku³, pro evropské pásmo je nutné

¹odkaz na Java aplikaci: <http://m2msupport.net/m2msupport/module-tester/>

²odkaz na blog: <http://dostmuhammad.com/blog/sim900-firmware-update-tutorials-appnotes>

³odkaz na stránky: <http://amichalec.net/2014/08/sim900a-fixed-for-europe>



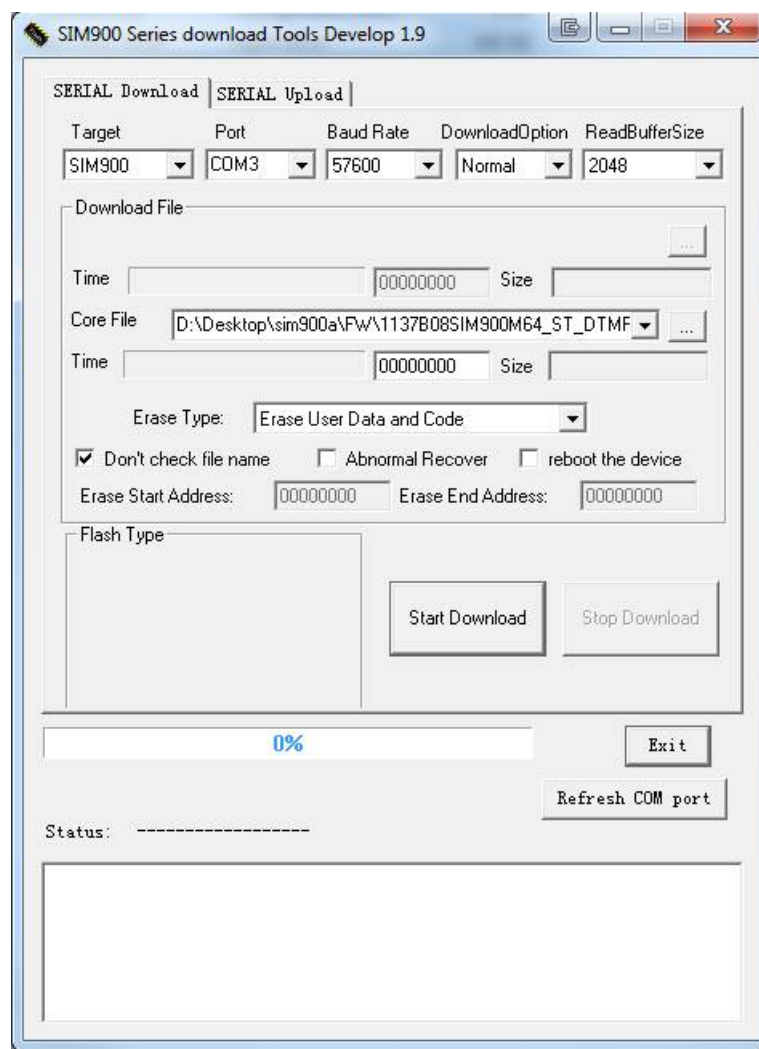
Obr. 6.5: Ovládání GSM modulu pomocí AT Command Tester

využít firmwaru pro starší model čipu, tedy SIM900. Prvním zkoušeným firmware byl 1137B01SIM900M64_ST_ENHANCE, pomocí kterého mi začaly chodit hlasové a textové služby, internet nikoliv. V tabulce 6.1 uvádím testované firmware. Bohužel se mi nepodařilo na internetu najít jejich porovnání, ani u výrobce. Zkoušení funkčnosti proběhlo metodou pokus-omyl.

Tab. 6.1: Seznam zkoušených firmware pro SIM900A

Označení firmware	Hov. a SMS	Internet
1137B03SIM900A64_ST_ENHANCE	ne	ne
1137B01SIM900M64_ST_ENHANCE	ano	ne
1137B08SIM900M64_ST_DTMF_JD_MMS	ano	ano
1137B03SIM900A64_ST_ENHANCE	ne	ne
1137B13SIM900A64_ST_DL	ne	ne

Pro nahrávání firmware doporučuji program SIM900 Series download Tools Develop 1.9⁴ Pro programování je zapotřebí připojit GND na RST pin (vyvedeno stranou)



Obr. 6.6: SIM900 Series download Tools Develop 1.9

⁴odkaz ke stažení: <https://drive.google.com/file/d/0B-rBpaSGS0dnMzQ/edit>

6.1 Odesílání SMS

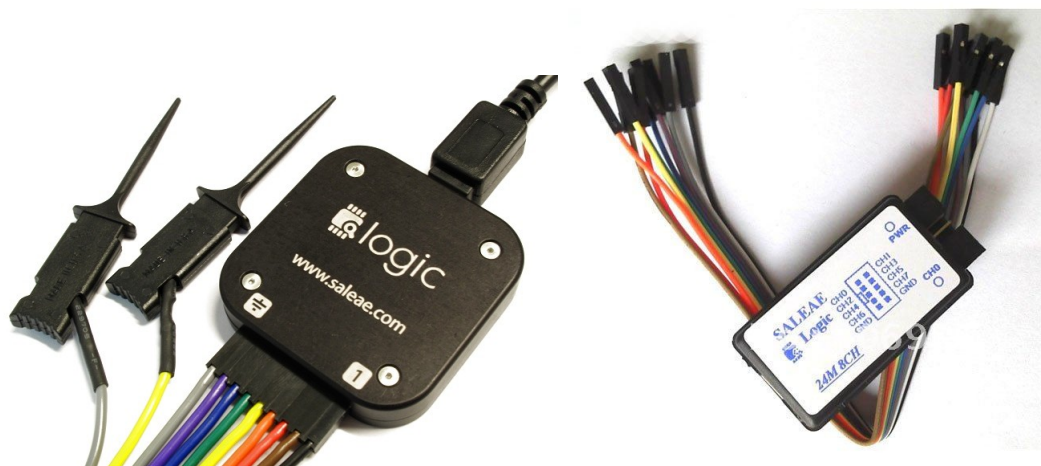
Pro odesílání SMS můžeme využít dvou způsobů, hexadecimální PDU nebo klasické odeslání řetězce. Standardně je nastavený příjem PDU pro odesílání sms. Pro snazší porozumění byla změněna původní hodnota na textový režim. Pro zjištění aktuálního nastavení slouží příkaz „AT+CMGF=?“, nastavení: 0 pro PDU mode, 1 pro Text mode

Tab. 6.2: Formát odeslání obsahu SMS do SIM900

Hexadecimal PDU Message	7/8/16 Bit PDU Message (readable)
07911356131313F311000A926021436 5870000AA0A41F45B0D9ADBCBF432	SMSC#+31653131313 Sender:0612345678 TP_PID:00 TP_DCS:00 TP_DCS-popis:Uncompressed Text class:0 Alphabet:Default Ahoj svete Length:10

6.2 Logický analyzátor

Během vývoje se stává, že zařízení nefunguje správně a je zapotřebí zanalyzovat probíhající komunikaci mezi mikrokontrolérem a moduly. Mně se osvědčilo využívání logického analyzátoru. Software je zdarma a funguje i s neoriginálním zařízením (klonem). Použití je snadné a při troše znalosti programu je možné nastavit i překlad komunikace.



Obr. 6.7: Logický analyzátor Saleae a jeho klon [26] [27]

Zaznamenané průběhy komunikace jsou umístěny v příloze na straně 51

Veškeré naměřené průběhy je možné ukládat a případně porovnávat. Toho jsem využil v případě, kdy mi při odeslání příkazů z počítače GSM modul vytvořil na FTP serveru soubor včetně dat v pořádku, ale při odeslání stejných příkazů z mikrokontroléru se soubor nevytvořil. Příkaz pro vytvoření souboru byl odeslán, vrátil se mi zpět do mikrokontroléru, ale vykonán a potvrzen byl až s 1,2 sekundy později. Během té doby nelze zadávat další operace a to jsem nedodržel. Problém jsem odstranil delší prodlevou k následujícímu příkazu. Viz následující kapitola.

6.3 Internet – FTP

Komunikaci s FTP serverem jsem opět ověřil pomocí webové stránky M2MSupport⁵. Celkem neobvyklým jevem se mi zdála nutná konfigurace APN před každým spojením s Internetem. Pro Vodafone internet musí být hodnota APN „internet“. Výpis komunikace pro vytvoření souboru na FTP (T - Transmit, R - Receive):

```
1 14.973 s
2 T: AT+SAPBR=4,3\r\n
3 R: AT+SAPBR=4,3\r\n\r\n
4 R: +SAPBR: "\r\nCONTYPE:"GPRS\r\nAPN="\r\nPHONENUM: "\r\nUSER: "\r\nPWD: "\r\nRATE: "2\r\n\r\nOK\r\n
5 24.140 s
6 T: AT+SAPBR=3,1,"APN","internet"\r\n
7 R: T:AT+SAPBR=3,1,"APN","internet"\r\n\r\nOK\r\n
8 26.140 s
9 T: AT+SAPBR=4,1\r\n
10 R: AT+SAPBR=4,1\r\n\r\n\r\n
11 R: +SAPBR: "\r\nCONTYPE:"GPRS\r\n APN: "internet\r\nPHONENUM: "\r\nUSER: "\r\nPWD: "\r\nRATE: "2\r\n\r\n\r\nOK\r\n
12 48.103 s
13 T: AT+CREG?\r\n
14 R: AT+CREG?\r\n\r\n\r\n+CREG: "0,1\r\n\r\n\r\nOK\r\n
15 49.640 s
16 T: AT+SAPBR=1,1\r\n
17 R: AT+SAPBR=2,1\r\n+SAPBR: "1,1\r\n
18 50.818 s
19 R: \r\nOK\r\n    **zde vznikal problém, příkaz byl vykonán až po 1.2 s.
20 51.141 s
21 T: AT+FTPCID=1\r\n
22 R: AT+FTPCID=1\r\n\r\n\r\nOK\r\n
23 51.540 s
24 T: AT+FTPSERV="3505.w5.wedos.net"\r\n
25 R: AT+FTPSERV="3505.w5.wedos.net"\r\n\r\n\r\nOK\r\n
26 51.940 s
27 T: AT+FTPUN="w3505"\r\n
28 R: AT+FTPUN="w3505"\r\n\r\n\r\nOK\r\n
29 52.343 s
30 T: AT+FTPPW="mmmm"\r\n
31 R: AT+FTPPW="mmmm"\r\n\r\n\r\nOK\r\n
32 52.743 s
33 T: AT+FTPPUTNAME="test1.txt"\r\n
34 R: AT+FTPPUTNAME="test1.txt"\r\n\r\n\r\nOK\r\n
35 53.143 s
36 T: AT+FTPPUTPATH="/www/"\r\n
```

⁵odkaz na stránku: <http://m2msupport.net/m2msupport/module-tester/>

```

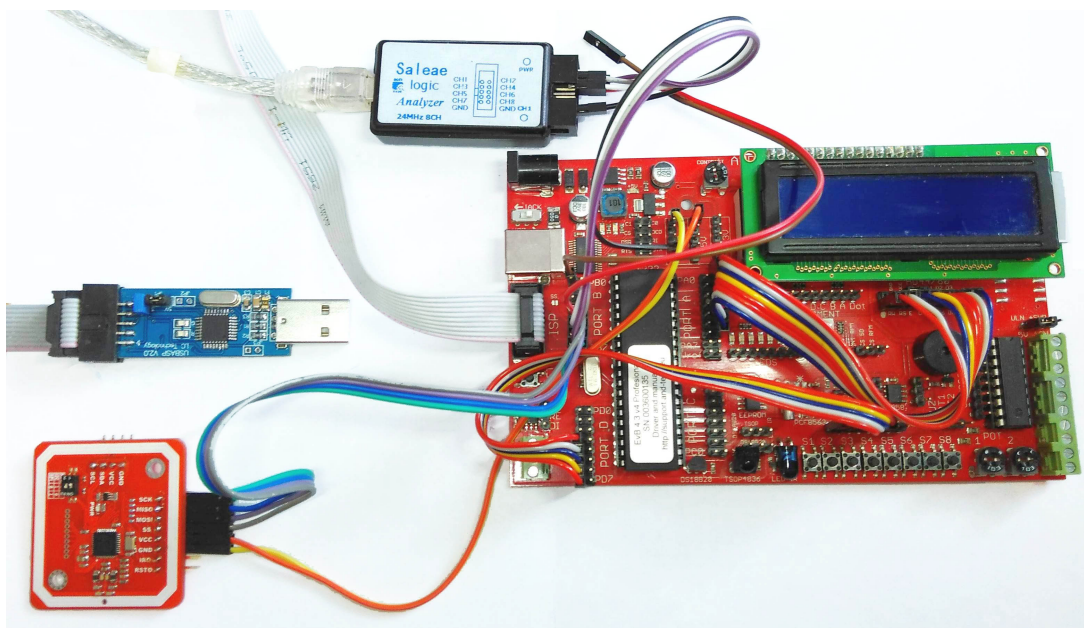
37 R: AT+FTPPUTPATH="/www/"\r\n\r\nOK\r\n
38 53.540 s
39 T: FTTPUT=1\r\n
40 R: FTTPUT=1\r\n\r\nOK\r\n
41 56.480 s
42 R: \n\r+FTTPUT:1,1,1260\r\n
43 56.532 s
44 T: AT+FTTPUT=2,2\r\n
45 R: AT+FTTPUT=2,2\r\n\r\n+FTTPUT=2,2\r\n
46 56.986 s
47 T: ST
48 R: \r\nOK\r\n
49 R: \r\n+FTTPUT:1,1,1260\r\n
50 57.430 s
51 T: AT+FTTPUT=2,0\r\n
52 R: AT+FTTPUT=2,0\r\n
53 R: \r\nOK\r\n
54 66.220 s
55 R: AT+FTTPUT=1,0\r\n

```

6.4 Čtečka NFC

Výsledné testování programu. Funkce: tlačítko S1 - zašifrování textu a uložení na kartu, tlačítko S2 přečtení zašifrovaného textu na kartě, tlačítko S3 - načtení a zobrazení UID + nahrání souboru na server. Údaje lze nahrávat na kartu šifrovaně pomocí AES nebo Shamir šifry. Knihovny jsou implementované a jejich funkčnost jsem ověřil.

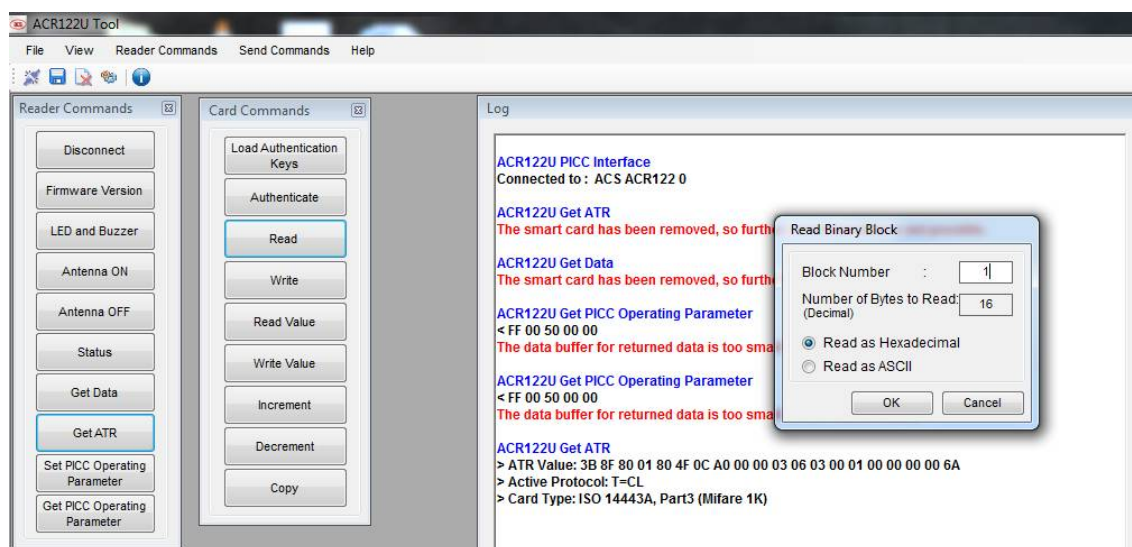
Pro pouhou identifikaci karty bohatě poslouží její unikátní číslo. V mnoha aplikacích to je dostačující údaj, v případě potřeby je možný zápis i čtení chráněných bloků. Pro ověření zápisu dat na kartu, mám externí čtečku k počítači. Ukázka obslužné aplikace viz obr 6.10.



Obr. 6.8: Vývojový kit, čtečka PN532, USBasp programátor, logický analyzátor

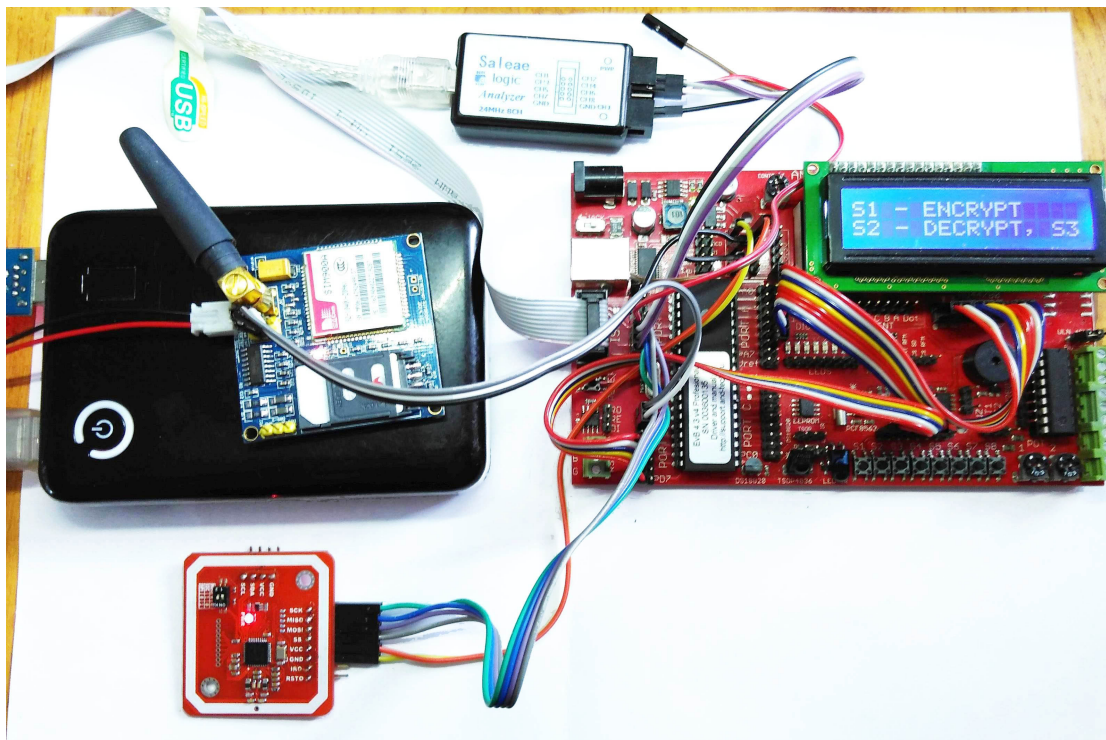


Obr. 6.9: NFC čtečka ACR122, pokusné karty a čipy



Obr. 6.10: Obslužný program pro NFC čtečku ACR122

Proudový odběr – Vývojový kit s čtečkou NFC: 100 mA, GSM modul: 20 mA (klidový odběr). Během několika pokusů nahrávání souboru na server jsem upozoroval určité kolísání napětí na vývojovém kitu. Způsobily to proudové výkyvy z GSM modulu, dle datasheetu mohou být až 2 A na 5 V. GSM modul je osazen tantalovým kondenzátorem, pro jeho nabití nebyly dráty dostatečně dimenzované. Problém jsem vyřešil externím zdrojem napětí z přídatného USB, pouze pro vývojové využití. Viz druhý USB kabel zapojený v power bank.



Obr. 6.11: Vývojový kit napájený z power bank, GSM modul, čtečka PN532

6.5 Odesílání dat na server

Na server je možné nahrávat data dvěma způsoby. První je vytvoření souboru na FTP serveru a následné zpracování souboru serverem. Druhý způsob je odeslání dat v proměnné v HTTP odkazu. Ten může mít srozumitelnou podobu `http://server.cz/upload.php?IDCard=123456789&IDReader=1`. Takový formát je srozumitelný, ale velmi snadno napadnutelný – může dojít k odeslání podvržených dat. Snadno lze implementovat další proměnnou do odkazu se složitějším kontrolním součtem a třeba i bezpečnostním kódem. Ve výsledku by koncová část odkazu vypadala následovně: `?IDCard=123456789&IDReader=1&S=1f2bb`. Asi nejlepší variantou je veškeré údaje šifrovat. Druhá varianta má výhodu okamžitého ukládání dat do databáze, naopak stahování dat do zařízení bych preferoval z FTP.

6.6 Nahrávání SW do vývojového kitu

Pomocí AND-Load⁶ programu lze nahrávat zkompileovaný program v HEX formátu přímo do Atmegy přes USB. Tato možnost je platná, pouze pokud Atmega obsahuje původní Bootloader. V případě jeho smazání je možné bootloader stáhnout

⁶Odkaz pro stažení SW AND-Load: <http://and-tech.pl/EvB5.1/ANDLoad.zip>

od výrobce a znovu nahrát přes ISP.

Jelikož v závěru své práce programuji mikrokontrolér v zařízení, kde mám jen vyvedené piny ISP rozhraní, přešel jsem na nahrávání EvB vývojového kitu také pomocí ISP rozhraní. Velmi se mi osvědčil program AVRDUDE, který podporuje velké množství mikrokontrolérů. Jeho výhoda spočívá i v možnosti ovládání přes konzoli. Pro snadné ovládání jsem vytvořil skript pro automatické nahrání SW do mikrokontroléru, dále skriptem odstraňuji problém AVRDUDE s nekompatibilitou mezer a diakritiky v pracovní cestě. Ve stručnosti funguje následovně: zkopíruj HEX soubor z projektu, nahraj do zařízení a soubor vymaž.

```
1 copy "C:\temp\druhy test\DP1\Debug\DP1.hex" "C:\TEMP\avrdude\temp"
2 C:\TEMP\avrdude\avrdude.exe -C C:\temp\avrdude\avrdude.conf -p m644p -c
   usbasp -U flash:w:C:\temp\avrdude\temp\DP1.hex:a
3 del "C:\temp\avrdude\temp\DP1.hex"
4 pause
```

6.7 Program a knihovny

Funkce jednotlivých modulů jsem nechal v oddělených knihovnách. Jsou to *LCD.c*, *pn532_spi.c*, *Shamir.c*, *uart.c* a *sim900.c*. Ve zkratce napíši základní informace o knihovnách a jejich nejdůležitějších funkcích. Některé funkce mají mnoho vstupních proměnných, podrobněji jsou vysvětleny v příslušné knihovně. Zde jsem je z důvodu úspory místa nahradil třemi tečkami.

6.7.1 lcd.c

knihovna je určena pro práci s LCD displejem, nejčastěji 2 řádky po 16 znacích. Obsahuje funkce pro inicializaci, zápis a nastavení displeje.

- `lcd_init(uint8_t dispAttr)` - proveden inicializaci a nastavení displeje
- `lcd_clrscr(void)` - vymaže veškeré znaky a změní pozici na první znak
- `lcd_home(void)` - změní pozici na první znak
- `lcd_gotoxy(uint8_t x, uint8_t y)` - změní pozici kurzoru na dané souřadnice
- `lcd_putc(char c)` - zapíše znak na místo kurzoru
- `lcd_puts(const char *s)` - zapíše řetězec znaků na aktuální pozici

6.7.2 Shamir.c

knihovna určena pouze pro šifrovací a dešifrovací algoritmus Shamir.

- `shamir_split(...)` - šifrování dat

- `shamir_join(...)` - dešifrování dat

6.7.3 aes256.c

knihovna určena pouze pro šifrovací a dešifrovací algoritmus AES.

- `aes256_init(aes256_context *, uint8_t *)` - zadání klíče
- `aes256_encrypt_ecb(aes256_context *, uint8_t *)` - šifrování dat
- `aes256_decrypt_ecb(aes256_context *, uint8_t *)` - dešifrování dat

6.7.4 pn532_spi.c

obsluhuje komunikaci mezi mikrokontrolérem a čtečkou NFC PN532.

- `setupPins()` - nastavení mikrokontroléru ke komunikaci pomocí SPI
- `void getFirmwareVersion()` - příkazy jsou přizpůsobeny několika verzím NFC čtečky, nutné k ověření kompatibility
- `void readPassiveTargetID(uint8_t cardbaudrate)` - přečtení UID přiložené karty
- `void authenticateBlock(...)` - přečtení zašifrovaného bloku karty
- `void readMemoryBlock(...)` - přečtení bloku dat na kartě
- `void writeMemoryBlock(...)` - zápis bloku dat na kartu
- `void sendCommandCheckAck(uint8_t *cmd, uint8_t cmdlen, uint16_t timeout)` - odeslání příkazu a čekání na odpověď
- `void spi_readack()` - čekání na odpověď od NFC čtečky
- `void readspidata(uint8_t* buff, uint8_t n)` - čtení dat z SPI
- `void spiwritecommand(uint8_t* cmd, uint8_t cmdlen)` - odeslání příkazu
- `void spiwrite(uint8_t c)` - odeslání dat přes SPI
- `void spiread()` - zachytávání dat z SPI do bufferu

6.7.5 uart.c

Uart je asi nejzákladnější komponentou mikrokontroléru. Výrobci pro tuto komunikaci vytvořili speciální přerušení *ISR(UART0_RECEIVE_INTERRUPT)*. Data jsou automaticky uložena do bufru a nastaven příznak přijetí dat. Obdobné je i vysílání *ISR (UART0_TRANSMIT_INTERRUPT)*, jakmile je možné odeslat data, vyvolá se přerušení programu a data se odvysílají. Některé mikrokontroléry obsahují 2 kanály komunikace UART, funkce pro příjem a odeslání dat jsou duplicitní pro každý kanál.

- `uart_init(unsigned int baudrate)` - nastavení komunikační rychlosti UART
- `uart_putc(unsigned char data)` - odeslání bajtu
- `uart_puts(const char *s)` - odeslání řetězce dat
- `uart_getc(void)` - přečte přijatý bajt

6.7.6 `sim900.c`

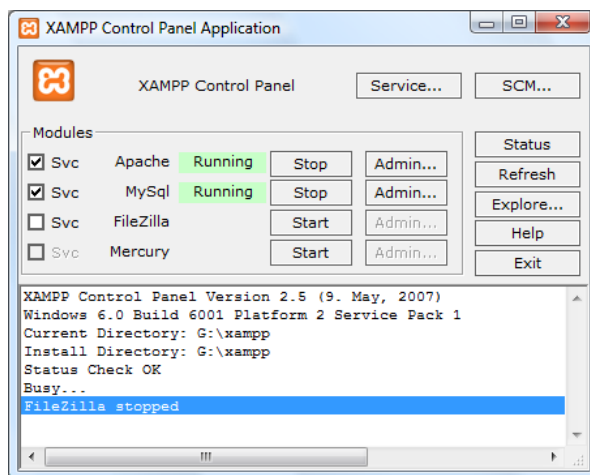
Knihovna obstarává potřebné funkce pro ovládání GSM modulu. Čtení i odesílání SMS, přijetí příchozího hovoru a zavolání, internetové služby jako je přístup na FTP a načtení webové stránky.

- `sim900_gprs_open_connection(...)` - aktivace připojení mobilního internetu
- `sim900_FTPPUT(const char *adata)` - odeslání dat přes FTP
- `sim900_init_uart(const uint16_t baudrate)` - nastavení komunikační rychlosti UARTu
- `sim900_send_cmd_wait_reply(...)` - odeslání příkazu a čekání na odpověď
- `sim900_send_sms(const uint8_t *aSenderNumber, const uint8_t *aMessage)`
- odeslání SMS na zvolené mobilní číslo

7 PROGRAM - SERVER

Databáze pro sbírání dat ze zařízení může být spuštěna na jakémkoliv serveru podporující PHP a MySQL. V domácím prostředí využívám aplikaci XAMPP. Je možné celý server (aplikaci) přenášet na flashdisku a spouštět kdekoliv. V sobě obsahuje server Apache, MySQL databázi, FileZilla pro přenos souborů přes FTP a Mercury emailového klienta.

Je možné pronajmout webhosting a serverovou aplikaci umístit tam.


















Obr. 7.1: XAMPP ovládací okno




Ukázka možného uložení ID karet do databáze. Počet ukládaných údajů se může libovolně změnit dle projektu.

Number of rows: 25 ▼

Sort by key: None ▼

+ Options

				ID	IDCard	Time Stamp	IDReader
<input type="checkbox"/>	 Edit	 Copy	 Delete	2	153062950	2015-05-11 13:19:24.000000	1
<input type="checkbox"/>	 Edit	 Copy	 Delete	3	478676648	2015-05-18 13:21:09.000000	1
<input type="checkbox"/>	 Edit	 Copy	 Delete	4	315936221	2015-05-18 13:25:12.000000	1
<input type="checkbox"/>	 Edit	 Copy	 Delete	5	742131368	2015-05-18 13:28:17.000000	1
<input type="checkbox"/>	 Edit	 Copy	 Delete	6	316702710	2015-05-18 13:29:12.000000	1

⬆ ☐ Check All With selected:  Change  Delete  Export

Number of rows: 25 ▼

Obr. 7.2: Ukázka záznamů načtených karet v PHPMyAdmin

8 ZÁVĚR

V rámci diplomové práce byly navrženy dvě zařízení pro osobní identifikaci a sdílení dat. První s grafickým displejem umožňující zobrazení podrobnějších informací a obrázků, navíc s možností pořízení fotografie. A levnější, energeticky méně náročnější zařízení - logger. Pro jednotlivé varianty zařízení byly vybrány konkrétní moduly: Raspberry Pi B+, LCD displej s dotykovou vrstvou, GSM modul SIM900A a NFC modul PN512. Po domluvě se zadavatelem byla zkonstruována druhá varianta zařízení. Při jeho vývoji byla oživena komunikace mezi jednotlivými moduly a ověřena kompatibilita jednotlivých bloků. Delší dobu jsem řešil problém nefunkčního GSM modulu. První závadou byl studený spoj mezi RS232 a samotným čipem SIM900A. Po odstranění první závady modul vyhledal mobilní operátory, ale nebylo možné se k nim přihlásit. Problém byl způsoben nahráním nesprávného firmware výrobcem, modul nebyl určen pro prodej v Evropě. Jelikož jednotlivé dostupné verze firmware nejsou přesně popsány a ne všechny podporují připojení k Internetu, musel jsem jich odzkoušet více a vybrat tu správnou.

Zrealizované zařízení nyní dokáže vyčíst unikátní číslo karty, zapisovat a číst zašifrovaná data pomocí kryptovacího algoritmu AES nebo Shamir, odeslat přečtená data na server a synchronizovat čas z internetu. Odeslané údaje server zapisuje do předem připravené tabulky v databázi. Dále dokáže vytvářet a číst textové soubory z FTP serveru. Během testování zařízení byly zkoušeny běžné dostupné čipové karty. Z InKarty od Českých drah a školní karty ISIC se mi podařilo načíst ID. Obsah karet jsem raději nezkoušel číst a přepisovat, pro identifikaci je ID karty dostačující. Navržený systém umožňuje nastavit dva pracovní režimy komunikace, může se chovat jako NFC čtečka a mobilní telefon jako čip a naopak. Což umožňuje uživateli získat relevantní data ze systému. Cílem celé práce bylo navrhnout, zkonstruovat a ověřit funkčnost systému pro osobní identifikaci a sdílení dat pro nový projekt zadavatele. Vytyčený cíl v úvodu diplomové práce byl splněn.

LITERATURA

- [1] ROOT.cz: *Raspberry Pi dorazil, revoluční minipočítač na vlastní kuži* [online]. 2014, poslední aktualizace 11.3.2007 [cit. 2014-12-1]. Dostupné z WWW: <<http://www.root.cz/clanky/raspberry-pi-dorazil-revolucni-minipocitac-na-vlastni-kuzi/>>.
- [2] zdroj obrázku: <http://www.raspberrypi.org/introducing-raspberry-pi-model-b-plus/>
- [3] zdroj obrázku: <http://cz.farnell.com/nxp/explore-nfc/add-on-board-nfc-for-raspberry/dp/2366201>
- [4] <http://elektronika.cz>: *SIMCOM: SIM900 nahradí SIM300* [online]. 2014, poslední aktualizace 3.5.2010 [cit. 2014-12-1]. Dostupné z WWW: <<http://elektronika.cz/2010042103/simcom-sim900-nahradi-sim300>>.
- [5] zdroj obrázku: http://imall.iteadstudio.com/media/catalog/product/cache/1/image/9df78eab33525d08d6e5fb8d27136e95/i/m/img_0806.jpg
- [6] EVB Elektronik *RFID Selection Guide* [online]. 2010, poslední aktualizace 1.9.2010 [cit. 2015-05-18]. Dostupné z WWW: <<http://www.adafruit.com/datasheets/rfid%20guide.pdf>>.
- [7] <http://elektronika.kvalitne.cz>: *Ovládání znakových LCD s řadičem HD44780* [online]. 2014, poslední aktualizace 11.3.2007 [cit. 2014-12-1]. Dostupné z WWW: <<http://elektronika.kvalitne.cz/ATMEL/necoteorie/LCDmatice.html>>.
- [8] zdroj obrázku: <http://elektronika.kvalitne.cz/ATMEL/necoteorie/LCD1602.html>
- [9] zdroj obrázku: <http://elektronika.kvalitne.cz/ATMEL/necoteorie/LCDmatice.html>
- [10] uArt.cz: *Elektronika do posledního uA... Obvod reálného času DS1307* [online]. 2011, poslední aktualizace 27.6.2011 [cit. 2015-05-12]. Dostupné z WWW: <<http://uart.cz/78/obvod-realneho-casu-ds1307/>>.
- [11] zdroj obrázku: <http://www.atomsindustries.com/assets/images/items/1078/1078.jpg>
- [12] Atmel.com: *Datasheet ATmega16 Atmel*. [Online] [cit. 2012-12-13] Dostupné z WWW: <http://www.atmel.com/Images/doc2466.pdf>

- [13] zdroj obrázku: <http://www.gme.cz/mikroprocesory-atmel-avr-mega/atmega644-20au-p958-166/>
- [14] Programujte.com: *AVR – blikáme* [Online] [cit. 2012-12-11] Dostupné z WWW: <http://programujte.com/clanek/2006070301-avr-blikame/>
- [15] Programujte.com: *AVR – přerušení* [Online] [cit. 2012-12-12] Dostupné z WWW: <http://programujte.com/clanek/2006092402-avr-preruseni/>
- [16] Programujte.com: *AVR - čítače* [Online] [cit. 2012-12-10] Dostupné z WWW: <http://programujte.com/clanek/2006091410-avr-citace/>
- [17] Wikipedia.cz: *P²C* [Online] Dostupné z WWW: <http://cs.wikipedia.org/wiki/I%C2%B2C>
- [18] www.and-tech.pl: *EvB 5.1 v5 Uživatelská příručka* [online]. 2014, překlad: www.onpa.cz poslední aktualizace 15.10.2013 [cit. 2015-5-5]. Dostupné z WWW: <<http://and-tech.pl/wp-content/uploads/downloads/2013/10/Instrukcja-EvB5.1-v1-cze.pdf>>.
- [19] zdroj obrázku: http://www.image.micros.com.pl/_icon_auto_s/m%20evb5.1%20atm32.jpg
- [20] Wikipedia *MIFARE* [online]. 2011, poslední aktualizace 18.5.2015 [cit. 2015-05-18]. Dostupné z WWW: <<http://en.wikipedia.org/wiki/Mifare>>.
- [21] EFFING, W. , *Smart Card Handbook* , 3rd edition, New York, John Wiley & Sons, 2003.
- [22] RANKL, W. *Smart Card Applications: Design Models for using and programming smart cards* , New York, John Wiley & Sons, 2007.
- [23] KALLA, Tomáš *Bezpečnost MIFARE karet: bakalářská práce.* [online]. Brno: Masarykova Univerzita, Fakulta informatiky, 2012. 49 s. Dostupné z WWW: <http://is.muni.cz/th/324974/fi_b/>.
- [24] zdroj obrázku: http://s.eeweb.com/members/nxp/blog/2013/11/19/NFC-Type-MIFARE-Classic-Tag-Operation_1-13848536041.png
- [25] zdroj obrázku: <http://www.best-microcontroller-projects.com/image-files/how-rs232-works-tx-logic-rs232-diag.png>
- [26] zdroj obrázku: http://www.simplelabs.co.in/376-thickbox_leometr/usb-logic-analyser-usb-saleae-clone.jpg

- [27] zdroj obrázku: <https://www.openlighting.org/wp-content/uploads/2013/12/Saleae-logic.jpg>
- [28] Wikipedia: *Shamir's Secret Sharing* [online]. 2015, poslední aktualizace 12.4.2015 [cit. 2015-05-4]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

A/D Analog/Digital

APN Access Point Name

DPS Deska Plošných Spojů

EEPROM Electrically Erasable Programmable Read-Only Memory

FAT File Allocation Table

FTP File transport Protocol

GND Ground

GSM Global System for Mobile Communication

GPRS General Packet Radio Service

HD High-Definition

HDMI High-Definition Multi-media Interface

HTTP Hypertext Transfer Protocol

I²C Inter-Integrated Circuit

IRQ Interrupt ReQuest

ISP In System Programming

JTAG Joint Test Action Group

LAN Local Area Network

LCD Liquid Crystal Display

LED Light-Emitting Diode

LSB Least significant bit

MB Megabyte

MMC MultiMediaCard

MS Microsoft

NFC Near Field Communication

OO Open Office

R/W Read/Write

RFID Radio Frequency Identification

RISC Reduced Instruction Set Computing

RTC Real-Time Clock

SCL Synchronous Clock

SD Secure Digital

SDA Synchronous Data

SPI Serial Peripheral Interface

SRAM Static Random Access Memory

TQFP44 Thin Quad Flat Package, počet pinů 44

UART Universal asynchronous receiver/transmitter

USB Universal Serial Bus

SEZNAM PŘÍLOH

A Ukázka průběhu komunikace

51

A UKÁZKA PRŮBĚHU KOMUNIKACE



Obr. A.1: Průběh celé komunikace TX, RX a detailnější pohled na průběh