

# **Využití mikropočítače Atmel pro implementaci autonomního systému kontroly vstupů**

Implementation of Autonomous Access Control System using  
Microcontroller Atmel

Filip Zaňka



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2010/2011

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Filip ZAŇKA**  
Osobní číslo: **A09743**  
Studijní program: **N 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Využití mikropočítače Atmel pro implementaci autonomního systému kontroly vstupů**

Zásady pro vypracování:

1. Vypracujte literární rešerši na téma autonomních systémů kontroly vstupů.
2. Vytvořte návrh řešení levného autonomního systému kontroly vstupů s využitím MCU Atmel.
3. Jako identifikační prvky použijte kontaktní předměty iButton připojené pomocí sběrnice 1-Wire.
4. Realizujte testovací (předváděcí) zapojení navrženého řešení formou propojených modulů stavebnice MLAB.
5. Navrhněte příslušné programové vybavení ve vhodném programovacím jazyku.
6. Do řešení zahrňte následující bezpečnostní prvky: ochrana proti generování jednotlivých kombinací klíčů (útok hrubou silou), kontrola čtení identifikačních čísel pomocí kontrolních součtů, ochranu přístupu k ovládací části zařízení, zápis logů na paměťové médium.
7. Provedte ekonomickou analýzu nákladů na 1 systém. Zhodnoťte všechny vámi dosažené výsledky.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. Matoušek, David. Práce s mikrokontroléry ATMEL AVR – ATmega16 – 4. díl. Praha : BEN – technická literatura, 2006. ISBN 80-7300-174-8.
2. ATMEL – Firemní literatura k mikrokontrolérům ATmega.
3. Maxim Integrated Products – Firemní literatura k produktům iButton.
4. Vobecký, Jan; Záhlava, Vít. Elektronika : součástky a obvody, principy a příklady : třetí, rozšířené vydání. Praha : Grada Publishing, 2005. ISBN 80-247-1241-5.
5. Záhlava, Vít. OrCAD pro Windows : praktický průvodce návrháře. Praha : Grada Publishing, 1999. ISBN 80-7169-876-8.
6. Váňa, Vladimír. Mikrokontrolery ATMEL AVR – programování v jazyce C. Praha : BEN, 2003. ISBN: 80-7300-102-0.

Vedoucí diplomové práce:

**Ing. Tomáš Sysala, Ph.D.**

Ústav automatizace a řídicí techniky

Datum zadání diplomové práce:

**25. února 2011**

Termín odevzdání diplomové práce:

**27. května 2011**

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.  
*děkan*



doc. RNDr. Vojtěch Křesálek, CSc.  
*ředitel ústavu*

## ABSTRAKT

Diplomová práce se zabývá návrhem a vytvořením testovacího zapojení bezpečnostní aplikace - levného systému kontroly vstupů, založeném na mikrokontroléru ATmega firmy Atmel. Jako identifikační prvky jsou použity kontaktní předměty iButton firmy Maxim Integrated Products. Testovací zapojení je realizováno jako modulární systém, aby bylo možné jej po odzkoušení funkcionality rozšířit o další části nebo naopak určité moduly odstranit za účelem případného snížení ceny zařízení. Zařízení je navrhováno s ohledem na předpokládané využití v rodinných (nájemních) domech.

Klíčová slova:

Mikrokontrolér, MCU, Atmel, ATmega, systém, kontroly, vstupů

## ABSTRACT

Master thesis deals with the design and creation of testing security appliance assembly – a low cost access control system based on the Atmel ATmega microcontroller. The iButton contact tokens from Maxim Integrated Products are used as identification devices. The testing appliance is implemented as a modular system in order to allow for its extending with further parts after testing its functionality or, conversely, eliminate certain modules to eventually reduce device costs. The appliance is designed with regard to the planned use in the family (rental) houses.

Keywords:

Microcontroller, MCU, Atmel, ATmega, Access, Control, System



Poděkování:

Děkuji vedoucímu diplomové práce panu Ing. Tomáši Sysalovi, Ph.D. za účinné metodické a cíleně orientované vedení při plnění úkolů realizovaných v průběhu zpracování diplomové práce. Dále děkuji tvůrcům a spolupracovníkům webového serveru MLAB za podporu a spolupráci při vytváření nových modulů stavebnice.

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD.....</b>	<b>10</b>
<b>I TEORETICKÁ ČÁST.....</b>	<b>11</b>
<b>1 ANALÝZA ZADÁNÍ .....</b>	<b>12</b>
1.1 OBECNÝ ROZBOR – PŘEHLED.....	13
1.2 ROZBOR – EKONOMICKÉ HLEDISKO .....	14
1.3 ROZBOR HARDWAROVÉ ČÁSTI.....	16
1.4 ROZBOR SOFTWAREOVÉ ČÁSTI .....	16
<b>2 SYSTÉMY KONTROLY VSTUPŮ .....</b>	<b>18</b>
2.1 ZÁKLADNÍ POJMY A DEFINICE.....	18
2.2 ZÁKLADNÍ FUNKCE SYSTÉMŮ KONTROLY VSTUPŮ.....	21
2.3 KOMPONENTY SYSTÉMŮ KONTROLY VSTUPŮ .....	23
2.4 ROZDĚLENÍ SYSTÉMŮ PRO KONTROLU VSTUPŮ.....	24
2.5 VŠEOBECNÉ POŽADAVKY - ČSN EN 50133-1 .....	25
2.5.1 Třídy identifikace .....	25
2.5.2 Třídy přístupu .....	26
2.5.3 Ochrana programování .....	26
2.6 ZPRACOVÁNÍ POVOLENÉHO PŘÍSTUPU .....	26
<b>3 POUŽITÉ TECHNOLOGIE A KOMPONENTY .....</b>	<b>28</b>
3.1 MIKROKONTROLÉR (MICROCONTROLLER UNIT - MCU).....	28
3.1.1 AVR Architektura .....	28
3.1.2 ATmega128.....	30
3.1.2.1 Paměť .....	32
3.1.2.2 Synchronní sériový port (SPI, Serial Peripheral Interface) .....	33
3.1.2.3 Univerzální synchronní/asynchronní sériový kanál (USART) .....	34
3.1.2.4 Synchronní sériový kanál (TWI) .....	35
3.2 KOMUNIKAČNÍ ROZHRANÍ 1-WIRE .....	36
3.3 DOTYKOVÉ IDENTIFIKAČNÍ PRVKY IButton.....	37
<b>II PRAKTICKÁ ČÁST.....</b>	<b>39</b>
<b>4 NÁVRH ŘEŠENÍ .....</b>	<b>40</b>

4.1	OBEČNÝ POPIS .....	40
4.2	BLOKOVÉ SCHÉMA .....	43
4.3	PROGRAMÁTOR .....	44
4.4	USART/USB PŘEVODNÍK .....	45
4.5	OVLÁDACÍ ROZHRAŇÍ – LCD DISPLEJ .....	46
4.6	HODINY REÁLNÉHO ČASU (RTC) .....	47
4.7	UKLÁDÁNÍ PŘÍSTUPOVÝCH TRANSAKČÍ – PAMĚŤOVÁ KARTA .....	48
4.8	PŘEVODNÍK NAPĚŤOVÝCH ÚROVNÍ (VOLTAGE LEVEL TRANSLATOR) .....	49
4.9	VÝKONOVÝ SPÍNAČ .....	50
4.10	NAPÁJECÍ ZDROJ .....	51
4.11	CELKOVÉ SCHÉMA ZAPOJENÍ .....	52
4.12	SEZNAM POUŽITÝCH VÝVODŮ MCU .....	52
4.13	PROPOJENÍ MODULŮ .....	54
<b>5</b>	<b>TESTOVACÍ ZAPOJENÍ NAVRŽENÉHO ZAŘÍZENÍ.....</b>	<b>56</b>
5.1	MODUL MIKROKONTROLÉRU (MCU) .....	56
5.2	MODUL PROGRAMÁTORU .....	57
5.3	MODUL USART/USB PŘEVODNÍKU .....	58
5.4	MODUL OVLÁDACÍHO ZAŘÍZENÍ .....	58
5.5	MODUL HODIN REÁLNÉHO ČASU .....	59
5.6	MODUL PŘEVODNÍKU NAPĚŤOVÝCH ÚROVNÍ.....	60
5.7	MODUL PAMĚŤOVÉ KARTY .....	61
5.8	VÝKONOVÝ SPÍNAČ .....	61
5.9	NAPÁJECÍ ZDROJ .....	62
5.10	ROZHRAŇÍ MÍSTA PŘÍSTUPU.....	63
<b>6</b>	<b>BEZPEČNOSTNÍ PRVKY ZAŘÍZENÍ.....</b>	<b>64</b>
6.1	OVĚŘENÍ TOKENU UŽIVATELE .....	64
6.2	OCHRANA PŘED ÚTOKEM HRUBOU SILOU .....	64
6.3	ULOŽENÍ IDENTIFIKAČNÍHO ČÍSLA TOKENŮ, ZÍSKÁNÍ ID.....	65
6.4	OCHRANA PŘÍSTUPU K OVLÁDACÍMU ZAŘÍZENÍ.....	66
6.5	OCHRANA SNÍMAČE (MCU) PŘED PŘIPOJENÍM ZDROJE NAPÁJENÍ.....	67
6.6	AUTOMATICKÝ RESET ZAŘÍZENÍ - WATCHDOG .....	68
<b>7</b>	<b>FYZICKÁ REALIZACE TESTOVACÍHO ZAPOJENÍ.....</b>	<b>69</b>
<b>8</b>	<b>POPIS OVLÁDÁNÍ .....</b>	<b>70</b>

8.1	ZAPNUTÍ ZAŘÍZENÍ .....	70
8.2	SIGNALIZACE STAVU .....	70
8.3	VLOŽENÍ PAMĚŤOVÉ KARTY .....	71
8.4	PROPOJENÍ S POČÍTAČEM .....	72
8.5	PRÁCE S MENU .....	73
8.6	FUNKCE MENU .....	74
8.7	PROVOZ ZAŘÍZENÍ .....	75
8.8	VYPNUTÍ ZAŘÍZENÍ, RESET .....	76
<b>9</b>	<b>SOFTWARE VYBAVENÍ .....</b>	<b>77</b>
9.1	AVR STUDIO .....	77
9.2	POUŽITÉ KNIHOVNY .....	78
9.3	STRUČNÝ POPIS PROGRAMU MIKROKONTROLÉRU .....	78
<b>10</b>	<b>EKONOMICKÁ ANALÝZA SESTAVENÉHO ZAŘÍZENÍ .....</b>	<b>82</b>
<b>11</b>	<b>DALŠÍ MOŽNÝ ROZVOJ ZAŘÍZENÍ .....</b>	<b>85</b>
	<b>ZÁVĚR .....</b>	<b>86</b>
	<b>CONCLUSION .....</b>	<b>87</b>
	<b>SEZNAM POUŽITÉ LITERATURY .....</b>	<b>88</b>
	<b>SEZNAM POUŽITÝCH ZKRATEK .....</b>	<b>90</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>91</b>
	<b>SEZNAM TABULEK .....</b>	<b>93</b>
	<b>SEZNAM PŘÍLOH .....</b>	<b>94</b>

## ÚVOD

V průběhu studia oboru Bezpečnostní technologie, systémy a management mě velmi zaujal předmět Mikropočítače a PLC. Zjistil jsem, že vytvoření hardwarové aplikace využívající mikrokontrolér je dnes poměrně jednoduchá a levná záležitost. Když jsem pak byl shodou okolností postaven před problém ztracení klíčů od domu, začal jsem řešit problematiku nasazení spolehlivého a bezpečného systému kontroly vstupů, který by splňoval mé požadavky, ale přitom byl levnější než výměna či překódování zámků. Po prozkoumání možných řešení jsem zjistil, že takových systémů na trhu mnoho není a ty existující bohužel nesplňují mé nároky. Začal jsem se tedy zabývat myšlenkou vlastního návrhu bezpečnostní aplikace - systému kontroly vstupů. Tak vzniklo testovací zapojení, které je zpracováno tak, aby před vlastní fyzickou realizací (zhotovením předvýrobního prototypu) bylo možné některé jeho moduly odebrat (například za účelem snížení ceny), či naopak přidat a rozšířit tak funkcionalitu zařízení. Testovací zapojení je postaveno na komponentech stavebnice MLAB a plně využívá moderní mikrokontrolérovou technologii. Na počátku vývoje jsem předpokládal využití výhradně existujících modulů stavebnice, ale již v průběhu analýzy vyšlo najevo, že je nutné navrhnout moduly nové, které později rozšíří portfolio stavebnice MLAB.

Testovací zapojení realizované pomocí modulů lze rovněž s výhodou použít pro výukové účely a doufám, že bude další studenty inspirovat k seznámení se s mikrokontrolérovou technikou.

## **I. TEORETICKÁ ČÁST**

## 1 ANALÝZA ZADÁNÍ

Cílem této práce je návrh bezpečnostní aplikace - autonomního systému kontroly vstupů a vytvoření testovacího zapojení pro ověření funkčnosti návrhu. Jak již bylo uvedeno v úvodu, plánované nasazení zařízení je v rodinných (bytových) domech, kde bude obsluhovat vždy 1 místo přístupu (elektromagnetický otevírač). Předpokládá se, že každé zařízení bude mít jinou sadu povolených identifikačních prvků (tokenů) a bude pracovat samostatně. Počet identifikačních prvků uložených v paměti zařízení pak bude maximálně v desítkách.

Pro výše uvedené nasazení je vhodné, aby identifikační prvky byly mechanicky co nejodolnější, levné a pokud možno pasivní. Z pohledu bezpečnosti by jejich kopírování mělo být složitější než vytvoření kopie běžně používaných klíčů a při vyhodnocování by neměla být možná záměna jednotlivých identifikačních prvků. Pro případné vyhodnocování přístupů (například v případě krádeže ve společných prostorách) by zařízení mělo umožňovat zpětně určit komu a kdy byl přístup umožněn. Ovládání zařízení by mělo být jednoduché, ideálně bez potřeby připojování dalších zařízení (programátoru, počítače atd.), ale vzhledem k umístění zařízení blízko místa přístupu by mělo být toto rozhraní vhodným způsobem chráněno. Dále musí být zařízení v reálném provozu schopno pracovat i v případě přerušení dodávky elektrické energie, což znamená, že musí být buď připojeno na okruh budovy, který je zálohován, nebo musí mít zajištěno vlastní napájení například z baterie.

Shrňme-li si výše uvedené požadavky, pak vznikající zařízení by mělo splňovat následující:

- Využívat mikrokontrolérovou techniku
- Být uživatelsky příjemné
- Umožňovat snadné odebrání ztraceného identifikačního prvku a registraci prvku nového
- Využívat vhodné identifikační prvky s ohledem na možnost jejich kopírování
- Ukládat informace o oprávněných i neoprávněných přístupech
- Obsahovat ochranu proti neoprávněnému přístupu k ovládacímu rozhraní
- Musí být schopné otevřít ovládací prvky bez ověření uživatele (například tlačítkem v případě nouze, či dálkově jako běžný elektronický vrátný)



- Cena zařízení by měla být srovnatelná s cenou výměny zámků v případě ztráty klíčů

Přestože zařízení bude prezentováno pouze ve stádiu předváděcího zapojení, je již ve fázi návrhu vhodné zajistit, aby navrhované zařízení nebylo v nesouladu s platnými normami, v tomto případě především s ČSN EN 50133 (Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích) [5].

## 1.1 Obecný rozbor – přehled

Na základě soupisu požadavků uvedeného v kapitole 1 byl zvolen mikrokontrolér řady ATmega [3], jehož rychlost, možnosti připojení periférií a kapacita jsou pro tento projekt více než dostačující. Jako identifikační prvky se z pohledu cena/užitná hodnota jeví jako výhodné kontaktní předměty iButton [1], jejichž jedinou nevýhodou je, že tyto prvky neumožňují přímou komunikaci s mikrokontrolérem, neboť využívají sběrnici 1-Wire [1], kterou je nutné softwarově emulovat.

Pro správu zařízení je sice možné použít standardní dvoudrátové sériové rozhraní a konkurenční zařízení tuto možnost využívají, v tom případě by ale bylo vždy nutné k zařízení připojit PC, což rozhodně není uživatelsky příjemné. Sériové rozhraní je proto využito výhradně pro podrobné výstupy, které mohou být potřebné při diagnostice. Pro správu zařízení je dle mého názoru daleko vhodnější použít jako ovládací rozhraní LCD displej s několika tlačítky i když to může zařízení prodražit o několik stokorun.

Ukládání informací o transakcích (povolení či zamítnutí přístupu) je možné řešit mnoha způsoby, pro cenovou dostupnost a snadnost implementace je vhodné zvolit ukládání dat do textového souboru umístěného na dnes běžné paměťové kartě typu SD/MMC. S ukládáním těchto informací ovšem souvisí problém se získáním aktuálního data a reálného času, což lze řešit použitím interních čítačů mikrokontroléru nebo pomocí nezávislého časového zdroje.

## 1.2 Rozbor – ekonomické hledisko

Aby se zařízení tohoto typu vyplatilo vyvinout a vyrobit, je zapotřebí dobře vyčíslit náklady na něj a dále náklady, které nám vzniknou, pokud toto zařízení nebudeme mít a budeme řešit zamykání domu standardními klíči. V tomto případě u rodinného domu předpokládejme existenci použití bezpečnostních cylindrických vložek. V případě ztráty je nutné buď zakoupit nové zámkové vložky a k nim nechat vyrobit příslušný počet klíčů, nebo (pokud to ovšem vložky umožňují) je nechat zámečnickem přestavět na novou kombinaci. První varianta obsahuje jisté riziko zneužití ztracených klíčů v době mezi ztrátou a výměnou vložek za nové, druhá varianta bude vyžadovat dočasné nahrazení všech vložek a jejich opětovnou výměnu po překódování.

Materiál	Cena za kus s DPH
Vložka FAB 1000 - bezp. stupeň 3 (40+55mm) 5 klíčů	864 Kč
Přestavení vložky na novou kombinaci (včetně 5 klíčů)	800 Kč
Přidělení 1 klíče	70 Kč

Tabulka 1 – Příklad nákladů - zakoupení bezpečnostních vložek a jejich přestavba

Výše uvedené náklady<sup>1</sup> zahrnují pouze samotnou cenu zámku a klíčů. Není zde započítána cena práce na výměnu zámkových vložek resp. zajištění dočasných vložek v případě přestavení původních a náklady související s distribucí klíčů uživatelům. Je velmi pravděpodobné, že tyto sekundární (vynucené) náklady ve výsledku přesáhnou cenu vlastního zámku a jeho výměny.

Budeme-li místo klasické bezpečnostní vložky zvažovat zakoupení a nasazení již existujícího elektronického zařízení, musíme provést průzkum současného trhu. Autonomních systémů kontroly vstupů není na našem trhu mnoho, většina výrobců se spíše zaměřuje na větší implementace v oblasti sledování pohybu zaměstnanců

---

<sup>1</sup> Zprůměrované ceny několika dodavatelů zjištěné ke dni 1.2.2011 na Internetu.

a autonomní systémy jsou spíše vedlejším produktem vývoje rozsáhlejších síťových systémů. Z tohoto důvodu drtivá většina těchto zařízení nedisponuje uživatelsky příjemným prostředím pro správu identifikačních prvků a v příslušné cenové hladině taktéž nemají možnost zaznamenání informace o přístupu.

Z existujících výrobků můžeme v příslušné kategorii vybrat následující:

1) Firma JABLOTRON ALARMS a.s. – zařízení **AS-80** [11]

Přístupový systém AS-80 je určen pro ovládání el. zámků, garážových vrat, poplachových systémů apod.

- připojení jedné nebo dvou klávesnic či čtečky RFID
- odděleně umístěná vyhodnocovací jednotka
- 120 uživatelských kódů nebo RFID karet
- otevření dveří pomocí tlačítka EXIT
- orientační cena vč. DPH 2 500 Kč + 2 000 Kč/1 600 Kč  
(klávesnice/čtečka RFID)

2) Firma **TETRONIK**, v.d. – zařízení **FX319DS2** [17]

Autonomní přístupová jednotka do 70 osob.

- možnost připojení externího snímače pro oboustranné otevírání dveří
- reléový výstup (turniket, brána, ...)
- možnost ovládání dveřního zámku
- kapacita jednotky max. 70 osob
- zadávání osob pomocí MASTER
- 80 x 80 x 15 mm / 0,15 kg
- orientační cena vč. DPH: 3 000 Kč

3) Firma **dstechnik.cz** s.r.o. – zařízení **VIDEX ART 4850** [8]

Autonomní bezdotykový přístupový systém až pro 100 účastníků.

- paměť až pro 100 bezdotykových karet VIDEX - ART 955C nebo přívěsků VIDEX - ART 955T
- napájení 12 V, 24 V AC, DC
- programování pomocí tlačítek

- výstupní relé - 1x
- vhodné pro instalaci do rámečku VIDEX řady 4000
- orientační cena vč. DPH 4 500 Kč

Na trhu jsou i další zařízení jiných výrobců, vždy se však jedná o podobný výrobek s cenou odpovídající výše uvedenému výběru. Zařízení, které by v této cenové kategorii blíže odpovídala našemu zadání, tedy se záznamem přístupů a alespoň trochu uživatelsky příjemným rozhraním, jsem v době zpracování této práce nenašel.

Z výše uvedeného vyplývá, že vývoj nového zařízení by se mohl vyplatit v případě, pokud by jeho koncová cena byla nižší než zhruba **3 000 Kč** vč. DPH a zařízení by disponovalo lepší funkcionalitou než existující konkurenční výrobky.

### 1.3 Rozbor hardwarové části

Návrh a vytvoření předváděcího zapojení vyžaduje použití spolehlivého testovacího prostředí a to nejen po stránce elektronické, ale také po stránce mechanické. Moderní elektronické součástky se již v řadě případů vyrábějí výhradně v provedení SMD (Surface Mounted Device), které není možné testovat na nepájivých kontaktních polích jako při použití starších technologií, a je tedy nutné přímo navrhnout a zhotovit prototyp, což je velmi nepružné a drahé. Jinou možností je použít nějaký typ modulární stavebnice, kterých je dnes k dispozici několik. Po prozkoumání jejich možností byla jako nejvhodnější vybrána výborná česká stavebnice MLAB [10], která obsahuje velké množství modulů, má dobrou mechanickou stabilitu a pro tento projekt je více než vyhovující. Tato stavebnice umožňuje pracovat s více typy mikrokontrolérů rodiny ATmega firmy Atmel [3].

### 1.4 Rozbor softwarové části

K programování mikrokontrolérů dodává firma Atmel vlastní vývojové prostředí pod názvem AVR Studio [3], které je v současnosti volně dostupné a které používá programovací jazyk C. Vzhledem k rozsáhlosti tohoto projektu, není smysluplné se zabývat vytvářením knihoven pro komunikaci s použitými zařízeními. Je totiž možné převzít již existující otestované knihovny, přičemž je samozřejmě nutné zohlednit autorská práva resp. licenci, pod níž byl kód uvolněn.

Pro plné pochopení logiky návrhu zařízení a vzhledem k nutnosti splnění technických norem, které se na navrhované zařízení vztahují, se v následující kapitole seznámíme se základní problematikou systémů kontroly vstupů a s vybranými částmi normy ČSN EN 50133, která se na tuto oblast vztahuje [4],[5],[6],[7].

## 2 SYSTÉMY KONTROLY VSTUPŮ

Smyslem systémů kontroly vstupů je především zamezení přístupu neoprávněných osob do chráněných prostor, znemožnění ovládnutí vyhrazených zařízení či zabránění přístupu k citlivým informacím. Pro účely vyhodnocení oprávnění uživatele k provedení určité akce (operace) mohou tyto systémy využívat celou škálu technických prostředků - od jednoduchých autonomních snímačů (bez ukládání informací o vstupu) po centralizované či integrované on-line systémy vyhodnocující identitu uživatele na základě biometricky (které využívají databázová úložiště jako zdroj informací o přístupových právech i jako úložiště všech událostí a transakcí s možností další analýzy).

Klíčovým je pro tyto systémy zejména způsob ověřování identity uživatele s ohledem na rizikovost prostředí, požadovaný stupeň zabezpečení a způsob přidělování příslušných oprávnění. S tím souvisí často zaměňované a někdy komolené pojmy autentizace a autorizace.

**Autentizace** – obecně můžeme říci, že se jedná o proces jednoznačného určení uživatele přistupujícího k systému. Požadavek na autentizaci uživatele je v praxi dán stupněm zabezpečení a může se pohybovat od jednoduchého PINu, přes použití identifikačního média (tokenu) po biometrické prostředky nebo kombinované (vícestupňové) ověření identity.

**Autorizace** – je proces ověření resp. udělení práv na základě zjištěné identity. V případě systému kontroly vstupů se může například jednat o udělení přístupu do chráněných prostor.

Systémy kontroly vstupů ovládají, po ověření identity uživatele a rozhodnutí o povolení přístupu, mechanické zabezpečovací systémy (MZS), které fyzicky zabraňují vstupu neoprávněných osob do chráněných oblastí.

### 2.1 Základní pojmy a definice

Pro systémy kontroly vstupů jsou v praxi používány nejrozličnější názvy a můžeme říci, že co výrobce či autor textu to jiné pojmenování. Nejčastěji se můžeme setkat s označením „vstupní systém“, které lze považovat za relativně výstižné označení bez nebezpečí záměny s jinými (podobnými) systémy. Méně vhodné jsou názvy „identifikační systém“,

„přístupový systém“ a další varianty, které se poměrně často zaměřují s implementacemi docházkových systémů, tedy aplikacemi pro kontrolu a evidenci přítomnosti zaměstnanců na pracovišti.

Jaké označení je tedy správné? Pro bezpečnostní aplikace platí technická norma ČSN EN 50133 s názvem „Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích“, která definuje název takového systému jako „Systém kontroly vstupů“ [5].

Tato norma je v platné podobě rozdělena do 3 dokumentů:

- **ČSN EN 50133-1** (Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky) včetně změny A1 [5],[4]
- **ČSN EN 50133-2-1** (Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty) [6]
- **ČSN EN 50133-7** (Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace) [7]

V této práci bude dále dodržována terminologie definovaná výše uvedenou normou. Pojdme si tedy projít základní názvosloví definované normou ČSN EN 50133-1 (kap. 3) [5]:

**přístup** (access): akce vstupu dovnitř nebo výstupu ven ze zabezpečeného prostoru

**systém kontroly vstupů** (access control system): systém obsahující všechna konstrukční a organizační opatření včetně těch, která se týkají zařízení nutných pro řízení vstupů

**jednotka řízení vstupů** (access control unit): zařízení, které rozhoduje o uvolnění jednoho nebo několika přístupových míst a řídí sled souvisejících ovládaní

**skupina přístupu** (access group): několik uživatelů se stejnou úrovní přístupu

**filtr přístupu** (access grid): jeden nebo několik zabezpečených prostorů přiřazených k přístupové úrovni

**úroveň přístupu** (access level): oprávnění uživatele z pohledu přístupu do stanoveného přístupového filtru a souvisejícího časového filtru

**místo přístupu** (access point): místo, ve kterém může být přístup ovládán pomocí dveří, turniketem nebo jinou zabezpečovací závorou

**rozhraní místa přístupu** (access point interface): zařízení, které ovládá uvolnění zabezpečení místa přístupu poté, co byl přístup poskytnut

**snímač místa přístupu** (access point reader): zařízení používané k získávání rozpoznávacích údajů z identifikačního zařízení nebo biometrie; v případě, kdy je vyžadováno osobní identifikační číslo, může mít toto zařízení připojenu klávesnici

**výstraha** (alert): požadavek na lidský zásah po aktivaci indikátoru

**hlášení** (annunciation): podávání informací pro správu systému nebo pro ostatní systémy

**apas** (výstupní ovládací prvky a senzory místa přístupu) (apas): ovládací prvky a senzory místa přístupu; příkladem ovládacích prvků jsou elektrické otvírače dveří, elektronické zámky, turnikety a závory; příkladem senzorů jsou kontakty, spínače, tlaková signalizační zařízení a dvevní spínače

**apas uzavřen** (apas closed): apas je uzavřen, pokud místo přístupu neumožňuje volný průchod

**apas otevřen** (apas open(ned)): apas je otevřen, pokud místo přístupu umožňuje volný průchod

**apas narušen** (apas violation): neoprávněná operace s místem přístupu

**biometrie** (biometric): informace, týkající se jedinečných fyziologických vlastností uživatele

**událost** (event): změna objevující se uvnitř systému kontroly vstupů

**chybné povolení** (false acceptance): poskytnutí přístupu neoprávněnému uživateli

**chybné odmítnutí** (false rejection): odepření přístupu oprávněnému uživateli

**poruchový stav** (fault condition): jakýkoli stav, který vede k přerušení nebo k postupnému zhoršování funkčnosti systému kontroly vstupů

**informace uložena v paměti** (memorised information): informace známá uživateli

**normální stav** (normal condition): systém kontroly přístupů je plně funkční a je schopen zpracovat všechny události v souladu s předvoleným postupy



**napájení** (power supply): ta část systému kontroly vstupů, která poskytuje napájení pro provoz systému nebo kterékoliv jeho části

**zpracování** (processing): srovnávání informací s předvolenými postupy s cílem rozhodnout o poskytnutí nebo odmítnutí přístupu uživatelům a/nebo srovnávání události s předvolenými postupy s cílem přijmout příslušné akce

**programování** (programmability): schopnost přijímat a ukládat předvolené postupy

**uvolnění** (release): signál do apas, že byl poskytnut přístup

**zabezpečený prostor** (security controlled area): prostor vytyčený fyzickými závorami včetně jednoho nebo více míst přístupu

**ochrana proti sabotáži** (tamper protection): metody používané k ochraně systému kontroly přístupů nebo jeho částí proti úmyslnému narušení

**časový filtr** (time grid): jedna nebo více časových zón přiřazených k přístupové úrovni

**časová zóna** (time zone): jeden nebo více časových intervalů kombinovaných s kalendářními informacemi

**časový interval** (time slot): časový interval mezi dvěma danými okamžiky indikujícími začátek a konec platné periody v rámci časové zóny

**identifikační prvek** (token): identifikační data poskytovaná ve formě přístupových karet, klíčů, štítků apod.

**transakce** (transaction): událost, která odpovídá uvolnění přístupového místa poté, co byla rozpoznána identita uživatele

**uživatel** (user): osoba žádající průchod místem přístupu

**identita uživatele** (user identity): informace, které jsou přenášeny přímo uživatelem do rozpoznávacího zařízení pomocí identifikačního prvku (tokenu) uživatele

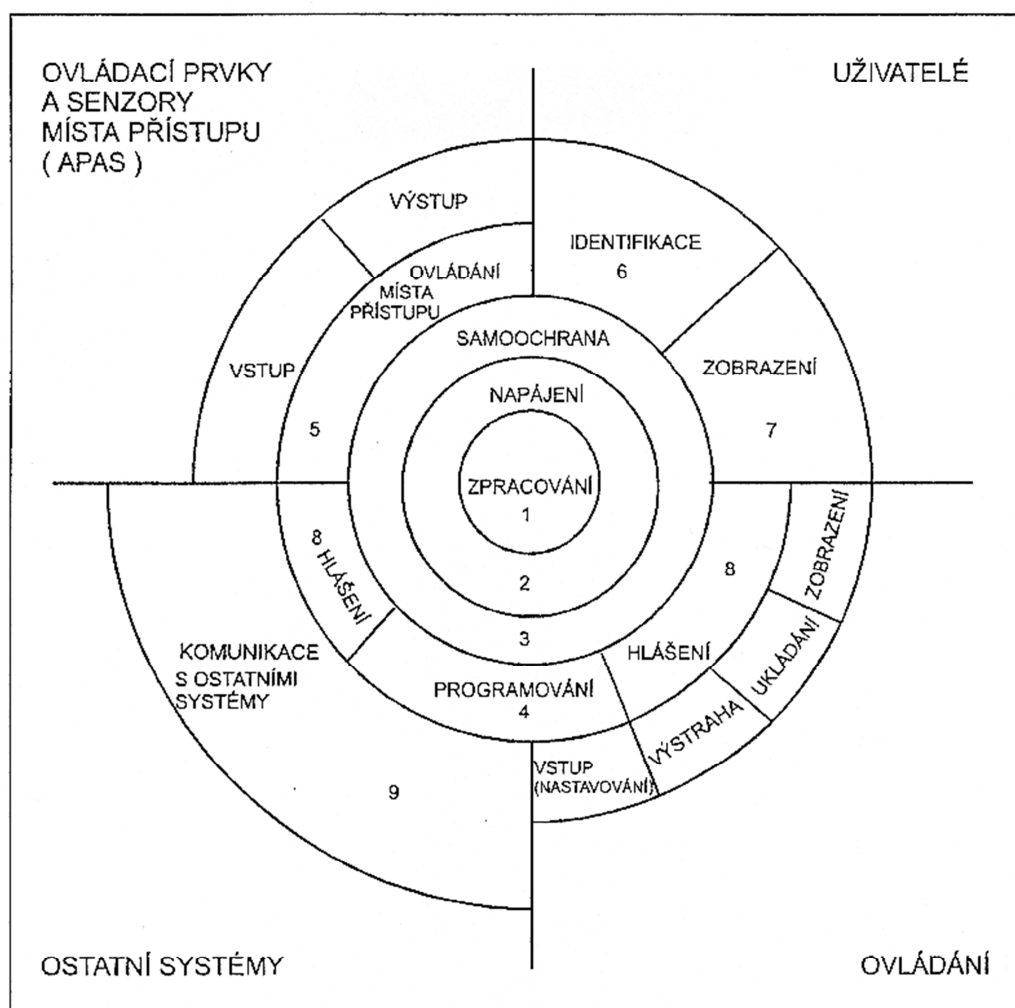
## 2.2 Základní funkce systémů kontroly vstupů

Základní funkce systémů kontroly vstupů slouží k zajištění provozuschopnosti zařízení, jeho ovládání a pro případné kombinace či integrace s ostatními bezpečnostními aplikacemi. Tyto funkce jsou nezbytné pro plnění úkolů, k nimž bylo zařízení

konstruováno. Mezi základní funkce systému kontroly vstupů řadí norma ČSN EN 50133-1:

- zpracování (1)
- napájení (2)
- samoochrana (vnitřní zabezpečení) (3)
- programování (4)
- ovládání místa přístupu (5)
- identifikace (6)
- zobrazování uživateli (7)
- hlášení (8)
- komunikace s ostatními systémy (9)

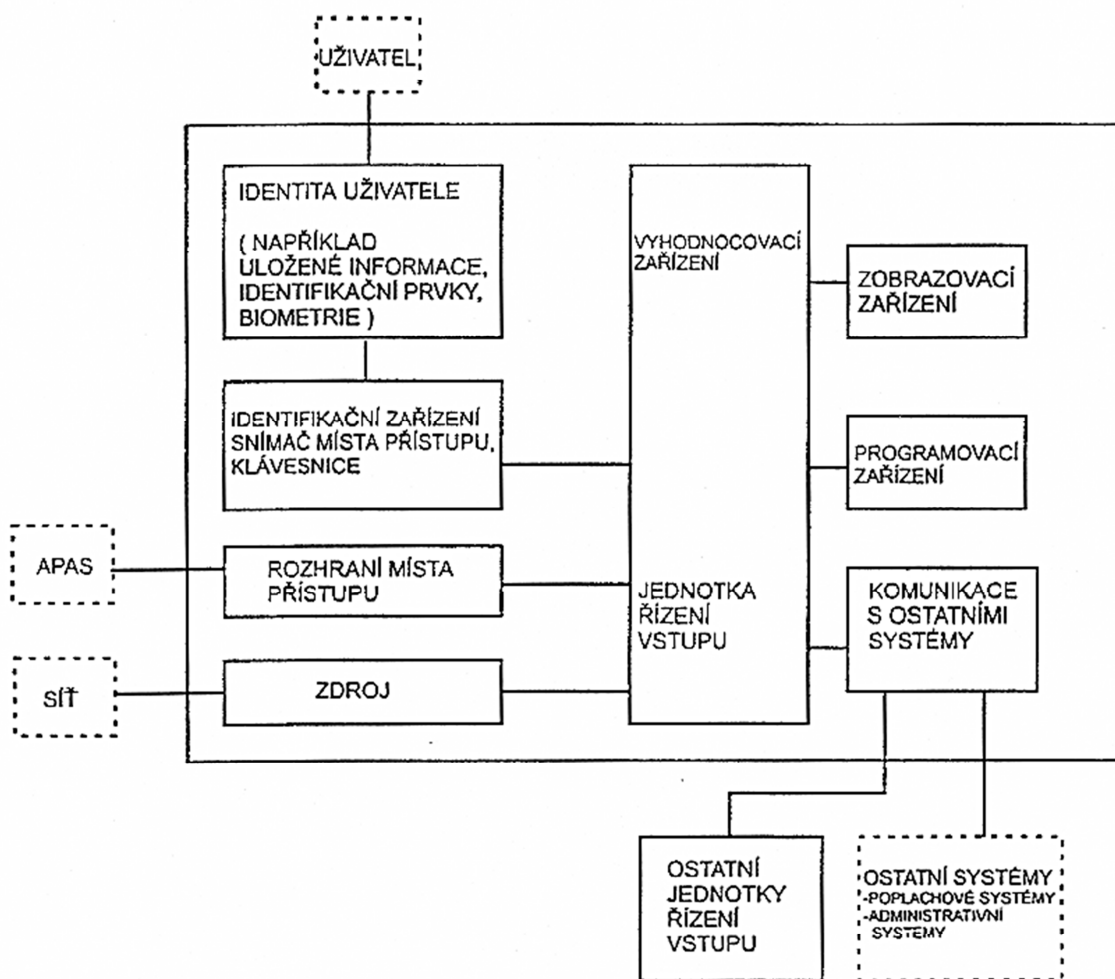
Zda zařízení obsahuje výše uvedené funkce, závisí především na jeho konfiguraci. Kupříkladu při nasazení autonomního systému není smysluplné vyvíjet funkce pro komunikaci s ostatními systémy, norma ani tuto povinnost nestanovuje [5].



Obrázek 1 – Základní funkce systému kontroly vstupů - ČSN EN 50133-1  
(kap. 4.1)

### 2.3 Komponenty systémů kontroly vstupů

Vyvíjené zařízení se může skládat z více komponentů (například vyhodnocovací jednotky, čtečky a komunikačního rozhraní), nebo může být homogenní, kdy jsou všechny funkce integrovány do jednoho modulu. V následujícím obrázku je příklad uspořádání funkcí v systému kontroly vstupů převzatý z normy ČSN EN 50133-1 [5]. Přerušovanou čarou jsou vyznačeny komponenty, které nejsou součástí této normy.



Obrázek 2 – Příklad uspořádání funkcí - ČSN EN 50133-1 (kap. 4.2)

## 2.4 Rozdělení systémů pro kontrolu vstupů

Systémy kontroly vstupů lze rozlišovat podle mnoha kritérií. Velmi často se můžeme setkat s rozdělením podle způsobu vyhodnocování, tedy jakým způsobem je do jednotky řízení přístupu dodávána informace o povolených identitách (identifikátorech) uživatelů. V tomto případě pak systémy můžeme členit na následující:

- 1) Autonomní – každá jednotka řízení vstupu je nezávislá a obsahuje vlastní seznam identit uživatelů a programuje se zvlášť.
- 2) Síťové – všechny jednotky předávají identitu uživatele centrálnímu prvku, který rozhodne o povolení či zamítnutí přístupu či provedení akce.
- 3) Hybridní – jednotky řízení přístupu rozhodují o udělení či zamítnutí přístupu autonomně, data reprezentující identitu uživatelů jsou však v určitých časových intervalech aktualizována z centrálního řídicího prvku.

Všechny uvedené varianty mohou být kombinovány nebo integrovány s ostatními bezpečnostními systémy.

Další možná dělení jsou dle stupně rizikovosti, způsobu identifikace osob atd. Pro naše účely si ovšem vystačíme s výše uvedeným rozdělením.

## 2.5 Všeobecné požadavky - ČSN EN 50133-1

Norma ČSN EN 50133-1 [5] definuje velmi komplexním způsobem požadavky na systém kontroly vstupů. Vzhledem k tomu, že se v tomto projektu jedná o návrh řešení jednoduchého autonomního systému a jeho testovací zapojení, není nutné brát v potaz všechny požadavky normy jako například testování výrobku, jeho umístění, zabezpečení proti sabotáži atd. Otázky tohoto charakteru by bylo nutné řešit až v případě uvádění konkrétního produktu na trh v rámci EU. Nám postačí splnění základních (všeobecných) požadavků na systém definovaných normou, tedy třídy identifikace, třídy přístupu a ochrany programování.

### 2.5.1 Třídy identifikace

Z důvodu požadavku na zajištění příslušné úrovně bezpečnosti rozdělené podle stupně rizikovosti definuje norma ČSN EN 50133-1 (kapitola 5.1.1) třídy identifikace [5]. Rozlišovány jsou čtyři úrovně identifikace uživatelů systémů kontroly vstupů. Tyto třídy vyjadřují jakost vztahu mezi identifikací použitou daným systémem a uživatelem. Třídy identifikace se mohou v rámci jednoho systému měnit v průběhu času a rovněž mohou být definovány zvlášť pro vstup/výstup z/do chráněné oblasti.

**Třída identifikace 0** – žádná přímá identifikace: Založena na prostém požadavku o přístup bez identity uživatele (tlačítko, kontakt, čidlo pohybu...).

**Třída identifikace 1** – informace uložena v paměti: Založena na heslech, osobních identifikačních číslech, atd.

**Třída identifikace 2** – identifikační prvek nebo biometrie: Založena na používání identifikačních prvků, karet, fyzických klíčů, otisku prstů atd.

**Třída identifikace 3** – identifikační prvek nebo biometrie spolu s informací uloženou v paměti: Založena na používání kombinace identifikačního prvku nebo biometrie a informace uložené v paměti.

### 2.5.2 Třídy přístupu

V reálném nasazení může nastat potřeba zajištění časového omezení přístupů uživatelů do chráněných oblastí (např. vstup uživatelů jen v pracovní době). Norma ČSN EN 50133-1 (kapitola 5.1.2) [5] proto definuje následující třídy přístupu:

**Třída přístupu A:** Tato třída platí pro místo přístupu, ve kterém požadovaný stupeň zabezpečení nevyžaduje ani časový filtr ani ukládání přístupové transakce.

**Třída přístupu B:** Tato třída platí pro místo přístupu, které zahrnuje časové filtry a funkce ukládání. Zahrnuje také podtřidu, která se vztahuje na místo přístupu zahrnující časové filtry, ale bez funkcí ukládání dat.

### 2.5.3 Ochrana programování

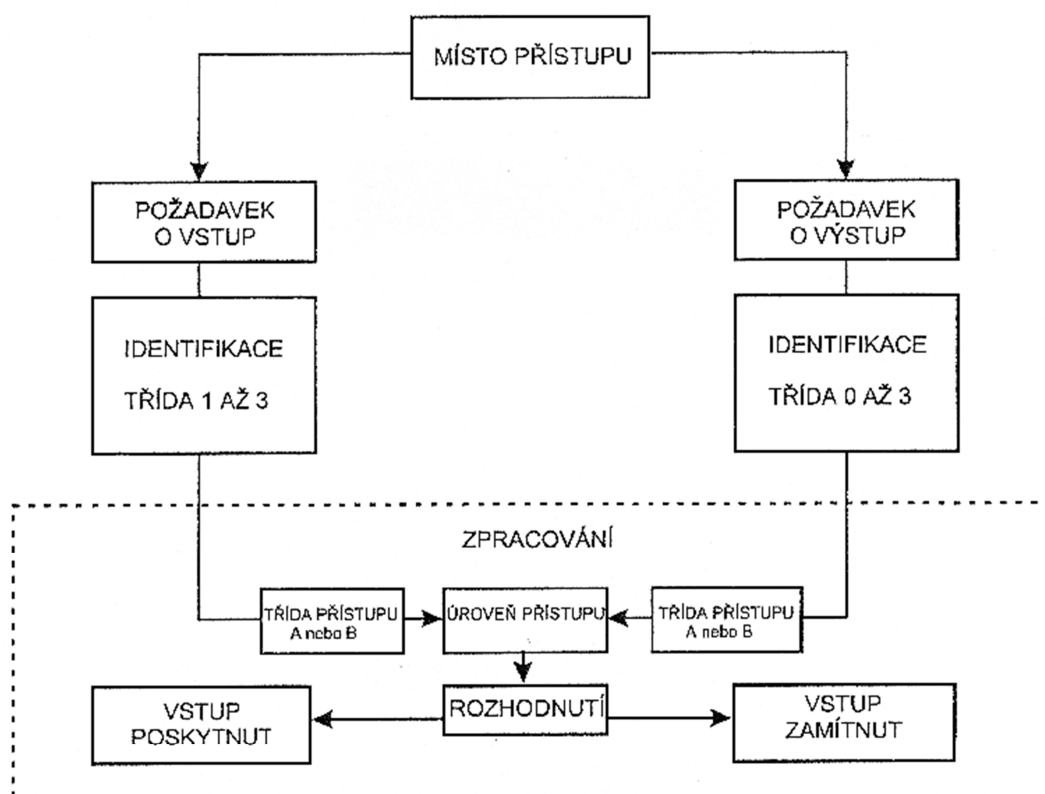
Každý systém kontroly vstupů splňující požadavky normy ČSN EN 50133-1 musí disponovat prostředky pro ochranu rozhraní určeného k programování zařízení. Ochrana před neoprávněnou změnou zadaných dat musí být zajištěna použitím vhodné technologie (například přístupového kódu), přičemž musí být zajištěno, aby minimální počet kombinací byl alespoň 10 000 a poměr počtu různých kombinací kódu k počtu oprávněných osob byl nejméně 1 000:1. Zároveň však správce systému musí mít možnost změnit kód programovacího rozhraní [5].

## 2.6 Zpracování povoleného přístupu

Rozhodnutí, zda bude uživateli udělen přístup, probíhá následujícím způsobem. Identifikační zařízení (například čtečka, klávesnice atd.) přijme informace o uživateli. Pak v závislosti na tom, zda se jedná o požadavek na vstup do chráněné oblasti či výstup z ní, proběhne identifikace uživatele. Zde je vhodné zdůraznit, že systém může být co do ověření uživatele asymetrický - při vstupu do chráněné oblasti může vyžadovat prokázání identity uživatele, ale při výstupu z ní již může uživatel odejít volně (například otevřením dveří pomocí tlačítka, nebo pouhým stisknutím kliky u dveří). Po identifikaci uživatele dojde ke zpracování požadavku a s ohledem na třídu a úroveň přístupu provede jednotka řízení přístupu rozhodnutí o povolení či odepření přístupu. Současně mohou probíhat další

operace jako je zaznamenání prováděné transakce, případně komunikace s dalšími bezpečnostními systémy jako jsou Intrusion Alarm System (IAS), či Closed Circuit Television (CCTV).

Následující obrázek ukazující zpracování přístupu je součástí normy ČSN EN 50133-1 [5]:



Obrázek 3 – Tradiční postup povoleného přístupu - ČSN EN 50133-1 (kap. 4.3)

### 3 POUŽITÉ TECHNOLOGIE A KOMPONENTY

#### 3.1 Mikrokontrolér (Microcontroller Unit - MCU)

Mikrokontrolér (občas označovaný také jako jednočipový mikropočítač) je zjednodušeně řečeno integrovaný obvod obsahující na jediném čipu kromě aritmeticko logické jednotky (ALU) také všechny periferní obvody potřebné pro samostatnou činnost, jako jsou například paměti, A/D převodníky, komunikační rozhraní, systémy čítačů, časovačů, obsluhy přerušení atd. V rámci tohoto projektu je MCU klíčovou součástí celého řešení, neboť obsluhuje celé zařízení a vykonává veškerou naprogramovanou logiku. V následujících kapitolách proto bude rozebrán poněkud podrobněji než ostatní části řešení. Cílem však není čtenáře dopodrobna seznámit s funkcemi MCU (jen produktový list ATmega128 s čistě technickým popisem má 391 stran), ale alespoň nastínit způsob práce mikrokontroléru a jeho možnosti.

##### 3.1.1 AVR Architektura

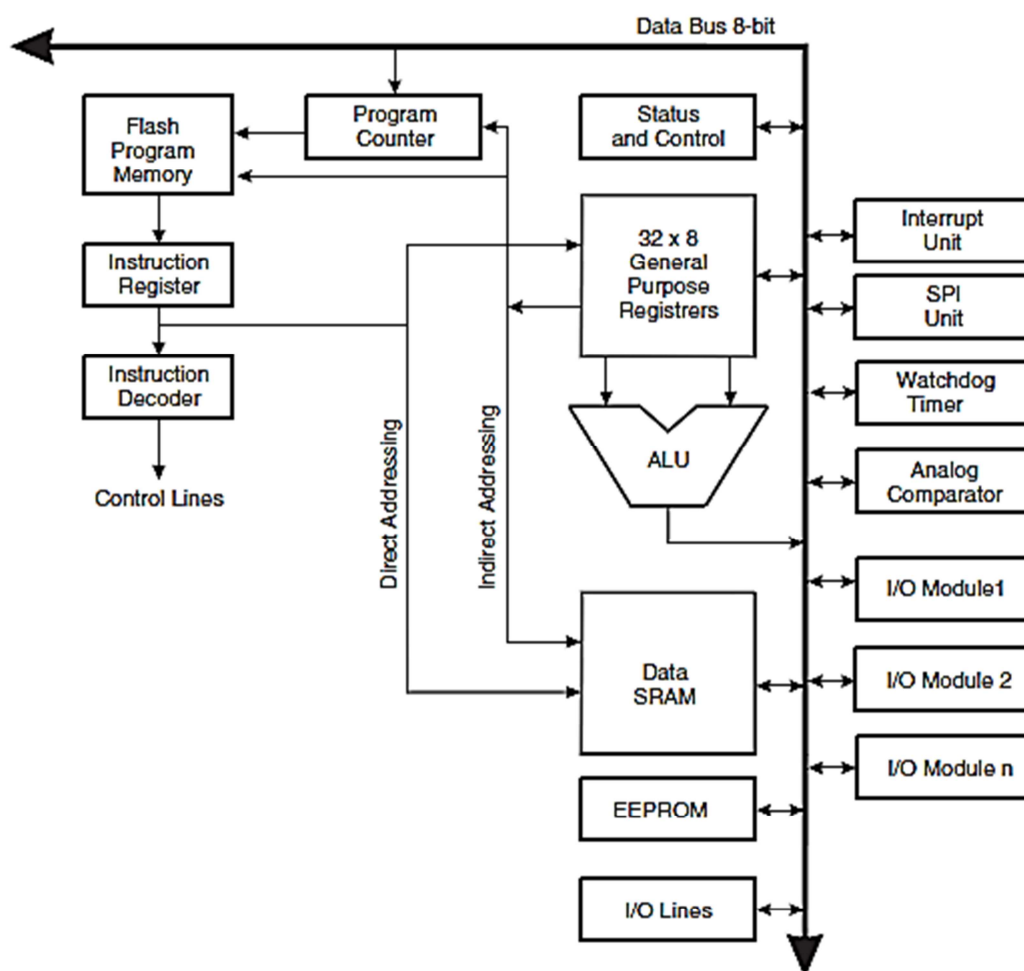
Architektura AVR byla vyvinuta v Norském vývojovém centru Nordic VLSI v Trondheimu. Základy této technologie položili dva studenti z Norského technického institutu - Alf-Egil Bogen a Vegard Wollan. Podle jejich jmen pak vznikla původní zkratka AVR (Alf-Egil Bogen, Vegard Wollan, RISC microcontroller), která je však nyní oficiálně prezentována jako Advanced Virtual RISC.

Procesory AVR jsou založené na Harvardské architektuře (mají oddělenou paměť pro program a data). Jedná se o procesory typu RISC, složené ze třiceti dvou stejných osmibitových registrů pro obecné použití (mohou obsahovat data i adresy). Registry jsou přímo propojeny s aritmeticko-logickou jednotkou (ALU), což znamená, že ALU je schopna v jednom hodinovém cyklu provést právě jednu instrukci (s výjimkou komunikace s pamětí).

Zkratky RISC a CISC představují dvě rozdílné architektury centrální procesorové jednotky (Central Processor Unit - CPU). CISC (Complex Instruction Set Computer) má instrukční soubor s takovými instrukcemi, které pod jedním operačním kódem vykonají složité operace. Koncepce procesorů RISC (Reduced Instruction Set Computer) je naopak založena na předpokladu, že četnost využití některých komplexních instrukcí (použitých v architektuře CISC) je v praxi tak malá, že se nevyplatí budovat na čipu mikroprocesoru řídicí obvody pro jejich zpracování. U RISC architektury zabírají řídicí obvody zhruba

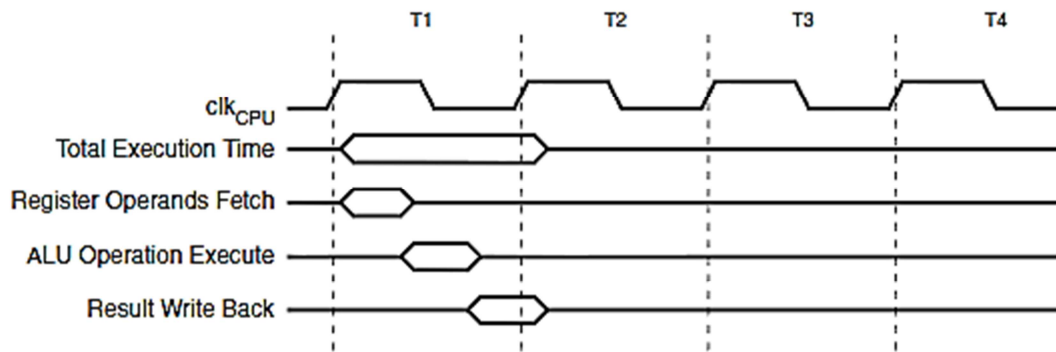


5-10% místa oproti asi 60% u architektury CISC. Takto získané místo je na čipu mikroprocesoru využito pro větší množství registrů, jejichž zpracování pomocí instrukcí je prováděno v rámci jednoho taktu procesoru.



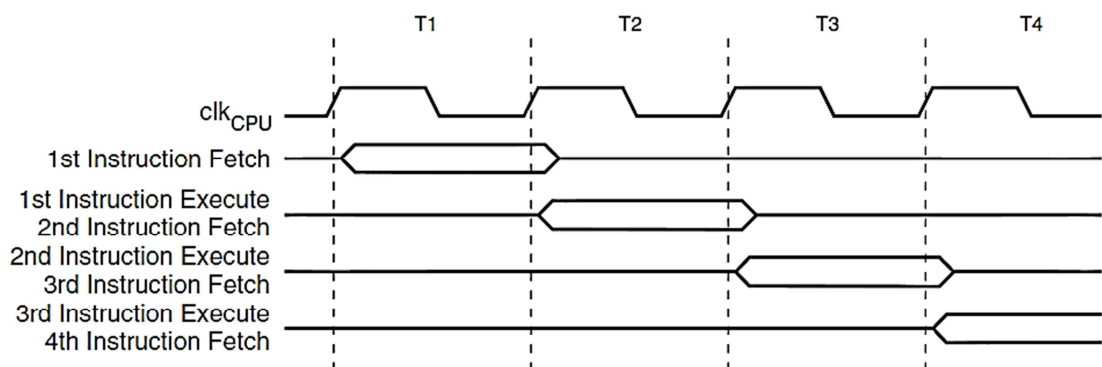
Obrázek 4 – Blokové schéma architektury AVR [2]

Zpracování operandů je následující: operandy jsou během jednoho taktu načteny z pracovních registrů, provede se operace a výsledek je opět uložen do příslušného registru. Vždy se jedná o operace registr-registr, na kterých je AVR technologie založená.



Obrázek 5 – Zpracování operace v rámci jednoho cyklu ALU [2]

Zatímco je jedna instrukce zpracovávána, další instrukce je připravována pro zpracování. Tento koncept umožňuje procesoru zpracovat v ideálním případě až 1 milión instrukcí za sekundu na 1 MHz taktu.



Obrázek 6 – Zpracování instrukcí [2]

Architektura RISC má ale i své záporné stránky. Redukovaná instrukční sada totiž svojí koncepcí způsobuje omezení při zpracování operací, neboť pouze některé instrukce umožňují pracovat s přímými datovými typy, navíc pouze s omezeným počtem registrů. Ostatní instrukce mohou pak pracovat pouze s registry.

### 3.1.2 ATmega128

ATmega128 je 8-bitový mikrokontrolér založený na architektuře AVR RISC s maximální taktovací frekvencí 16 MHz při řízení externím krystalem [2]. Díky vykonávání

1 instrukce v rámci jednoho taktu dosahuje výkonu až 16 MIPS. Tento mikrokontrolér je velmi bohatě vybaven. Mezi základní funkce patří:

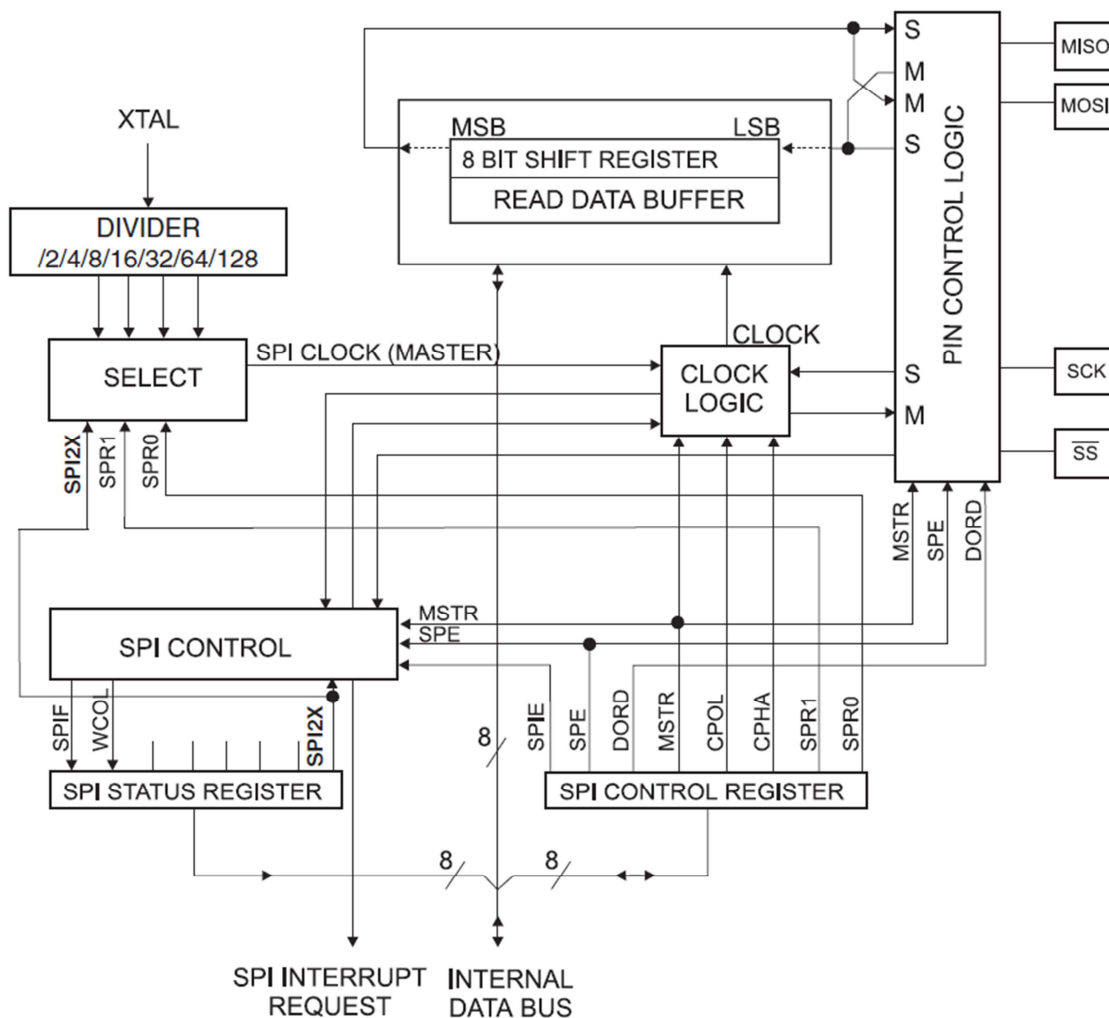
- 133 výkonných instrukcí, většinou jedno-cyklových
- 32 osmibitových pracovních registrů
- Maximální výpočetní výkon 16 MIPS při maximálním kmitočtu 16 MHz
- Programová FLASH paměť o velikosti 128 kB, programovatelná přímo v aplikaci s možností uzamknutí, 10.000 zápisových/mazacích cyklů s volitelnou velikostí bootloader sekce
- 4 kB datové paměti typu EEPROM
- 4 kB vnitřní datové operační paměti typu SRAM
- Data jsou uložena 20 let při 85 °C nebo 100 let při 25 °C
- Možnost zablokování programové paměti proti čtení či zápisu
- Možnost programování pomocí rozhraní JTAG nebo SPI
- Dva osmibitové čítače/časovače
- Dva rozšířené šestnáctibitové čítače/časovače
- Dva osmibitové PWM kanály
- 6 PWM kanálů s programovatelným rozlišením 2-16 bitů
- Osmikanálový 10-bitový A/D převodník
  - Osm jednoduchých kanálů
  - Sedm diferenčních kanálů
  - Dva diferenční kanály s programovatelným zesílením 1x, 10x nebo 200x
- Analogový komparátor
- Dvě programovatelná USART komunikační rozhraní
- Možnost komunikace pomocí SPI, TWI
- Šest módů snížené spotřeby
- Programovatelný Watch-dog časovač s oscilátorem na čipu
- Možnost nastavení interního RC oscilátoru
- 53 programovatelných vstupně výstupních pinů (vývodů)
- Napájecí napětí 4.5 - 5.5 V.



Jak již bylo zmíněno výše, rodina MCU AVR je založena na Harvardské architektuře, která odděluje paměť pro data programu (uložená v paměti SRAM) od programového kódu (uloženého v paměti typu FLASH). Paměť EEPROM je nevolatilní a v našem případě bude využita pro uložení identifikačních čísel zaregistrovaných tokenů. Tato oblast paměti má velikost 4 kB, což znamená, že při potřebě 8 bytů na uložení jednoho identifikátoru iButton bychom do této paměti mohli uložit informace o 512 předmětech. V rámci tohoto projektu se předpokládá, že jeden autonomní vstupní systém bude obsluhovat maximálně desítky předmětů. Kapacita paměti pro uložení identifikátorů je tedy navržena s dostatečnou rezervou.

### ***3.1.2.2 Synchronní sériový port (SPI, Serial Peripheral Interface)***

Sběrnice SPI je jednou z variant sériových sběrnic sloužících pro vzájemné propojení dvou a více komunikujících uzlů. Tato sběrnice má všestranné využití a v praxi je použita pro velkou škálu činností - od programování mikrokontroléru až po připojení externích pamětí a dalších zařízení. Aby bylo možné sběrnici provozovat v synchronním (a obousměrném) režimu, vystupuje jeden uzel jako řadič sběrnice (master), ostatní uzly pracují v režimu slave. Uzel s rolí master obsahuje generátor hodinového signálu, který je pomocí sběrnice rozveden ke všem uzlům. Hodinový signál je rozváděn vodičem, který je označován jako SCK. Kromě něj obsahuje sběrnice ještě následující vodiče: MISO (Master In, Slave Out) a MOSI (Master Out, Slave In), sloužící k obousměrné (full duplex) komunikaci. Posledním signálem, který se u této sběrnice používá, je signál SS (Slave Select), určený ke zvolení uzlu pracujícího v režimu slave. U mikrokontroléru ATmega128 jsou funkce SS, SCK, MOSI a MISO dostupné na vývodech PB0-PB3.

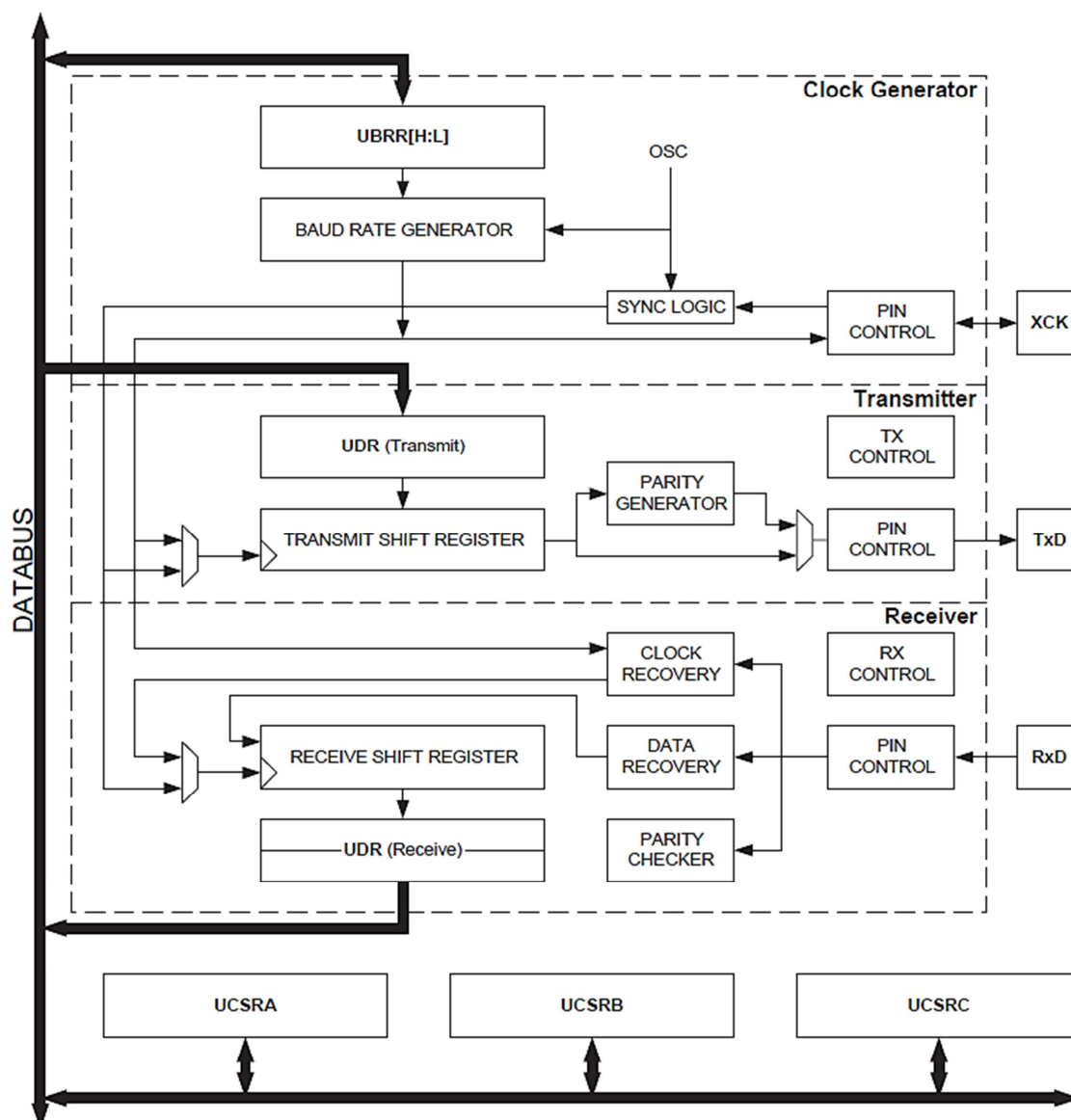


Obrázek 8 – Schéma sériového rozhraní SPI – ATmega128 [2]

### 3.1.2.3 Univerzální synchronní/asynchronní sériový kanál (USART)

USART je rozhraním pro sériovou komunikaci umožňující práci v synchronním (half duplex) nebo asynchronním (full duplex) režimu. Komunikace je realizována pomocí dvou vodičů označovaných jako Tx (Transmit - odeslání) a Rx (Receive – příjem). Rozhraní má vestavěný generátor parity a je schopno rovněž paritu při příjmu dat kontrolovat. Dále je vybaveno detekcí chybných stavů na sběrnici.

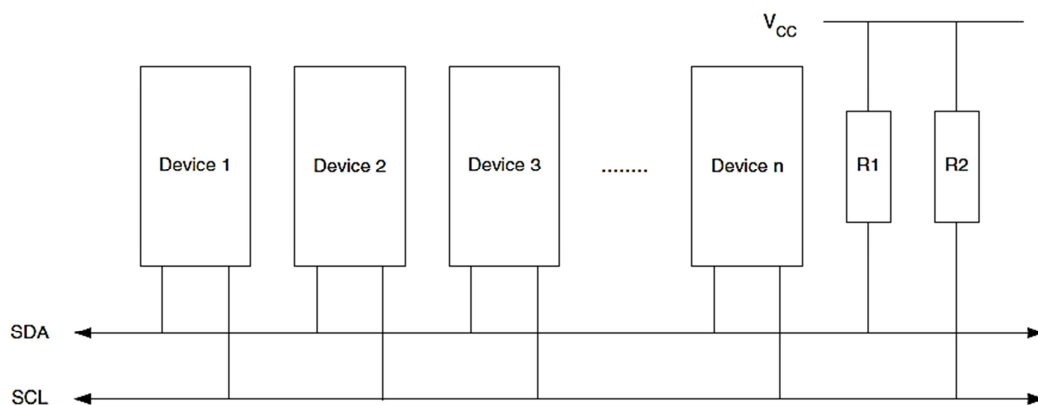
Mikrokontrolér ATmega128 disponuje dvěma rozhraními USART umístěnými na vývodech PE0, PE1 (USART0) a PD2, PD3 (USART1) [2].



Obrázek 9 – Blokové schéma sériového kanálu USART [2]

### 3.1.2.4 Synchronní sériový kanál (TWI)

Mikrokontrolér ATmega128 disponuje jedním rozhraním TWI (Two-Wire Interface), což je v podstatě modifikace licenčně chráněné sběrnice I2C firmy Philips. Sběrnice TWI je ideální pro potřeby mikrokontrolérových aplikací, neboť umožňuje připojení až 128 různých zařízení pomocí dvou vodičové obousměrné sběrnice, kdy jeden vodič slouží pro časování (SCL) a druhý pro data (SDA). Oba vodiče musí být vybaveny pull-up odpory, sběrnice je tedy typu open-drain. Na mikrokontroléru ATmega128 je TWI rozhraní přítomno na vývodech PD0 (SCL) a PD1 (SDA) [2].

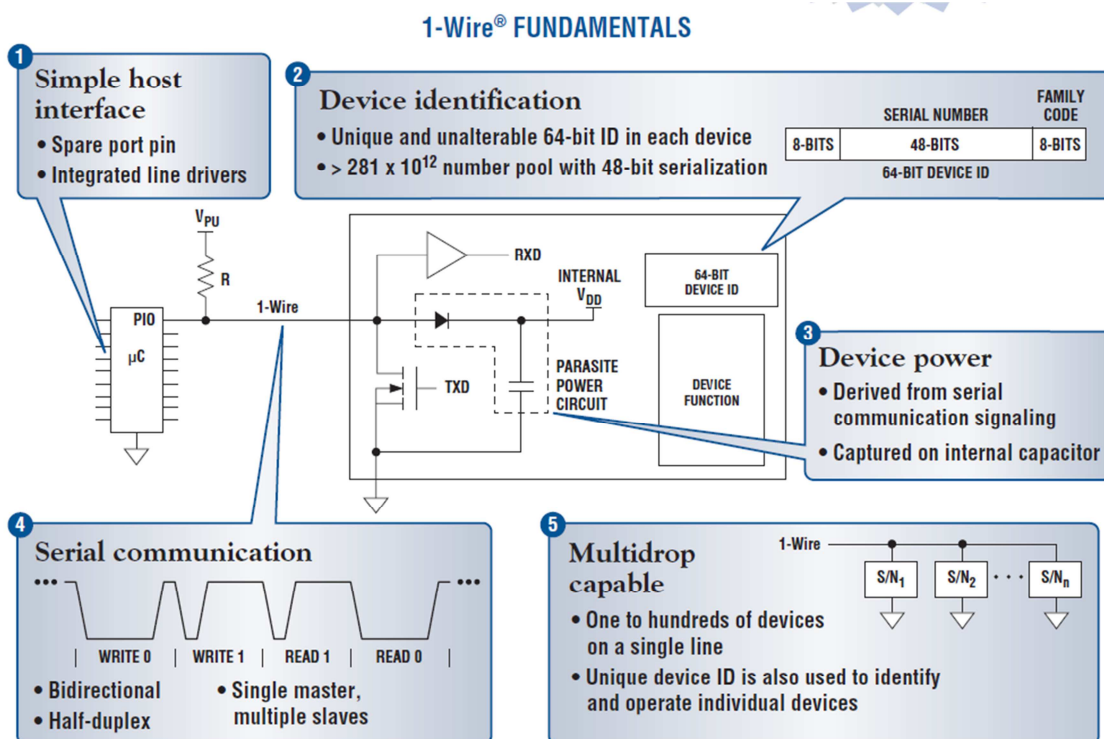


Obrázek 10 – Propojení zařízení pomocí TWI [2]

### 3.2 Komunikační rozhraní 1-Wire

1-Wire je sběrnice navržená firmou Dallas Semiconductor (která byla v roce 2001 zakoupena firmou Maxim Integrated Products) [1]. Jedná se o sériovou sběrnici umožňující připojení několika ovládaných zařízení (Slave) a řídicí jednotky (Master) pomocí jediného datového vodiče (a společné země). Komunikace na sběrnici je obousměrná, asynchronní a poloduplexní. Sběrnice pracuje na rychlostech 15.4 kbps resp. 125 kbps (Overdrive režim). Ačkoli byla tato sběrnice koncipována pro připojení blízkých zařízení, je v současnosti její délka závislá na použité topologii - například maximální vzdálenost mezi dvěma zařízeními Master/Slave je 750 m. Běžně se používá do vzdálenosti několika metrů. Snímače mohou být napájeny přímo ze sběrnice (Parasite-Power), což je ideální pro bezpečnostní aplikace, pro které je sběrnice často využívána. 1-Wire bohužel není přímo implementována v mikrokontrolérech ATmega, je jí však relativně jednoduché emulovat softwarově, protože obsahuje pouze čtyři základní operace: zápis 1, zápis 0, čtení a reset. Klíčové je však při softwarové implementaci časování. Aby mohlo více zařízení komunikovat po jednom vodiči, definuje 1-Wire časové úseky (timeslots) v jejichž rámci zařízení komunikují. Datový vodič je přes odpor připojen na napájecí napětí a určuje tak logickou jedničku. Uzemněním datového vodiče pak zařízení definují logickou nulu. Detailní popis komunikace je složitější a její podrobný popis je možné získat na stránkách výrobce [1].





Obrázek 11 – Základní schéma sběrnice 1-Wire – Maxim Integrated Products [2]

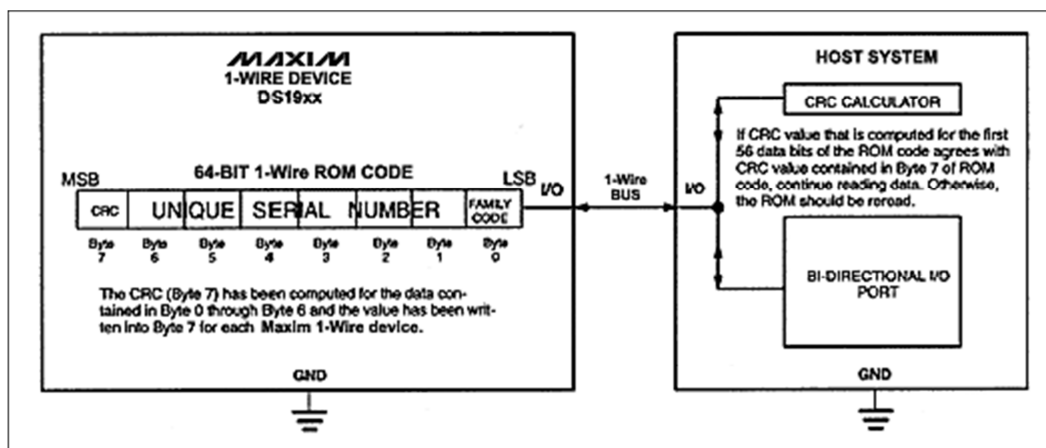
### 3.3 Dotykové identifikační prvky iButton

Firma Maxim Integrated Products vyrábí velké množství různých typů identifikačních prvků (tokenů) s komerčním názvem iButton [1], které je možné využít pro nejrůznější systémy kontrolu vstupů, docházkové systémy atd. Jedná se o počítačový čip (integrováný obvod) uzavřený v malém nerezovém pouzdře o průměru 16 mm. Prvky iButton využívají své pouzdro jako kontakt pro komunikační rozhraní sběrnice 1-Wire [1], přes kterou jsou ve své základní verzi rovněž napájeny. Každý prvek je identifikován pomocí nezměnitelného unikátního 64bitového identifikačního čísla, které je u některých verzí laserem vygravírováno na povrchu pouzdra.



Obrázek 12 – Identifikační prvek iButton

Aby byla zajištěna bezpečná identifikace konkrétního tokenu, používá se kontrola načtení identifikačního čísla výpočtem kontrolního součtu (CRC) pomocí polynomu  $X^8+X^5+X^4+1$ . Pokud je vypočtený kontrolní součet prvních 56 bitů načteného identifikačního čísla zařízení shodný s hodnotou uloženou v sedmém bytu, lze čtení prohlásit za platné.



Obrázek 13 – Načtení kontrolního součtu prvku iButton

Prvky iButton [1] se vyrábějí ve zhruba dvaceti různých verzích a mohou kromě identifikačního čísla obsahovat i další funkce. Základní provedení jsou následující:

- Address Only (základní verze, obsahuje 64 bitů ROM)
- Memory (NV RAM, EPROM, EEPROM)
- Real-Time Clock (kalendáře, hodiny, stopky apod.)
- Secure (bezpečnostní zařízení jako např. elektronické zámky, parkovací hodiny, softwarová autorizace a další)
- Data Logger (záznam teploty, vlhkosti apod.)

Pro účely tohoto projektu postačí nejlevnější základní verze s identifikačním číslem označovaná jako iButton DS1990A [1].

## **II. PRAKTICKÁ ČÁST**

## 4 NÁVRH ŘEŠENÍ

Po analýze zadání, prostudování příslušné literatury, technických listů a norem je možné přistoupit k vlastnímu návrhu zařízení. Návrh vychází z požadavků na funkčnost zařízení (kap. 1), zohledňuje provedenou technickou i ekonomickou analýzu, předpokládanou úroveň zabezpečení a požadavky dané příslušnou normou. Plánované nasazení určuje terminologií normy ČSN EN 50133 výslednou Třídou přístupu A [5]. Při vstupu směrem do chráněné oblasti pak odpovídá Třídě identifikace 2 a směrem ven z chráněné oblasti Třídě identifikace 0. Zařízení nebude konstruováno jako funkční prototyp, ale jako testovací zapojení ověřující funkčnost návrhu, nebude tedy beze zbytku splňovat všechny požadavky normy ČSN EN 50133. Ačkoli je cílem této práce navrhnout bezpečnostní aplikaci, tedy autonomní systém kontroly vstupů, bude nutné se zabývat i elektronikou pro tento účel využitou. Zde není nutné vymýšlet již vymyšlené, pro tyto účely lze s výhodou využít stávajících modulů stavebnice MLAB [10]. Podrobný popis existujících modulů by byl pouhým přebíráním velmi dobře zpracovaného webu stavebnice, charakteristika modulů bude proto přiměřeně stručná. Detailní popis funkce, osazení a oživení existujících modulů je možné nalézt na uvedené URL adrese stavebnice, odkud jsou se svolením autorů převzata níže uvedená schémata zapojení. V případě neexistujících, tedy nově vytvářených modulů bude uveden podrobnější popis jejich funkce.

### 4.1 Obecný popis

Navržené zapojení je založeno na mikrokontroléru ATmega vyráběného firmou Atmel [3]. V době přípravy tohoto řešení (léto 2010) bohužel nebyl k dispozici jiný typ než pětivoltová varianta těchto mikrokontrolérů, protože firma Atmel právě měnila svůj výrobní program a připravovala novou řadu produktů. Z počátku nebylo možné přesně zvolit minimální model s odpovídající kapacitou paměti, protože ještě nebyly známy požadavky na velikost kódu, který bude tvořit obsluhu zařízení. Z dostupné nabídky MCU byl tedy vybrán ATmega 128, který disponuje 128 kB FLASH pamětí, 4 kB EEPROM (použita pro uložení ID tokenů) a 4 kB vnitřní paměti SRAM. Dále bylo nutné zohlednit, že jako identifikační prvky budou sloužit nosiče iButton, komunikující pomocí sběrnice 1-Wire [1], která nemá hardwarovou podporu u žádného z běžně používaných mikrokontrolérů. Řešení by tedy bylo buď použít specializované integrované obvody nebo komunikační protokol 1-Wire emulovat softwarově. Mikrokontroléry ATmega mají

dostatečný výkon a při taktování pomocí krystalu jsou natolik časově stabilní, že bylo možné použít softwarovou emulaci, byť za cenu většího kódu a využití více paměti. Zvolený procesor se ukázal jako dostačující, pro reálné nasazení by vyhovoval i procesor s menší kapacitou paměti FLASH.

Jak již bylo řečeno, požadovanou uživatelskou přívětivost rozhraní bylo možné řešit buď pomocí komunikace dvoudrátové sériové sběrnice (která je v ATmega128 přítomna) s osobním počítačem nebo vytvořit ovládací rozhraní s LCD displejem. Obě varianty mají své výhody a nevýhody. U komunikace pomocí sériové linky je nutné mít v počítači sériové rozhraní, což dnes již není běžné, u LCD je nutné zohlednit omezený počet zobrazitelných znaků. Po zvážení obou variant byla zvolena kombinace obou řešení, kdy ovládání zařízení zajistí menu realizované na textovém LCD displeji se zobrazovací kapacitou 16x2 znaky, rozsáhlejší informační výstupy potřebné pro ladění a diagnostiku pak budou zasílány na sériovou linku, která bude přes převodník USART/USB zakončena dnes běžným USB rozhraním.

Pro zápis přístupových transakcí a informací o změnách systému provedených správcem je ideální paměťová karta typu SD/MMC. Aby měl zápis těchto informací smysl, je zapotřebí zaznamenávat časové údaje a je tedy nezbytné aby zařízení disponovalo hodinami reálného času. Tento požadavek je dle dostupné literatury v praxi často řešen připojením hodinového krystalu s frekvencí 32768 Hz a softwarovou implementací pomocí přerušení a čítače. Toto řešení je však pro naše účely nevýhodné, protože v případě odpojení napájení je nutné při restartu zařízení znovu zadat datum a čas. Další nevýhodou je pak složitost kódu nutná pro vytvoření kalendáře (délky měsíců, přechodné roky atd.) a s tím související náročnost na paměťový prostor MCU. Existuje ovšem možnost využít specializovaný integrovaný obvod, který již bude mít funkce kalendáře implementované a bude umožňovat nezávislé zálohování data a času pomocí knoflíkové baterie. Takových integrovaných obvodů je na trhu velké množství, jedním z nich je model DS1307 firmy Maxim Integrated Products. Proč padla volba právě na tento integrovaný obvod, bude zřejmé z následujícího. S volbou LCD displeje jako ovládacího rozhraní celého zařízení bylo totiž nutné navrhnout ochranu ovládacího a programovacího rozhraní. Máme-li funkční LCD zobrazovač a implementované menu pro správu, je nejjednodušší a uživatelsky nejprívětivější, zajistit ochranu pomocí přístupového kódu vyžadovaného při vstupu do menu. Tento kód musí být uložen někde v zařízení a jako první se zde nabízí paměť EEPROM mikrokontroléru. Pokud ale obsluha kód zapomene, do ovládacího menu

se nedostane a paměť MCU je v tomto případě možné přepsat pouze programátorem. Elegantnější řešení by tedy bylo uložit PIN do oblasti, kterou by bylo možné po otevření zařízení jednoduchým způsobem smazat. A právě zde je možné využít 56 bytů paměti typu NV SRAM, kterou IO DS1307 rovněž obsahuje a která je zálohována stejnou baterií jako obvod reálného času. Výsledkem je tak zapojení, které nejen že udržuje hodiny reálného času a kalendář, ale také zajišťuje uložení přístupového kódu a umožňuje jeho změnu. Po otevření zařízení je tedy možné vyjmutím knoflíkové baterie provést smazání administrátorského kódu z paměti integrovaného obvodu, přitom však zůstanou zachována všechna ostatní nastavení včetně naprogramovaných uživatelských tokenů.

Jak již bylo řečeno, v době návrhu řešení a technického zpracování této práce nebyly na trhu k dispozici mikrokontroléry ATmega s napájením 3.3 V ale pouze 5 V varianty. To přineslo další problém, který bylo nutné při návrhu vyřešit. Paměťové karty typu SD/MMC totiž pracují s napětím 3.3 V, zatímco zbytek zařízení pracuje s 5 V logikou. V praxi by se tento problém (především z ekonomického hlediska) zřejmě řešil pomocí napětového děliče tvořeného odpory s tím, že napětí z 5 V části by bylo redukováno na požadovaných 3.3 V, opačným směrem by se pak spoléhalo na to, že 3.3 V již budou vyhodnoceny na straně 5 V logiky jako logická jednička. Tento přístup by zřejmě byl funkční, ale existuje technicky lepší řešení, kterým je nasazení převodníku napětových úrovní (Voltage Level Translator). Vyhovující je například osmibitový převodník napětových úrovní TXB0108 firmy Texas Instruments [19].

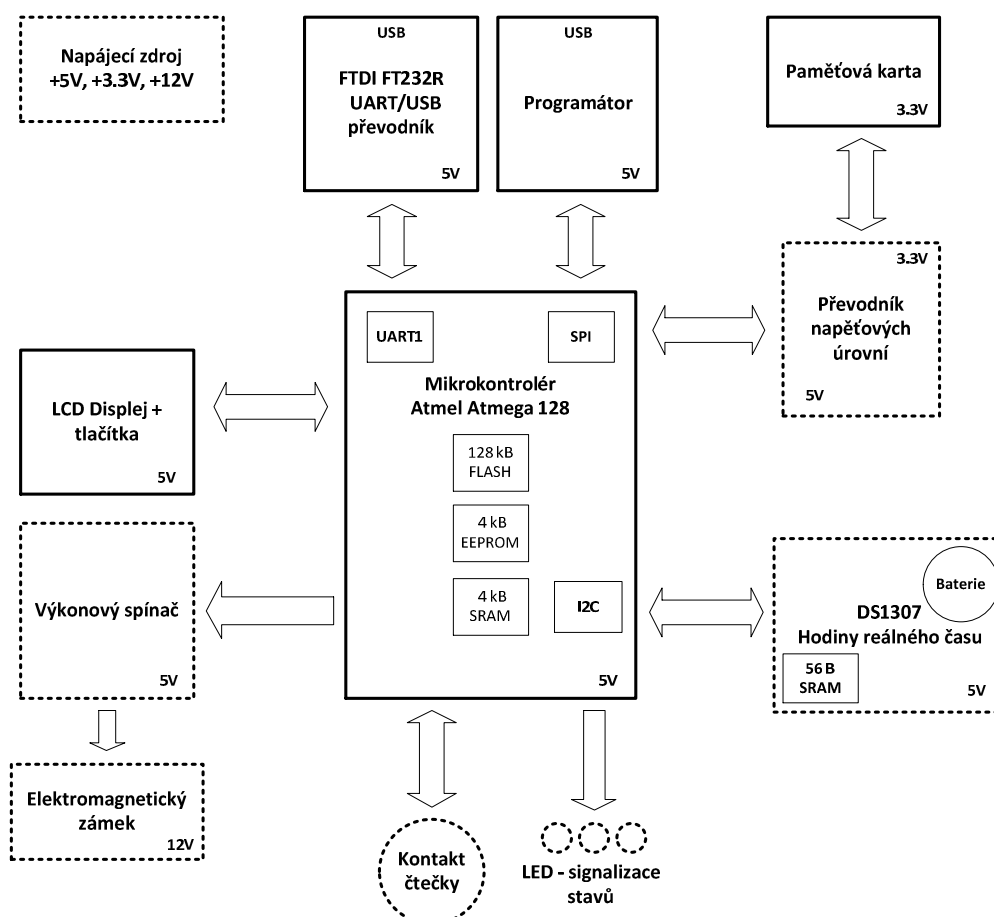
Navrhované zařízení musí být schopno iniciovat výstupní ovládací prvky (apas), v našem případě dveřní elektromagnetický zámek. Výstup mikrokontroléru ale samozřejmě nedisponuje výkonem pro takovou aplikaci, elektromagnetické zámky jsou navíc napájeny vyšším napětím (12 V). Mezi MCU a zámek proto bylo nutné vložit polovodičový výkonový spínač.

Jako poslední bylo na této úrovni návrhu nutné vyřešit napájení celého zařízení. Zařízení lze napájet 12 V, toto napětí používat pro buzení cívky elektromagnetického zámku a pomocí stabilizátorů získávat nižší napětí pro zbytek zařízení. Pro tyto účely byl upraven jeden z existujících modulů stavebnice.

## 4.2 Blokové schéma

Dalším logickým krokem bylo vytvoření blokového schématu sloužícího k naplánování propojení jednotlivých komponent zařízení. Schéma obsahuje následující části:

- Mikrokontrolér
- Programátor
- USART/USB převodník
- Ovládací rozhraní – LCD displej
- Hodiny reálného času (RTC)
- Ukládání přístupových transakcí – SD karta
- Převodník napětových úrovní (Voltage Level Translator)
- Rozhraní místa přístupu - výkonový spínač
- Napájecí zdroj

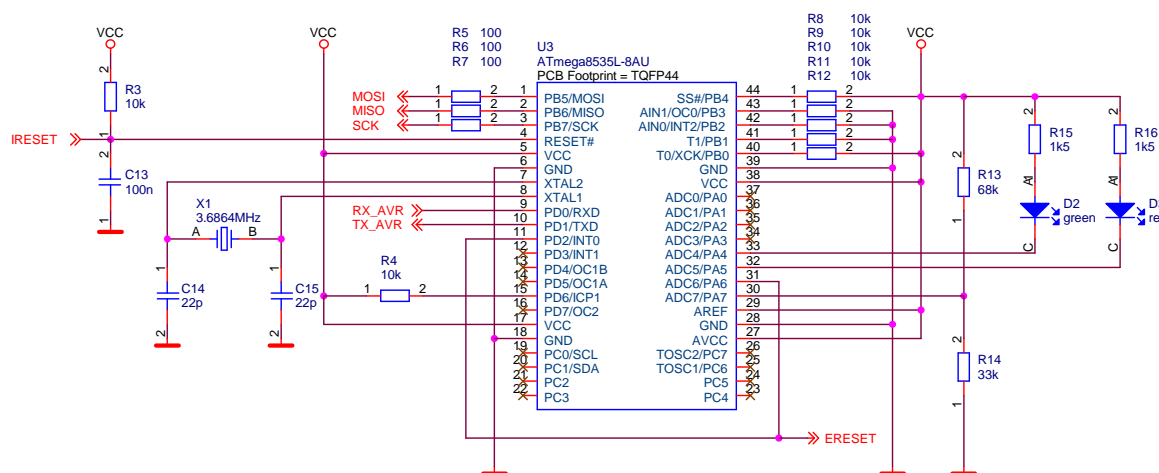


Obrázek 14 – Blokové schéma navrženého řešení

Při práci na tomto schématu již bylo nutné zohlednit budoucí fyzickou realizaci, kdy každému bloku bude odpovídat jeden fyzický modul. Přestože primárním cílem tohoto projektu není návrh elektronických obvodů jednotlivých modulů, z blokového schématu je zřejmé, že pro projekt autonomního systému kontroly vstupů bylo nutné navrhnout a vyrobit specifické moduly, které nejsou součástí stavebnice MLAB [10]. Tyto bloky jsou zobrazeny čárkovaně.

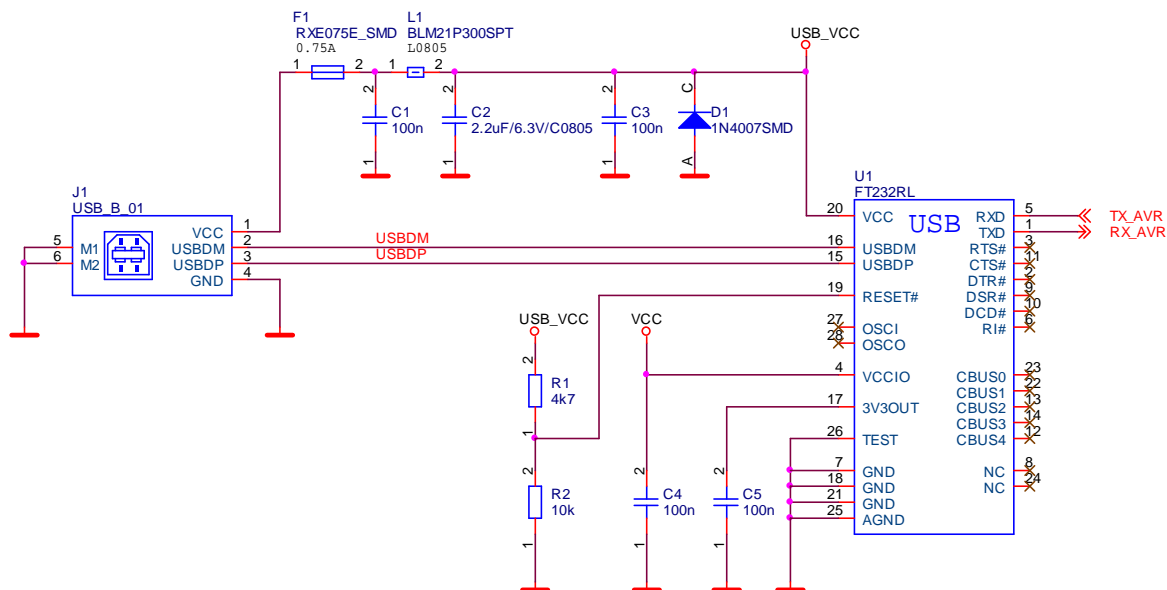
### 4.3 Programátor

Programátor slouží k nahrání programu do MCU pomocí SPI rozhraní. Na trhu existuje mnoho komerčních a snad ještě více různých nekomerčních implementací programátorů. Mé požadavky splnil programátor ATprogISPUSB02A stavebnice [10], který je založen na mikrokontroléru ATmega8535 a zároveň obsahuje převodník RS232/USB s obvodem FTDI TF232R. Důležitá pro mne byla i možnost naprogramovat MCU přímo z vývojového prostředí AVR studio bez nutnosti používat pro tento účel specializovaný program. Programátor je připojen na rozhraní ISP k vývodům PE0 a PE1 mikrokontroléru.



Obrázek 15 – Schéma mikrokontroléru programátoru

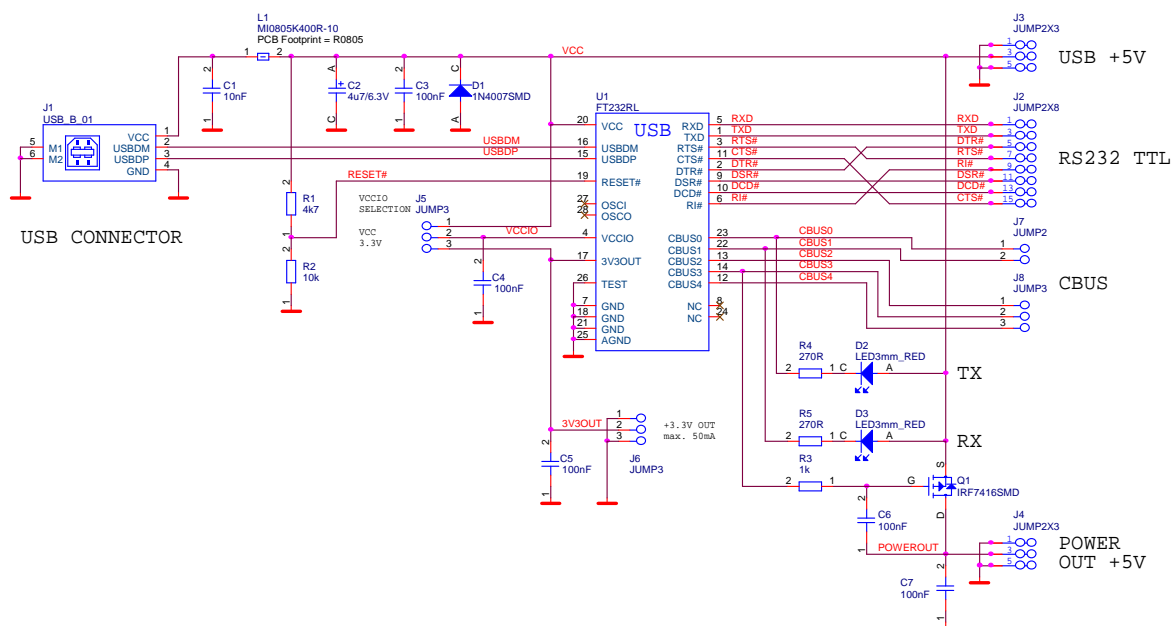




Obrázek 16 – Schéma převodníku RS232/USB programátoru

#### 4.4 USART/USB převodník

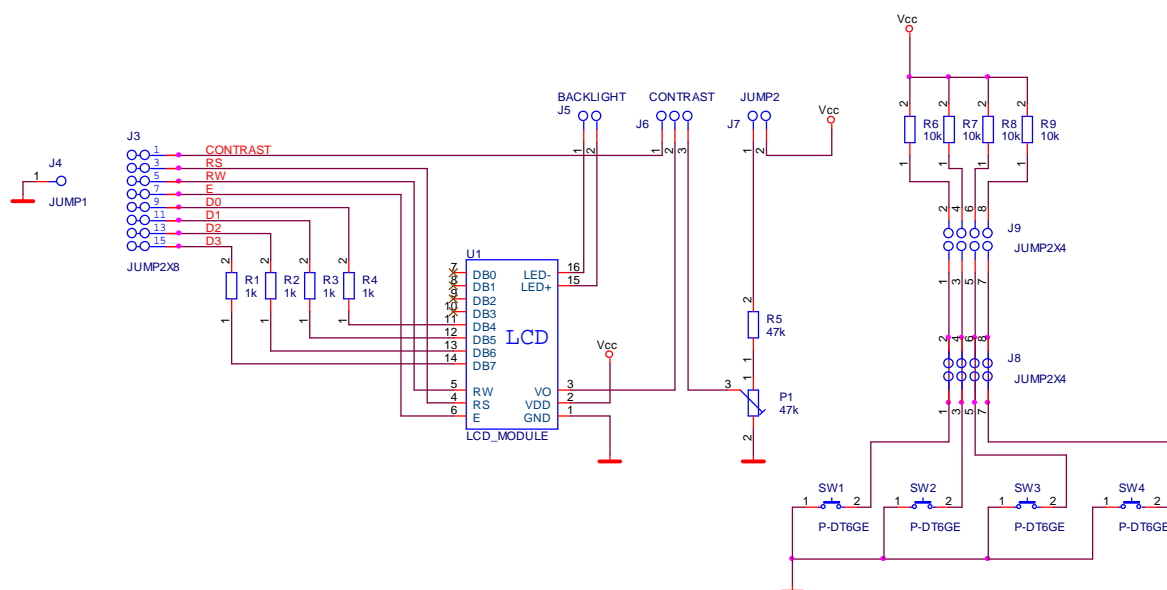
Sériový port, ke kterému by bylo možné přímo připojit dvoudrátové sériové rozhraní přítomné v mikrokontroléru ATmega128, se již v moderních počítačích nachází velmi zřídka. Vzhledem k rozhodnutí využívat sériovou linku pro podrobnější výpis hlášení ovládacího programu, však bylo nutné zajistit konverzi signálů v úrovních TTL ze sériové na dnes běžně používané USB rozhraní. Pro tento účel se jako vhodný jeví modul USB232R01B [10] stavebnice. Ten je založen na stejném IO jako v případě programátoru, tedy FTDI TF232R, který je široce podporován ve všech obvyklých operačních systémech. Zapojení obvodu je podobné jako v předchozím případě, ale pracuje s více signály a umožňuje nastavení HW i SW řízení toku dat. Při návrhu připojení převodníku k mikrokontroléru bylo možné využít přítomnosti druhé sériové sběrnice u ATmega128 a připojit jej k USART1 na vývody číslo PD2 a PD3. Tím bylo eliminováno zobrazování nežádoucích znaků při programování zařízení (vývody č. PE0 a PE1 jsou využívány jak pro USART0, tak pro programování MCU).



Obrázek 17 – Schéma USART/USB převodníku

## 4.5 Ovládací rozhraní – LCD displej

Modul ovládacího rozhraní je pro celý projekt velmi důležitý, neboť jeho pomocí bude zařízení ovládáno a programováno. Nad původně zvažovanou variantou komfortnějšího grafického displeje, nakonec z důvodu kompaktnosti zařízení, nízké ceny a dostupnosti zvítězilo využití modulu LCD2L4P02A [10]. Ten je vybaven dvouřádkovým LCD displejem (2x16 znaků) řízeným řadičem Hitachi HD44780, čtyřmi tlačítky a piezoelementem pro případnou zvukovou signalizaci, což by v případě vhodně navrženého ovládacího rozhraní mělo postačovat pro základní práci se zařízením. Obvod displeje je připojen přímo k vývodům PC0 až PC6, pro ovládání pomocí tlačítek jsou použity vývody PA4 až PA7 mikrokontroléru.



Obrázek 18 – Schéma LCD displeje

#### 4.6 Hodiny reálného času (RTC)

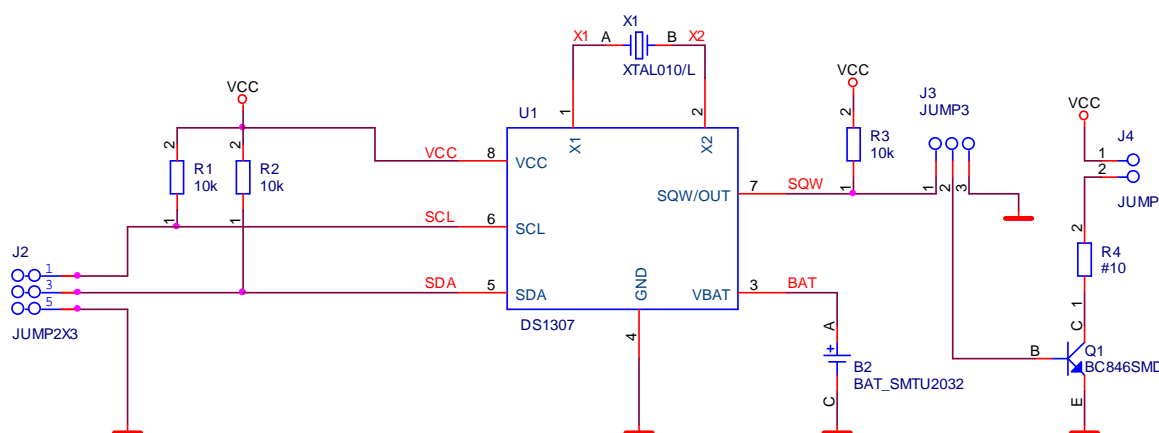
Modul (obvod) pro udržování data a hodin reálného času není součástí stavebnice MLAB [10], proto bylo nutné jej navrhnout a vyrobit. Po prostudování produktových listů byl vybrán IO DS1307 firmy Maxim Integrated Products. Návrh vychází z doporučeného zapojení uvedeného v produktovém listu [15]. Obvod pro svoji práci potřebuje externí hodinový krystal o frekvenci 32.768 kHz. Nemí-li obvod napájen, je čas a obsah paměti zálohován pomocí baterie. V tomto režimu je odběr pouhých 500 nA a obvod by měl udržet čas a obsah paměti více než 10 let (při použití baterie o kapacitě 48 mAh a teplotě +25 °C).

Velkou výhodou této řady IO je snadnost získání data a času, protože ten je reprezentován pomocí BCD (Binary Coded Decimal) a je možné jej přímo odečíst z interních registrů. Paměť typu NV SRAM přítomná na integrovaném obvodu na adrese 08H-3FH je využita pro uložení PIN (viz kapitola 4.1). Obvod hodin je připojen pomocí sběrnice TWI (I2C) k vývodům PD0 a PD1 mikrokontroléru.

ADDRESS	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0	FUNCTION	RANGE
00H	CH	10 Seconds			Seconds				Seconds	00–59
01H	0	10 Minutes			Minutes				Minutes	00–59
02H	0	12	10 Hour	10 Hour	Hours				Hours	1–12 +AM/PM 00–23
		24	PM/ AM							
03H	0	0	0	0	0	DAY			Day	01–07
04H	0	0	10 Date		Date				Date	01–31
05H	0	0	0	10 Month	Month				Month	01–12
06H	10 Year				Year				Year	00–99
07H	OUT	0	0	SQWE	0	0	RS1	RS0	Control	—
08H-3FH									RAM 56 x 8	00H-FFH

Obrázek 19 – DS1307 – popis interního registru

Pomocí řídicího registru je možné na vývodu číslo 7 získat výstup v podobě obdélníkového signálu o frekvencích 1 Hz, 4.096 kHz, 8.192 kHz a 32.768 kHz. Modul je proto vybaven tranzistorem a propojkami pro případné využití této funkce v rámci jiných projektů.

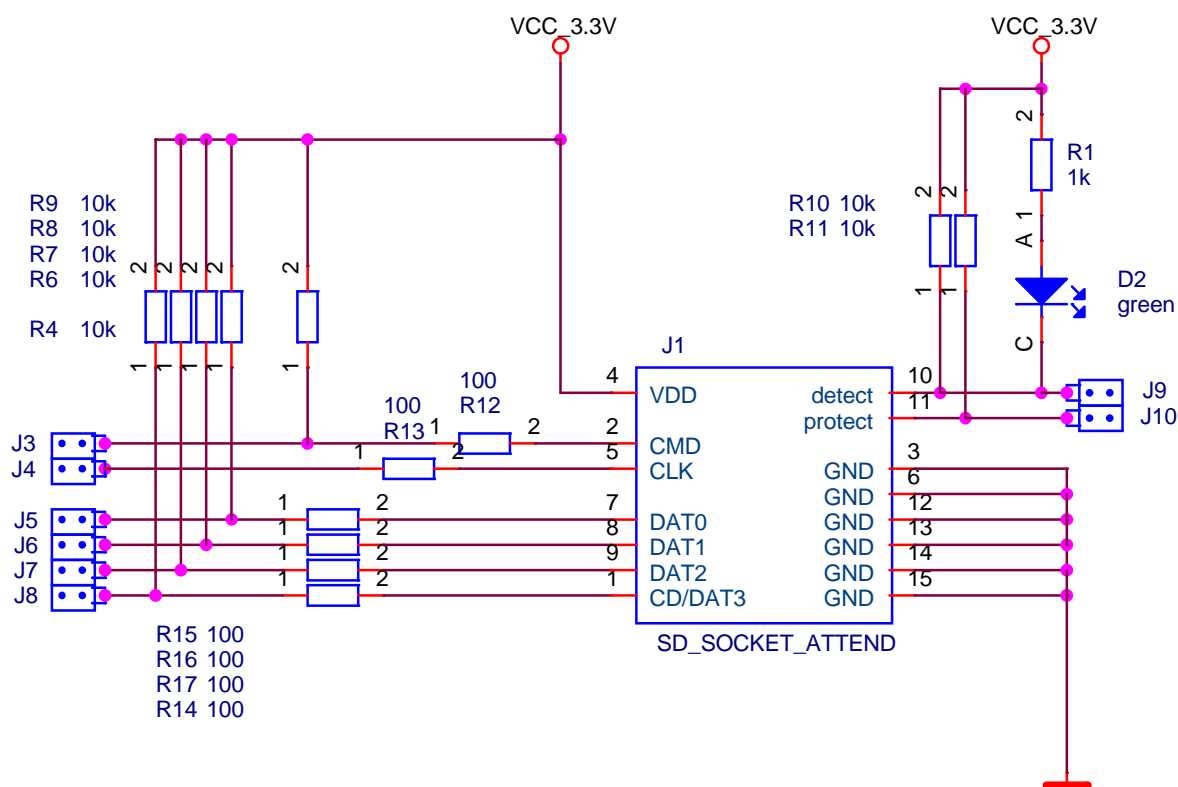


Obrázek 20 – Schéma obvodu RTC DS1307

#### 4.7 Ukládání přístupových transakcí – paměťová karta

Obvod paměťové karty je realizován modulem SDcard01B – jeho podrobný popis zatím není na webu stavebnice MLAB [10] dostupný. Jedná se v podstatě pouze o zapojení patice pro připojení paměťových karet typu SD/MMC. Vstupy jsou chráněné sériovými

odpory pro větší přepět'ovou odolnost. Vzhledem k tomu, že paměťové karty pracují s napětím 3.3 V (modul je osazen potřebným stabilizátorem napětí), je nutné vložit mezi paměťovou kartu a mikrokontrolér převodník napět'ových úrovní popsany v následující kapitole.



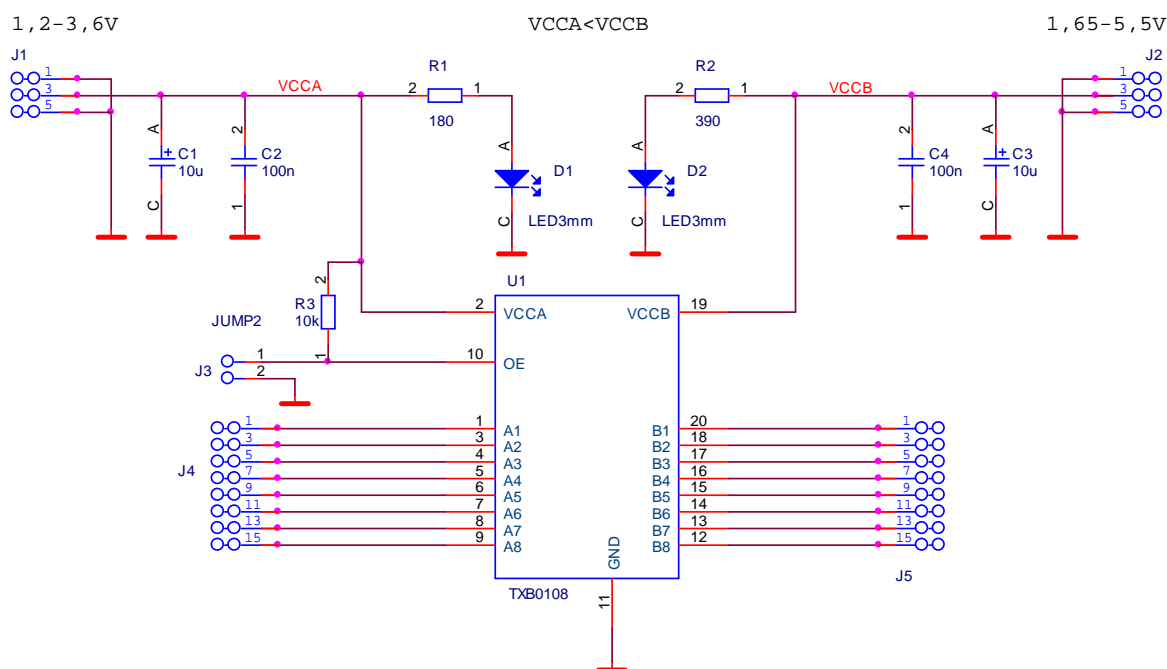
Obrázek 21 – Základní zapojení paměťové karty

#### 4.8 Převodník napět'ových úrovní (Voltage Level Translator)

Obvod pro oddělení 5 V a 3.3 V logiky je založen na integrovaném obvodu TXB0108 firmy Texas Instruments [19], což je osmibitový obousměrný napět'ový převodník s automatickou detekcí směru toku dat a ESD ochranou. Pro tento projekt by stačil převodník 4-bitový, tedy TXB0104, ten však nebyl v době návrhu obvodu na trhu k dostání. Osmibitový převodník je navíc univerzálnější a bude jej možné využít i pro jiné projekty.

Obvod se skládá ze dvou rozhraní, kdy každá část reprezentuje jednu úroveň napájení (napět'ovou úroveň logiky). Port A může být provozován v rozmezí 1.2 V až 3.6 V (zde bude zapojena paměťová karta), port B může být provozován v rozmezí 1.65 V až 5.5 V (zde bude mikrokontrolér). Návrh obvodu odpovídá doporučenému zapojení definovanému

v produktovém listu. Převodník je na straně mikrokontroléru připojen k vývodům PB0 až PB3 (karta je provozována v režimu SPI), pro detekci karty jsou použity porty PE6 a PE7. Na straně paměťové karty jsou připojeny vývody CMD (MOSI), CLK, DAT0 (MISO) a DAT3.



Obrázek 22 – Schéma zapojení převodníku napěťových úrovní

## 4.9 Výkonový spínač

Výstupním ovládacím prvkem bude běžný elektromagnetický zámek (elektromagnetický otevírač), který pro svůj provoz potřebuje napájení 12 V stejnosměrným nebo střídavým napětím, špičkový proud se při provozu pohybuje okolo 2 A. Těmito hodnotami samozřejmě výstup mikrokontroléru nedisponuje, takže bylo nutné navrhnout odpovídající výkonový spínač. Stavebnice MLAB [10] má tyto spínače zpracované ve formě modulů osazených dvěma až čtyřmi tranzistory. Pro účel tohoto projektu je to zbytečné, zde postačí jeden výkonový tranzistor, čili polovina modulu NFET2X01A. Nově vzniklý modul je osazen jedním tranzistorem N-FET, ochranným odporem R1 a velkým odporem R2, který udržuje nepřipojený tranzistor v rozpojeném stavu. Protože se při rozpínání indukční zátěže (cívka zámku) zátěž brání změně protékajícího proudu indukovaným napětím, mohlo by na kolektoru tranzistoru vznikat takové napětí, které by jej mohlo prorazit. Aby k tomu nedošlo, je v obvodu zařazena záchytná dioda D1.



### 4.11 Celkové schéma zapojení

Schéma celkového zapojení obsahuje propojení použitých modulů a je součástí této práce jako Příloha č. I. Z důvodu přehlednosti zde nejsou zobrazeny s návrhem nesouvisející části jednotlivých modulů, jako jsou propojovací hřebínky, switche atd.

### 4.12 Seznam použitých vývodů MCU

Propojení mikrokontroléru s jednotlivými moduly popisuje následující tabulka. V závorce je uvedeno označení vývodu modulu nebo zařízení, na které je propojení přivedeno. Zem je společná pro celou desku testovacího zapojení, propojovací kabely země (GND) nejsou z důvodu přehlednosti uvedeny.

Vývod MCU	Využití	Propojen na (modul/vývod)	Pull-up
PA0	1-Wire	Přímý kontakt čtečky	Dynamicky
PA1	LED signalizace - vstup povolen - 5s Výkonový spínač	RGB LED (zelená) Výkon. spínač (Input)	-
PA2	LED signalizace - vstup zamítnut	RGB LED (červená)	-
PA3	LED signalizace - vstup povolen - 0,2s	LED (zelená)	-
PA4	Tlačítko pro otevření dveří	LCD (S4)	Externí
PA5	Tlačítko menu - Vlevo	LCD (S1)	Externí
PA6	Tlačítko menu - Vpravo	LCD (S2)	Externí



Vývod MCU	Využití	Propojen na (modul/vývod)	Pull-up
PA7	Tlačítko menu - Select	LCD (S3)	Externí
PC0	LCD Data0	LCD (D0)	-
PC1	LCD Data1	LCD (D1)	-
PC2	LCD Data2	LCD (D2)	-
PC3	LCD Data3	LCD (D3)	-
PC4	LCD Enable signál	LCD (E)	-
PC5	LCD RW signál	LCD (RW)	-
PC6	LCD RS signál	LCD (RS)	-
PD0	RTC - SCL	RTC (SCL)	-
PD1	RTC - SDA	RTC (SDA)	-
PD2	USART1 - RX	USART/USB (TXD)	-
PD3	USART1 - TX	USART/USB (RXD)	-
PB0	Paměťová karta - SS	Převodník nap. úrovní (B1)	-
PB1	Paměťová karta - SCK	Převodník nap. úrovní (B3)	-
PB2	Paměťová karta - MOSI	Převodník nap. úrovní (B2)	-
PB3	Paměťová karta - MISO	SD karta (DAT0)	-

Vývod MCU	Využití	Propojen na (modul/vývod)	Pull-up
PB4	LED signalizace - heartbeat	RGB LED (modrá)	-
PE6	Paměťová karta - přítomna	SD karta (Detect) Externí Pull-Up 10k	Externí
PE7	Paměťová karta - zamknuta	Externí Pull-Up 10k	Externí
PE0	Programátor	ISP konektor	-
PE1	Programátor	ISP konektor	-
VCC	Napájení MCU	Zdroj napětí 5V	-
XTAL1, XTAL2	Taktování MCU	Externí krystal 16MHz	-
PG3, PG4	Taktování interního RTC	Externí krystal 32768 Hz	-

Tabulka 2 – Seznam použitých vývodů MCU

#### 4.13 Propojení modulů

Všechny moduly jsou napájeny stabilizovaným napětím 5 V. Napětí 3.3 V je, jak již bylo uvedeno, získáno pomocí stabilizátoru na modulu paměťové karty, odkud je přivedeno na převodník napěťových úrovní.

Zbývající propojení mezi moduly je uvedeno v následující tabulce:

Modul (číslo vývodu)	Využití	Propojen na modul (číslo vývodu)	Pull-up
Převodník nap. úrovní (A1)	Paměťová karta – Data3	SD karta (Data3)	-
Převodník nap. úrovní (A2)	Paměťová karta – CMD	SD karta (CMD)	-
Převodník nap. úrovní (A3)	Paměťová karta – CLK	SD karta (CLK)	-
Zdroj 12V	Napájení elmag. otevírače	Výkonový spínač (Power 12V)	-
Výkonový spínač (Vcc Out)	Napájení elmag. otevírače	Elmag. otevírač	-

Tabulka 3 – Seznam propojení modulů

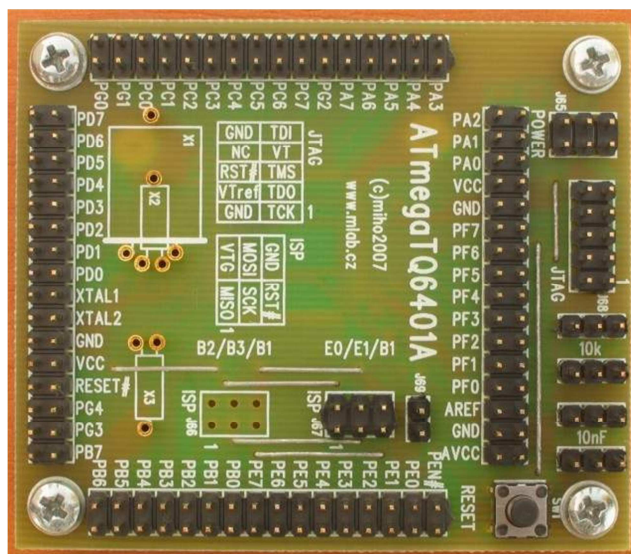
## 5 TESTOVACÍ ZAPOJENÍ NAVRŽENÉHO ZAŘÍZENÍ

Před vytvořením funkčního prototypu je v praxi téměř vždy nutné vytvořit testovací zapojení navrženého zařízení nebo jeho jednotlivých částí v případě, že je zařízení složitější. V průběhu vývoje a testování zařízení pak opravujeme vzniklé problémy a korigujeme návrh tak, aby výsledný produkt splňoval požadavky na něj kladené. V našem případě byla pro testovací zapojení s výhodou využita již zmíněná stavebnice MLAB [10], která je založena na modulech vykonávajících vždy specifickou činnost. K dispozici tedy máme například různé moduly s mikrokontroléry, perifériemi, výkonovými částmi, senzory atd. Mechanickou stabilitu spojovaných částí zajišťuje deska z jednostranného plošného spoje nebo hliníku s předvrtanými otvory o rozteči 400 mils (10.16 mm). Do této desky se pomocí šroubů M3 uchycují jednotlivé moduly, přičemž použité šrouby slouží jak pro pevné uchycení, tak jako distanční sloupky. Uchycení modulů je provedeno vždy v jejich rozích. K propojování vstupů a výstupů modulů se používají různě dlouhé a různě barevné kablíky, opatřené na koncích konektory pro standardní kontaktní hřebínky v rastru 100 mils (2.54 mm).

Testovací zapojení navazuje na návrh zpracovaný v předešlé kapitole. Tento návrh si nyní rozvedeme do fyzické realizace modulů. Popis oživení jednotlivých modulů je uveden na webových stránkách stavebnice a je zbytečné jej zde uvádět. Pro úplnost je však vhodné popsat případné modifikace (resp. klíčové vlastnosti), kterými se budeme zabývat ve zbytku této kapitoly.

### 5.1 Modul mikrokontroléru (MCU)

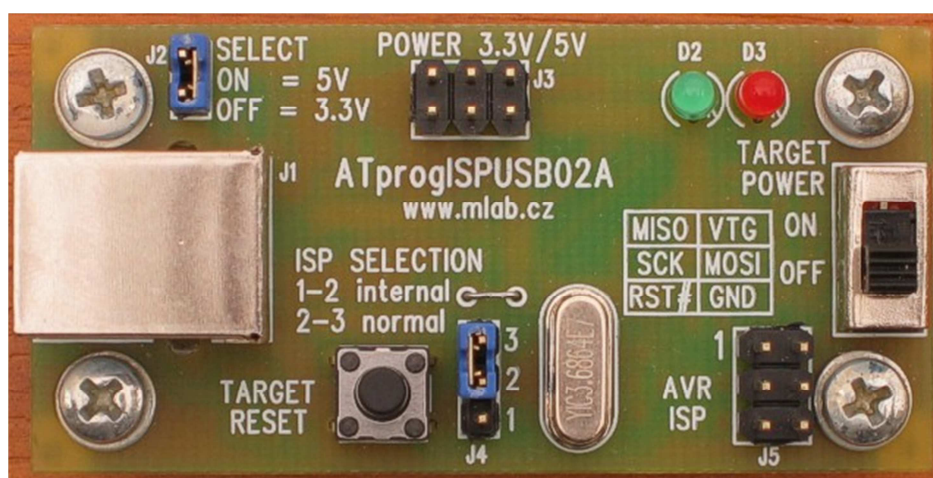
Mikrokontrolér ATmega128 může být taktován buď vnitřním oscilátorem, pak je maximální frekvence procesoru 8 MHz, nebo může být osazen externím krystalem o taktu až 16 MHz. Při použití vnitřních hodin reálného času je nutné zapojit také hodinový krystal o frekvenci 32.768 kHz. Kromě osazení modulu oběma krystaly nejsou nutné žádné další úpravy.



Obrázek 25 – Modul MCU ATmega128

## 5.2 Modul programátoru

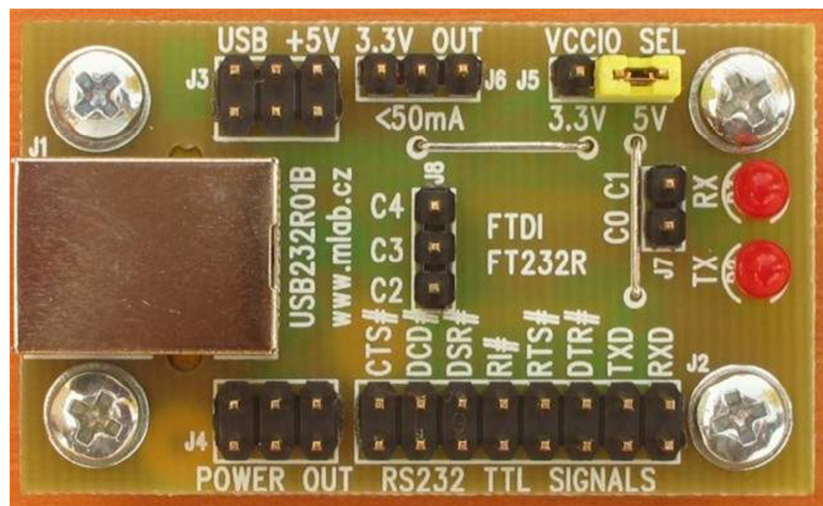
Tento modul nebude v reálu součástí výsledného zařízení, pro zprovoznění MCU je však nezbytný, takže byl zahrnut do celého řešení. Po osazení modulu je nutné jej naprogramovat, neboť obsahuje vlastní mikrokontrolér. Použijeme tedy jiný, externí programátor a do našeho modulu zavedeme firmware, který je k dispozici na webu stavebnice MLAB [10]. Pro správnou funkci je ještě nutné do PC nainstalovat drivery pro USB převodník FT232R. Pak je programátor připraven k použití.



Obrázek 26 – Modul programátoru

### 5.3 Modul USART/USB převodníku

Stejně jako v případě programátoru je po osazení a oživení modulu nutné do počítače nainstalovat drivery pro USB převodník (pokud jsme tak již neučinili při ožiování programátoru). Ačkoli obvod FT232R umožňuje změnu konfigurace jeho parametrů pomocí programu mprog.exe, není to v našem případě nutné a je možné jej používat se standardním nastavením.

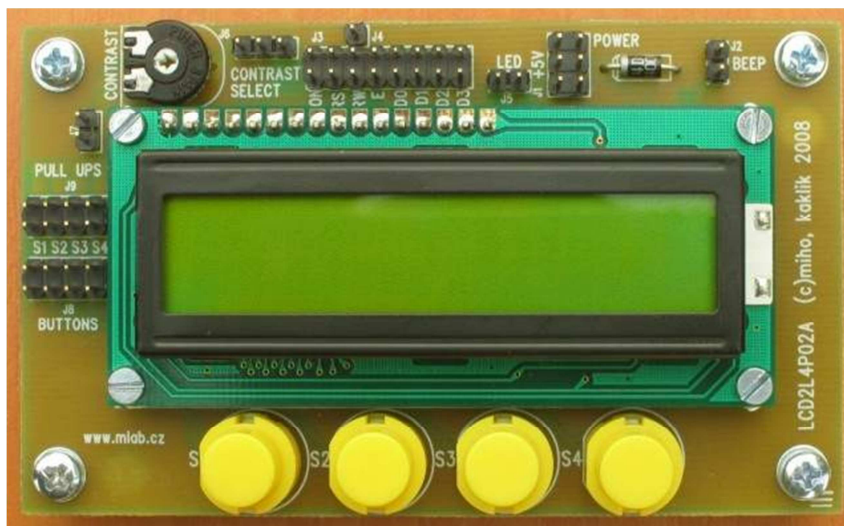


Obrázek 27 – Modul USART/USB převodníku

### 5.4 Modul ovládacího zařízení

Rozhraní pro ovládání navrženého zařízení se skládá z dvouřádkového displeje o šestnácti znacích a čtyř tlačítek, z nichž jsou tři vyčleněna pro ovládání menu, čtvrté tlačítko je určeno pro přímé otevření elektromagnetického zámku. Zapojení obsahuje rovněž čtyři odpory 10 kΩ využité jako PULL-UP pro tlačítka. Modul je navíc osazen piezoelementem, který je sice v rámci tohoto projektu nevyužitý, ale kvůli citlivosti CMOS obvodu jeho budiče se stačí k modulu přiblížit rukou a začíná chytat brumy. Řešením je připojení odporu na vstup. V průběhu testování se ukázalo, že tlačítka dodávaná s modulem nejsou ideálním řešením, protože jsou určena pro zabudování a potřebují vedení v jejich horní části. Stávalo se tedy, že tlačítko mechanicky cvaklo, ale k sepnutí mikrospínače nedošlo, což bylo při ovládání zařízení poněkud frustrující. Tlačítko bylo nutné vyměnit za jiný typ, který je navíc vyšší, čímž se komfort ovládání zvýšil. Při ladění softwarové části v pozdních nočních hodinách byl shledán nevyhovujícím displej bez podsvícení a poslední

změnou na tomto modulu je tedy jeho výměna za displej stejných parametrů, ale modrobílý s podsvícením, který je daleko lépe čitelný ve vnitřních podmínkách. Následující obrázek zobrazuje původní verzi modulu.

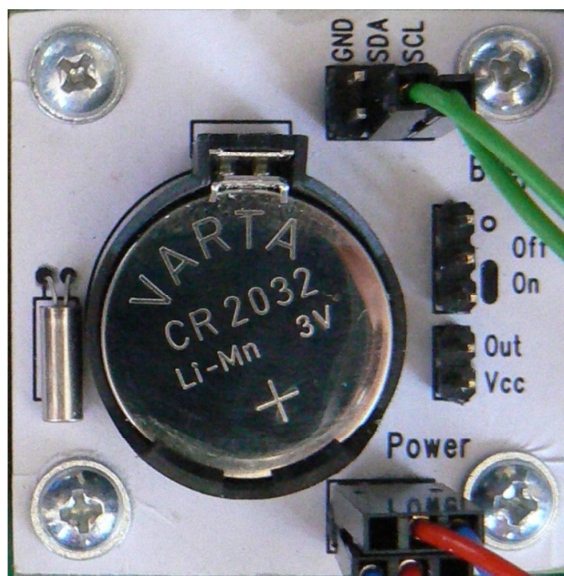


Obrázek 28 – Modul LCD s tlačítky

## 5.5 Modul hodin reálného času

Modul RTC nebyl součástí stavebnice a bylo nutné jej vytvořit. Návrh obvodu je uveden v kapitole 4.6. Obvod je tak jednoduchý, že zřejmě nemá smysl popisovat osazení a oživení modulu. Za zmínku však stojí, že je navržen jako univerzální, a umožňuje osadit jak IO DS1307 v provedení 8 SO (150 mils), tak DS1339 v provedení 8  $\mu$ SOP [15]. DS1339 obsahuje 2 programovatelné alarmy, takže je možné jej použít v jiných aplikacích jako časový spínač (budík). Z tohoto důvodu je do výstupu modulu zapojen tranzistor, který je možné aktivovat pomocí propojky (hřebínku). Provoz hodin a kalendáře je pro případ odpojení od zdroje elektrické energie zálohován 3 V knoflíkovou baterií typu 2032.

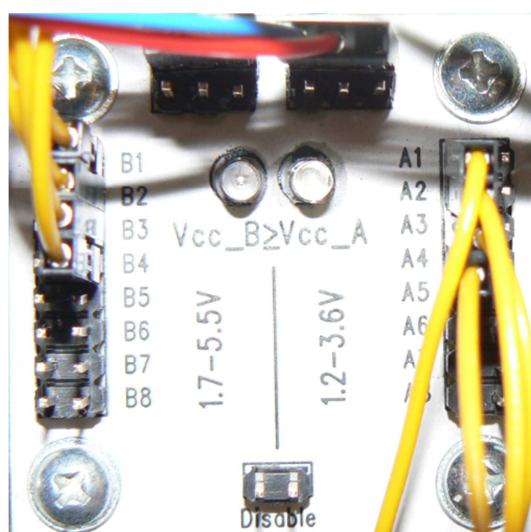




Obrázek 29 – Modul RTC

## 5.6 Modul převodníku napět'ových úrovní

Pro připojení paměťové karty v režimu SPI potřebujeme 4 bity (viz kapitola 3.1.2.2). Navržený modul je opět univerzální a proto využívá osmibitového převodníku realizovaného integrovaným obvodem TXB0108. Kromě této součástky jsou na modulu ještě osazeny 2 LED pro kontrolu napájení, příslušné odpory a vyhlazovací kondenzátory. Činnost převodníku lze zastavit propojením pinů (Disable).

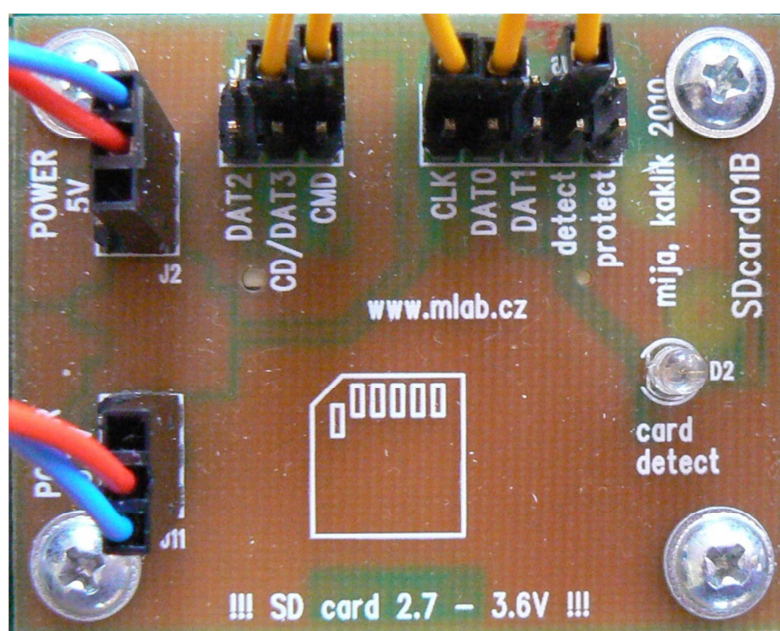


Obrázek 30 – Modul převodníku napět'ových úrovní



## 5.7 Modul paměťové karty

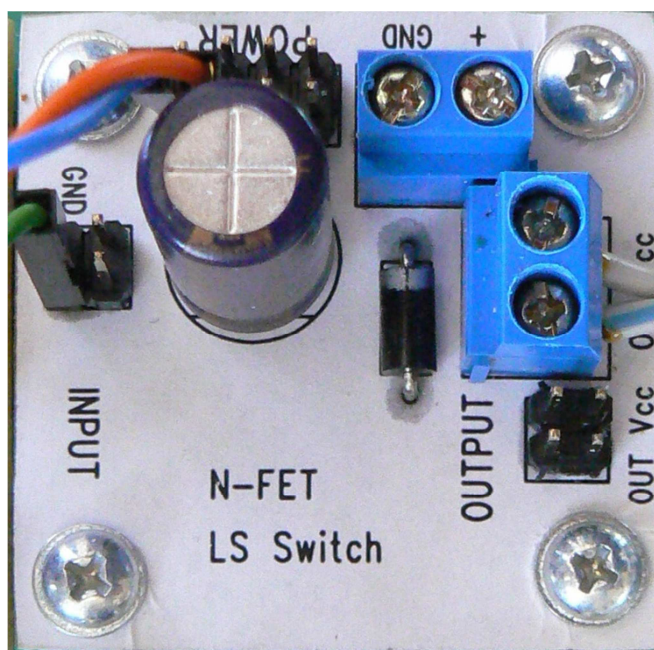
Modul paměťové karty se skládá z konektoru pro paměťovou kartu typu SD nebo MMC, ochranných odporů a je vybaven monolitickým stabilizátorem pro získání napájecího napětí 3.3 V. Na modulu nebylo nutné provádět žádné úpravy.



Obrázek 31 – Modul paměťové karty

## 5.8 Výkonový spínač

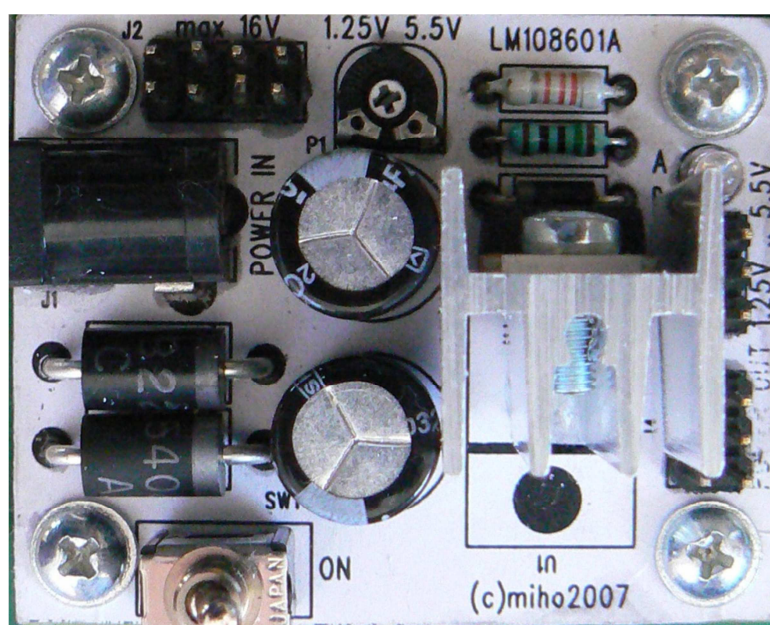
Výkonový spínač byl vytvořen jako nový modul a jedná se o modifikaci existujícího zapojení, které je osazeno pouze jedním výkonovým tranzistorem. Spínané napětí 12 V a jeho výstup je řešen osazením jak standardních hřebínků, tak pomocí šroubovacích konektorů.



Obrázek 32 – Modul výkonového spínače

## 5.9 Napájecí zdroj

Napájecí zdroj vznikl modifikací existujícího modulu (viz 4.10). Odporový dělič tvořený odporovým trimrem a odporem R1 byl vypuštěn a místo původního stabilizátoru byl použit monolitický stabilizátor LM317T. Dostatečné chlazení zajišťuje mohutný hliníkový chladič, který shodou okolností do modulu velmi těsně pasuje.



Obrázek 33 – Modul napájecího zdroje

## 5.10 Rozhraní místa přístupu

Rozhraní místa přístupu je tvořeno snímačem kontaktních prvků iButton [1] a elektromagnetickým zámkem (otevíračem). Vzhledem k tomu, že sběrnice 1-Wire pro komunikaci s tokeny je realizována pomocí softwarové emulace, není nutné, aby snímač disponoval logikou pro zpracování informací - jedná se pouze o vhodný mechanický kontakt. Pro odblokování místa přístupu je možné využít libovolný elektromagnetický otevírač dveří napájený stejnosměrným napětím 12 V. Je lhostejno, zda se bude jednat o otevírač s pamětí (aktivovaný impulsem, deaktivovaný mechanicky po otevření dveří) nebo zda bude použit klasický zámek (deaktivovaný v okamžiku ukončení napájení elektromagnetu). Návrh toto zohledňuje a k dispozici jsou oba typy výstupů o délce impulzů 5 s a 0,2 s (viz kapitola 4.12).

## 6 BEZPEČNOSTNÍ PRVKY ZAŘÍZENÍ

Při návrhu bezpečnostní aplikace, jakou je autonomní systém kontroly vstupů, je nutné provést analýzu možných útoků na zařízení a pokusů o jeho obelstění. Jakým způsobem by tedy mohl potencionální útočník zařízení oklamat? Odpověď na tuto otázku je dána způsobem ověřování uživatelů. Uživatel se systému identifikuje pomocí iButtonu, ten načte jeho číslo, které porovná se seznamem povolených tokenů ve své paměti. Pokud číslo souhlasí, povolí přístup (uvolní apas). Útočník má tedy několik možností. Nemá-li k dispozici originální token, musí vlastnit nějaké zařízení, které by umožňovalo se z pohledu systému tvářit jako povolený token. Takové zařízení by samozřejmě bylo možné sestavit, byť to není zcela triviální záležitost. Použití takového zařízení však ještě neznamená, že útočník získá přístup. Musí znát buď přesné číslo povoleného tokenu, nebo zkusit generovat všechny možné kombinace, čemuž se v bezpečnostní terminologii informačních technologií říká útok hrubou silou. V dalších kapitolách budou rozebrány jednotlivé varianty a bude navržena obrana proti každému typu útoků.

### 6.1 Ověření tokenu uživatele

Postup načtení 64-bitového identifikačního čísla byl popsán v kapitole 3.3. Zopakujme zde pouze to, že po načtení 56 bitů je spočítán kontrolní součet a pokud je shodný s posledním načteným bytem, je čtení prohlášeno za úspěšné a v přenosu nenastala chyba. Znamená to, že útočník nemůže počítat s tím, že by získal přístup v situaci, kdy by použil nezaregistrovaný token a nastala by chyba při přenosu dat do MCU, případně pokud by sběrnici 1-Wire uměle rušil. Útočník tedy musí znát konkrétní povolené iButton ID, nebo se snažit jej uhodnout.

### 6.2 Ochrana před útokem hrubou silou

Bude-li se útočník snažit uhodnout identifikační číslo způsobem, kdy bude zkoušet jednotlivé kombinace, je zřejmé, že jeho úspěšnost bude velmi záležet na době zpracování jednoho pokusu. Pomocí jednoduchého čítače bylo zjištěno, že zpracování identifikačního čísla předmětu je provedeno několik set krát za sekundu. To je výhodné pro právoplatného uživatele, protože stačí, aby se dotknul čtečky na libovolně krátkou dobu, a je vpuštěn. Z bezpečnostního hlediska to však není ideální a umožňuje to v rychlém sledu opakovat pokusy o získání přístupu. Je tedy žádoucí, aby v případě že identifikační číslo nebude souhlasit, bylo zpracování na nějakou dobu pozastaveno. Aby se nám s tím dobře

pracovalo řekněme, že po neplatném pokusu se bude čekat 1 sekundu a pojdme si spočítat dobu potřebnou pro prolomení do systému.

iButton používá 64-bitové identifikační číslo, jehož poslední byte je využit pro uložení CRC [1]. To znamená, že máme 56 bitů pro uložení jednotlivých kombinací, což činí  $2^{56}$  variant (více než  $7 \times 10^{16}$ ). Narazí-li útočník na správnou kombinaci v polovině zkoumaného intervalu a bude-li zkoušet kombinace rychlostí 1 pokus za sekundu, bude mu udělen přístup za 1 142 462 658 roků. Aby to neměl tak jednoduché (a abychom stačili přečíst hlášení na LCD), byla nastavena doba čekání po neplatném pokusu na 5 sekund.

### 6.3 Uložení identifikačního čísla tokenů, získání ID

Ukázali jsme si tedy, že pomocí hrubé síly zřejmě útočník přístup v rozumné době nezíská. Co tedy druhý způsob - zjistit si identifikační číslo jinak? Jednou z možností je vybavit se čtečkou, tedy podobným zařízením, které využívá vstupní systém, nějakým způsobem se zmocnit registrovaného tokenu uživatele a načíst jeho číslo. Druhá možnost je jednodušší, i když také vyžaduje fyzický přístup k tokenu - identifikační číslo je totiž na některých typech vygravírované laserem. Ochrana proti tomuto způsobu zneužití je zřejmá. V prvním případě zajistit fyzickou bezpečnost identifikačního předmětu, v druhém pak buď používat tokeny bez vygravírovaného čísla, nebo je lehce přeleštit a odstranit tak možnost číslo přečíst.

Nyní jsme si probrali možnosti získání čísla na straně uživatele, ale co na straně systému kontroly vstupů? Zde je situace složitější. Identifikační čísla s povoleným vstupem jsou, jak již bylo řečeno, uložena v nevolatilní části paměti (EEPROM), ale kvůli možnosti zpětně dohledat komu a kdy byl přístup povolen, se transakce ještě logují na paměťovou kartu a diagnostické údaje se vypisují na sériovou linku. Aby bylo možné ztracený iButton zablokovat, je nutné, aby jej bylo možné vyhledat pomocí rozhraní pro ovládání (LCD displeje). Pro získání dat načtením obsahu paměti, z paměťové karty nebo monitorováním sériové komunikace by tedy bylo třeba, aby útočník zařízení odpojil, rozebral a připojil programátor (resp. klienta sériového rozhraní), nebo vyjmul kartu a zkopíroval si její obsah. Ochranou je dostatečná fyzická bezpečnost zařízení a v souladu s normou by u komerčního zařízení nesměla chybět ani detekce sabotáže (otevření krytu přístroje). Pro uživatele však musí být dostupné ovládací menu, jehož ochranu tedy musíme zajistit jinak. V našem případě může být po správci před vstupem do menu volitelně požadováno zadání PINu (viz kapitola 6.4).

Pro úplnost je třeba dodat, že v případě testovacího zapojení se transakce (ID tokenů) zobrazují z výukových účelů rovněž na LCD. To však nemusíme považovat za bezpečnostní problém, v reálném provozu by tato funkce samozřejmě nebyla implementovaná.

Poslední variantou získání identifikačního čísla je odposlech sběrnice 1-Wire, který je sice technicky proveditelný, ale opět se jedná o vysoce sofistikovanou a na vybavení nákladnou záležitost, neboť vzhledem k parazitnímu napájení předmětů a časování komunikace dojde při připojení běžných zařízení spíše než k odposlechu k selhání komunikace na sběrnici. Mnohem jednodušší jsou tedy výše popsané způsoby napadení systému.

## 6.4 Ochrana přístupu k ovládacímu zařízení

Zajištění ochrany ovládacího rozhraní tvořeného LCD displejem a tlačítky musí být realizováno v souladu s normou ČSN EN 50133, která vyžaduje, aby minimální počet zadatelných kombinací byl 10 000 [5]. Z bezpečnostního hlediska je to zřejmě dostačující počet, naopak v případě zapomenutí PINu správcem zařízení může být problém.

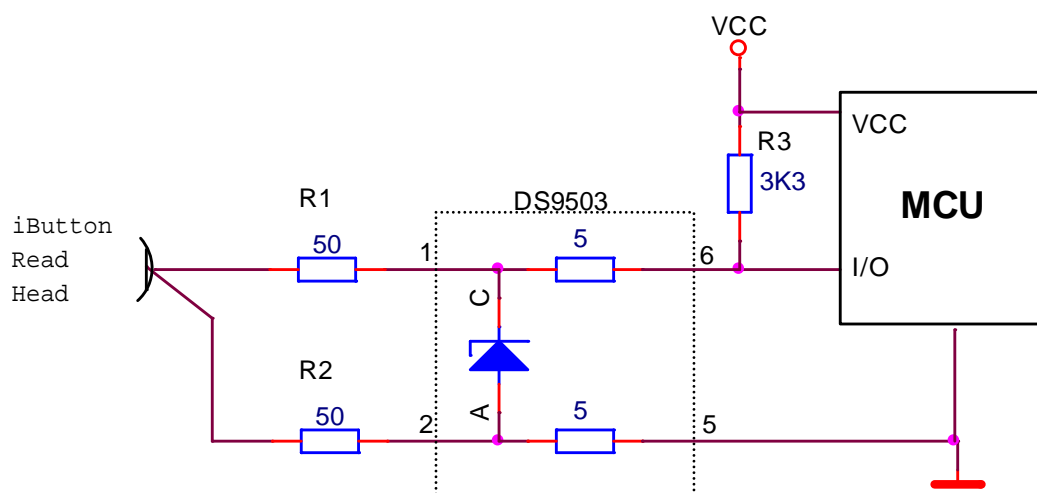
Z důvodu možného resetu (znovunastavení) PINu bylo navrženo následující řešení. Informace o PINu a jeho vyžadování pro vstup do menu jsou uloženy ve volatilní paměti integrovaného obvodu DS1307, který je vybaven baterií pro zajištění napájení obvodu hodin reálného času. Tato baterie zároveň udržuje stav paměti. Pro reset PINu správce tedy stačí vyjmout knoflíkovou baterii, což ovšem znamená otevření krytu zařízení, které musí být vybaveno sabotážním kontaktem. V paměti IO DS1307 jsou využity pouze první 4 byty, kdy první byte určuje, zda při vstupu do menu bude nebo nebude požadováno zadání PINu. Druhý a třetí byte reprezentují vždy 2 číslice PINu, horní nibble obsahuje první číslici, dolní pak druhou. Podle údajů výrobce není oblast paměti po prvním připojení napájení nijak inicializována, a ačkoli je to velmi málo pravděpodobné, mohlo by se stát, že by se první 3 byty nacházely v takové kombinaci, která by odpovídala vyžadování náhodného PINu. Proto byl do řešení zahrnut zmíněný čtvrtý byte, který slouží jako kontrolní součet. V něm je uložena hodnota operace XOR druhého a třetího byte. Pokud ovládací software zjistí při startu zařízení, že vypočtený výsledek výše uvedené operace se neshoduje s hodnotou kontrolního součtu, požadavek na PIN se automaticky deaktivuje.

## 6.5 Ochrana snímače (MCU) před připojením zdroje napájení

V předchozích částech jsme analyzovali způsoby útoku na navrhovaný systém. Vzhledem k plánovanému nasazení není příliš pravděpodobné, že by se případný útočník pokoušel o tak sofistikovanou činnost, jakou je výroba emulátoru iButtonu. Pravděpodobnější by byl pokus průchod do chráněné oblasti s jinou osobou, případně násilné vniknutí do objektu. Umístění čtečky (kontaktu) ve veřejně přístupném prostoru však vystavuje zařízení jinému riziku, dle mého názoru daleko pravděpodobnějšímu a tím je pokus o poškození zařízení (vandalismus).

Kontakt snímače je v navrženém zapojení přímo připojen k vývodu mikrokontroléru, což je z bezpečnostního hlediska nevhodné. Externí zdroj napětí, ať již ve formě elektrostatického výboje nebo při úmyslném poškození, by při připojení ke kontaktům čtečky mohl způsobit zničení celého MCU, což je klíčová (a nejdražší) komponenta zařízení. Z tohoto důvodu bylo navrženo základní zapojení ochrany MCU, založené na IO DS9503 [1]. Jedná se o aplikaci Zenerovy diody a čtyř odporů zapojených tak, aby při dosažení limitu napájecího napětí došlo na diodě k vratnému průrazu a obvod se uzavřel přes odpory R1 a R2. V případě překročení úrovně ESD ochrany, která je v případě obvodu DS9503 27 kV (udáváno dle IEC 801-2), nebo při nadlimitním proudu je obvod proražen ve stavu trvalého zkratu, což sice znemožní další funkci snímače, ale mikrokontrolér je tím ochráněn. Obvod by samozřejmě bylo možné realizovat i pomocí diskretních součástek ovšem s tím, že při použití běžné Zenerovy diody není v případě proražení P/N přechodu zajištěn zkrat součástky.

Navržený obvod ochrany MCU proti ESD (vandalismu) není smysluplné v rámci ověřovacího zapojení dále rozpracovávat, fyzicky proto nebude realizován.



Obrázek 34 – Obvod ochrany MCU

## 6.6 Automatický reset zařízení - Watchdog

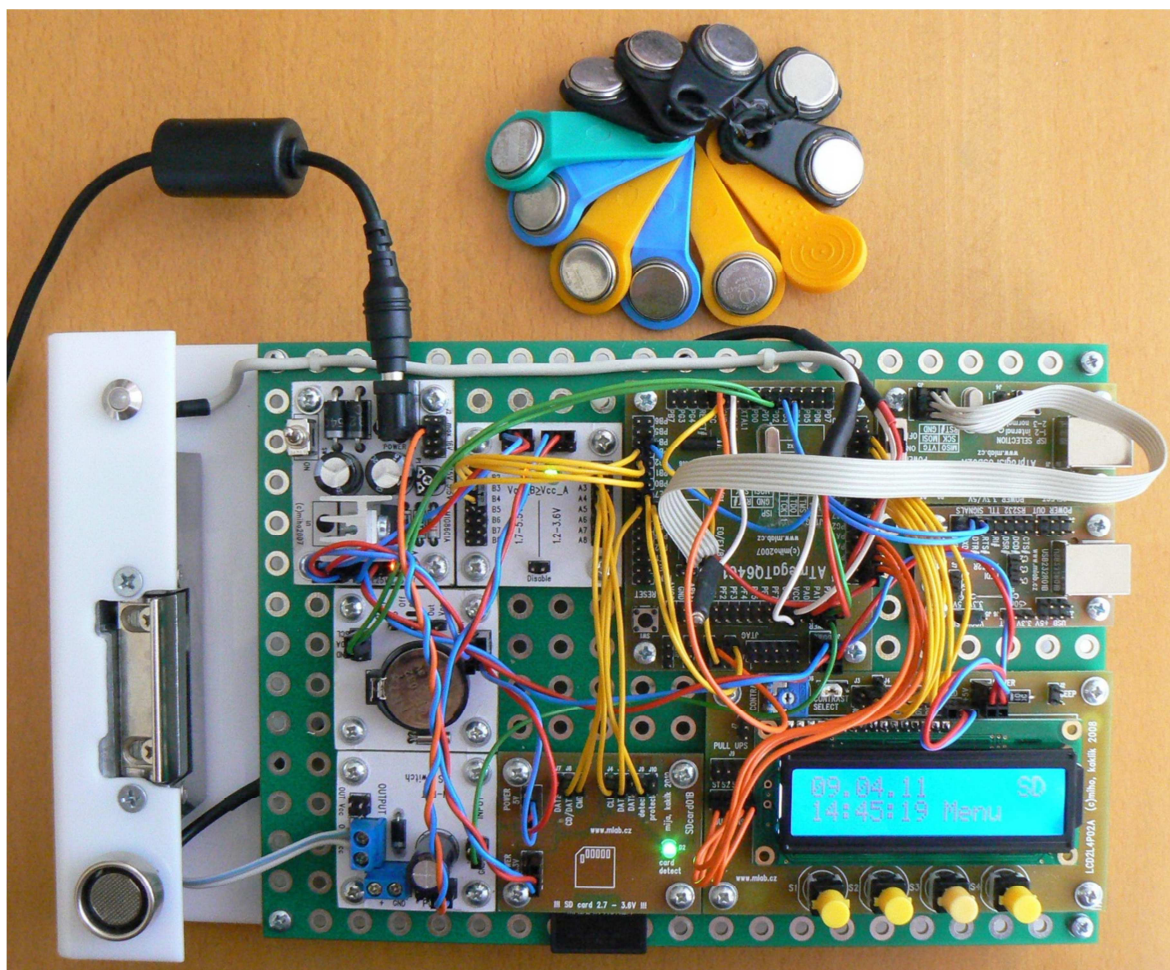
Při zpracování bezpečnostní části návrhu zařízení bylo nutné zvážit, zda je vhodné do implementace zahrnout využití interního časovače Watchdog, který v případě „zatuhnutí“ mikrokontroléru zajistí jeho reset. Jeho využití by ale otevřelo cestu k dalším možným typům útoků, například by bylo možné zabránit zapsání transakcí na paměťovou kartu. Z bezpečnostních důvodů tedy Watchdog nebyl implementován a to i za cenu rizika, že zařízení by teoreticky mohlo přestat pracovat a muselo by být resetováno ručně.



## 7 FYZICKÁ REALIZACE TESTOVACÍHO ZAPOJENÍ

Testovací zapojení je provedeno výše popsáním propojením jednotlivých modulů přišroubovaných pomocí šroubků M3 k desce stavebnice MLAB [10]. Pro účely prezentace funkce zařízení je celá deska ještě umístěna na plexisklovou podložku o tloušťce 3 mm, která slouží pro uchycení elektromagnetického otevírače, signalizační LED a kontaktu čtečky prvků iButton.

Následující obrázek zachycuje realizaci navrženého zařízení krátce před dokončením.



Obrázek 35 – Fyzická realizace testovacího zapojení zařízení

## 8 POPIS OVLÁDÁNÍ

Ovládání zařízení je velmi jednoduché. Jediným úskalím by pro uživatele zpočátku mohla být práce s menu, které je trochu netradičně řešeno pomocí pouhých 3 tlačítek (čtvrté tlačítko je použito pro přímé ovládání elektromagnetického otevírače). Bude-li však zařízení ovládáno pomocí menu, uživatel se nedostane do žádné situace, v níž by mohl zařízení nějakou nevhodnou volbou poškodit (například nějakým způsobem vymazat jeho program).

### 8.1 Zapnutí zařízení

Při prvotním zapnutí zařízení (nebo po vyjmutí baterie z obvodu RTC) je nutné v menu nastavit datum a čas. Po provedení této akce si zařízení díky vlastní baterii uchová informace o aktuálním datu a času i po odpojení napájení. Před začátkem používání zařízení nejsou v jeho paměti uloženy žádné identifikátory umožňující vstup pomocí předmětu iButton, povolené identifikátory je nutné před zahájením používání zadat.

Po připojení napájení (resetu) jsou na LCD, sériové rozhraní a paměťovou kartu vypsány základní údaje o stavu zařízení, jako je počet zaregistrovaných tokenů, jejich ID, požadavek na PIN, velikost paměťové karty atd.

### 8.2 Signalizace stavu

Zařízení signalizuje jednotlivé stavy pomocí trojbarevné LED. Červenou barvou je signalizován stav odmítnutí přiloženého prvku (uzavřený apas), zelenou pak otevření elektromagnetického otevírače (otevřený apas). Po dobu svitu těchto dvou signálů zařízení nevykonává žádnou další činnost a efektivně tak brání možnému útoku „hrubou silou“ (viz kapitola 6.2). Modrou barvou je signalizována připravenost zařízení k provozu. Zde jsou rozlišeny dva stavy. Pomalé blikání označuje provozní režim bez poruch s inicializovanou paměťovou kartou a funkčním zápisem transakcí. Rychlé blikání upozorňuje na problém s ukládáním transakcí na paměťovou kartu (například karta není inicializována, chybí soubor pro zápis událostí atd.), což ovšem nebrání provozu zařízení.

Pokud se uživatel pohybuje v menu, je LED zhasnutá, apas je zavřený a zařízení neobsluhuje uživatele.

Pro potřeby testování a demonstrace funkčnosti zařízení je na výstupu PA3 mikrokontroléru umístěna zelená dioda, která při povolení přístupu svítí zhruba 200 ms.

Tento výstup je použitelný pro elektromagnetické otevírače s pamětí nebo například pro aktivaci záznamového zařízení (fotoaparát, CCTV atd.).

### 8.3 Vložení paměťové karty

Zařízení pracuje s paměťovými kartami SD/MMC. Bylo testováno pouze s kartami s nižší kapacitou (karty SDHC nebyly testovány), pro ukládání dat byl zvolen souborový systém FAT, jehož implementace zabírá nejméně prostoru v paměti. Data se ukládají v rootu souborového systému do textového souboru pojmenovaného „access.log“. Záznamy jsou ukládány bez diakritiky. V případě, že souborový systém neobsahuje výše uvedený soubor, je tento vytvořen při inicializaci karty, která je provedena při jejím zasunutí do slotu nebo při restartu zařízení. Zde je nutné poznamenat, že ačkoli jsou algoritmy pro inicializaci karty připraveny na její vložení resp. vyjmutí za chodu, ne u všech karet tato funkce funguje korektně. Evidentně záleží na druhu karty, neboť dvě testované, na první pohled identické karty MicroSD firmy Kingston o kapacitě 2 GB se chovaly naprosto odlišně. Doporučuji tedy po vložení či výměně karty provést reset zařízení. V předváděcím zapojení je připravena karta MMC s kapacitou 32 MB, kterou je možné bez problémů vyjmout a vložit za chodu zařízení (bez resetu).

Na kartu jsou ukládány informace o jednotlivých transakcích, povolených ID tokenů a dále informace bezpečnostního charakteru, jako například datum a čas změny PINu, odemčení pomocí interního tlačítka, změna data a času atd. PIN je ve výpisu uložen v čitelné formě.

Detekce zákazu zápisu na paměťovou kartu je vypnuta a zařízení bude na vloženou kartu zapisovat vždy, pokud se mu ji podaří inicializovat.

Příklad výpisu souboru access.log:

```
09.04.11 11:51:35 Restart-AACS 1.0
=====
09.04.11 11:51:35 Zarizeni nevyzaduje PIN!
09.04.11 11:51:35 Vypis platnych EEPROM ID:
09.04.11 11:51:42 Neplatny ID - 01 00 00 01 14 04 65 CRC:97
- Pridan novy Button
09.04.11 11:51:51 Neplatny ID - 01 00 00 02 1B 1E 29 CRC:20
- Pridan novy Button
09.04.11 11:52:09 Platny ID - 01 00 00 01 14 04 65 CRC:97
09.04.11 11:52:16 Neplatny ID - 01 00 00 00 E9 B2 ED CRC:48
09.04.11 11:52:24 Platny ID - 01 00 00 02 1B 1E 29 CRC:20
09.04.11 11:52:37 PIN nastaven - 4534
09.04.11 11:52:50 Odemceno internim tlacitkem
09.04.11 11:52:57 Neplatny ID - 01 00 00 00 E9 B2 ED CRC:48
09.04.11 11:53:04 Platny ID - 01 00 00 01 14 04 65 CRC:97
09.04.11 11:53:21 Cas nastaven - puvodni: 10:53:12 novy 11:54:21
```

```

09.04.11 11:53:31: Datum nastaven - puvodni: 08.04.11 novy 09.04.11
09.04.11 11:53:46: 01 00 00 01 14 04 65 CRC:97 - predmet odebran
zevnitr pole
09.04.11 11:53:57 Platny ID - 01 00 00 02 1B 1E 29 CRC:20
09.04.11 11:54:03 Neplatny ID - 01 00 00 01 14 04 65 CRC:97
09.04.11 11:54:15: Odemceno internim tlačítkem
09.04.11 11:54:30: PIN nebude vyžadovan!
09.04.11 11:55:17 Platny ID - 01 00 00 02 1B 1E 29 CRC:20

```

## 8.4 Propojení s počítačem

Při vzniku testovacího zapojení bylo nutné zajistit výpis diagnostických informací. Pro tyto účely se LCD příliš nehodí, protože jeho zobrazovací možnosti jsou limitovány počtem zobrazitelných znaků (16x2) a rolování textu není vzhledem k rychlosti transakcí použitelné. Rozšířené výpisy jsou tedy zasílány na sériové rozhraní USART1, které je pomocí převodníku připojitelné k osobnímu počítači dnes běžným USB portem (viz kapitola 4.4). Po instalaci driverů sloužících ke komunikaci s obvodem FT232R vznikne v počítači virtuální sériový port. K tomuto portu se po připojení zařízení můžeme přihlásit libovolným terminálovým programem podporujícím sériovou komunikaci (např. Putty, Hyperterm atd.).

Parametry komunikace jsou následující:

Modul (číslo vývodu)	Využití
Port	Číslo virtuálního COM portu - většinou vyšší než 20 (např. COM 22)
Rychlost	38400
Počet bitů	8
Stop bity	1
Parita	žádná
Řízení toku	XON/XOFF

Tabulka 4 – Parametry komunikace rozhraní USART1

Na sériové rozhraní jsou vypisovány podrobné informace o stavu zařízení a probíhajících transakcích, které je možné využít pro diagnostiku. V reálném nasazení by zřejmě bylo vhodné upravit formát a obsah vypisovaných hlášení. Snížením počtu vypisovaných hlášení (či jejich úplným vynecháním) by bylo možné podstatně redukovat požadavky na velikost paměti mikrokontroléru.

Příklad výpisu na sériové rozhraní:

```
Karta vložena
size: 30MB
free: 30/0 30

Proběhl restart: 18.04.11 13:08:46
AACS 1.0
-----
Zarizeni nevyzaduje PIN!
Vypis platnych EEPROM ID:
1
[0]:01 00 00 02 1B 1E 29 CRC:20
18.04.11 13:09:00 Neplatny ID - 01 00 00 01 14 04 65 CRC:97
18.04.11 13:09:08 Neplatny ID - 01 00 00 00 E9 B2 ED CRC:48
18.04.11 13:09:15 Platny ID - 01 00 00 02 1B 1E 29 CRC:20
18.04.11 13:09:22 Neplatny ID - 01 00 00 01 14 04 65 CRC:97
- Pridan novy Button
18.04.11 13:09:40 Platny ID - 01 00 00 01 14 04 65 CRC:97
18.04.11 13:09:46 Odemceno internim tlačítkem
18.04.11 13:10:03 PIN nastaven - 1199
18.04.11 13:10:34 Platny ID - 01 00 00 01 14 04 65 CRC:97
18.04.11 13:10:58 PIN nebude vyžadovan!
18.04.11 13:11:22 Platny ID - 01 00 00 02 1B 1E 29 CRC:20
18.04.11 13:11:28 Neplatny ID - 01 00 00 00 E9 B2 ED CRC:48
```

## 8.5 Práce s menu

Ovládání menu je poněkud netradičně realizováno pomocí pouhých třech tlačítek, čtvrté tlačítko slouží k přímému otevření elektromagnetického otevírače. Vzhledem k tomu, že testovací zapojení nemá žádnou krycí desku, na niž by bylo možné vyznačit význam tlačítek, byly pro rozlišení funkcí použity různé barvy hmatníků a popis v podobě symbolů resp. písmen.

Pro změnu zvolené hodnoty slouží dvě žlutá tlačítka s popisky „<<“ a „>>“, kde levé tlačítko má logicky funkci posuvu vlevo (změnu hodnoty dolů) a pravé posuvu vpravo (změnu hodnoty nahoru). Na dvojřádkovém displeji se po vstupu do menu zobrazují na horním řádku měněné (měnitelné) hodnoty (pro změnu se používají žlutá tlačítka), na dolním se pomocí znaku „^“ zobrazuje místo měněné hodnoty. Mezi jednotlivými hodnotami se lze přemisťovat pomocí zeleného tlačítka s písmenem „S“ (Select).

Otevření elektromagnetického otevírače lze iniciovat stiskem červeného tlačítka s písmenem „D“ (Door).

Výše uvedený popis zní složitě, ale ovládání je velmi rychle pochopitelné.

Pokud je zapnuta funkce vyžadování PIN správce, je před vstupem do menu nutné zadat správnou kombinaci, jinak je přístup odmítnut.

## 8.6 Funkce menu

V průběhu ovládání zařízení pomocí menu není z bezpečnostních důvodů prováděno ověřování tokenů (modrá LED je zhasnutá). Po vstupu do menu má správce zařízení dostupné následující volby:

- **Nastav PIN**

Tato volba určuje hodnotu čtyřmístného čísla PIN správce zařízení, zároveň je zde možné vynutit či zakázat požadavek na jeho zadání při vstupu do menu pomocí voleb <Zap> a <Vyp>. Hodnota PINu je vždy zobrazena.

- **Nastav čas**

Jak již název napovídá, slouží tato volba k nastavení času. Čas se nastavuje ve 24hodinovém formátu HH:MM:SS. Zařízení nehlídá posuvy při přechodu mezi letním a zimním časem.

- **Nastav datum**

Tato volba slouží k nastavení data ve formátu DD:MM:YY. Kalendář je automatický včetně přestupných roků a díky IO DS1307 je schopen udržovat aktuální datum až do roku 2100 [15].

- **Nauc iButton**

Pomocí této funkce můžeme přidávat do zařízení nové identifikační předměty. V průběhu „učení se“ je na displeji zobrazena výzva k přiložení nového identifikačního předmětu. Po jeho identifikaci a kontrole zda již není evidováno je ID iButtonu zapsáno do paměti EEPROM. Tímto způsobem je možné postupně

zaregistrovat více identifikačních předmětů, pro ukončení je nutné potvrdit volbu „Konec“.

- **Smaz iButton**

Tato funkce zajišťuje postupné procházení registrovaných identifikačních čísel iButtonů, zobrazených v hexadecimálním tvaru a umožňuje odstranění vybraného předmětu z paměti EEPROM a tím zákaz přístupu. Protože se předpokládá mazání pouze ztracených předmětů, je po provedené akci proveden návrat do hlavní nabídky menu.

- **SD info**

Pomocí této volby je možné zobrazit informace o stavu paměťové karty, její kapacitě a volném místě. V případě, že je použita paměťová karta s velkou kapacitou a množstvím souborů na ní uložených, může operace trvat delší dobu.

- **Konec**

Po provedení této volby se zařízení vrátí k provoznímu režimu, modrá LED začne blikat a je možné obsluhovat držitele tokenů.

## 8.7 Provoz zařízení

Z bezpečnostních důvodů je nezbytné, aby zařízení umožňovalo průchod autorizovaným osobám i v případě výpadku dodávky elektrické energie, což je možné realizovat centralizovaně (pomocí zálohovaného okruhu) nebo lokálně (pomocí UPS či baterie).

S ohledem na nutnost zablokování tokenu v případě jeho ztráty je nutné, aby si správce zařízení vedl evidenci identifikačních čísel vydaných předmětů. Včasná blokace minimalizuje riziko zneužití, shromážděná identifikační čísla je však nutné chránit, neboť při jejich znalosti by bylo teoreticky možné vytvořit jejich emulátor (viz kapitola 6). Stejným způsobem je nutné chránit PIN správce pro přístup k ovládacímu rozhraní. Pokud správce PIN zapomene, je možné jej po otevření zařízení resetovat vyjmutím baterie RTC.

V případě bezpečnostního incidentu je možné zpětně analyzovat data uložená na paměťové kartě a získat tak přehled o vstupu jednotlivých osob do chráněných oblastí. Paměťovou kartu lze vyjmout ze zařízení i za chodu, zařízení pak zůstává v provozním režimu a dál obsluhuje uživatele, ale samozřejmě není schopno zapisovat transakce na paměťové médium. Tento stav je indikován rychle blikající modrou barvou LED. Po opětovném vložení karty do zařízení doporučuji provést jeho reset (viz kapitola 8.3).

## 8.8 Vypnutí zařízení, reset

Zařízení je možné v kterémkoli okamžiku vypnout pomocí vypínače, před vypnutím není třeba provádět žádnou akci. V případě, že bude provedeno vypnutí uprostřed transakce, může se stát, že data bufferu ještě nebyla zapsána na paměťovou kartu a poslední transakce tak nebude zaznamenána.

Reset zařízení může být vykonán pomocí tlačítka reset na modulu programátoru či na modulu mikrokontroléru. U prototypu zařízení by bylo možné vyvést tlačítko pro reset z vývodu číslo 20 (RESET), ale lze jej vynechat a případný reset zařízení řešit pomocí jeho zapnutí a vypnutí.

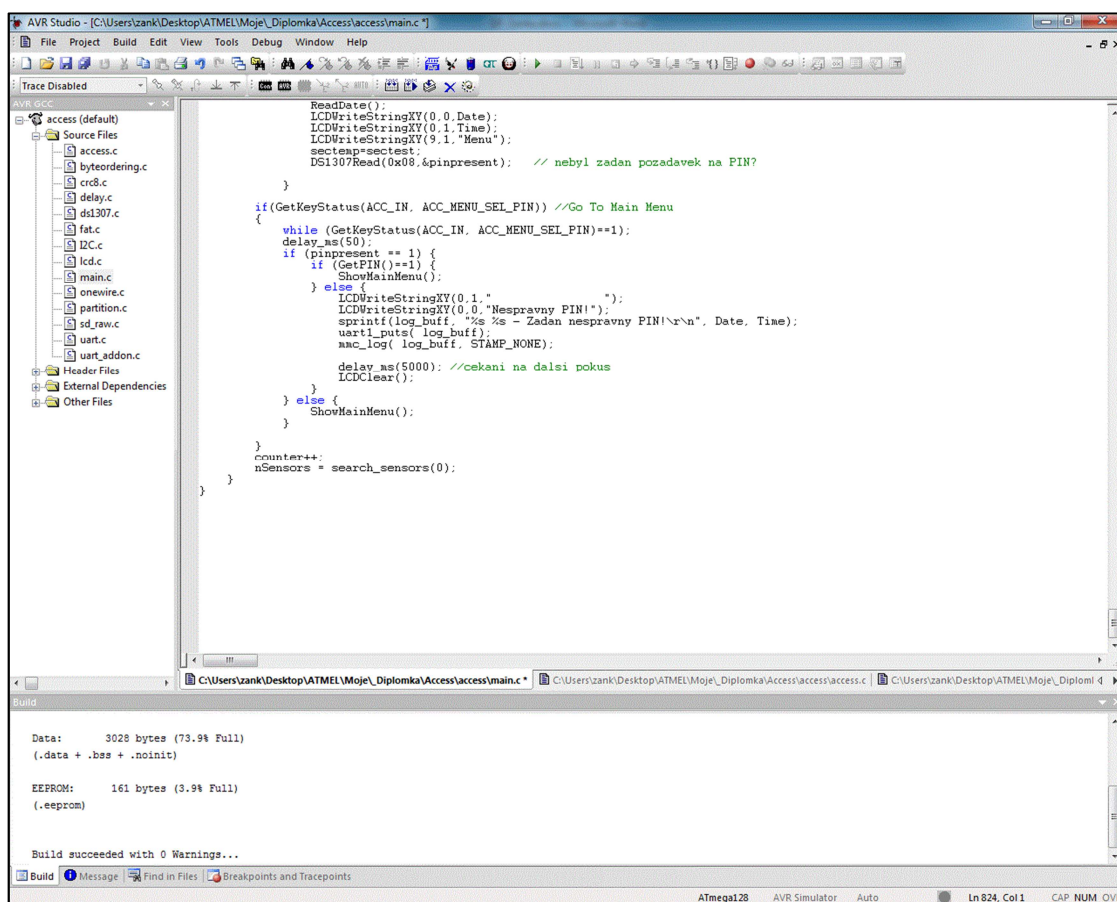


## 9 SOFTWARE VYBAVENÍ

Programové vybavení mikrokontroléru provádějící veškerou logiku je vytvořeno ve vývojovém prostředí AVR Studio verze 4.18, které používá programovací jazyk C. Vzhledem k tomu, že program je poměrně rozsáhlý – obsahuje téměř deset tisíc řádků kódu, není smysluplné jej uvádět v tištěné formě a je tedy umístěn na CD, které je součástí této práce.

### 9.1 AVR Studio

Firma Atmel poskytuje pro potřeby vývojářů aplikací využívajících mikrokontroléry ATmega vlastní vývojové prostředí nazvané AVR Studio [3]. Toto prostředí umožňuje za pomoci nástroje AvrGCC vytvářet optimalizovaný program pro konkrétní řady mikrokontrolérů bez znalosti syntaxe jazyka symbolických adres (assembleru). Jedná se o plně grafické prostředí, k němuž je možné pro jednoduché aplikace připojit softwarové simulátory periférií jako například HAPSIM [20]. To velmi usnadňuje a urychluje vývoj v počátečních fázích projektu.



Obrázek 36 – Vývojové prostředí AVR Studio

## 9.2 Použité knihovny

Vzhledem k tomu, že se nezabývám programováním na profesionální úrovni, jsem se při vývoji programového vybavení snažil o maximální využití již existujícího kódu pro obsluhu periférií mikrokontroléru. S ohledem na autorská práva však byly použity pouze ty zdrojové kódy, jejichž licence toto užití dovoluje. Základem pro kostru programu je demo napsané Martinem Thomasem pro vyčítání teplot ze součástek řady DS18x20 pomocí sběrnice 1-Wire [18]. Tento program samozřejmě není přímo použitelný pro tento projekt, nicméně byl velmi dobrý pro inspiraci a navíc obsahuje již hotové části upotřebitelného kódu uvolněného v rámci licence GNU GPL.

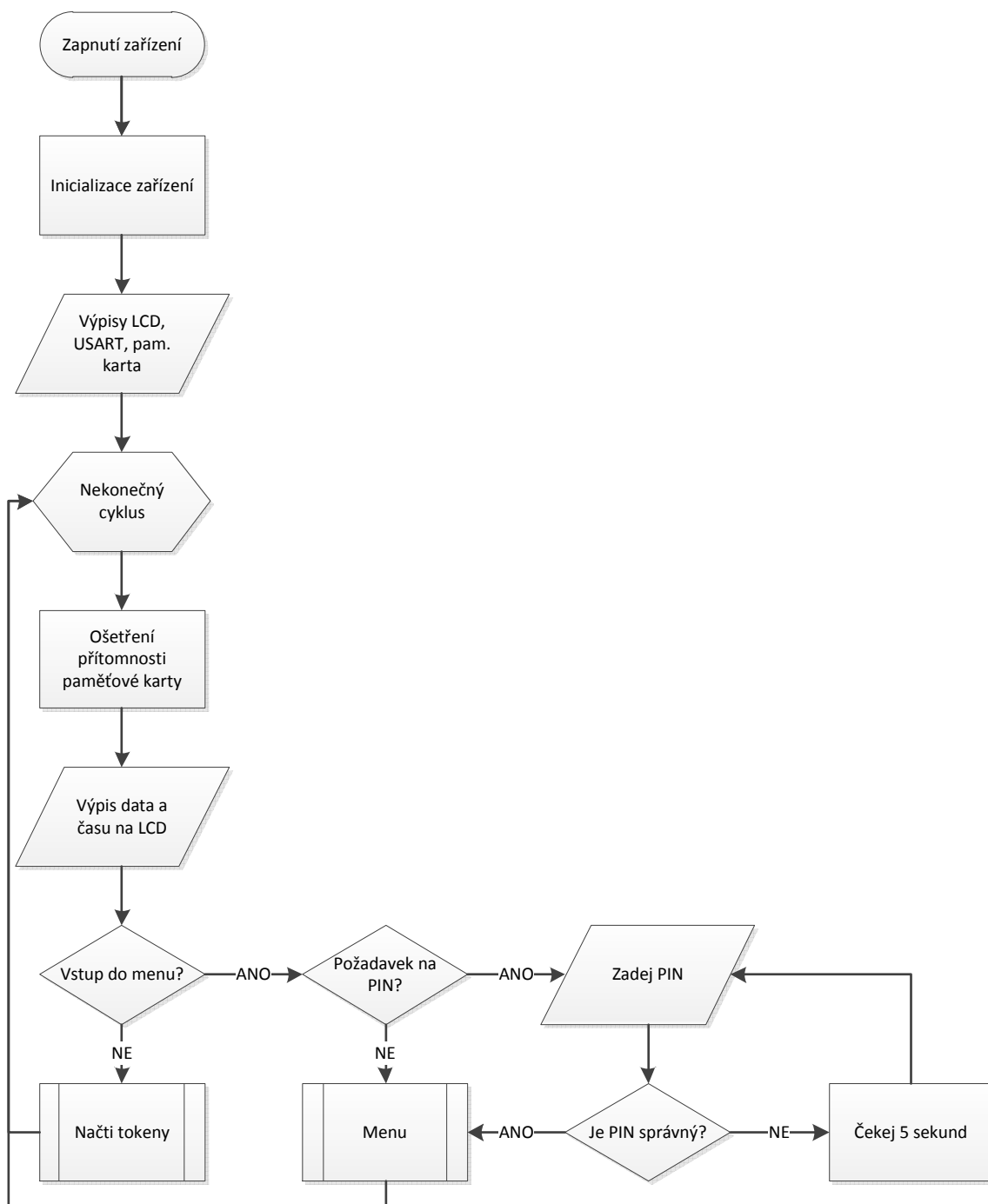
Práci s ovládacím rozhraním popisují celkem zdařile zpracované stránky firmy eXtreme Electronics, které obsahují rovněž příklady využití zvoleného dvouřádkového displeje [9]. Ačkoli se jedná o veřejně publikované tutoriály, jsou některé části zdrojových kódů označené copyrightem. Autorem těchto stránek i zdrojových kódů je Avinash Gupta, s jehož písemným svolením byla upravena část zdrojových kódů pro vytvoření menu a práci s RTC.

Poslední částí, kterou bylo vhodné převzít, je implementace souborového systému pro práci s paměťovou kartou. V této oblasti existuje velké množství různě propracovaných projektů, z nichž se jako nejpoužitelnější jeví projekt „MMC/SD/SDHC card library“, jehož autorem je Roland Riegel [16]. Zdrojové kódy tohoto projektu jsou navíc publikovány v licencích GNU GPL a GNU LGPL, takže je možné je plně využít.

## 9.3 Stručný popis programu mikrokontroléru

Hlavní část programu je poměrně jednoduchá. Po zapnutí zařízení proběhne inicializace jednotlivých periférií. Po diagnostických výstupech se zpracování dostává do nekonečného cyklu, v jehož rámci probíhá testování přítomnosti tokenu na sběrnici 1-Wire. Frekvence testování je závislá na taktu mikrokontroléru - při osazení externím krystalem 16 MHz se jedná řádově o stovky otestování za sekundu. Z hlavního cyklu je pak možné vstoupit do menu, které je zpracováváno ve výhradním režimu. Před vstupem do menu je proveden test požadavku na PIN. Pokud je vyžadován, je uživatel nucen zadat čtyřmístné číslo správce zařízení. Nežadá-li uživatel správný pin, je zpracování pozastaveno na 5 sekund.

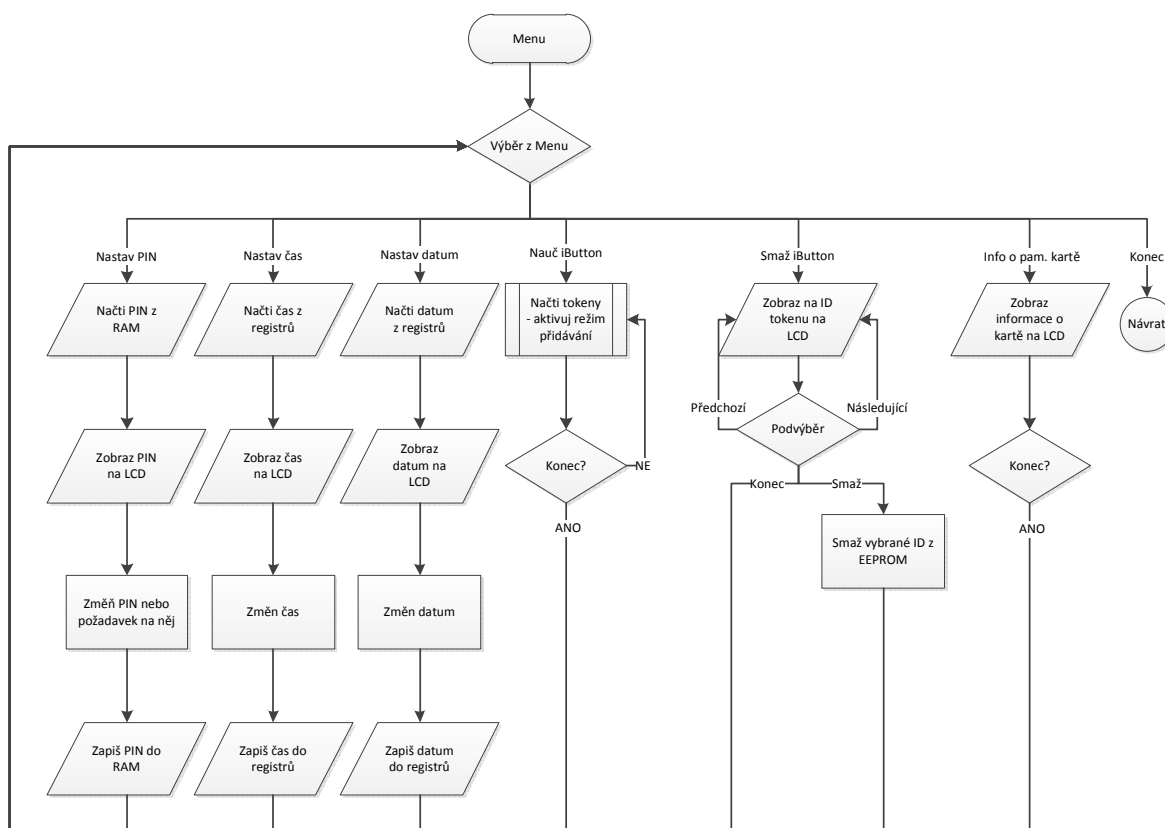
Zpracování hlavního cyklu programu je zobrazeno v následujícím vývojovém diagramu:



Obrázek 37 – Vývojový diagram hlavního cyklu programu

Po vstupu do menu je možné vybírat z výše uvedených voleb (viz kapitola 8.6), nastavovat jednotlivé hodnoty, přidávat a mazat registrované tokeny atd. Z bezpečnostních důvodů je každá akce ukončena zápisem hodnot do příslušné oblasti paměti ještě před opuštěním menu a přechodem zařízení do provozního stavu.

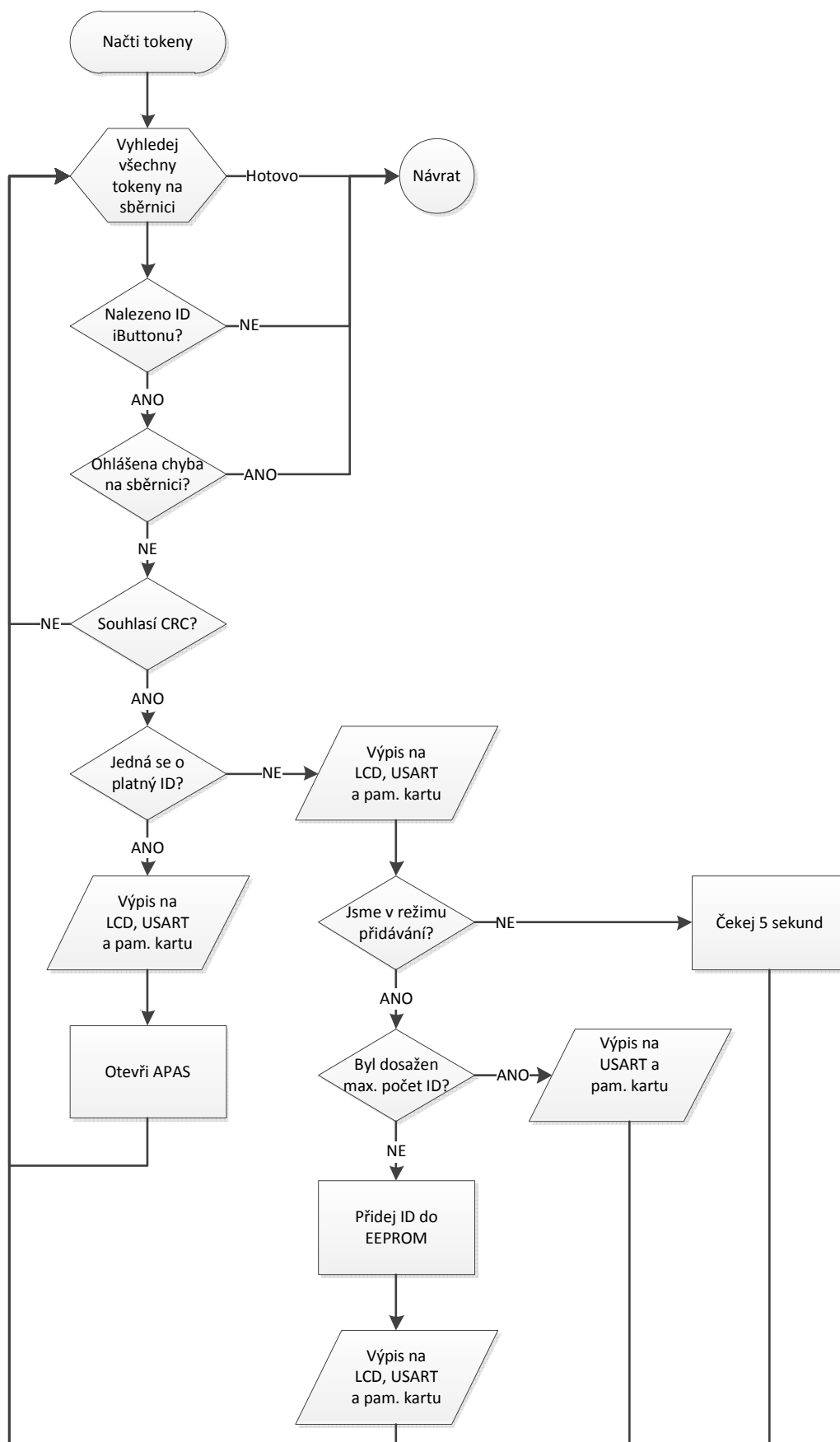
Vývojový diagram algoritmu pro obsluhu menu je následující:



Obrázek 38 – Vývojový diagram obsluhy menu

Program obsluhující zařízení se samozřejmě skládá ze značného množství různých funkcí a procedur. Pro pochopení funkce zařízení je však důležité pouze volání funkce zajišťující detekci tokenů a zpracování načtených identifikačních čísel. Funkce se skládá z cyklu, který předpokládá možnost koexistence více identifikačních prvků na sběrnici 1-Wire v jednom okamžiku (resp. existenci více sběrnic). V průběhu cyklu je testováno vždy jedno načtené identifikační číslo a jsou provedeny základní kontroly - zda na sběrnici nevznikla chyba a zda CRC načteného předmětu souhlasí. Pokud ano, je rozlišeno, jestli se jedná o registrovaný předmět či nikoli. Pro povolené tokeny je po zalogování transakce povolen přístup (apas otevřen). V případě že načtený předmět není registrován, proběhne ještě kontrola, zda byla funkce volána v režimu přidání předmětu a poté, zda není překročen maximální počet zaregistrovaných ID. Při odmítnutí přístupu vstupuje zařízení do čekací smyčky o délce 5 sekund.

Popsaný algoritmus je znázorněn v následujícím diagramu:



Obrázek 39 – Vývojový diagram zpracování ID tokenu

## 10 EKONOMICKÁ ANALÝZA SESTAVENÉHO ZAŘÍZENÍ

Cílem této práce je vytvoření testovacího zapojení bezpečnostní aplikace, což je předpokladem pro výrobu komerčního zařízení. Předtím, než může být zahájena sériová výroba, je však nutné, aby bylo splněno mnoho zákonných podmínek pro uvedení na trh - například byl ověřen soulad s potřebnými normami, bylo vydáno ES prohlášení o shodě (CE Conformity Declaration) atd. Ekonomická analýza tohoto charakteru není předmětem této práce. Nás v tuto chvíli spíše zajímá, zda je možné vyrobit navržený autonomní systém kontroly vstupů založený na výsledcích této práce v kusové či malosériové výrobě.

Pro odhad ceny tedy předpokládáme malosériovou testovací výrobu několika kusů zařízení (cca 10 ks). Vznikající zařízení nebude potřebovat programátor, neboť se nepředpokládá změna programového vybavení uživatelem. Rovněž elektromagnetický otevírač není a ani nemůže být součástí dodávky. Pro konkrétní nasazení je vždy nutné vybrat z velkého množství druhů a výrobců typ s rozměry a parametry odpovídajícími konkrétnímu umístění.

Před vlastním zahájením výroby zařízení je nutné navrhnout vhodný jednostranný plošný spoj, jehož velikost by dle mého názoru neměla překročit  $1 \text{ dm}^2$ . Aby byla garantována technicky dokonalá montáž, bylo by vhodné, aby výrobu a osazování plošného spoje součástkami prováděla profesionální firma. Před výrobou i takto malého počtu kusů je nezbytné provést některé předvýrobní operace shodné s výrobou tisícových sérií, jako je vytvoření filmové předlohy, příprava programů pro CNC stroje atd. Naštěstí je dnes díky počítačové podpoře výroby možné tyto náklady minimalizovat a při použití jednostranného plošného spoje by neměly překročit 1000 Kč na celou sérii. Cena osazení a dokončovacích prací (lakování, umístění do krabičky) by se pak měla pohybovat okolo 250 Kč na jedno zařízení.

Následující cenový odhad vychází z koncových cen součástek firem GM Electronic, spol. s r.o., TME Czech Republic s.r.o. a Premier Farnell plc. V případě více možností byla vždy volena cena nižší. Pro odhad nákladů na předvýrobní přípravu byly použity reálné cenové nabídky na výrobu prototypů podobně velkých zařízení několika českých firem z konce roku 2010, jejichž cena byla zprůměrována. Všechny ceny jsou uvedeny včetně 20 % DPH.

(Modul) Součástka	ks	Cena/ks	Celkem
<b>(Napájecí zdroj)</b>			
7805	1	7,00 Kč	7,00 Kč
LM1117_33 Stabilizátor 3.3V	1	32,00 Kč	32,00 Kč
1N5820	1	3,00 Kč	3,00 Kč
1N5408	1	1,60 Kč	1,60 Kč
1N4007	1	1,10 Kč	1,10 Kč
Konektor napájecí	1	20,00 Kč	20,00 Kč
<b>(MCU)</b>			
ATmega128	1	157,00 Kč	157,00 Kč
Krystal 16Mhz	1	15,00 Kč	15,00 Kč
Krystal 32768Hz	1	11,00 Kč	11,00 Kč
<b>(USART převodník)</b>			
USB-B konektor	1	12,00 Kč	12,00 Kč
FT232RL	1	78,00 Kč	78,00 Kč
IRF7416SMD	1	14,00 Kč	14,00 Kč
MI0805K400R-10	1	11,00 Kč	11,00 Kč
<b>(LCD displej)</b>			
4x tlačítka	1	36,00 Kč	36,00 Kč
LCD 16x2 znaků – zelený, podsvícený	1	172,00 Kč	172,00 Kč
<b>(Výkonový spínač)</b>			
IRFD110PBF	1	10,00 Kč	10,00 Kč
<b>(Čtečka)</b>			
Kontakt čtečky	1	137,00 Kč	137,00 Kč
<b>(RTC)</b>			
DS1307Z+	1	36,00 Kč	36,00 Kč
Baterie 2032	1	9,00 Kč	9,00 Kč
Kontakt baterie	1	20,50 Kč	20,50 Kč
Krystal 32768Hz	1	11,00 Kč	11,00 Kč
<b>(Voltage Level Translator)</b>			
TXB0104	1	45,00 Kč	45,00 Kč
paměťová karta	1	50,00 Kč	50,00 Kč
SD konektor	1	16,00 Kč	16,00 Kč
<b>(Ochrana vstupu)</b>			
DS9503 nebo Zenerova dioda	1	24,00 Kč	24,00 Kč
<b>(Ostatní)</b>			
Konektor pro připojení el. otevírače - 6PIN	1	8,00 Kč	8,00 Kč
Napájecí zdroj 230V/12V DC	1	100,00 Kč	100,00 Kč
iButton DS1990A	3	76,00 Kč	228,00 Kč
Kondenzátory SMD	18	1,50 Kč	27,00 Kč
Diody	5	2,00 Kč	10,00 Kč
RGB LED – 1ks	1	8,00 Kč	8,00 Kč

(Modul) Součástka	ks	Cena/ks	Celkem
LED 5ks	2	1,40 Kč	2,80 Kč
Odpory (SMD0805)	40	0,15 Kč	6,00 Kč
Krabička	1	20,00 Kč	20,00 Kč
Deska 1dm <sup>2</sup>	1	80,00 Kč	80,00 Kč
Osazení 1ks výrobku	1	200,00 Kč	200,00 Kč
podíl 1ks výrobku na přípravě při 10ks	1	100,00 Kč	100,00 Kč
dokončovací práce – 1ks výrobku	1	50,00 Kč	50,00 Kč
<b>Celková cena vč. DPH:</b>			<b>1765,00 Kč</b>

Tabulka 5 – Soupis použitých součástek

Z výše uvedeného rozpisu je zřejmé, že maximální cena samotného zařízení by se při využití všech modulů a výrobě několika kusů pohybovala okolo 1800 Kč včetně DPH. Tato cena je odvozená od ceny součástek pro koncového uživatele, při sériové výrobě by byla samozřejmě nižší, navíc by náklady na předvýrobní přípravu byly rozpočítány mezi více kusů. Pro další snížení ceny by bylo žádoucí, abychom zařízení s ohledem na reálné využití paměti FLASH osadili mikrokontrolérem nižší řady resp. s nižší kapacitou paměti. Bez jakýchkoli úprav zdrojového kódu by stačil jakýkoli MCU ATmega s kapacitou paměti FLASH 64kB, po optimalizaci zdrojového kódu či vynechání některých funkcí by zřejmě bylo možné použít i typ s 32 kB FLASH. Modulární návrh zařízení rovněž umožňuje po úpravě programového vybavení vynechat některé moduly, jako například paměťovou kartu či dokonce RTC a LCD displej, tím snížit cenu, ovšem s dopadem na uživatelskou přívětivost při ovládání zařízení.

Ve výše kalkulované ceně samozřejmě nejsou zahrnuty náklady na provedení testů a prací vedoucích k vydání prohlášení o shodě ani marže pokrývající zisk a náklady související s prodejem zařízení (přímé a nepřímé náklady na marketing, distribuci, reklamace, podporu atd.). Přesto je cena v porovnání s ostatními, na trhu dostupnými zařízeními (viz kapitola 1.2) a s přihlédnutím na jejich funkcionalitu více než přijatelná. I s marží by se při sériové výrobě mohla pohybovat okolo poloviny ceny konkurence.



## 11 DALŠÍ MOŽNÝ ROZVOJ ZAŘÍZENÍ

Přestože byl návrh zařízení dopracován do co největších detailů, stále existují oblasti, které by bylo možné v budoucnu rozvinout a dále tak zvýšit funkcionalitu zařízení.

Pozornost by bylo možné věnovat například následujícím námětům:

- Navržené zapojení by bylo možné rozšířit o bezkontaktní část a vytvořit tak autonomní vstupní systém s volitelně kontaktní a/nebo bezkontaktní částí.
- Uložením PINu uživatele tokenu do EEPROM a připojením jednoduché číselné klávesnice by bylo možné zvýšit úroveň zabezpečení na Třidu identifikace 3 dle ČSN EN 50133-1.
- Revizí zdrojového kódu, jeho optimalizací a případným vypuštěním některých textových výpisů by bylo možné dosáhnout podstatného snížení velikosti výsledného kódu. Pak by bylo možné použít mikrokontroléry s nižší kapacitou paměti.
- Vhodné by bylo rovněž vylepšit práci s paměťovou kartou, zejména zajistit kompatibilitu zařízení s různými druhy karet vyšší kapacity.
- Při vytváření funkčního prototypu by bylo možné jít i druhou cestou, tedy nezvyšovat funkcionalitu zařízení pomocí dalších obvodů, ale naopak minimalizovat jejich počet a vše ovládat pomocí sériové komunikace. Tak by vzniklo velmi levné (a velmi jednoduché) zařízení, které by pro svůj provoz potřebovalo pouze mikrokontrolér (případně ještě USART/USB převodník). Ovládat by jej ovšem bylo možné pouze pomocí připojeného počítače.

## ZÁVĚR

Cílem této diplomové práce bylo vytvoření testovacího zapojení bezpečnostní aplikace – autonomního systému kontroly vstupů, které by odpovídalo zadání a zároveň by splňovalo vytyčené ekonomické cíle, tedy bylo by při vyšší funkcionalitě levnější než na trhu již existující zařízení. Řešení se skládá ze dvou částí – z hardwarové části, která je realizována pomocí propojených modulů stavebnice MLAB a softwarové části, jež je napsána ve vývojovém prostředí AVR Studio 4 při použití programovacího jazyku C.

Hardwarová část je založena na mikrokontroléru ATmega128 a podpůrných obvodech jako jsou hodiny reálného času, převodník napětíových úrovní atd. Navržené zařízení se ovládá pomocí LCD displeje a čtyř tlačítek a je schopno komunikovat pomocí sériového rozhraní s libovolným PC vybaveným portem USB. Události o transakcích se ukládají na paměťovou kartu. Pro realizaci HW části jsem na počátku práce předpokládal využití již existujících modulů stavebnice MLAB, v průběhu analýzy však vyvstala potřeba vytvořit moduly specifické pro tento projekt. Nově vzniklé moduly jsou tedy navrženy jako univerzální a do budoucna obohatí portfolio stavebnice.

Hardwarová část neslouží pouze k otestování zapojení, ale s ohledem na možné využití k výukovým účelům je realizována ve formě kompletní sestavy včetně elektromagnetického otevírače a čtečky umístěné společně s vývojovou deskou na plexisklovém držáku, čímž je zajištěna potřebná mechanická odolnost. Celé zařízení je pak umístěno v transparentním ochranném plastovém boxu.

Při návrhu testovacího zapojení a programového vybavení bylo dbáno na bezpečnostní hledisko a výsledné zařízení tak nejenže vyhovuje zadání, ale obsahuje další bezpečnostní prvky, které zvyšují odolnost zařízení proti poškození a útoku. Zohledněny byly rovněž požadavky příslušných norem, především ČSN EN 50133.

Provedená ekonomická analýza ukázala, že zařízení by bylo možné vyrábět při zhruba poloviční ceně ve srovnání s již existujícími výrobky a to při vyšší funkcionalitě. V porovnání s klasickým bezpečnostním zámkem je zařízení sice při počáteční investici dražší, to ale platí pouze do okamžiku první ztráty klíčů.

Výstupem této práce je tedy plně funkční zařízení splňující všechny požadavky zadání, které je ve stavu, kdy by bylo možné vyrobit prototyp a po jeho certifikaci zahájit sériovou výrobu.

## CONCLUSION

The goal of this master thesis was to create a testing security appliance – an autonomous access control system that would fulfill the requirements while meeting the set economic goals and thus being cheaper even with more functionality than that of the devices already present on the market. The solution consists of two parts – the hardware part, which is realized through interconnected modules of the MLAB kit, and software part, which is written in a development environment AVR Studio 4 in the C programming language.

The hardware part is based on the ATmega128 microcontroller and support circuits such as real-time clock, voltage level translator, etc. The proposed device is controlled through the LCD display and four buttons and is able to communicate via a serial interface with any PC equipped with a USB port. Records of the transactions are stored on the memory card. At the beginning of the work I have assumed to use the already existing MLAB kit modules for the realization of the hardware, during the analysis, however, there arose a need to create modules specific to this project. The newly created modules are therefore designed to be versatile and they enrich the future portfolio of the kit.

The purpose of the hardware part is not just testing its functionality, but with regard to the possible use for educational purposes it is implemented as a complete assembly including an electromagnetic opener and reader placed together with the development board on the Plexiglas holder, which ensures the necessary mechanical robustness. The entire device is then placed in a protective transparent plastic box.

When designing the test circuitry and software care was taken to the safety aspect and the resulting device will not only conform to specification, but includes additional security features that increase resistance against equipment damage and attacks. Also the relevant requirements of standards, notably EN 50133, were taken into account.

The conducted economic analysis showed that the device could be produced at about half price compared to existing products and at a higher functionality. Compared with conventional security lock the device is still more expensive because of the initial investment, but this only holds until the first loss of keys.

The outcome of this work is thus a fully functional device meeting all requirements, which is in a state where it would be possible to produce prototype and after its certification to start mass production.

## SEZNAM POUŽITÉ LITERATURY

- [1] *I-Wire and iButton* [online]. c2011 [cit. 2011-04-09]. Dostupné z WWW: <[http://www.maxim-ic.com/auto\\_info.cfm](http://www.maxim-ic.com/auto_info.cfm)>.
- [2] *Atmel Corporation –ATmega128* [online]. c2011 [cit. 2011-04-09]. Dostupné z WWW: <[www.atmel.com/dyn/products/product\\_card.asp?part\\_id=2018](http://www.atmel.com/dyn/products/product_card.asp?part_id=2018)>.
- [3] *Atmel Corporation Home* [online]. c2011 [cit. 2011-04-09]. Dostupné z WWW: <[www.atmel.com](http://www.atmel.com)>.
- [4] ČSN EN 50133-1 Změna A1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích : Část 1: Systémové požadavky*. [s.l.] : Český normalizační institut, Červen 2003. 7 s.
- [5] ČSN EN 50133-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích : Část 1: Systémové požadavky*. [s.l.] : Český normalizační institut, Březen 2001. 26 s.
- [6] ČSN EN 50133-2-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích : Část 2-1: Všeobecné požadavky na komponenty*. [s.l.] : Český normalizační institut, Březen 2001. 10 s.
- [7] ČSN EN 50133-7. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích : Část 7: Pokyny pro aplikace*. [s.l.] : Český normalizační institut, Listopad 2000. 13 s.
- [8] *DS Technik* [online]. c2011 [cit. 2011-04-09]. Autonomní bezdotykový přístupový systém až pro 100 účastníků autonomní přístupové systémy VIDEX ART 4850. Dostupné z WWW: <<http://www.dstechnik.cz/autonomni-bezdotykovy-pristupovy-system-az-pro-100-ucastniku/autonomni-pristupove-systemy-videx-art-4850-samostatna-bezdotykova-ctecka-3949.html>>.
- [9] GUPTA, Avinash. *eXtreme Electronics* [online]. Oct-23rd-2009 [cit. 2011-04-09]. Interfacing DS1307 RTC Chip with AVR Microcontroller. Dostupné z WWW: <[extremeelectronics.co.in/avr-tutorials/interfacing-ds1307-rtc-chip-with-avr-microcontroller/](http://extremeelectronics.co.in/avr-tutorials/interfacing-ds1307-rtc-chip-with-avr-microcontroller/)>.
- [10] *Hlavní stránka MLAB* [online]. c2011 [cit. 2011-04-09]. Dostupné z WWW: <[www.mlab.cz/](http://www.mlab.cz/)>.

- [11] *Jablotron* [online]. c2008 [cit. 2011-04-09]. AS-80 přístupový systém. Dostupné z WWW:  
<[www.jablotron.cz/cz/Katalog/automatizace/pristupove+systemy/as80+pristupovy+system/](http://www.jablotron.cz/cz/Katalog/automatizace/pristupove+systemy/as80+pristupovy+system/)>.
- [12] MATOUŠEK, David. *Práce s mikrokontroléry ATMEL AVR - ATmega16*. Praha : BEN – technická literatura, 2006. 320 s. ISBN 80-7300-174-8.
- [13] MATOUŠEK, David. *Práce s mikrokontroléry Atmel AVR*. 2. vydání. Praha : BEN – technická literatura, 2006. 376 s. ISBN 80-7300-209-4.
- [14] MATOUŠEK, David. Praktické aplikace obvodu FT232RL - konvertoru USB/UART. *Konstrukční elektronika - Amatérské Radio*. 2009, 1, s. 3-39. ISSN 1211-3557.
- [15] *Real-Time Clocks (RTCs)* [online]. c2011 [cit. 2011-04-09]. Dostupné z WWW:  
<[www.maxim-ic.com/products/rtc/real-time-clocks.cfm](http://www.maxim-ic.com/products/rtc/real-time-clocks.cfm)>.
- [16] RIEGEL, Roland. *www.roland-riegel.de* [online]. c2011 [cit. 2011-04-09]. MMC/SD/SDHC card library. Dostupné z WWW:  
<[www.roland-riegel.de/sd-reader/index.html](http://www.roland-riegel.de/sd-reader/index.html)>.
- [17] *Tektronik* [online]. c2011 [cit. 2011-04-09]. FX319 (E, DS2). Dostupné z WWW:  
<[www.tetronik.cz/pruvodce-produkty/pristupovy-system/kategorie/kontakti-1/fx319/](http://www.tetronik.cz/pruvodce-produkty/pristupovy-system/kategorie/kontakti-1/fx319/)>.
- [18] THOMAS, Martin. *AVR-Projects* [online]. 9.2.2011 [cit. 2011-04-09]. DS18X20 with AVR. Dostupné z WWW:  
<[gandalf.arubi.uni-kl.de/avr\\_projects/tempsensor/index.html](http://gandalf.arubi.uni-kl.de/avr_projects/tempsensor/index.html)>.
- [19] *Voltage Level Translation* [online]. c2011 [cit. 2011-04-09]. Dostupné z WWW:  
<[focus.ti.com/paramsearch/docs/parametricsearch.tsp?familyId=705&family=analog&uiTemplateId=NODE\\_STRY\\_PGE\\_T](http://focus.ti.com/paramsearch/docs/parametricsearch.tsp?familyId=705&family=analog&uiTemplateId=NODE_STRY_PGE_T)>.
- [20] WALLNER, Helmut. *HAPSIM* [online]. c2009 [cit. 2011-04-09]. HAPSIM - Helmi's AVR Periphery Simulator V2.17. Dostupné z WWW:  
<[www.helmix.at/hapsim](http://www.helmix.at/hapsim)>.

## SEZNAM POUŽITÝCH ZKRATEK

AVR	<i>Advanced Virtual RISC</i> – označení pro rodinu 8bitových mikročipů typu RISC s harvardskou architekturou od firmy Atmel
BCD	<i>Binary Coded Decimal</i> – Dvojkově reprezentované dekadické číslo
CRC	<i>Cyclic Redundancy Check</i> – Cyklický redundantní součet
EEPROM	<i>Electrically Erasable Programmable Read-Only Memory</i> – Elektricky mazatelná nevolatilní paměť
FAT	<i>File Allocation Table</i> – Tabulka obsahující informace o obsazení disku daty
FLASH	Nevolatilní elektricky programovatelná (zapisovatelná) paměť s libovolným přístupem (jedná se o druh EEPROM)
IC (IO)	<i>Integrated Circuit</i> – Integrovaný obvod
ID	<i>Identification Data</i> – Identifikační číslo (identifikátor)
LCD	<i>Liquid Crystal Display</i> – Displej z tekutých krystalů
LED	<i>Light-Emitting Diode</i> - Dioda vyzařující světlo
Master	Řídící zařízení v rámci komunikace
MCU	<i>Microcontroller Unit</i> – Mikrokontrolér
MMC	<i>MultiMedia Card</i> – Typ paměťové karty
NV	<i>Non-volatile</i> – Nezávislá na napájení (nejčastěji paměť)
PC	<i>Personal computer</i> – Osobní počítač
PLC	<i>Programmable Logic Controller</i> – Programovatelný logický automat
RTC	<i>Real Time Clock</i> – Obvod reálného času
SD	<i>Secure Digital</i> – Typ paměťové karty
Slave	Řízené zařízení v rámci komunikace
UPS	<i>Uninterruptible Power Supply</i> – zařízení zajišťující nepřetržitou (souvislou) dodávku elektřiny

## SEZNAM OBRÁZKŮ

Obrázek 1 – Základní funkce systému kontroly vstupů - ČSN EN 50133-1 (kap. 4.1) .....	23
Obrázek 2 – Příklad uspořádání funkcí - ČSN EN 50133-1 (kap. 4.2) .....	24
Obrázek 3 – Tradiční postup povoleného přístupu - ČSN EN 50133-1 (kap. 4.3).....	27
Obrázek 4 – Blokové schéma architektury AVR [2] .....	29
Obrázek 5 – Zpracování operace v rámci jednoho cyklu ALU [2] .....	30
Obrázek 6 – Zpracování instrukcí [2] .....	30
Obrázek 7 – Blokové schéma MCU ATmega128 [2].....	32
Obrázek 8 – Schéma sériového rozhraní SPI – ATmega128 [2].....	34
Obrázek 9 – Blokové schéma sériového kanálu USART [2] .....	35
Obrázek 10 – Propojení zařízení pomocí TWI [2] .....	36
Obrázek 11 – Základní schéma sběrnice 1-Wire – Maxim Integrated Products [2].....	37
Obrázek 12 – Identifikační prvek iButton .....	37
Obrázek 13 – Načtení kontrolního součtu prvku iButton .....	38
Obrázek 14 – Blokové schéma navrženého řešení .....	43
Obrázek 15 – Schéma mikrokontroléru programátoru .....	44
Obrázek 16 – Schéma převodníku RS232/USB programátoru .....	45
Obrázek 17 – Schéma USART/USB převodníku .....	46
Obrázek 18 – Schéma LCD displeje .....	47
Obrázek 19 – DS1307 – popis interního registru .....	48
Obrázek 20 – Schéma obvodu RTC DS1307 .....	48
Obrázek 21 – Základní zapojení paměťové karty .....	49
Obrázek 22 – Schéma zapojení převodníku napět'ových úrovní .....	50
Obrázek 23 – Schéma výkonového spínače .....	51
Obrázek 24 – Zapojení napájecího zdroje .....	51
Obrázek 25 – Modul MCU ATmega128 .....	57
Obrázek 26 – Modul programátoru .....	57
Obrázek 27 – Modul USART/USB převodníku .....	58
Obrázek 28 – Modul LCD s tlačítky .....	59
Obrázek 29 – Modul RTC .....	60
Obrázek 30 – Modul převodníku napět'ových úrovní .....	60
Obrázek 31 – Modul paměťové karty .....	61
Obrázek 32 – Modul výkonového spínače .....	62

Obrázek 33 – Modul napájecího zdroje .....	62
Obrázek 34 – Obvod ochrany MCU .....	68
Obrázek 35 – Fyzická realizace testovacího zapojení zařízení.....	69
Obrázek 36 – Vývojové prostředí AVR Studio .....	77
Obrázek 37 – Vývojový diagram hlavního cyklu programu .....	79
Obrázek 38 – Vývojový diagram obsluhy menu .....	80
Obrázek 39 – Vývojový diagram zpracování ID tokenu .....	81



**SEZNAM TABULEK**

Tabulka 1 – Příklad nákladů - zakoupení bezpečnostních vložek a jejich přestavba .....	14
Tabulka 2 – Seznam použitých vývodů MCU .....	54
Tabulka 3 – Seznam propojení modulů .....	55
Tabulka 4 – Parametry komunikace rozhraní USART1 .....	72
Tabulka 5 – Soupis použitých součástek .....	84

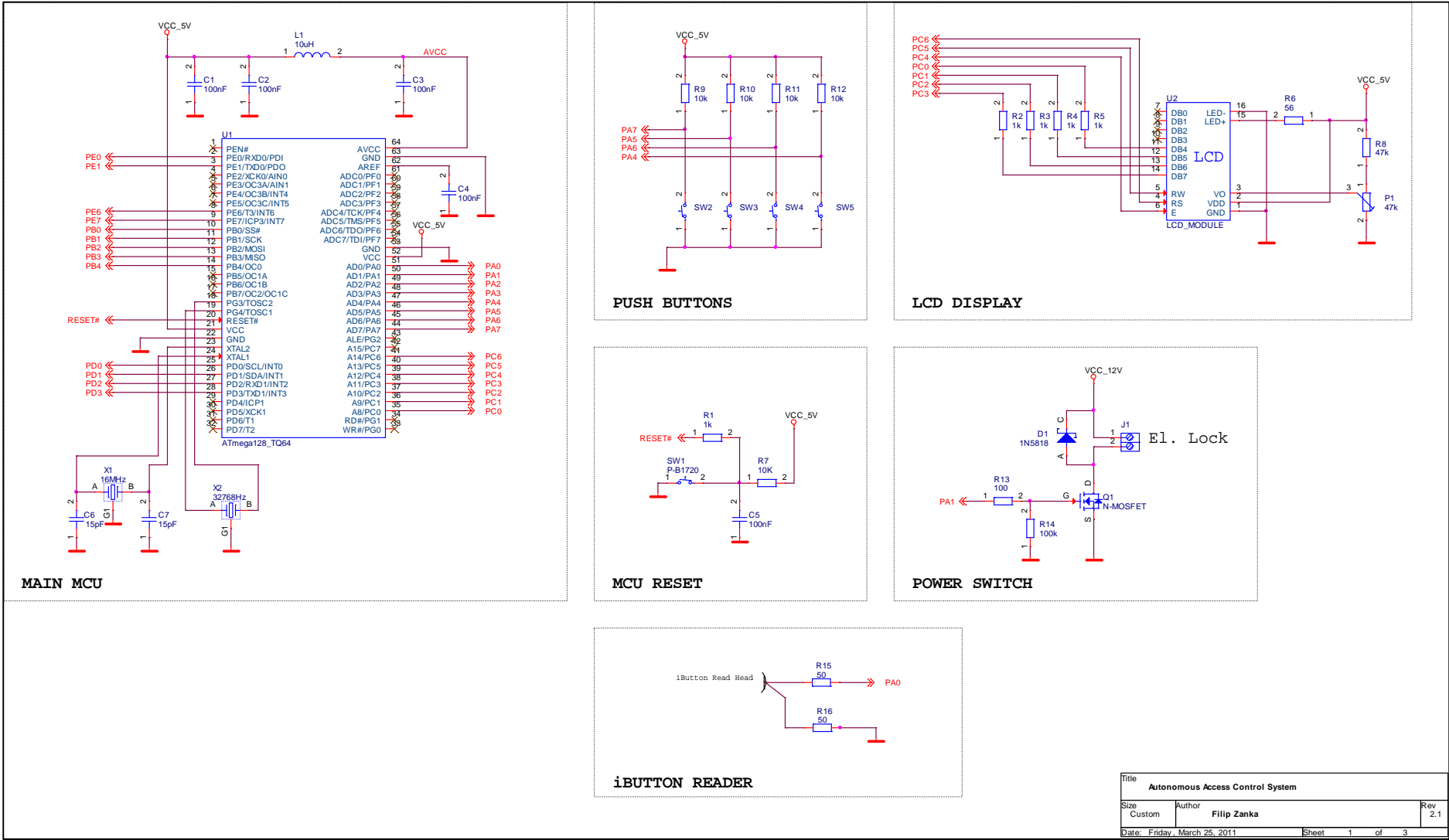
## **SEZNAM PŘÍLOH**

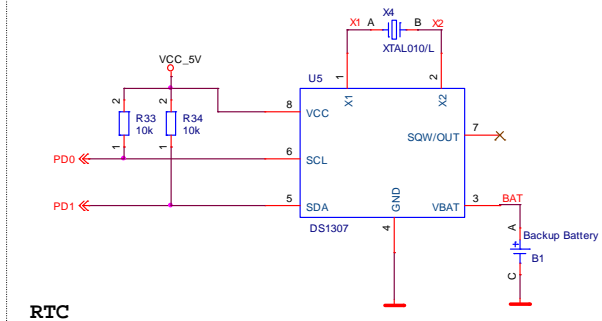
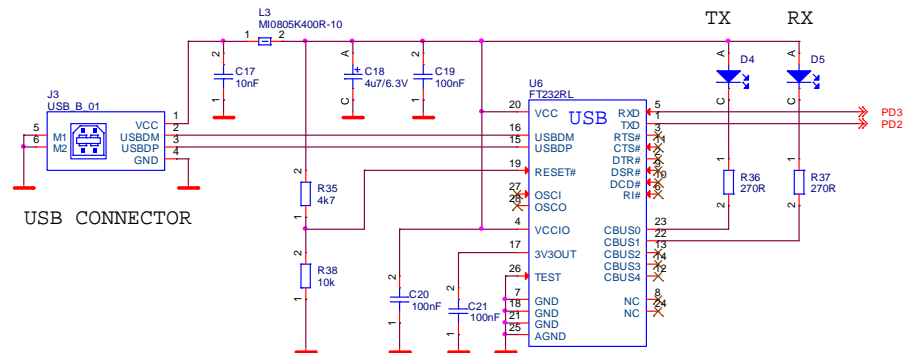
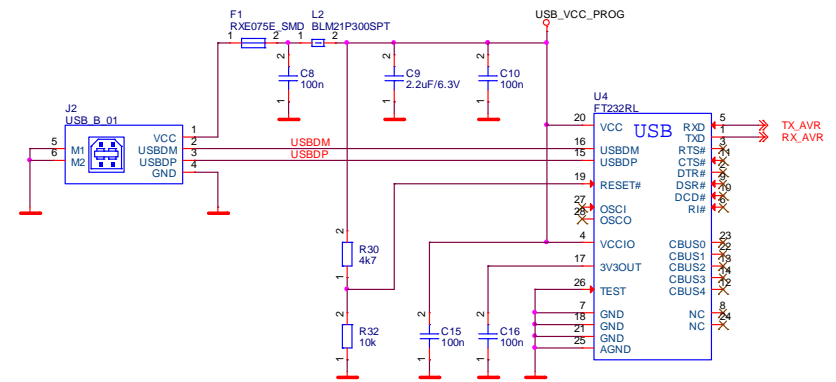
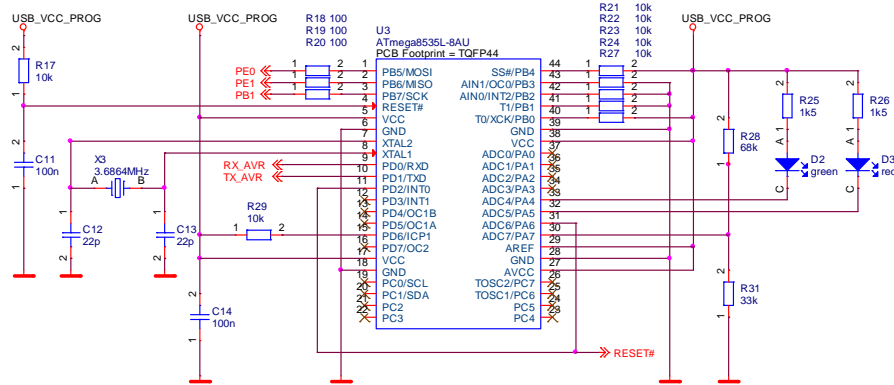
PŘÍLOHA P I: Schéma zapojení

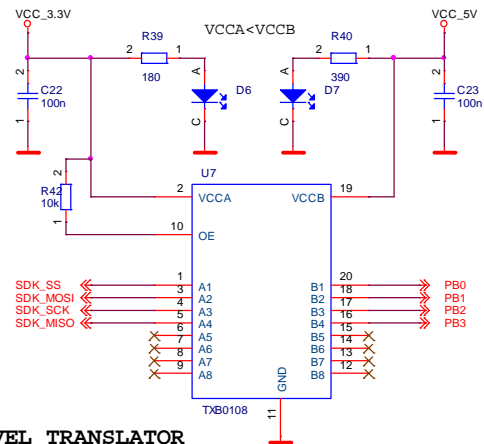
PŘÍLOHA P II: Zdrojový kód – vzhledem k rozsahu uložen na přiloženém CD

PŘÍLOHA P III: Katalogové listy klíčových součástí - uloženy na přiloženém CD

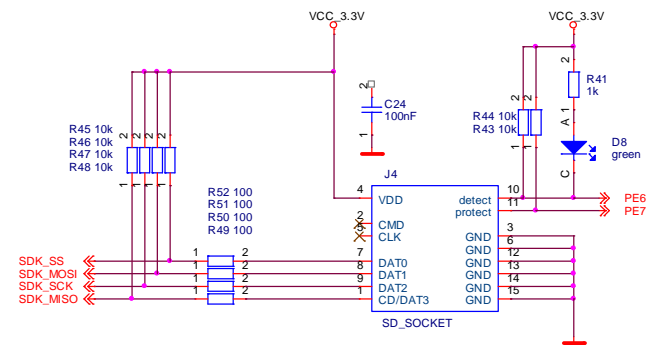
Příloha P I: Schéma zapojení



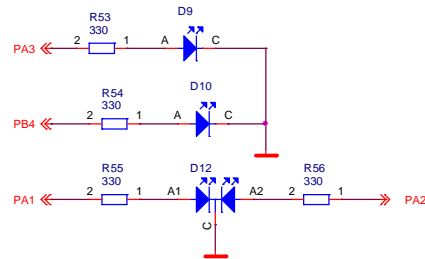




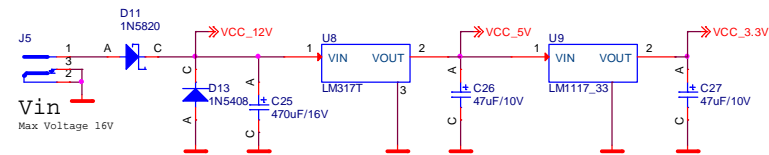
VOLTAGE LEVEL TRANSLATOR



MEMORY CARD



LED INDICATORS



POWER SUPPLY

Title			
Autonomous Access Control System			
Size	Custom	Author	Filip Zanka
Date:	Friday, March 25, 2011	Sheet	3 of 3
		Rev	2.1