

UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

Elektronická zabezpečovací a monitorovací jednotka

Petr Černohlávek

Bakalářská práce

2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Petr Černohlávek**
Osobní číslo: **I10279**
Studijní program: **B2646 Informační technologie**
Studijní obor: **Řízení procesů**
Název tématu: **Elektronická zabezpečovací a monitorovací jednotka**
Zadávací katedra: **Katedra řízení procesů**

Z á s a d y p r o v y p r a c o v á n í :

Cílem práce bude konstrukce zabezpečovací a monitorovací jednotky pro zpracování signálů z vybraných požárních a zabezpečovacích senzorů. Ke konstrukci jednotky bude použit mikrokontrolér fy Atmel řady AT mega. Zabezpečovací jednotka bude mít možnost připojení externí poplachové signalizační jednotky pro indikaci vzniku poplachového stavu. Dále bude provádět monitorování a zobrazování aktuálního stavu střeženého objektu.

Teoretická část:

- rešerše tématu,
- popis konstrukce vybraných typů senzorů,
- popis strategie elektronické ostrahy budov.

Implementační část:

- návrh konstrukčního řešení,
- realizace elektronické jednotky,
- testování elektronické jednotky.

Požadavky na studenta:

Základní orientace v návrhu a realizaci elektronických zařízení s mikrokontrolérem. Práce v návrhovém software EAGLE.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

Matoušek David, Práce s mikrokontroléry ATMEL AVR - 3.díl - edice uP a praxe 2.vydání, BEN - technická literatura, Praha 2006

Plíva Zdeněk, Eagle Prakticky, BEN-technická literatura, Praha 2010

Záhlava Vít, Návrh a konstrukce DPS, BEN-technická literatura, Praha 2010

Vedoucí bakalářské práce:

Ing. Libor Havlíček, Ph.D.

Katedra řízení procesů

Datum zadání bakalářské práce:

8. listopadu 2012

Termín odevzdání bakalářské práce:

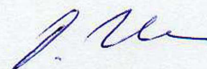
10. května 2013



prof. Ing. Simeon Karamazov, Dr.
děkan



L.S.



Ing. Daniel Honc, Ph.D.
vedoucí katedry

V Pardubicích dne 29. března 2013

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích 10. 5. 2013

Petr Černohlávek

Poděkování

Úvodem bych chtěl poděkovat vedoucímu práce Ing. Liborovi Havlíčkovi, Ph.D., za cenné rady, podporu a poskytnutí technických prostředků, nutných pro vývoj tohoto zařízení. Dále nesmím zapomenout na své rodiče, kteří mi zajistili nejen finanční, ale i psychickou podporu, po dobu mého studia a babičku, které vděčím za pomoc na začátku mých školních let.

Anotace

Tato práce se zabývá elektronickou ostrahou budov. Hlavním předmětem je konstrukce zabezpečovací jednotky, která umožňuje připojení, běžně vyráběných zabezpečovacích čidel a poplachových zařízení. Zmiňovanou zabezpečovací jednotku je možné ovládat prostřednictvím ovládací klávesnice, která dále slouží k monitorování stavů ve střeženém objektu. Konstrukce ovládací klávesnice je také předmětem této práce.

Klíčová slova

Ostraha budov, systém EZS, zabezpečení.

Title

Electronic security and monitoring unit

Annotation

This thesis is deal with in electronic security of buildings. The main subject is the construction of security unit, which allows you to connect, commonly produced security sensors and alarms. Mentioned security unit can be controlled through the control keyboard that also allows to monitor state in the secure object. Construction of a control keyboard is also the subject of this thesis.

Keywords

Security of buildings, system EZS, security.

Obsah

Seznam zkratk	10
Seznam obrázků	12
Seznam tabulek	14
Úvod	15
1 Zabezpečení objektů	16
1.1 Mechanické zábranné prostředky	16
2 Elektronická zabezpečovací signalizace EZS	17
2.1 Ovládací zařízení	17
2.2 Signalizační zařízení	18
2.3 Přenosové zařízení	19
3 Čidla používaná v EZS	20
3.1 Čidla obvodové ochrany	20
3.1.1 Mikrofonické kabely	20
3.1.2 Zemní tlakové hadice	21
3.2 Čidla plášťové ochrany	21
3.2.1 Magnetické kontakty	22
3.2.2 Detektor tříštění skla	23
3.3 Čidla prostorové ochrany	24
3.3.1 Pasivní infračervené čidlo PIR	24
3.3.2 Ultrazvuková čidla	25
3.4 Čidla předmětové ochrany	26
3.4.1 Závěsová čidla	27
3.5 Čidla tísňové ochrany a speciální čidla	27
3.5.1 Optická požární čidla	27
4 Poplachové ústředny EZS	28
4.1 Smyčkové ústředny	29

4.2	Ústředny s přímou adresací čidel	30
4.3	Ústředny smíšeného typu	31
4.4	Ústředny s bezdrátovým přenosem	31
5	Možnosti připojení čidel ke smyčkovým ústřednám.....	32
6	Strategie elektronické ostrahy budov	34
7	Popis použitých hardwarových prostředků	35
7.1	Použité mikroprocesory	35
7.2	Obvod reálného času PCF8583	36
7.3	Převodník FT232RL.....	36
7.4	Nabíjecí obvod MAX712.....	37
7.5	Alfanumerický LCD.....	37
7.6	Sběrnice I ² C	38
7.7	Sběrnice UART.....	39
8	Hardwarové řešení.....	40
8.1	Zabezpečovací a monitorovací jednotka	40
8.1.1	Vstupní obvody.....	41
8.1.2	Výstupní obvody.....	42
8.1.3	Zapojení mikroprocesoru	43
8.1.4	Návrh plošného spoje a osazený plošný spoj.....	45
8.2	Ovládací klávesnice	46
8.2.1	Návrh plošného spoje a osazený plošný spoj.....	48
8.3	Zálohovaný napájecí zdroj	48
8.3.1	Návrh plošného spoje a osazený plošný spoj.....	50
9	Softwarové řešení	51
9.1	Softwarové řešení zabezpečovací jednotky	51
9.2	Softwarové řešení ovládací klávesnice	54
9.3	Softwarové řešení GUI.....	56

10	Testování a možná rozšíření	58
	Závěr	60
	Literatura.....	61
	Příloha A: Schémata zapojení.....	A – 1
	Příloha B: Návrhy plošných spojů.....	B – 1
	Příloha C: Kompletní zařízení	C – 1

Seznam zkratek

EZS	Elektronická Zabezpečovací Signalizace
EPS	Elektronická Požární Signalizace
GSM	Global System for Mobile communications
PCO	Pult Centralizované Ochrany
RFID	Radio Frequency Identification
ISDN	Integrated Services Digital Network
LAN	Local Area Network
SMS	Short Message Service
CCTV	Closed Circuit Television
PIR	Passive Infra Red
RISC	Reduced Instruction Set Computer
EEPROM	Electrically Erasable Programmable Read Only Memory
ISP	In System Programing
BCD	Binary Coded Decimal
I ² C	Inter-Integrated Circuit
USB	Universal Serial Bus
UART	Universal Asynchronous Receiver Transmitter
GUI	Graphic User Interface
LCD	Liquid Crystal Display
RAM	Random Access Memory
RS	Register Selector
E	Enable
RXD	Receive Data
TXD	Transmit Dat
SDA	Serial Data
SCL	Serial Clock
TWI	Two-Wire Serial Interface
ACK	Acknowledge
LED	Light Emitting Diode
RJ	Registered Jack
DB	Data Bit
MISO	Master In Slave Out

SCK	Serial Clock
INT	Interrupt
TWBR	Two-Wire Serial Interface Bit Rate Register
TWPS	Two-Wire Serial Interface Bit Rate Prescaler
G	Gate
D	Drain
S	Source

Seznam obrázků

Obrázek 1: Obecné blokové schéma EZS.....	17
Obrázek 2: Ovládací klávesnice Jablotron JA-81F-RGB [2]	18
Obrázek 3: Venkovní siréna Jablotron JA-80A [3]	19
Obrázek 4: GSM komunikátor Jablotron JA-82Y [4]	20
Obrázek 5: Příklad provedení mikrofonického kabelu [1]	21
Obrázek 6: Magnetický kontakt Jablotron SA-201-A [5]	22
Obrázek 7: Blokové schéma detektoru tříštění skla.....	23
Obrázek 8: Detektor tříštění skla Jablotron JA-85B [6]	23
Obrázek 9: Nejčastější snímací charakteristiky PIR čidla [1]	25
Obrázek 10: PIR čidlo Jablotron JA-83P [7]	25
Obrázek 11: Snímací charakteristika ultrazvukového čidla [1].....	26
Obrázek 12: Požární čidlo Jablotron JA-63S-80 [8].....	28
Obrázek 13: Poplachová ústředna Jablotron OASIS JA-83K [9].....	29
Obrázek 14: Blokové schéma zapojení smyčkových ústředen.....	30
Obrázek 15: Blokové schéma zapojení ústředny s přímou adresací čidel.....	30
Obrázek 16: Blokové schéma zapojení ústředen smíšeného typu	31
Obrázek 17: Blokové schéma komunikace ústředny s bezdrátovým přenosem.....	32
Obrázek 18: Schéma zapojení čidla do nevyvážené smyčky	33
Obrázek 19: Schéma zapojení čidla do jednoduše vyvážené smyčky	33
Obrázek 20: Schéma zapojení čidla do dvojitě vyvážené smyčky	33
Obrázek 21: Schématické značky prvků tvořících systém EZS	34
Obrázek 22: Příklad návrhu zabezpečovacího systému konkrétního objektu	35
Obrázek 23: Diagram přenosu dvou bytů po I ² C sběrnici [10]	39
Obrázek 24: Diagram přenosu rámce po UART sběrnici [11]	40
Obrázek 25: Blokové schéma zabezpečovací a monitorovací jednotky.....	41
Obrázek 26: Schéma zapojení vstupních obvodů.....	42
Obrázek 27: Schéma zapojení výstupních obvodů.....	43
Obrázek 28: Schéma zapojení mikroprocesoru	44
Obrázek 29: Použitý komunikační modul s obvodem FT232RL	44
Obrázek 30: Návrh plošného spoje.....	45
Obrázek 31: Osazený plošný spoj.....	45
Obrázek 32: Blokové schéma ovládací klávesnice.....	46

Obrázek 33: Schéma zapojení ovládací klávesnice	47
Obrázek 34: Schéma zapojení maticové klávesnice 4×3 klávesy.....	47
Obrázek 35: Návrh plošného spoje	48
Obrázek 36: Osazený plošný spoj.....	48
Obrázek 37: Blokové schéma zálohovaného napájecího zdroje.....	49
Obrázek 38: Schéma zapojení zálohovaného napájecího zdroje	50
Obrázek 39: Návrh plošného spoje	50
Obrázek 40: Osazený plošný spoj.....	51
Obrázek 41: Stavový diagram popisující chování zabezpečovací jednotky	52
Obrázek 42: Vývojový diagram hlavní části algoritmu zabezpečovací jednotky	53
Obrázek 43: Vývojový diagram hlavní části algoritmu ovládací klávesnice	55
Obrázek 44: GUI sloužící k nastavení parametrů zabezpečovací jednotky.....	57
Obrázek 45: Okno s výpisem událostí	58
Obrázek 46: Schéma zapojení zabezpečovací jednotky	A – 1
Obrázek 47: Schéma zapojení ovládací klávesnice	A – 2
Obrázek 48: Návrh plošného spoje zabezpečovací a monitorovací jednotky	B – 1
Obrázek 49: Návrh plošného spoje ovládací klávesnice	B – 1
Obrázek 50: Návrh plošného spoje zálohovaného napájecího zdroje	B – 1
Obrázek 51: Osazovací schéma zabezpečovací jednotky.....	B – 2
Obrázek 52: Osazovací schéma ovládací klávesnice.....	B – 2
Obrázek 53: Osazovací schéma zálohovaného napájecího zdroje.....	B – 2
Obrázek 54: Zabezpečovací jednotka	C – 1
Obrázek 55: Ovládací klávesnice	C – 1
Obrázek 56: Obě zařízení	C – 2

Seznam tabulek

Tabulka 1: Hodnoty odporů zabezpečovacích smyček, dle stavu čidla.....	34
Tabulka 2: Tabulka konfiguračních možností zabezpečovací jednotky.....	56

Úvod

Cílem této práce je navrhnout a zkonstruovat zabezpečovací a monitorovací jednotku, která předává stavy ze střeženého objektu, pomocí ovládací klávesnice, jejíž další funkcí je, celý zabezpečovací systém ovládat. V České republice se touto problematikou zabývá společnost Jablotron, s. r. o., která se může pyšnit úspěchy nejen na tuzemském trhu, ale i v zahraničí. Vstupní obvody zabezpečovací jednotky jsou vhodně navrženy pro možnost připojení běžných zabezpečovacích a požárních detektorů, aby bylo možné, prostřednictvím získaných informací, vyhodnotit stav ve střeženém objektu. Výstupní obvody jsou vhodně uzpůsobeny pro připojení signalizačního zařízení, zejména sirény, pro vnitřní i venkovní použití. Komunikace mezi zabezpečovací jednotkou a ovládací klávesnicí je fyzicky řešena pomocí čtyř-vodičového telefonního kabelu, osazeného konektorem RJ-11. Programové řešení komunikace, spočívá v použití sběrnice I²C, která je jednou z periferií, použitých mikroprocesorů ATmega8.

Ovládací klávesnice tvoří samostatné elektronické zařízení, které zobrazuje stavy ze střeženého objektu, pomocí LCD a umožňuje ovládání celého bezpečnostního systému. Systém je možné uvádět do stavu střežení a zpět do stavu klidu, pomocí zadání nastaveného uživatelského kódu, přičemž ve stavu klidu, je aktivní střežení požární smyčkou a sabotážním kontaktem víka zabezpečovací jednotky. Uživatel má možnost, zadáním servisního kódu, tato střežení deaktivovat, a tím je umožněno sejmutí víka zabezpečovací jednotky, bez vyvolání poplachu a provést údržbu, či konfiguraci.

Pohodlnou konfiguraci umožňuje GUI, které komunikuje se zabezpečovací jednotkou, prostřednictvím USB portu. Hlavními konfigurovatelnými parametry jsou samozřejmě kódy, pro ovládání celého systému, ale také čas, datum a příslušná zpoždění. Odchodové zpoždění slouží k opuštění střeženého prostoru, je to tedy doba, která uplyne od zadání kódu, do doby, kdy je střežení aktivováno. Naopak příchodové zpoždění slouží k možnosti zadání kódu, při návratu uživatele objektu, je to tedy doba od aktivace některého z detektorů, po dobu spuštění poplachu. Další funkcí GUI je načtení událostí, které jsou průběžně ukládány do paměti mikroprocesoru.

Napájení celého bezpečnostního systému, je řešeno adaptérem, který je zálohován, prostřednictvím záložního akumulátoru. Plošné spoje, obou elektronických zařízení, jsou navrženy pro vhodnou montáž do odpovídající krabičky.

1 Zabezpečení objektů

Zabezpečení je dnes nedílnou součástí většiny objektů, jak novostaveb, u kterých se s montáží zabezpečovacího systému počítá již při stavbě budovy, tak i u starších objektů, kdy se majitel rozhodne zlepšit ochranu, většinou z důvodu zvýšení kriminality v jeho lokalitě, nebo může být zabezpečení objektu výhodně rozšířeno, při jeho rekonstrukci. Do celkového zabezpečení objektu, počítáme ochranu mechanickou, označovanou jako mechanické zábranné prostředky, tak i ochranu elektronickou, která se označuje jako elektronická zabezpečovací signalizace EZS. Tyto dva prvky zabezpečení tedy slouží k zabránění vstupu do objektu, či vstupu na pozemek, nebo k signalizaci, že došlo k překonání mechanického zabezpečení střeženého prostoru, k čemuž slouží elektronické zabezpečení objektu. Zvláštním případem jsou prvky, které slouží k signalizaci vzniku požárů ve střeženém objektu, tyto prvky jsou označovány, jako prvky systému EPS, což je elektronická požární signalizace. Některé systémy jsou tzv. hybridní, to znamená, že systém zabezpečení EZS, umožňuje i připojení prvků EPS. Zabezpečení se dnes netýká pouze prostorů pro komerční použití, jako jsou bankovní instituce, muzea, galerie, obchody apod., ale i soukromých objektů, mezi které patří hlavně rodinné domy, byty i např. garáže, ve kterých se často používají i prvky EPS.

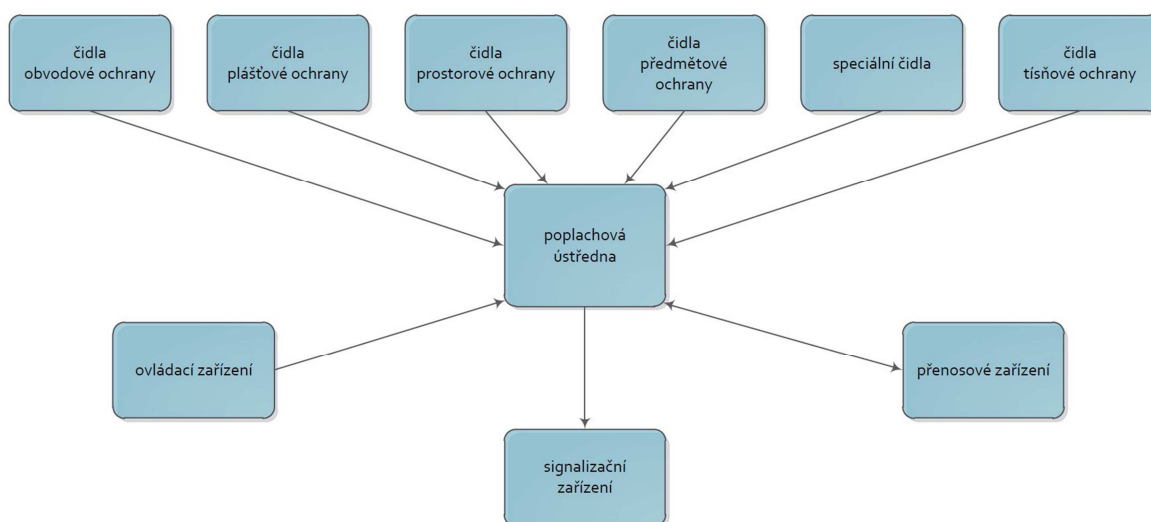
1.1 Mechanické zábranné prostředky

„Mechanickými zábrannými prostředky se rozumí zejména prostředky pro ohraničení prostor, vstupní bezpečnostní systémy dveří a oken, mříže, bezpečností skla a fólie a vlastní uzamykací systémy. Vzhledem ke skutečnosti, že mechanické zábranné systémy patří do širší problematiky bezpečnostního zabezpečení, můžeme je rozdělit zhruba do tří oblastí“ [1].

- **Prostředky obvodové ochrany** – zde máme na mysli zejména prostředky určené k zamezení vstupu na chráněný pozemek, které jsou instalovány na katastrální hranici pozemku, zejména se jedná o ploty, zdi, vrata, závory apod.
- **Prostředky objektové ochrany** – zde se jedná o prvky, které mají pachateli zamezit vstup do chráněného objektu, takže se jedná zejména o prostupy, což znamená otvory v obvodových zdech objektu, mezi prvky této ochrany patří bezpečností okna, dveře, zámky, mříže na oknech, fólie a také zabezpečení ventilačních otvorů.
- **Prostředky individuální ochrany** – tím se rozumí prvky určené zejména pro ochranu předmětů, jako jsou bezpečnostní skřínky, trezory apod.

2 Elektronická zabezpečovací signalizace EZS

Parametry prvků EZS jsou formulovány evropskou normou EN ČSN 50 131-1. Hlavním jádrem systému je poplachová ústředna, která přijímá signály od jednotlivých čidel a vyhodnocuje, zda nenastal stav poplachu, na který ústředna nějakým způsobem reaguje. Většinou spuštěním optické a akustické signalizace pomocí sirény, a pokud je ústředna vybavena i telefonním nebo GSM komunikátorem, dochází ke komunikaci, nejčastěji s mobilním telefonem majitele objektu, či s pultem centralizované ochrany PCO, což je zpoplatněná služba soukromých subjektů, zahrnující i odborný zásah proti případnému pachateli, či kontrolu zajištění objektu, při vzniku planého poplachu. Rozdělení a propojení jednotlivých členů systému EZS, znázorňuje blokové schéma na následujícím obrázku.



Obrázek 1: Obecné blokové schéma EZS

2.1 Ovládací zařízení

Ovládacím zařízením se rozumí rozhraní mezi poplachovou ústřednou a uživatelem objektu, jehož hlavním úkolem je umožnit uživateli celý systém EZS ovládat, to znamená hlavně zajištění a odjištění systému, ale v některých případech i nastavování parametrů. Nejpoužívanějším ovládacím zařízením je kódová klávesnice, která umožňuje zadáním nastaveného kódu, přecházet mezi stavem „střežení“ a stavem „klidu“ poplachové ústředny, a také vizualizaci současného stavu, většinou prostřednictvím displaye. Další častou možností ovládacích zařízení jsou bezdrátová, která komunikují prostřednictvím rádiového signálu a systém je tak možné ovládat na dálku. Moderní možností ovládnutí systému EZS, je také použití RFID čteček, které umožňují měnit stavy poplachové

ústředny, pouhým přiložením magnetické karty nebo čipu. Tento způsob ovládání, je vhodný zejména v rozsáhlých objektech, kde může systém ovládat velké množství osob, výhodná je možnost zpětného dohledání identity uživatele, který do daného objektu, či jeho části vstoupil.



Obrázek 2: Ovládací klávesnice Jablotron JA-81F-RGB [2]

2.2 Signalizační zařízení

Signalizačním zařízením označujeme prvky, které se aktivují v okamžiku narušení střeženého objektu, to znamená při přechodu poplachové ústředny do stavu poplachu. Nejčastějším signalizačním zařízením je siréna, která umožňuje akustickou a optickou signalizaci vzniku poplachového stavu. Sirény můžeme rozdělit do dvou skupin, na venkovní a vnitřní, venkovní siréna je většinou složitějším subsystémem s vlastním záložním zdrojem a řídicí logikou, což umožňuje, že siréna nelze po její aktivaci vyřadit pouhým „přeštípnutím“ přívodního kabelu. Dalším prvkem, těchto sirén jsou také sabotážní kontakty, které aktivují sirénu při sejmutí vrchního krytu, nebo stržení ze zdi. Nedílnou součástí venkovní sirény, je také maják pro optickou signalizaci, která slouží k lepší identifikaci objektu, při zásahu policie nebo zaměstnanců PCO. Vnitřní sirény jsou výrazně jednodušší, jedná se zejména o akustický měnič a budicí generátor, který se spouští přivedením stejnosměrného napětí z ústředny EZS při poplachu. Hlavní funkcí vnitřních sirén je zastrašení pachatele.



Obrázek 3: Venkovní siréna Jablotron JA-80A [3]

2.3 Přenosové zařízení

Hlavním úkolem přenosového zařízení, je dopravit informaci o narušení střeženého objektu na místo vzdálené obsluhy, většinou PCO, nebo tuto informaci předat majiteli objektu. Ústředna EZS musí obsahovat tzv. komunikační modul, který plní funkci přenosového zařízení. V dnešní době jsou nejpoužívanější, tři druhy komunikátorů, a to automatické telefonní hlásiče, komunikátory ISDN, nebo komunikátory GSM. Automatický telefonní hlásič umožňuje uložit do paměti cca. 30 s dlouhou, hlasovou zprávu, která je při poplachu předána na zvolené telefonní číslo, klasickou telefonní linkou. Dnes se začínají objevovat i komunikátory, které kombinují komunikaci po klasické telefonní lince s komunikací po síti LAN, umožňující ovládání systému pomocí sítě internet. Komunikátor ISDN, používá digitální datové přenosy poplachových, ale i např. poruchových zpráv ze střeženého objektu, k přenosu je použito metalické vedení, shodné s klasickou telefonní linkou. Tento způsob je vhodný, jak ke komunikaci s PCO, tak ke komunikaci s majitelem objektu. Třetí, dnes nejpoužívanější možností komunikace s poplachovou ústřednou je GSM komunikátor, jeho hlavní výhodou je, že pracuje bezdrátově a může snadno komunikovat, jak s PCO, tak s mobilním telefonem majitele, či uživatele objektu. Nevýhodou je však možnost výpadku sítě GSM, a tím znemožnění předání poplachové zprávy, ale u předchozích způsobů komunikace je snazší porušení telefonní linky narušitelem objektu, a tím vyřazení komunikátorů z provozu. Pro objekty s vyšším rizikem napadení je výhodné používat redundanci komunikačních cest, to znamená, při výpadku např. GSM sítě, je pro komunikaci použita např. linka ISDN. Komunikátory GSM, jsou většinou nejnákladnější, ale umožňují uživateli objektu komfortní dálkové ovládání systému EZS, např. pomocí SMS zprávy, je možné na dálku spínat vytápění objektu, nebo může systém majiteli předávat na mobilní telefon

informace o poruchách, např. výpadek síťového napájení a přechod na záložní akumulátor.



Obrázek 4: GSM komunikátor Jablotron JA-82Y [4]

3 Čidla používaná v EZS

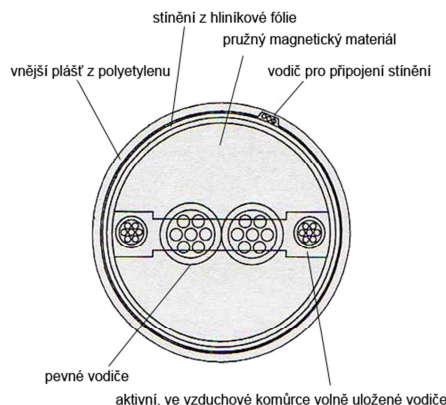
Z blokového schématu EZS vyplývá, že můžeme střežený prostor rozdělit do čtyř hlavních kategorií, a to na ochranu obvodovou (perimetrickou), plášťovou, prostorovou a předmětovou, pro které máme specializovaná čidla. Zvláštní kategorií jsou speciální čidla a čidla tísňové ochrany.

3.1 Čidla obvodové ochrany

Tato skupina čidel, detekuje vnik pachatele na střežený pozemek, to znamená, překonání mechanických zábranných prostředků obvodové ochrany, katastrální hranice pozemku. Z toho vyplývá, že střežený prostor bude mnohem rozsáhlejší, než při střežení budov a požadavky na jednotlivá čidla, budou specifické pro venkovní použití, čidla musí být odolná proti dešti, povětrnostním podmínkám, sněhu, mrazu a vibracím od různých zdrojů. Protože se ve většině případů jedná o velmi rozsáhlý prostor, je vhodné u objektů s vyšším stupněm rizika, kombinovat obvodovou ochranu se systémem průmyslových televizí CCTV.

3.1.1 Mikrofonické kabely

„Mechanické namáhání nebo záchvěvy citlivého mikrofonického kabelu se převádějí na elektrický signál, který je dále zpracováván ve vyhodnocovací jednotce. Akustický odposlech slouží k rozpoznání charakteru narušení, úroveň odezvy odpovídající vyhlášení poplachu je nastavitelná. Elektrické připojení je specifické a vychází z instalačních manuálů konkrétního výrobku. Zásady ochrany proti sabotáži i velikost napájecího napětí bývají standardní“ [1].



Obrázek 5: Příklad provedení mikrofonického kabelu [1]

Mikrofonické kabely slouží k detekci narušení drátěného oplocení, dokáží detekovat, jak přelezení, tak i stříhání. Doporučovaná montáž je s novým oplocením, protože je nutná, jeho dostatečná tuhost, kvůli minimalizaci působení vnějších vlivů, jako pohyb oplocení při větru, který musí být filtrován vyhodnocovací elektronikou mikrofonických kabelů. Montáž se provádí vplétáním do drátěného oplocení.

3.1.2 Zemní tlakové hadice

Na rozdíl od mikrofonických kabelů, kterými je možné detekovat pouze překonání drátěného oplocení, zemní tlakové hadice jsou čidlem univerzálnějším, dají se použít, jak ke střežení oplocení, tak i k detekci překonání obvodových zdí pozemku a také různých prostupů, jako jsou vrata, brány, závory apod. Princip detekce narušení, je založen na tlakovém diferenciálním čidle, do kterého jsou přivedeny tlakové hadice a vyhodnocují se změny tlaku v nemrznoucí kapalině, která tvoří náplň tlakových hadic. Tlakové diferenciální čidlo převádí vzniklé změny tlaku kapaliny na elektrický signál, který je dále vyhodnocovací elektronikou filtrován, z důvodu minimalizace falešných poplachů, vzniklých např. pohybem drobné zvěře po střeženém pozemku. Zemní tlakové hadice se instalují v páru s roztečí asi 1m, po obvodu pozemku pod povrch, čidlo je po zatravnění neviditelné a je možná i instalace pod povrch vozovky, ale nese to s sebou případné vyšší náklady při poškození hadice, nebo údržbě.

3.2 Čidla plášťové ochrany

Čidla plášťové ochrany, detekují překonání pláště budovy pachatelem, používají se zejména ke střežení prostupů, to znamená hlavně dveří, oken a ventilačních otvorů. Pro

objekty s vyšším stupněm rizika existují i čidla, která dokáží detekovat probourání obvodové zdi, většinou se jedná o čidla destrukční, jako jsou např. poplachové tapety, jejichž destrukce je způsobena narušením pláště budovy, nebo čidla vibrační detekující specifické vibrace, vzniklé při probourání obvodové zdi.

3.2.1 Magnetické kontakty

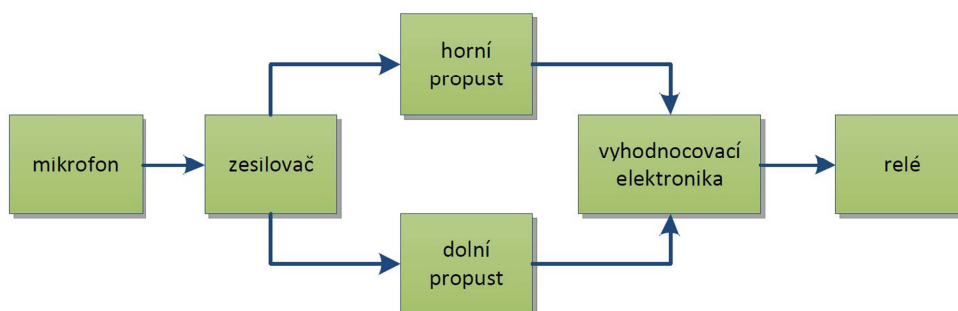
Jedná se o nejjednodušší čidlo, ze všech možných skupin a jeho velkou výhodou je, že nepotřebuje vlastní napájecí napětí, jako většina ostatních čidel. Magnetický kontakt slouží k detekci otevření oken, dveří, či rolet a skládá se ze dvou částí, jazýčkového kontaktu a permanentního magnetu. Jazýčkový kontakt je skleněná trubička, naplněná ochrannou atmosférou, ve které jsou umístěny dva feromagnetické kontakty, které jsou vyvedeny z trubičky. Permanentní magnet je tvořen nejčasněji zmagnetovaným válečkem z feritu. Obě části jsou zapouzdřeny do vhodně tvarovaného pouzdra, specifického způsobu montáže a oblasti použití. V klidovém stavu je jazýčkový kontakt sepnut magnetickým polem permanentního magnetu, při jeho oddálení, dojde k rozepnutí jazýčkového kontaktu, a tím k rozpojení proudové smyčky, tvořené vyhodnocovacím obvodem poplachové ústředny. Existují různá provedení pouzder magnetických kontaktů, jak pro zapuštění do okenního, či dveřního tělesa, tak i pro povrchovou montáž, nebo speciální odolná pouzdra pro venkovní použití, např. detekce otevření vrat, takže z toho vyplývá, že magnetické kontakty se dají použít i jako čidla obvodové ochrany. Montáž se provádí připevněním permanentního na pohyblivou část okna, či dveří, jazýčkový kontakt se upevňuje na okenní rám, či zárubeň dveřního otvoru, přívodní kabel je vhodné vést v instalačních trubkách, aby byl chráněn proti poškození, přímo do rozbočovací krabice, která je napojena na poplachovou ústřednu.



Obrázek 6: Magnetický kontakt Jablotron SA-201-A [5]

3.2.2 Detektor tříštění skla

Oproti předchozímu čidlu, které dokáže detekovat pouze otevření oken, či dveří, slouží detektor tříštění skla, k detekci destrukce skleněné výplně. Hlavním vstupním zařízením je citlivý mikrofon, který sejme zvuk vzniklý tříštěním skla a převede ho na odpovídající elektrický signál, který je následně zesílen zesilovačem a filtrován přes pásmovou propust, která propustí pouze tu část frekvenčního spektra, typickou pro tříštění skla. Vyfiltrovaný signál je zpracován vyhodnocovací elektronikou, která v případě poplachu rozepne relé, což způsobí odpovídající reakci, připojené poplachové ústředny EZS. Kvalitnější čidla obsahují více pásmových propustí, protože pro tříštění skla jsou typické vyšší frekvence signálu, a po této vysoké frekvenci, vznikají nižší frekvence, generované bortěním skleněné tabule. Vyhodnocovací elektronika, potom reaguje na správný sled nízké a vysoké frekvence signálu, což snižuje riziko falešných poplachů. Montáž těchto čidel se provádí naproti skleněné výplni, jejíž rozbití chceme detekovat, pro testování dodává většinou výrobce konkrétního čidla, zařízení generující zvuk tříštění skla.



Obrázek 7: Blokové schéma detektoru tříštění skla



Obrázek 8: Detektor tříštění skla Jablotron JA-85B [6]

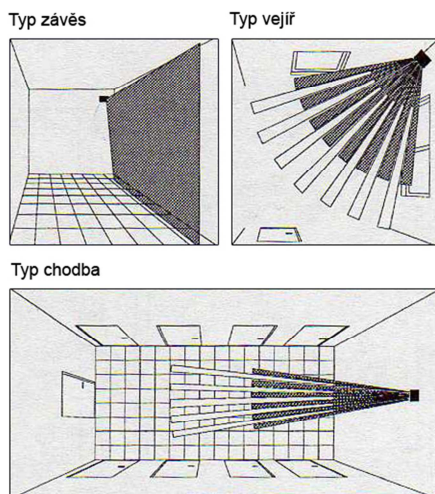
3.3 Čidla prostorové ochrany

Tato skupina čidel, detekuje narušení střeženého prostoru uvnitř objektu, většinou detekcí pohybu, z toho vyplývá, že se většinou pro ochranu prostoru, využívají čidla pohybová. Pro detekci pohybu se nejčastěji používají fyzikální principy, založené na infračerveném, ultrazvukovém nebo mikrovlnném záření. Čidla musí být odolná proti vlivům vytápění, slunečnímu svitu, či jiným nežádoucím zdrojům světla, či tepla.

3.3.1 Pasivní infračervené čidlo PIR

Toto čidlo je označování těžištěm prostorové ochrany, neboť se používá ve většině objektů, jako nejčastěji zvolené, od jeho použití se upouští až při extrémních podmínkách, při kterých by použití PIR čidel přinášelo vysokou četnost planých poplachů. Princip je založený na faktu, že každé těleso, jehož teplota je vyšší než absolutní nula, vyzařuje infračervené záření. Mezi hlavní části PIR čidla patří optika, detektor a vyhodnocovací elektronika. Optika může být dvojího druhu, Fresnelovy čočky, nebo soustava křivých zrcadel. U kvalitnějších PIR čidel je použita soustava křivých zrcadel, protože optický obraz skutečnosti, promítaný na detektor, je takřka ideálním obrazem skutečnosti, ale jejich výroba je komplikovanější, oproti výrobě Fresnelových čoček, které mají ovšem tu nevýhodu, že obraz promítaný na detektor, není ideálně skutečný. Jako detektor je použit materiál, vykazující tzv. pyroelektrický jev, založený na změně prostorového náboje monokrystalu, při změně teploty, jedná se o měnič gradientní povahy, to znamená, že není schopen detekovat stálou úroveň záření, ale pouze změny záření na detektor dopadající. Zorné pole PIR čidla je rozděleno na aktivní a pasivní zóny, čidlo tedy nevyhodnocuje infračervené záření v prostoru se pohybujícího tělesa na detektor dopadající, ale pouze difference záření tělesa a jeho pozadí s rozdílnou teplotou, přičemž těleso se pohybuje z aktivních zón zorného pole do pasivních a zpět. Zorné pole optiky, může mít různé tvary, a tím je možné přizpůsobit snímací charakteristiku střežené místnosti, nejčastější typy zorného pole čidla PIR, jsou závěs, vějíř a chodba, existují stropní čidla, která dokáží snímat pod úhlem 360° , a tím pojmout velký prostor. Pohyb je možné detekovat až do vzdálenosti 15 m s charakteristikou vějíř, s charakteristikou chodba, u kvalitních čidel až na vzdálenost 60 m. Montáž je doporučována tak, aby byl předpokládáný pohyb pachatele tangenciální, na myšlený průmět aktivních a neaktivních zón zorného pole. Pro montáž je vhodný pevný povrch bez vibrací a montážní místo, by mělo být vybráno vhodně tak, aby čidlo nemohl osvětit nežádoucí zdroj světla, většinou

se jedná o sluneční svit, či reflektor automobilu. V místnosti s okny, je vhodná montáž v horních rozích, nad úrovní oken, naproti vstupním dveřím do střeženého prostoru.



Obrázek 9: Nejčastější snímací charakteristiky PIR čidla [1]



Obrázek 10: PIR čidlo Jablotron JA-83P [7]

3.3.2 Ultrazvuková čidla

Fyzikální princip ultrazvukových čidel, je založen na vysílání mechanického vlnění, nad pásmem slyšitelnosti lidského ucha, jedná se tedy o kmitočty nad 20 kHz a zpětné přijímání tohoto odraženého vlnění, od překážek ve střežené místnosti. Čidlo tedy obsahuje vysílací, přijímací část a vyhodnocovací elektroniku. Pokud se vyslané vlnění odrazí od pohybujícího se tělesa, změní se tak kmitočet vlnění přijatého, vzhledem k vlnění vyslanému. Při detekci pohybu v místnosti, není třeba rozlišovat velikost změny, ale stačí pouze detekovat přítomnost změny kmitočtu, která je větší, než případné změny vyvolané odchylkami systému. Jedná se tedy na rozdíl od PIR čidel o čidla aktivní, protože vysílají do prostoru energii, což způsobuje problémy při nasazení více ultrazvukových čidel v místnosti, potom je nutná dostatečná kmitočtová stálost, aby

nedocházelo k jejich vzájemnému ovlivňování. Tento druh čidel, má většinou nastavitelný dosah, který musí být otestován, pokud se výrazně změní akustické vlastnosti místnosti, většinou vlivem změn interiéru. Montáž se provádí na pevný podklad tak, aby byl přepokládáný pohyb pachatele radiální, nevhodné jsou místnosti se zavěšenými předměty a přístroji vyzařujícími vlnění v širokém kmitočtovém spektru. Princip je založený na tzv. Dopplerovu jevu, popisujícím změny kmitočtu, při odrazu mechanického vlnění, od pohybujícího se tělesa, který je vyjádřen následujícím vztahem.

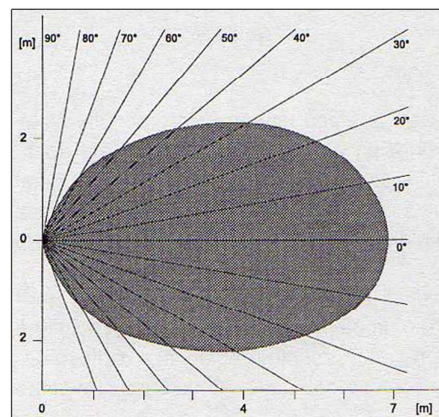
$$f_p = \frac{f_v}{1 - \frac{v}{c}} \quad (1)$$

kde f_p – kmitočet přijatý přijímačem

v – rychlost pohybu pachatele

f_v – kmitočet vyslaný vysílačem

c – rychlost šíření zvuku



Obrázek 11: Snímací charakteristika ultrazvukového čidla [1]

3.4 Čidla předmětové ochrany

Čidla předmětové ochrany slouží k detekci manipulace se střeženými předměty, zde je možné využít spoustu čidel, která jsou původně určena pro jiné stupně ochrany. Příkladem může být magnetický kontakt, kterým je možné střežit daný předmět připevněním permanentního magnetu a jazýčkového kontaktu na plochu, které se předmět dotýká. Většinou se předmětová ochrana aplikuje na umělecké předměty, vystavené v různých muzeích, či galeriích, které je potřeba hlídat i v době provozu pro veřejnost.

Další možností aplikace předmětové ochrany, je střežení trezorových skříní, kde se používají výhradně seismická čidla, která dokáží rozpoznat i charakter narušení, dle specifických signálů, vzniklých při možných technikách vniknutí do trezorových skříní, digitální spektrální analýzou sejmутého signálu.

3.4.1 Závěsová čidla

Tento druh čidel, je využíván převážně ke střežení obrazů, zavěšených v uměleckých galeriích. Střežený předmět je zavěšen na háku a dochází k vyhodnocování síly, působící na tento hák, který je spojen s elektromechanickým měničem. Jako měnič je použit piezokeramický krystal, jímž vygenerovaný elektrický signál, je následně zesílen a zpracován vyhodnocovací elektronikou. Citlivost čidla je nastavitelná, proto je možné detekovat, jak sejmутí předmětu z háku, tak i pouhý dotek. Velkou výhodou je, že předmět je možné střežit neustále, to znamená i v době provozu pro veřejnost.

3.5 Čidla tísňové ochrany a speciální čidla

Tísňová ochrana zajišťuje možnost nepozorovaného spuštění, většinou „tichého“ poplachu uživatelem daného objektu při ohrožení, a tím přivolání pomoci. Využívá se většinou v bankovních institucích, kde je vysoké riziko napadení, které může ohrozit nejen zaměstnance, ale i zákazníky. Čidla jsou většinou představována magnetickými kontakty, či mikrospínači, které jsou obsahem vhodného pouzdra. Montáž musí být provedena tak, aby nebylo čidlo viditelné ze strany zákazníka, ale také se musí dbát na vhodnou montáž, z hlediska nechtěné aktivace. Jedná se většinou o nožní lišty, skrytá tlačítka, ale někdy i falešné peněžní svorky, jejichž zvednutím je rozepnut spínač a vyhlášen poplach. Speciálními čidly se v rámci EZS rozumí hlavně čidla požární, která pracují většinou na optickém principu, dále sem můžeme zahrnout čidla, pro detekci úniku hořlavých plynů nebo čidla zaplavení.

3.5.1 Optická požární čidla

Princip funkce je založený na zeslabení intenzity infračerveného paprsku, dopadajícího na fotodiodu. Čidlo se skládá z komory, obsahující infračervenou diodu, která vysílá pulzující infračervený paprsek na fotodiodu, do této komory nesmí vniknout světlo z žádného cizího zdroje. Při hoření vzniká většinou kouř, který vnikne do této komory a dojde k zeslabení intenzity infračerveného paprsku, dopadajícího na fotodiodu,

pokud toto zeslabení trvá po dobu dvou, po sobě jdoucím pulzů, dochází k digitální analýze výstupního signálu z fotodiody, prostřednictvím vyhodnocovací elektroniky čidla z důvodu předcházení falešným poplachům. Druhý způsob realizace je takový, že infračervený paprsek, emitovaný infračervenou diodou nedopadá v klidovém stavu na fotodiodu, ale dopadá na ní pouze vlivem odrazu paprsku od částic kouře, vzniklého při požáru. Protože je tento typ čidla založen na detekci kouře vzniklého při hoření, není možné detekovat např. hoření kapalin, při kterém vzniká většinou pouze malé množství kouře, jehož částice jsou velmi malé. Z tohoto důvodu se často doplňuje optické čidlo o teplotní snímač, který předpokládá, že při hoření dojde vždy ke zvýšení teploty a tento teplotní snímač, může reagovat buď na zvýšení teploty nad určitou mez, nebo může diferenciatně vyhodnocovat, prudký nárůst teploty v místě instalace. Požární čidlo většinou obsahuje i vlastní sirénu, pro zajištění lokální signalizace požáru, a při propojení se systémem EZS, je samozřejmé i vyhlášení požárního poplachu v celém objektu. Montáž se provádí na místech, kde hrozí vznik požáru, jako jsou kuchyně, garáže apod., dále na místech, kde je při požáru objektu předpokládáno největší množství nashromážděného kouře, jako jsou např. schodiště.

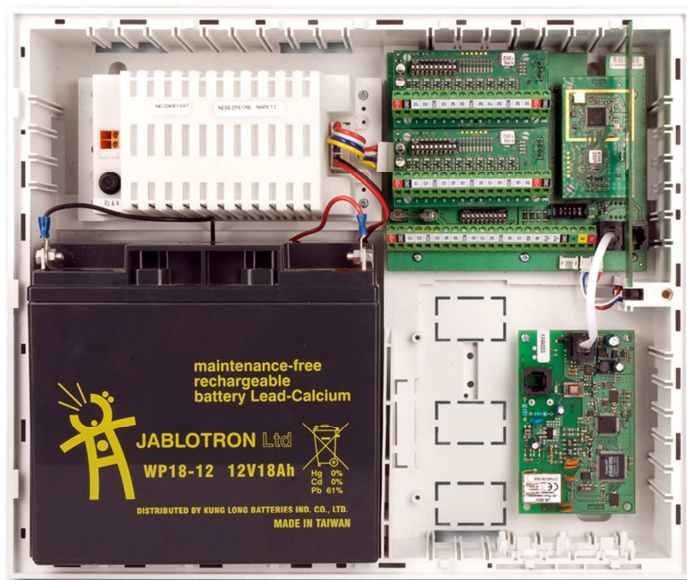


Obrázek 12: Požární čidlo Jablotron JA-63S-80 [8]

4 Poplachové ústředny EZS

Poplachová ústředna je elektronické zařízení, které přijímá a vyhodnocuje signály od jednotlivých čidel. V případě aktivace, některého z čidel, dochází k odpovídající reakci, to znamená ovládání signalizačního a přenosového zařízení, pro předání poplachové zprávy, buď okolí, nebo na místo vzdálené obsluhy, či PCO. Další důležitou funkcí, je možnost připojení ovládacího zařízení, kterým je možné celý systém, nebo jeho část uvádět do stavu střežení, nebo stavu klidu. Ústředna EZS musí umožňovat nastavení svých parametrů, nejčastěji pomocí ovládací klávesnice, či připojením k počítači

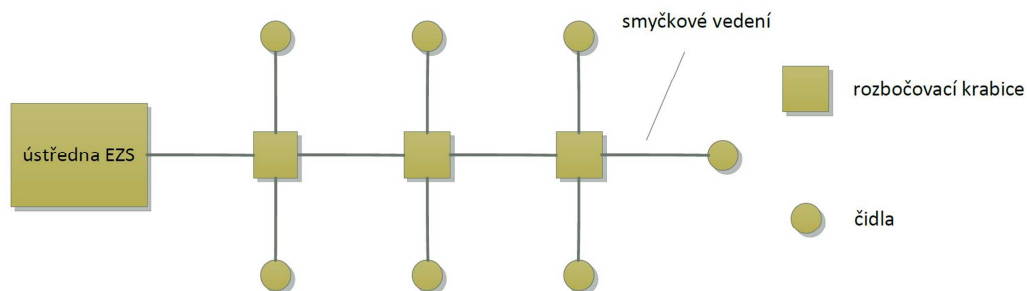
a použitím příslušného softwaru, což je lepší možnost, z důvodu, že nastavení parametrů pomocí ovládací klávesnice, může být v některých případech zdlouhavé a nepřehledné. Poplachové ústředny EZS můžeme rozdělit do čtyř kategorií, dle komunikace s čidly a ostatními prvky systému, na ústředny smyčkové, ústředny s přímou adresací čidel, ústředny smíšeného typu a ústředny s bezdrátovým přenosem, nebo ústředny vzniklé sloučením, některých z přechozích typů.



Obrázek 13: Poplachová ústředna Jablotron OASIS JA-83K [9]

4.1 Smyčkové ústředny

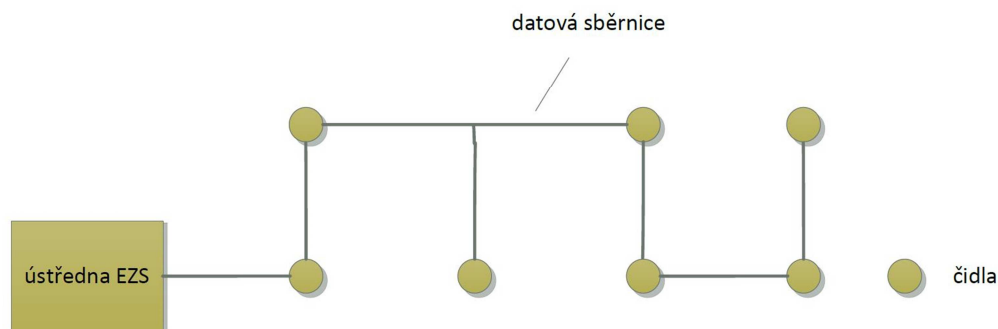
Smyčkové ústředny mají většinou vstupy, pro více zabezpečovacích smyček, vstupní vyhodnocovací obvody tohoto typu ústředny, jsou řešeny většinou jako dělič napětí s komparátorem, nebo vyvážený měřicí můstek. V převážných případech je možné připojit více zabezpečovacích smyček, pro které jsou vždy samostatné vyhodnocovací obvody. Jedná se o proudovou smyčku, která je většinou zatížena, zatěžovacím odporem a do této smyčky jsou v nejjednodušším případě sériově zapojeny sabotážní a poplachové kontakty, všech čidel do dané smyčky připojených, ústředna tedy vyhodnocuje odpor této smyčky. Z toho vyplývá, že čidla určená pro smyčkové ústředny, musí mít na výstupu rozpínací kontakt, který je většinou součástí elektromagnetického relé, které je v klidovém stavu sepnuté, a po aktivaci čidla, dochází k jeho rozepnutí, a tím rozpojení proudové smyčky. Nevýhodou je rozsáhlejší kabeláž, protože každé čidlo musí být přes rozbočovací krabici připojeno samostatným kabelem, k vyhodnocovacímu obvodu, dané zabezpečovací smyčky ve smyčkové ústředně.



Obrázek 14: Blokové schéma zapojení smyčkových ústředn

4.2 Ústředny s přímou adresací čidel

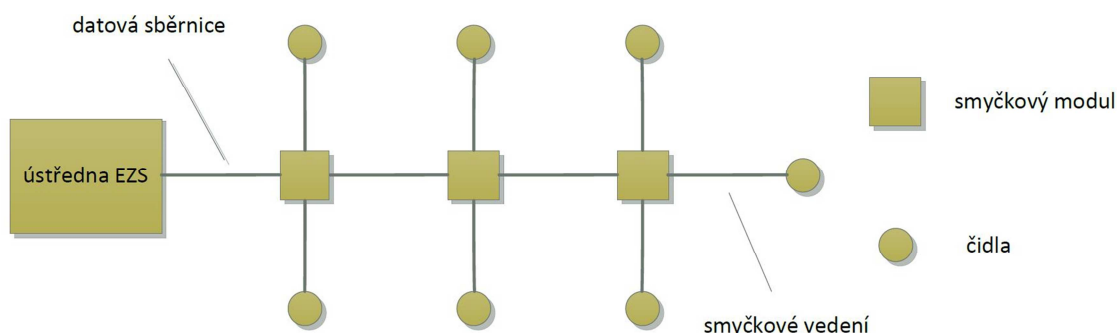
Komunikace mezi poplachovou ústřednou a čidly probíhá v tomto případě prostřednictvím datové sběrnice, kabelové vedení obsahuje celkem čtyři vodiče, dva slouží k napájení jednotlivých čidel, ostatní tvoří datovou sběrnici. Komunikace je polo duplexní, master-slave orientovaná a probíhá ve směru ústředna-čidla, to znamená, že ústředna představuje zařízení master a čidla představují zařízení slave. Každé čidlo připojené na sběrnici, má svojí jedinečnou adresu a komunikace probíhá tak, že poplachová ústředna periodicky generuje adresy, jednotlivých čidel připojených na sběrnici a zjišťuje jejich stavy. Velkou výhodou tohoto systému EZS je, že dojde-li k aktivaci některého z čidel, je vždy známá jeho adresa i událost, která změnu stavu způsobila a obsluha objektu tak snadno zjistí, místo, kde je aktivované čidlo instalované. Z toho vyplývá, že je tento druh ústředn vhodný pro rozsáhlé objekty, kde je třeba přesně znát umístění aktivovaného čidla, pro rychlý zásah proti případnému pachateli, což by nebylo možné v případě smyčkových ústředn, kde známe vždy jen smyčku, ve které se nachází aktivované čidlo, kterých může být na jedné smyčce mnoho. Ústředny s přímou adresací, mají omezený počet čidel na sběrnici, který je dán úbytkem napětí na napájecích vodičích, většinou lze na jednu sběrnici, umístit desítky čidel, při celkové délce vedení, řádově stovky metrů.



Obrázek 15: Blokové schéma zapojení ústředny s přímou adresací čidel

4.3 Ústředny smíšeného typu

Tento typ poplachových ústředn je v jistých ohledech podobný, jako typ předchozí, ale má výrazně větší možnosti, co se týká omezení délky kabelového vedení. Komunikace probíhá po analogové, či digitální sběrnici, mezi samotnou ústřednou a tzv. smyčkovým modulem (koncentrátorem), na který jsou prostřednictvím klasických proudových smyček, připojena jednotlivá čidla. Vyhodnocení signálů z jednotlivých čidel, může probíhat dvojím způsobem, jednou z možností je koncentrátor s analogovým multiplexem, který přepíná jednotlivé smyčky, na daný koncentrátor připojené a odpor těchto smyček je prostřednictvím analogové sběrnice, vyhodnocen v poplachové ústředně. Druhou možností je vyhodnocení odporu smyčky v samotném koncentrátoru, kdy komunikace s ústřednou probíhá v datové podobě. Tento systém umožňuje celkovou délku datového vedení, až do 1 km, ale je možné tuto délku výrazně prodloužit, použitím opakovače, mezi ústřednou a koncentrátorem. Výhodou je použití stejných druhů čidel s reléovým výstupem, jako u smyčkových ústředn, která jsou podstatně levnější, než čidla bezdrátová, nebo čidla s přímou adresací.

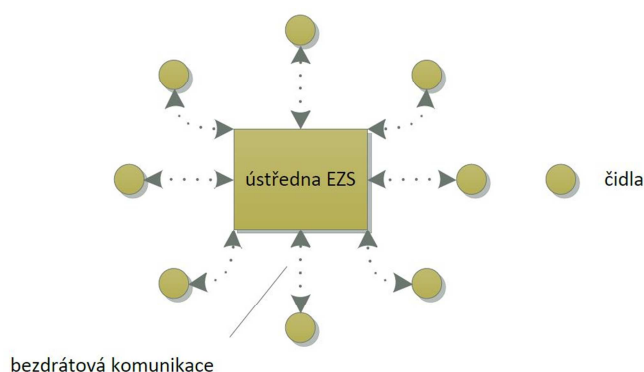


Obrázek 16: Blokové schéma zapojení ústředny smíšeného typu

4.4 Ústředny s bezdrátovým přenosem

Jak už jejich název napovídá, tak tento typ poplachových ústředn, nepotřebuje ke komunikaci s ostatními prvky systému EZS, žádné kabelové vedení, kromě síťového napájení samotné ústředny. Komunikace probíhá většinou v kmitočtových pásmech 433 MHz nebo 868 MHz, a tato komunikace může být buď polo duplexní, nebo duplexní. U polo duplexní komunikace, může komunikovat pouze čidlo, nebo jiný člen systému s poplachovou ústřednou, což je svým způsobem bezpečnostní riziko, protože ústředna nemůže žádným způsobem kontrolovat, zda nedošlo k poruše, či úmyslnému poškození některého z členů systému. Z tohoto ohledu je mnohem bezpečnější duplexní přenos, kde je komunikace obousměrná a ústředna tak může kontrolovat funkci všech členů, pomocí

periodicky, nebo náhodně generovaných kontrolních zpráv, na které musí jednotlivé prvky systému reagovat, a tím je možné zaručit správnou funkci všech zařízení, nebo indikaci případné poruchy, či úmyslného poškození. Systém je bezdrátový, z toho vyplývá, že všechna čidla i ovládací a signalizační zařízení, musí mít bateriové napájení, stav těchto baterií, musí být měřen samotným zařízením a indikace nutnosti výměny baterie, může být prováděna komunikací s poplachovou ústřednou, nebo místní akustickou signalizací. Jedná se o zabezpečovací systém, tudíž je nutností rádiovou komunikaci šifrovat a chránit proti rušení, případného narušitele střeženého objektu, moderní ústředny mají funkci automatického přeladění komunikace na jiný kanál, v případě rušení kanálu současného, a tím zajistit bezpečnou komunikační cestu a funkčnost celého systému. Tento typ poplachových ústředen, má výhodu dodatečné montáže do zrekonstruovaných prostor, kde se při návrhu budovy se systémem EZS nepočítalo, instalační stavební zásahy jsou minimální. V novostavbách je výhodné se zabezpečovací technikou počítat dopředu, protože použitím např. smyčkových ústředen, odpadá nutnost výměny baterií, ale minimalizují se také finanční náklady, protože bezdrátové prvky systému, jsou mnohem nákladnější, než drátové.

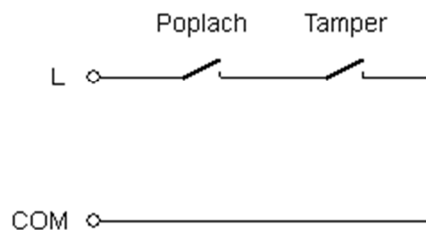


Obrázek 17: Blokové schéma komunikace ústředny s bezdrátovým přenosem

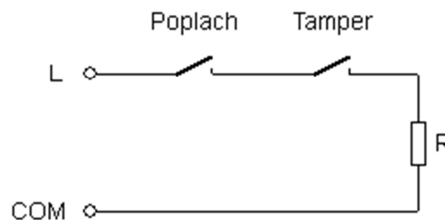
5 Možnosti připojení čidel ke smyčkovým ústřednám

Jak bylo řešeno dříve, ke smyčkovým ústřednám se připojují čidla pomocí proudových smyček a veličinou vyhodnocovanou vstupním obvodem ústředny je odpor. Nejjednodušší vstupní obvod, dokáže vyhodnotit pouze dva stavy, a to v ideálním případě odpor nulový, nebo odpor nekonečný při rozpojení smyčky, v tomto případě se jedná o smyčku nevyváženou. Ústředny vyššího standardu vyhodnocují v klidovém stavu hodnotu tzv. vyvažovacího odporu, potom se jedná o smyčku jednoduše vyváženou, která má v klidovém stavu odpor rovný hodnotě vyvažovacího odporu, v případě rozpojení

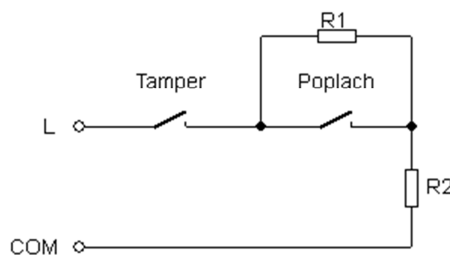
smyčky je hodnota odporu nekonečná. Dalším způsobem je připojení čidel do dvojité vyvážené smyčky, což je způsob nejlepší, protože vstupní obvody ústředny jsou potom schopny vyhodnotit, zda byl rozpojen poplachový nebo sabotážní kontakt čidla. Sabotážní kontakt, tzv. Tamper je rozpojen při sejmutí krytu čidla a ústředna by na něj měla reagovat, i když je systém uveden do stavu klidu, což je možné pouze u tohoto zapojení, protože v předchozích dvou případech, jsou jak poplachové rozpínací kontakty relé, tak sabotážní kontakty všech čidel v dané smyčce zapojeny do série, takže se nedá určit, který z kontaktů byl rozpojen. V moderních ústřednách je možné u dané smyčky nastavit její druh zapojení, hodnoty vyvažovacích odporů se u jednotlivých výrobců liší. Vstupní obvod ústředny musí vyhodnocovat odpor v určitých tolerancích, protože samotné kabelové vedení, má také svůj odpor, který se sčítá s vyvažovacím odporem.



Obrázek 18: Schéma zapojení čidla do nevyvážené smyčky



Obrázek 19: Schéma zapojení čidla do jednoduše vyvážené smyčky



Obrázek 20: Schéma zapojení čidla do dvojité vyvážené smyčky

Tabulka 1: Hodnoty odporů zabezpečovacích smyček, dle stavu čidla

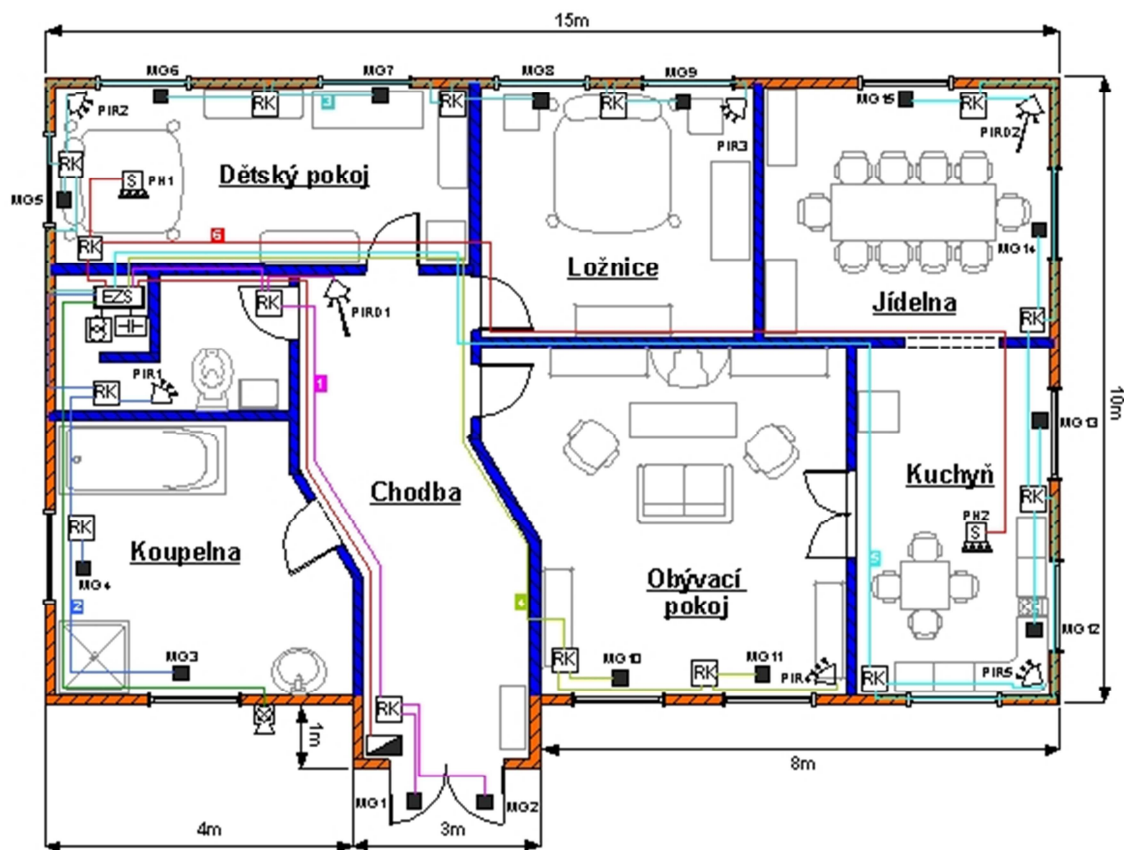
Stav	Odpor nevyvážené smyčky	Odpor jednoduše vyvážené smyčky	Odpor dvojité vyvážené smyčky
Klid	Nulový	R	R2
Poplach	Nekonečný	Nekonečný	R1 + R2
Sabotáž	Nekonečný	Nekonečný	Nekonečný

6 Strategie elektronické ostrahy budov

Při návrhu systému EZS, pro konkrétní objekt postupujeme vždy podle předpokládaného chování pachatele, to znamená možností vniknutí do objektu a dalšího pohybu. Nejdůležitějším prvkem celého systému je poplachová ústředna, která by měla být instalována na skrytém místě, střeženém samotným systémem EZS. Při montáži jednotlivých čidel, je důležité dodržení pokynů výrobce konkrétního čidla, aby se předešlo vzniku falešných poplachů. U čidel s nastavitelným dosahem, začínáme vždy na minimální hodnotě, která se postupně zvyšuje, dokud se nepokryje požadovaný prostor. Kabeláž celého systému, by měla být nejlépe v kabelových trubkách pod omítkou, případně v kabelových lištách, aby byla co nejméně přístupná případnému narušiteli objektu. Pro připojení čidel ke smyčkovým ústřednám se nejčastěji používají kabely typu SYKFY o průřezu jedné žíly 0,5 mm², které slouží i k napájení jednotlivých prvků systému. Tento typ kabelu je stíněný, což je nezbytné pro zabránění indukce elektromagnetických rušivých vlivů, které mohou vést ke vzniku falešných poplachů.



Obrázek 21: Schématické značky prvků tvořících systém EZS



Obrázek 22: Příklad návrhu zabezpečovacího systému konkrétního objektu

7 Popis použitých hardwarových prostředků

7.1 Použité mikroprocesory

Pro hardwarovou realizaci elektronické zabezpečovací a monitorovací jednotky resp. poplachové ústředny EZS i ovládací klávesnice je použit mikroprocesor fy Atmel z rodiny AVR s označením ATmega8. Jedná se o mikroprocesor Harvardské architektury, to znamená, že program není uložený ve stejné paměti jako data. Architektura AVR je obvyklá spíše pro 8-bitové, ale i pro některé typy 32-bitových mikroprocesorů. S ohledem na instrukční sadu se jedná o mikroprocesory typu RICS, to znamená redukovaná instrukční sada, která obsahuje pouze omezený počet základních instrukcí, jejichž vhodným spojením vznikají instrukce složitější. Architektura AVR obsahuje 32 pracovních registrů, do kterých je možné použitím instrukcí ukládat operandy, výsledky operací i adresy, další paměťovou výbavou je programová paměť typu flash a datová paměť typu EEPROM. Rodina mikroprocesorů s označením MEGA, disponuje velkým množstvím periférií, proto je do jisté míry univerzální. Konkrétně použitý mikroprocesor ATmega8 je 8-bitový, obsahuje programovou paměť o velikosti 8 kB a datovou paměť o

velikosti 512 B. Součástí jsou klasické periferie, specifické pro rodinu mikroprocesorů MEGA, jedná se zejména o čítače/časovače, A/D převodníky a nejčastěji používané sériové sběrnice, mezi které patří UART, SPI a I²C resp. TWI. Tento mikroprocesor se vyrábí v provedení PDIP i TQFP, jedním z možných zdrojů hodinové signálu je interní RC oscilátor, nebo je zde možnost využít externí rezonátor, či krystal o kmitočtu až 16 MHz, při rozmezí napájecího napětí 4,5 V až 5,5 V. Zvláštní variantou je ATmega8L, který lze napájet napětím 2,7 V až 5,5 V, ale je zde omezení externího zdroje hodinového signálu na maximální kmitočet 8 MHz. Programování, to znamená zápis do programové paměti je možné pomocí ISP rozhraní.

7.2 Obvod reálného času PCF8583

Tento obvod je výhodný pro aplikace, kde je nutné zajistit znalost aktuálního času, či data vzniku nějaké asynchronní události. Reálný čas je možné naimplementovat čistě programově, pomocí mikroprocesoru, nese to s sebou ovšem nevýhody ve složitém kódu, nutnosti použití časovače a také nemožnosti uvedení mikroprocesoru do některého ze sleep módů. Činnost tohoto obvodu je nezávislá na samotném mikroprocesoru, který je použit pouze při počáteční konfiguraci, nastavení času a samozřejmě při zjištění aktuálního času. Obvod PCF8583 je realizován jako paměť RAM o velikosti 240×8 bitů. První paměťové místo slouží pro uložení konfigurace, to znamená hlavně nastavení zdroje hodinového signálu, formátu času a kódování informace o čase, kde je možnost binárního, nebo BCD kódování. Další paměťová místa ukládají samotnou informaci o čase, tím způsobem, že vyšší nibble představuje desítky a nižší nibble jednotky daných hodin, minut, sekund, dní a měsíců. Jako zdroj hodinového signálu je použit externí krystal o kmitočtu 32 768 Hz. Připojením napájecího napětí dochází k inkrementaci hodnoty v příslušných paměťových místech v závislosti na čase. Komunikace s obvodem PCF8583 je řešena pomocí I²C sběrnice s hodinovým signálem maximálně 100 kHz, adresu obvodu na sběrnici je možné vybrat ze dvou možností, připojením pinu A₀ na zem, nebo napájecí napětí.

7.3 Převodník FT232RL

Jelikož použitý mikroprocesor ATmega8 neumožňuje komunikaci pomocí USB sběrnice, je tento obvod snadným řešením. Jedná se o převodník komunikace pomocí rozhraní UART na komunikaci pomocí rozhraní USB, či naopak pomocí emulace

sériového portu COM v počítači. Nejedná se o jedinou možnost, jak vyřešit komunikaci pomocí USB u mikroprocesorů, kterým tato sběrnice chybí, ale jedná se o možnost nejjednodušší, existuje i řešení pomocí programové implementace USB protokolu pomocí instrukcí mikroprocesoru, což je ovšem značně složité a náročné na programovou paměť. Tento obvod je možné napájet externě, nebo přímo z USB konektoru. Pro tuto aplikaci je využít ve formě hotového komunikačního modulu, který umožňuje konfiguraci elektronické zabezpečovací a monitorovací jednotky, prostřednictvím GUI, komunikujícího přes sériové rozhraní počítače.

7.4 Nabíjecí obvod MAX712

Tento integrovaný obvod slouží k řízení nabíjecího cyklu NiCd nebo NiMH akumulátorů. Obvod je možné použít pro nabíjení 1 až 16 článků v sériovém zapojení, přičemž napětí zdroje použitého pro nabíjení, musí být minimálně o 3 V větší, než je součet napětí těchto akumulátorů. Pro napájení nabíjecí logiky, slouží integrovaný stabilizátor 5 V, přičemž odběr samotného obvodu, při neaktivním nabíjení je pouze 5 μ A. Napěťová křivka nabíjecího cyklu je sledována pomocí integrovaného A/D převodníku, jehož vzorkovací perioda je nastavitelná, dle doby nabíjení akumulátorů. Nabíjení je ukončeno při detekci inflexního bodu nabíjecí křivky.

7.5 Alfanaumerický LCD

V této aplikaci je pro zobrazování informací o stavech elektronické zabezpečovací a monitorovací jednotky, prostřednictvím ovládací klávesnice použit znakový, neboli alfanaumerický LCD. Samotný display je řízen, dnes už standartním řadičem HD44780, který ovládá jednotlivé pixely, což velmi usnadňuje práci s LCD tohoto typu. Každý řadič má v paměti uloženou znakovou sadu, kde se na jednotlivých paměťových místech nachází informace nutné pro zobrazení příslušného znaku. Další paměť, kterou obsahuje řadič je paměť typu RAM, která má velikost závislou na počtu zobrazitelných znaků, kód uložený na příslušnou adresu, zobrazí na příslušné pozici znak odpovídající kódu ze znakové sady řadiče. V paměti typu RAM je tedy uložen aktuální obsah LCD. Pro komunikaci s touto paměťí máme dvě možnosti, 8-bitovou a 4-bitovou, jejíž zvolení je většinou závislé na počtu pinů mikroprocesoru. Display s tímto řadičem je třeba v prvním kroku nakonfigurovat, což se provádí přivedením logické 0 na pin RS, kterým se rozlišuje, zda se jedná o instrukci, či zápis znaku do paměti. Samotný konfigurační byte

se přivádí na sběrnici a potvrzení zápisu do paměti je provedeno impulzem o délce 37 μ s na pin E. Při zvolení 4-bitové komunikace je nutné komunikovat s pamětí řadiče po nibblech, kde musí být zápis každého nibblu potvrzen impulzem na E. Zobrazení znaku na LCD probíhá obdobně, rozdíl je pouze v logické 1 na pinu RS, kterou je řadiči sděleno, že se jedná o zápis znaku.

7.6 Sběrnice I²C

Sběrnice I²C, patří mezi sériové, synchronní, polo duplexní sběrnice, to znamená, že dochází k přenosu hodinového signálu, mezi komunikujícími zařízeními a v každém okamžiku mohou být data přenášena pouze jedním směrem. Společností, která tuto sběrnici vyvinula, je společnost Philips, tudíž vlastní autorská práva, která obchází některé společnosti jiným názvem, ale sběrnice jsou plně kompatibilní. U mikroprocesorů Atmel, je proto tato sběrnice pojmenována TWI. Komunikace je MASTER, SLAVE orientovaná a probíhá prostřednictvím dvojice vodičů, SCL, pro přenos hodinové signálu a SDA, pro sériový přenos dat. Velikost rámce je jeden byte, jehož přenos je zahájen tzv. start condition bitem, který posílá MASTER zařízení, zahajující vždy komunikaci. Start condition bit je shoení úrovně datového vodiče SDA na logickou 0, v klidovém stavu je úroveň na SDA v logické 1, kterou zajišťuje PULL-UP rezistor. Zařízení typu SLAVE, odpovídá tzv. ACK bitem, což je potvrzení přijetí start condition bitu. Poté MASTER vysílá byte, jehož obsahem je adresa SLAVE zařízení, s délkou obvykle 7 bitů, nejméně významným bitem, sděluje MASTER, jestli zahájí zápis, nebo čtení dat ze SLAVE zařízení. Přijetí adresy je opět potvrzeno ACK bitem, po kterém následuje jeden, nebo více datových bytů, z nichž každý musí být opět potvrzen pomocí ACK. Při větším počtu SLAVE zařízení na sběrnici, dochází k porovnání adresy vyslané zařízením MASTER, na všech SLAVE zařízeních, která jsou aktivní. Protože počet zařízení na sběrnici je omezen pouze počtem možných adres, je možné použít i 10-bitovou adresu, jejíž přenos je proveden po dvou bytech, prostřednictvím speciální kombinace, přidané k samotné adrese. Komunikace je ukončena zařízením typu MASTER, tzv. stop condition bitem, který uvolní datový vodič SDA, do stavu logické 1. Tato sběrnice, umožňuje i multimaster mód, který ovšem přináší nutnost arbitrace, to znamená zvolení zařízení MASTER, které má právo zahájit komunikaci, arbitrace je z větší části řešena hardwarově. Výpočet pro nastavení přenosové rychlosti sběrnice TWI, na mikroprocesorech fy Atmel je popsán následujícím vztahem.

$$f_{SCL} = \frac{f_{CPU}}{16 + 2 \cdot TWBR \cdot 4^{TWPS}} \quad (2)$$

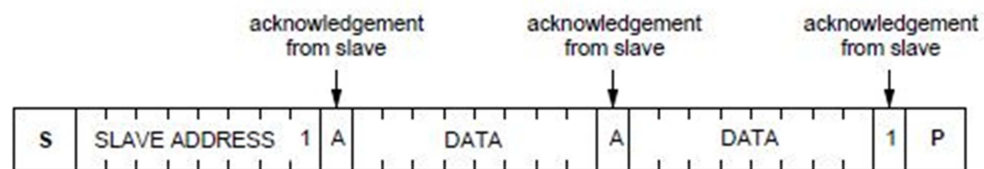
kde f_{SCL} – taktovací kmitočet TWI sběrnice

f_{CPU} – taktovací kmitočet mikroprocesoru

$TWBR$ – registr, v němž uložená hodnota, určuje rychlost TWI sběrnice

$TWPS$ – dělicí poměr taktovací kmitočtu mikroprocesoru

S – start condition bit, P – stop condition bit, A – ACK (acknowledgement)



Obrázek 23: Diagram přenosu dvou bytů po I²C sběrnici [10]

7.7 Sběrnice UART

Jedná se o sériovou, asynchronní, duplexní sběrnici, to znamená, že nedochází k přenosu hodinového signálu mezi komunikujícími zařízeními a je možné v každém okamžiku přenášet data oběma směry. Přenos dat probíhá prostřednictvím dvou vodičů připojených na piny RXD a TXD „kříženým“ způsobem. Základní přenášenou jednotkou je rámeček, který může mít 5 až 9 bitů, dle nastavení sběrnice. Přenos rámečku je zahájen tzv. start bitem, poté následuje přenášený rámeček, jehož přenos je signalizován jedním, nebo dvěma stop bity. Přenosová rychlost baud rate určuje počet přenesených bitů za sekundu a je konfigurovatelná. U asynchronních přenosů je velmi důležité časování, jehož přesnost je závislá na zdroji hodinového signálu, který řídí generátor přenosových rychlostí. Při použití UART sběrnice ke komunikaci s mikroprocesorem, je výhodnější zvolit zdrojem hodinového signálu externí krystal, který je přesnější než interní RC oscilátor. Volba kmitočtu tohoto krystalu je závislá na zvolené přenosové rychlosti, protože pokud není tento kmitočet beze zbytku dělitelný přenosovou rychlostí, vzniká určitá chyba, která se při přenosu každého bitu sčítá, a to může způsobit problémy při přenosu většího bloku dat. Sběrnice UART má prostředky, které umožňují kontrolu

integrity dat, jedná se o tzv. paritu, kdy při sudém počtu logických jedniček dochází k doplnění jedničky na místo paritního bitu, potom se jedná o lichou paritu, analogicky funguje sudá parita. Následující obrázek popisuje přenos jednoho rámce.

St – start bit, Sp – stop bit, P – paritní bit, IDLE – pasivní sběrnice



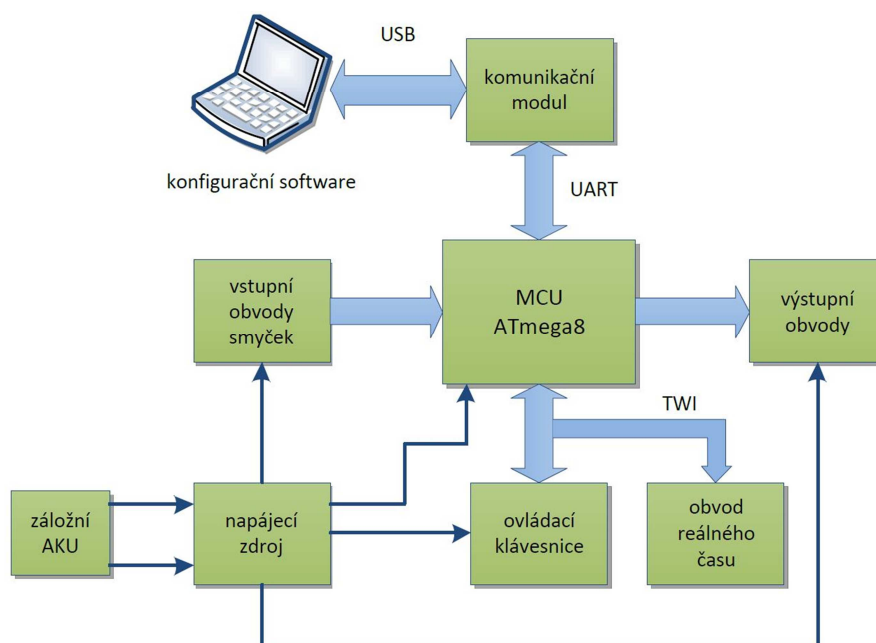
Obrázek 24: Diagram přenosu rámce po UART sběrnici [11]

8 Hardwarové řešení

Elektronická zabezpečovací a monitorovací jednotka, resp. poplachová ústředna EZS, je ovládána klávesnicí, tvořící samostatné elektronické zařízení. Tyto členy jsou řízeny pomocí mikroprocesorů typu ATmega8, komunikace mezi ústřednou a ovládací klávesnicí, probíhá prostřednictvím čtyř vodičů, dva slouží k napájení ovládací klávesnice, přímo ze zálohovaného zdroje napětí, který je součástí ústředny. Zbylé vodiče, tvoří sběrnici I²C, která zajišťuje obousměrnou komunikaci. V jednom směru dochází k přenosu informace o stisknuté klávese do ústředny, kde je vyhodnocováno, zda je stisknutá klávesa součástí příslušného kódu. Druhý směr komunikace, slouží k přenosu současného stavu ústředny, který se mění při zadání správného kódu, nebo při asynchronních událostech, např. poplachu nebo sabotáži ústředny, Současný stav a čas přechodu do tohoto stavu, jsou zobrazovány na alfanumerickém LCD, který je součástí ovládací klávesnice. Čas je získán z obvodu reálného času, který komunikuje také prostřednictvím stejné sběrnice I²C. Poplachová ústředna je konfigurovatelná pomocí GUI, které komunikuje po sériovém portu, emulovaném prostřednictvím převodníku FT232RL. Konfigurace je tedy možná, připojením k USB portu počítače.

8.1 Zabezpečovací a monitorovací jednotka

Jednotlivé části hardwaru, tvořícího zabezpečovací a monitorovací jednotku, jsou zobrazeny na následujícím blokovém schématu. Komunikační modul je samostatným členem, který není součástí této práce.

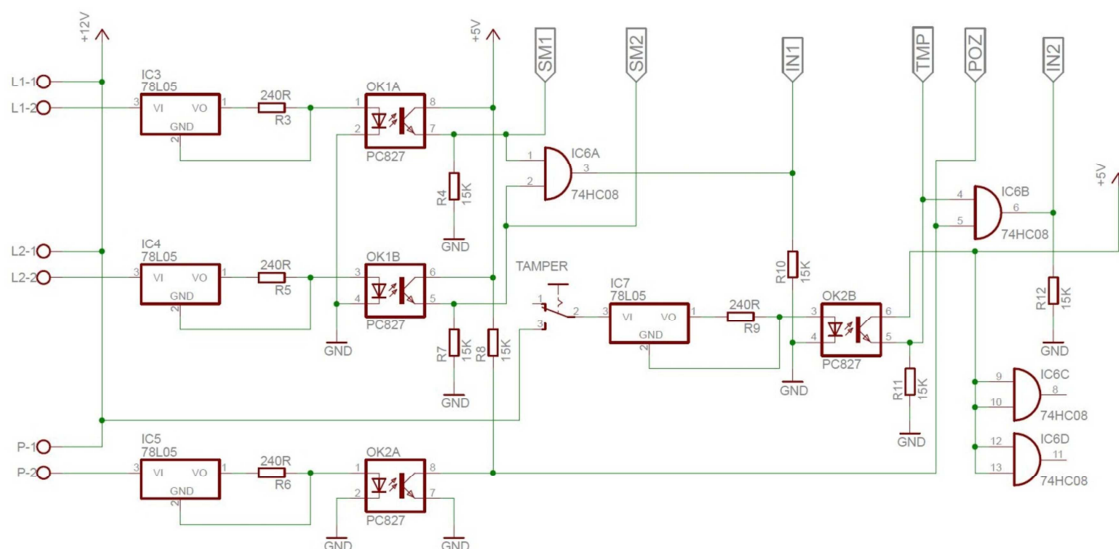


Obrázek 25: Blokové schéma zabezpečovací a monitorovací jednotky

8.1.1 Vstupní obvody

Vstupní obvody jsou schopny vyhodnotit dva stavy, smyčka uzavřená a smyčka rozpojená. Poplachový kontakt připojeného čidla, v klidovém stavu uzavírá proudovou smyčku, tvořenou integrovaným stabilizátorem napětí 78L05, zapojeným jako zdroj proudu. Tento zdroj proudu, vytváří konstantní proud o hodnotě 20 mA, který spíná připojený optočlen PC827. Při sepnutém fototranzistoru, je na výstupu z optočlenu 5 V, tedy logická 1. Tyto poplachové smyčky jsou dvě a naprosto totožné. Jejich výstup je veden na vstup hradla typu AND, které je součástí integrovaného obvodu 74HC08, který obsahuje čtyři hradla typu AND. Při rozpojení poplachového kontaktu čidla, připojeného do libovolné smyčky, dojde ke změně napětí výstupu optočlenu na 0 V, tedy logickou 0. Jakmile se toto stane na jednom, nebo obou vstupech hradla AND, dojde ke změně logické úrovně výstupu hradla na logickou 0. Výstup hradla je veden na pin externího přerušení mikroprocesoru, které reaguje na sestupnou hranu impulzu, aby bylo možné rozeznat, která z poplachových smyček poplach způsobila, jsou vstupy hradla připojeny na piny mikroprocesoru, a tak je možné, při vyvolání přerušení zjistit, která ze smyček byla rozpojena. Stejným způsobem je vyřešen i vstup sabotážního kontaktu ústředny, který je rozpojen v případě otevření víka krabice. Požární smyčka je řešena s malým rozdílem, na výstupu optočlenu je v klidovém stavu logická 1, při rozpojení proudové smyčky a při jejím uzavření, dochází ke změně úrovně na logickou 0, tedy k poplachovému stavu. Důvodem této odlišnosti je způsob funkce vyráběných požárních

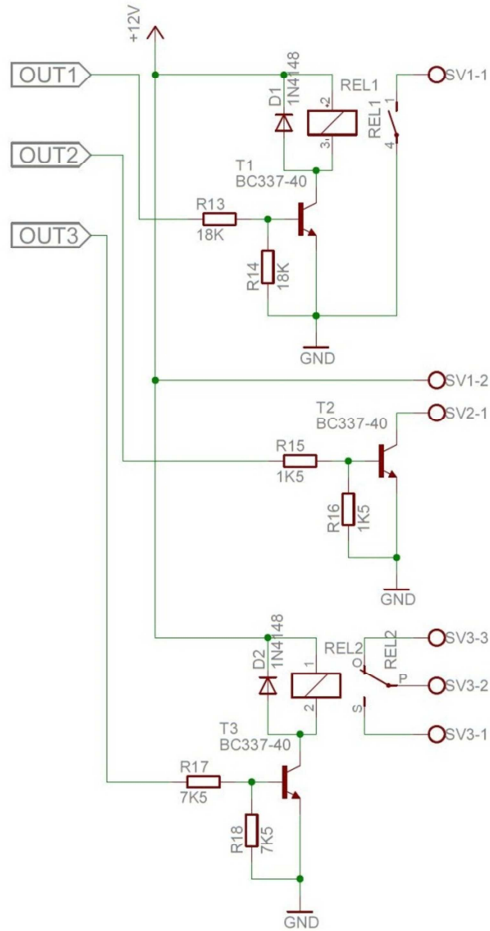
čidel, která při vyhodnocení poplachového stavu, poplachový kontakt spínají, na rozdíl od čidel zabezpečovacích.



Obrázek 26: Schéma zapojení vstupních obvodů

8.1.2 Výstupní obvody

Výstupní obvody slouží k připojení signalizačních zařízení, většinou sirény, jedná se tedy o obvody spínací, které sepnou při vyhodnocení poplachového stavu. K připojení venkovní sirény, slouží spínací kontakt relé, který v případě poplachu připojí vstupní obvod sirény na zem, a tím dojde k její aktivaci. Většina vyráběných venkovních sirén, je aktivována tímto způsobem. Naopak většina vyráběných vnitřních sirén, je spuštěna pouhým připojením napájecího napětí 12 V, proto je výstup pro tento typ sirén řešen spínacím tranzistorem BC337-40, který spíná napětí 12 V, při vyhodnocení poplachového stavu. Pracovní bod tohoto tranzistoru je nastaven na maximální kolektorový proud 600 mA, který by měl postačit pro napájení většiny vyráběných vnitřních sirén. Zabezpečovací jednotka je opatřena i silovým výstupem relé s maximální zatížitelností 250 V/10 A stejnosměrných, pro možnost spínání např. osvětlení, při poplachovém stavu. Pro sepnutí relé použitých ve výstupních obvodech, slouží již zmíněný spínací tranzistor BC337-40 s vhodně nastaveným pracovním bodem.

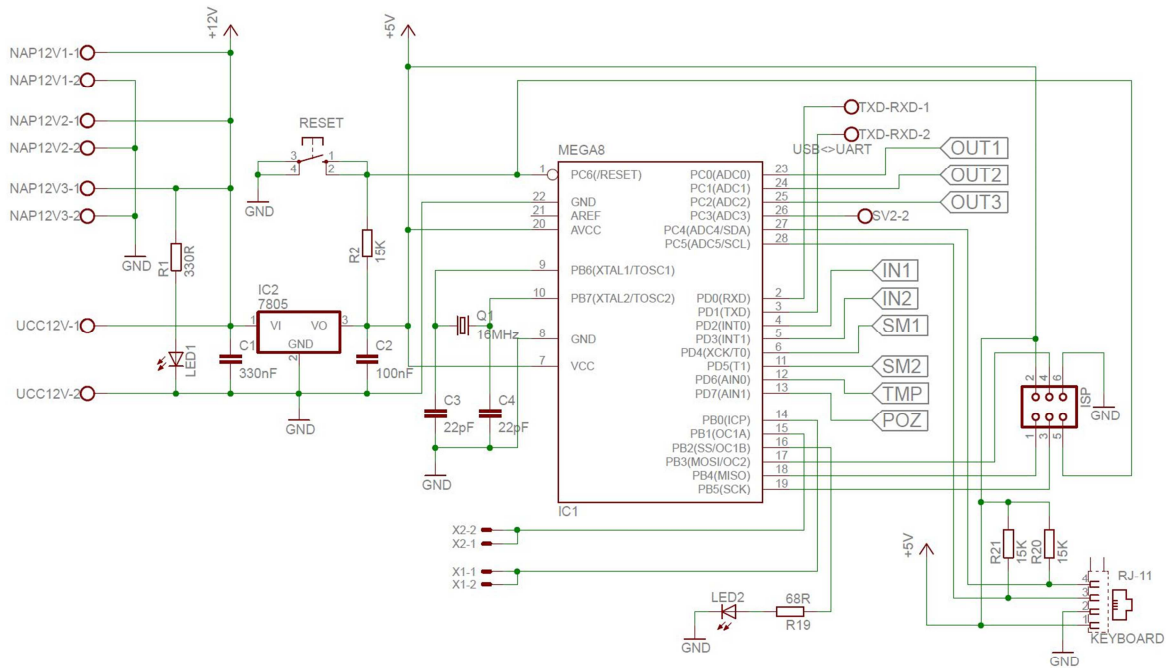


Obrázek 27: Schéma zapojení výstupních obvodů

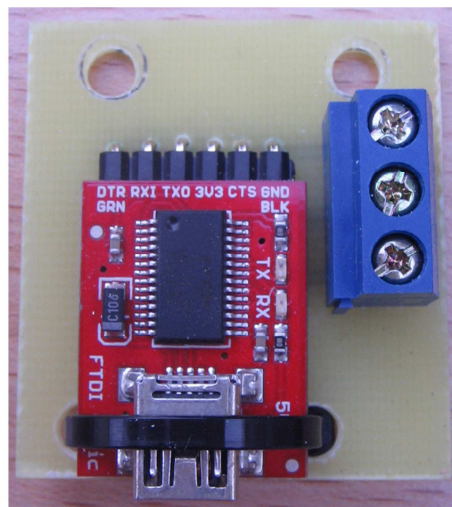
8.1.3 Zapojení mikroprocesoru

Napájení mikroprocesoru, řídicího poplachovou ústřednu je vyřešeno použitím integrovaného stabilizátoru 7805. Výstup tohoto stabilizátoru je veden na zdířku RJ-11, která slouží k napájení a komunikaci s ovládací klávesnicí, prostřednictvím sběrnice I²C. Odporů R20 a R21, slouží jako PULL-UP, pro držení logické 1 na vodičích SDA a SCL, tvořících I²C sběrnici. Pro indikaci centrálního napájecího napětí 15 V, na svorkovnici s označením UCC, slouží LED1 na vstupu stabilizátoru. Svorkovnice s označením NAP, slouží k napájení čidel, zapojeným do jednotlivých smyček. Použitý mikroprocesor má aktivní úroveň RESETU na logické 0, proto je při běžné činnosti tato úroveň držena na logické 1, příslušným PULL-UP odporem. Jako zdroj hodinového signálu, je použit externí krystal o kmitočtu 14 745 600 MHz, připojený na piny XTAL. Paralelně připojené kondenzátory slouží jako externí kapacity, umožňující vnitřní strukturu oscilátoru, tvorbu hodinového signálu. Kmitočet krystalu je zvolen s ohledem na použití asynchronní sběrnice UART s přenosovou rychlostí 9600 bit/s, kdy je s tímto hodinovým

signálem, chyba přenosu nulová. Pro indikaci přijetí konfiguračních dat po sběrnice UART, je použita LED2. Komunikační modul je připojen pomocí svorkovnice s označením TXD-RXD, kromě těchto vodičů, je třeba připojit ke komunikačnímu modulu zem, ze společného napájecího zdroje. Pro účely programování mikroprocesoru, jsou potřebné signály vyvedeny na 6-pinový konektor, sloužící k připojení ISP programátoru.



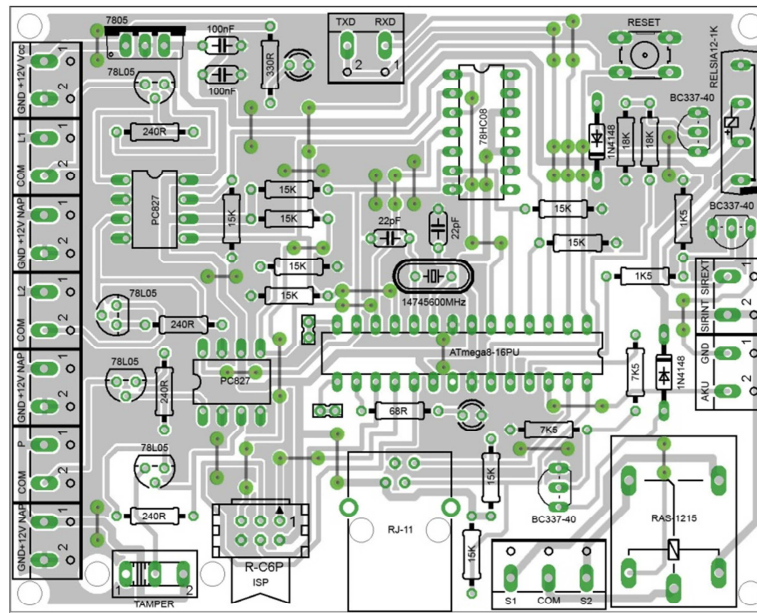
Obrázek 28: Schéma zapojení mikroprocesoru



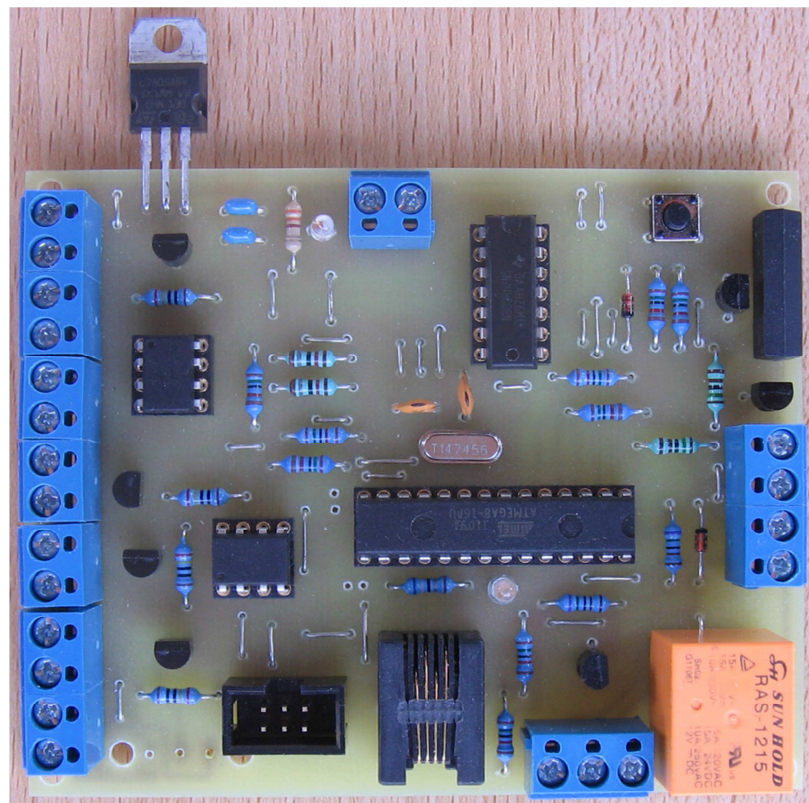
Obrázek 29: Použitý komunikační modul s obvodem FT232RL

8.1.4 Návrh plošného spoje a osazený plošný spoj

K návrhu plošného spoje byl použit software Eagle, plošný spoj je jednostranný o rozměrech 8×10 cm.



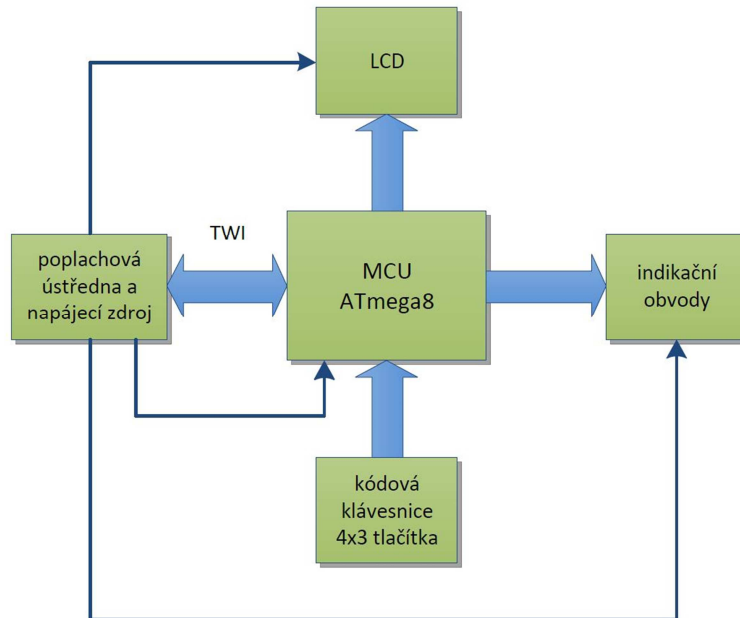
Obrázek 30: Návrh plošného spoje



Obrázek 31: Osazený plošný spoj

8.2 Ovládací klávesnice

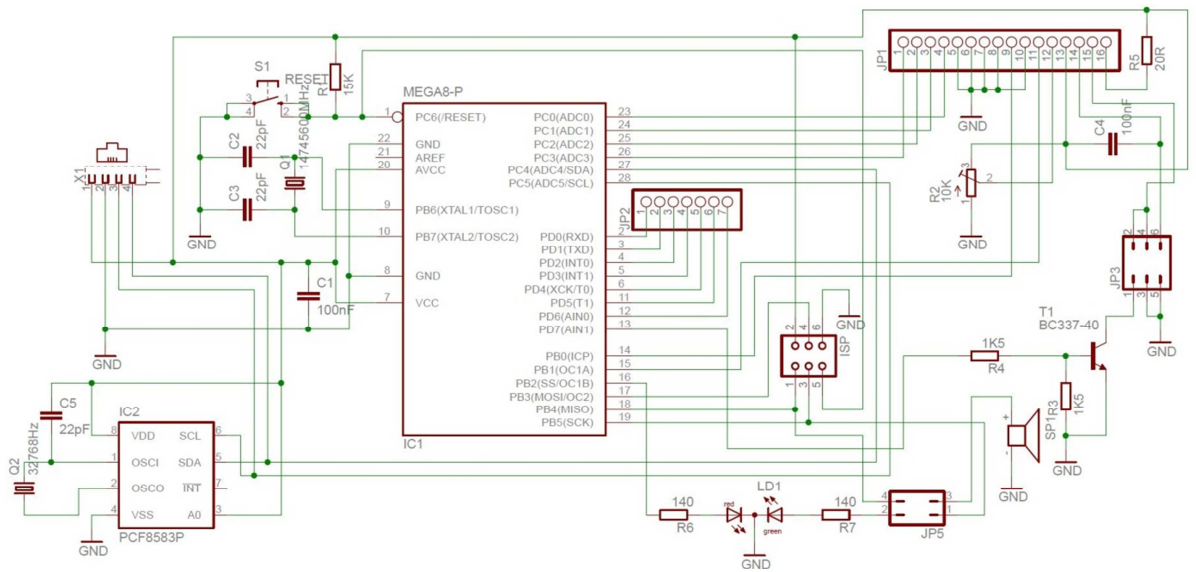
Hardwarové prvky tvořící ovládací klávesnici, jsou vyobrazeny v následujícím blokovém schématu. Blokem indikačních obvodů je myšlena dvojbarevná LED, signalizující stav střežení nebo klidu, dále akustický indikátor spouštěný stiskem klávesy a odchodovým, či příchodovým zpožděním.



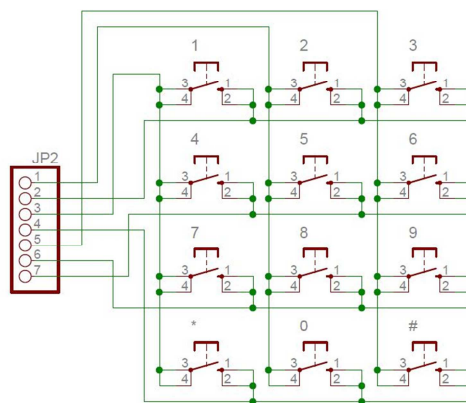
Obrázek 32: Blokové schéma ovládací klávesnice

Zapojení mikroprocesoru je obdobné, jako v zabezpečovací jednotce, napájecí napětí je ovšem přivedeno prostřednictvím zdířky RJ-11, z integrovaného stabilizátoru 7805, který je součástí zabezpečovací jednotky, do ovládací klávesnice je tedy přivedeno již stabilizované napětí 5 V. Připojení I²C sběrnice, RESETU, ISP programátoru i krystalu s kmitočtem 14 745 600 MHz je stejné. Obvod reálného času PCF8583 je připojen na I²C sběrnici, což přináší možnost komunikace s tímto obvodem, oběma zařízeními na sběrnici. Zdrojem hodinové signálu tohoto obvodu je krystal Q2 s kmitočtem 32 768 Hz. Způsobem řízení LCD je zvolena 4-bitová komunikace, probíhající prostřednictvím pinů LCD, označených jako DB7-DB4, které tvoří paralelní sběrnici. Řízení kontrastu LCD je zabezpečeno pomocí odporového trimru 10 k Ω , který tvoří napěťovou úroveň pro příslušný kontrast. Podsvícení displaye je možné připojit přímo na napájecí napětí, nebo spínat spínacím tranzistorem pouze při stisknutí klávesy, či nějaké asynchronní události, v klidových stavech se tak podsvícení automaticky vypíná, což přináší úsporu energie. Režim podsvícení je možné ovládat pomocí vhodného umístění jumperu na piny JP3. Indikace stavů je podpořena dvojbarevnou LED

s označením LD1 a akustickým indikátorem SP1, který je možné odpojit vyjmutím jumperu s pinů JP5. Dalším důvodem pinů JP5 je možnost odpojení LD1 a SP1 od mikroprocesoru, protože z důvodu nedostatku pinů ATmega8, musely být tyto prvky připojeny na signály určené pro připojení ISP programátoru, konkrétně MISO a SCK. Kódová klávesnice 4×3 klávesy je připojená k pinům mikroprocesoru a její funkce bude popsána v softwarové části této práce, jedná se o maticovou klávesnici, jejíž zapojení je na Obrázek 34: Schéma zapojení maticové klávesnice 4×3 klávesy.



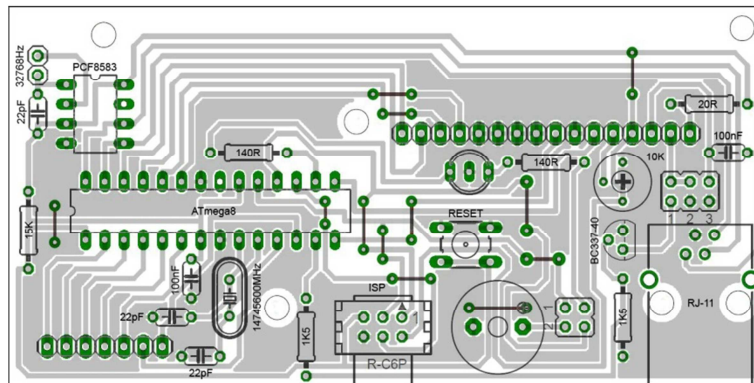
Obrázek 33: Schéma zapojení ovládací klávesnice



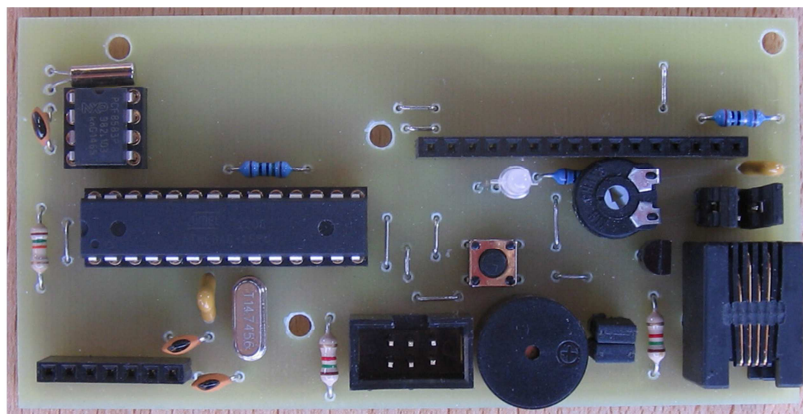
Obrázek 34: Schéma zapojení maticové klávesnice 4×3 klávesy

8.2.1 Návrh plošného spoje a osazený plošný spoj

Jedná se o jednostranný plošný spoj o rozměrech 5×10 cm. Maticová klávesnice a LCD jsou připojeny pomocí dutinkových lišt.



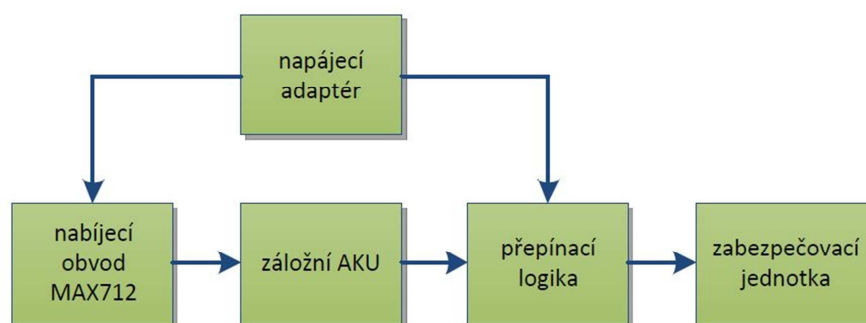
Obrázek 35: Návrh plošného spoje



Obrázek 36: Osazený plošný spoj

8.3 Zálohovaný napájecí zdroj

Blokové schéma na následujícím obrázku, popisuje strukturu zálohovaného napájecího zdroje s přepínací logikou. Zdrojem napětí je adaptér, sloužící k napájení celého zařízení a dobíjení akumulátoru. Záložní akumulátor je tvořen osmi sériově zapojenými NiMH články typu AA, s kapacitou 2400 mAh, které jsou hlídány a dobíjeny prostřednictvím integrovaného obvodu MAX712. Přepínací obvod je řešen pomocí FET tranzistoru, který zajišťuje dostatečně rychlé přepnutí na záložní akumulátor, při výpadku, či sabotáži napájecího adaptéru.



Obrázek 37: Blokové schéma zálohovaného napájecího zdroje

Zapojení obvodu pro dobíjení akumulátoru je převzato z časopisu *Elektuur electronics* [12]. V běžném provozu je celé zařízení napájeno připojeným adaptérem, který slouží také k dobíjení akumulátoru. Napětí tohoto akumulátoru je hlídáno prostřednictvím obvodu MAX712, který spustí v případě poklesu napětí nabíjecí cyklus. Vybíjení akumulátoru nastává samozřejmě jeho používáním, ale může být také samovolné. Zapojení tohoto obvodu je řešeno univerzálně, pro možnost použití jiného záložního akumulátoru. K nastavení a měření nabíjecího proudu, slouží odpor R4, na velikosti tohoto proudu, nepřímo úměrně závisí doba nabíjení akumulátoru. Obvod MAX712 je možné nastavovat prostřednictvím pinů s označením PGM. Počet připojených článků je nastavitelný pomocí pinů PGM0 a PGM1. Dále je možné nastavit maximální dobu nabíjení a vzorkovací periodu, sledující nabíjecí napětíovou křivku, pomocí pinů PGM2 a PGM3. Při detekci inflexního bodu, této napětíové křivky je akumulátor plně nabitý. Přepnutí na záložní akumulátor, zajišťuje FET tranzistor IRF9530. Jedná se o P kanál, to znamená, že připojením napětí 15 V z adaptéru na řídicí elektrodu G, dojde k jeho zavření. Odpojením tohoto napětí z G, dochází k otevření tranzistoru, na jehož elektrodě D je připojen záložní akumulátor a proud z tohoto akumulátoru, může protékat přes elektrodu S na výstupní svorky. Pro udržení napětí po dobu přechodu na záložní zdroj, slouží kondenzátor C12. Aby bylo možné detekovat mikroprocesorem výpadek napájecího napětí, je výstup z adaptéru veden na integrovaný stabilizátor 78L05, jehož výstup je připojen na jeden z pinů mikroprocesoru.

Výpočet nabíjecího proudu akumulátoru:

$$I_n = \frac{0,25}{R_4} = \frac{0,25}{0,22} \doteq 1,14 \text{ A} \doteq 1140 \text{ mA} \quad (3)$$

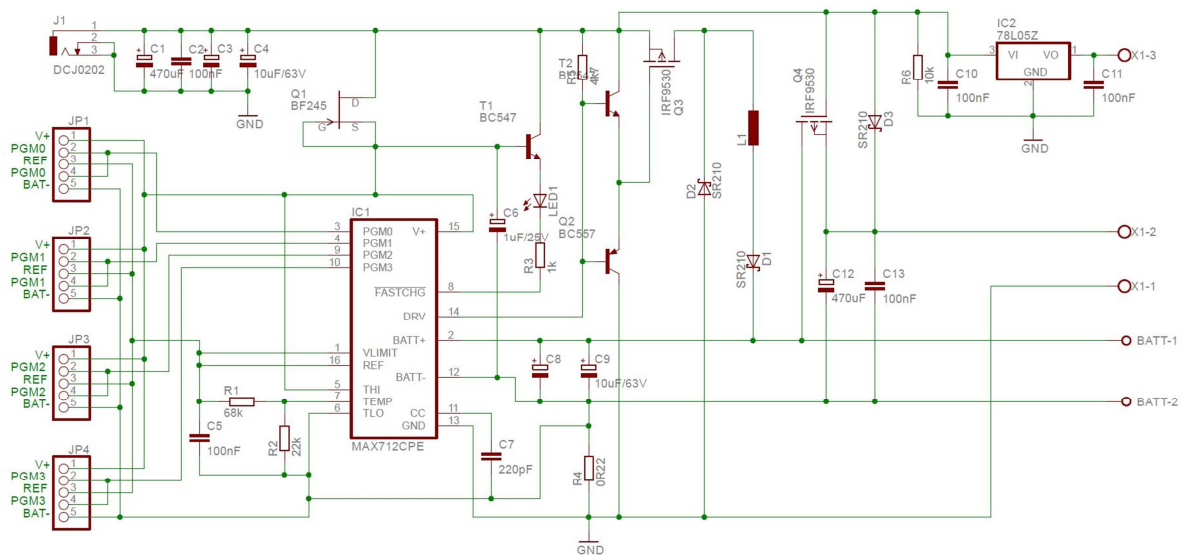
kde I_n – nabíjecí proud

Výpočet doby nabíjení akumulátoru:

$$t = \frac{C}{I_n} = \frac{2400}{1140} \doteq 2 \text{ h} \quad (4)$$

kde I_n – nabíjecí proud

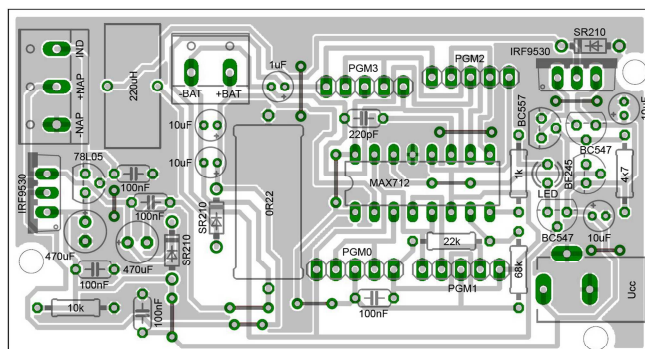
C – kapacita akumulátoru



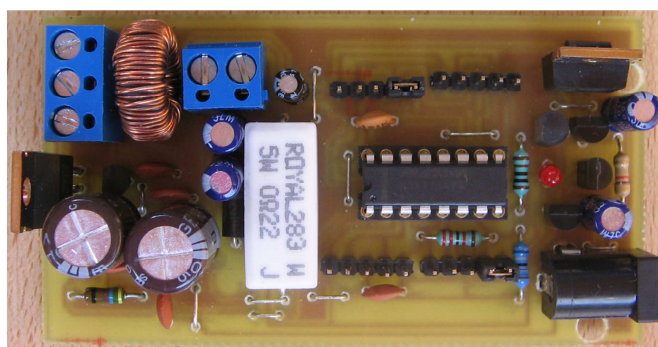
Obrázek 38: Schéma zapojení zálohovaného napájecího zdroje

8.3.1 Návrh plošného spoje a osazený plošný spoj

Jedná se o jednostranný plošný spoj o rozměrech 4,5×8,5 cm.



Obrázek 39: Návrh plošného spoje



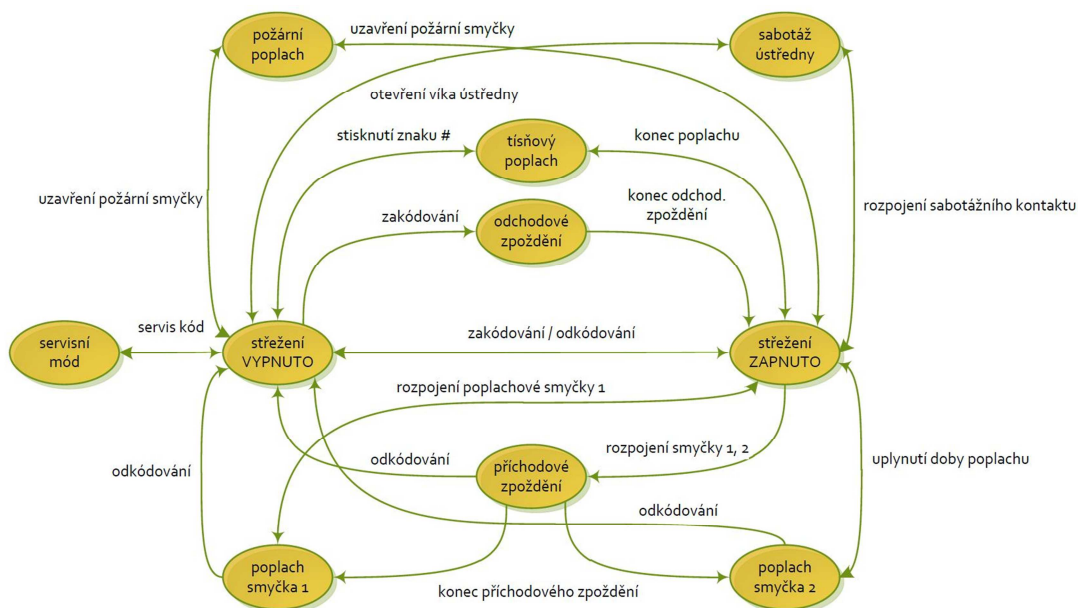
Obrázek 40: Osazený plošný spoj

9 Softwarové řešení

Mikroprocesory ATmega8 řídící zabezpečovací jednotku i ovládací klávesnici jsou naprogramovány pomocí programovacího jazyka C, ve vývojovém prostředí Atmel Studio 6.1, které používá předdefinované knihovny z řady WinAVR. Grafické uživatelské rozhraní je navrženo pomocí programovacího jazyka C# na platformě Microsoft .NET Framework 4.5, ve vývojovém prostředí Microsoft Visual Studio Express 2012.

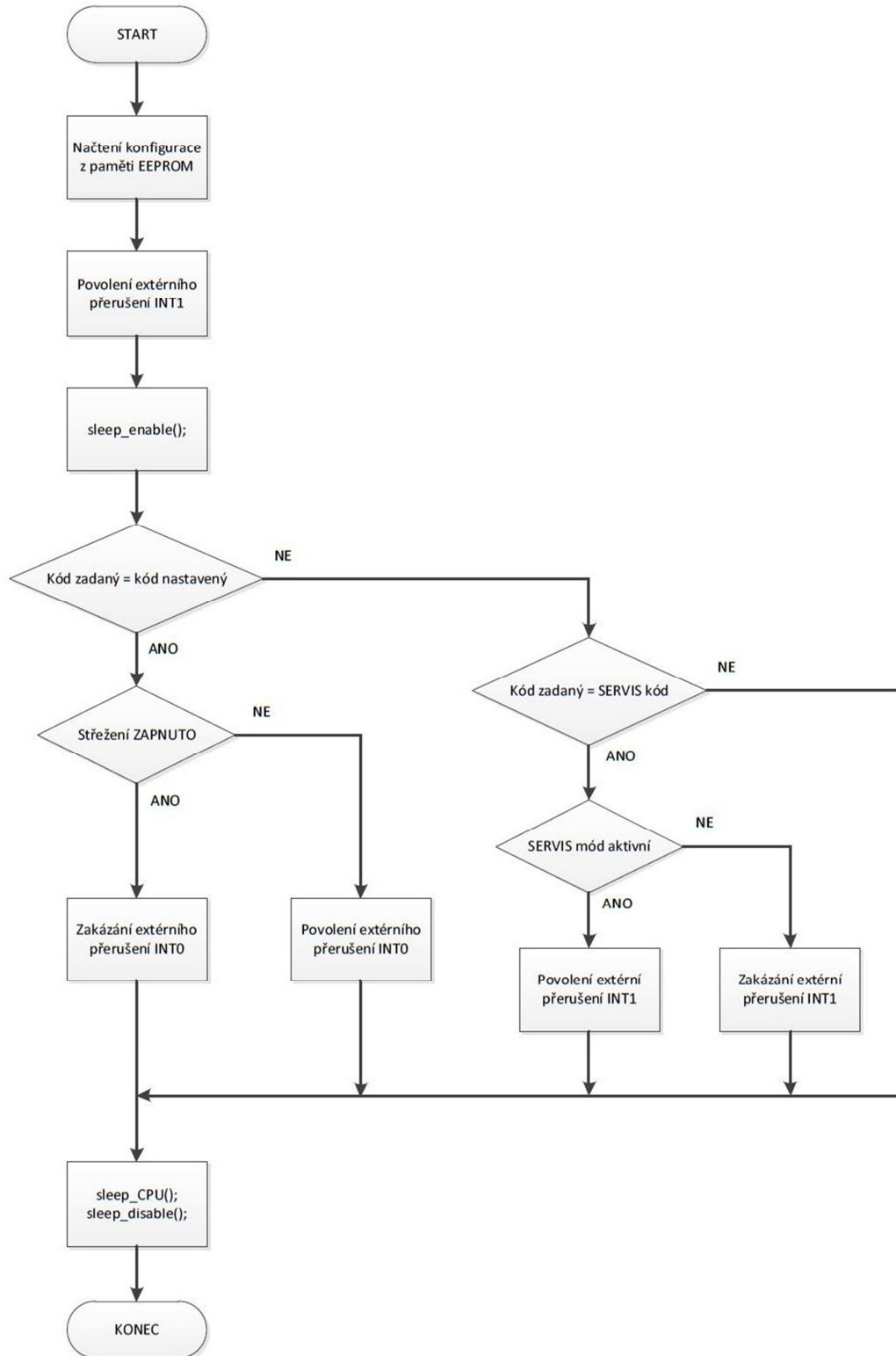
9.1 Softwarové řešení zabezpečovací jednotky

Algoritmus řídící zabezpečovací jednotku je koncipován tak, aby byl zajištěn bezpečný a bezporuchový chod tohoto zařízení. Po připojení napájecího napětí ze síťového adaptéru, či záložního akumulátoru, dojde k načtení konfiguračních dat z paměti typu EEPROM, která je součástí mikroprocesoru. Z bezpečnostních důvodů, je do této paměti ukládán i současný stav zařízení, který je vždy po připojení napájení načten, zabezpečovací jednotka je tedy přepnuta do stejného stavu, jako byla před odpojením zdroje napájení. Chování zabezpečovací jednotky můžeme přirovnat ke stavovému automatu, který pracuje na principu přechodů mezi definovanými stavy. Přejít mezi těmito stavy, může nastat pouze při určitých událostech, které jsou v tomto případě vždy asynchronní, vzhledem k činnosti zabezpečovací jednotky. Definované stavy a události způsobující přechod mezi nimi, jsou znázorněny v následujícím stavovém diagramu.



Obrázek 41: Stavový diagram popisující chování zabezpečovací jednotky

Jak už bylo uvedeno dříve, komunikace mezi zabezpečovací jednotkou a ovládací klávesnicí, probíhá prostřednictvím I²C sběrnice, která je MASTER, SLAVE orientovaná. V tomto ohledu bylo výhodné využít faktu, že komunikace probíhá v každém okamžiku pouze jedním směrem, proto jsou ve výchozím stavu obě zařízení nastavena na SLAVE, pouze v případě, že chce jedno ze zařízení komunikovat, nastaví se na MASTER, provede potřebný přenos dat a opět se nastaví na SLAVE. Zabezpečovací jednotka komunikuje pouze při asynchronních událostech, jako je např. poplach, nebo změna stavu vyvolaná uživatelem, v ostatních případech je zabezpečovací jednotka nastavena na SLAVE a může přijímat povely uživatele prostřednictvím ovládací klávesnice. Při stisknutí libovolné klávesy na ovládací klávesnici, dochází k přijetí hodnoty stisknuté klávesy zabezpečovací jednotkou a následné vyhodnocení, zda souhlasí hodnota na příslušné pozici nastaveného kódu. Po stisknutí čtvrté klávesy, dochází v případě správného zadání všech cifer nastaveného kódu k zakódování, či odkódování zabezpečovací jednotky, tedy povolení, či zakázání extérního přerušení INT0, na jehož pin jsou připojeny poplachové smyčky. Na pin druhého extérního přerušení INT1 je připojena požární smyčka a sabotážní kontakt víka krabice ústředny, problémem je, že toto přerušení musí zůstat aktivní i při odkódování, aby bylo možné detekovat požární, či sabotážní poplach v klidovém stavu. Z tohoto důvodu je v tomto algoritmu implementován i tzv. servisní kód, který musí být různý od uživatelského kódu, sloužícího k zakódování, či odkódování.

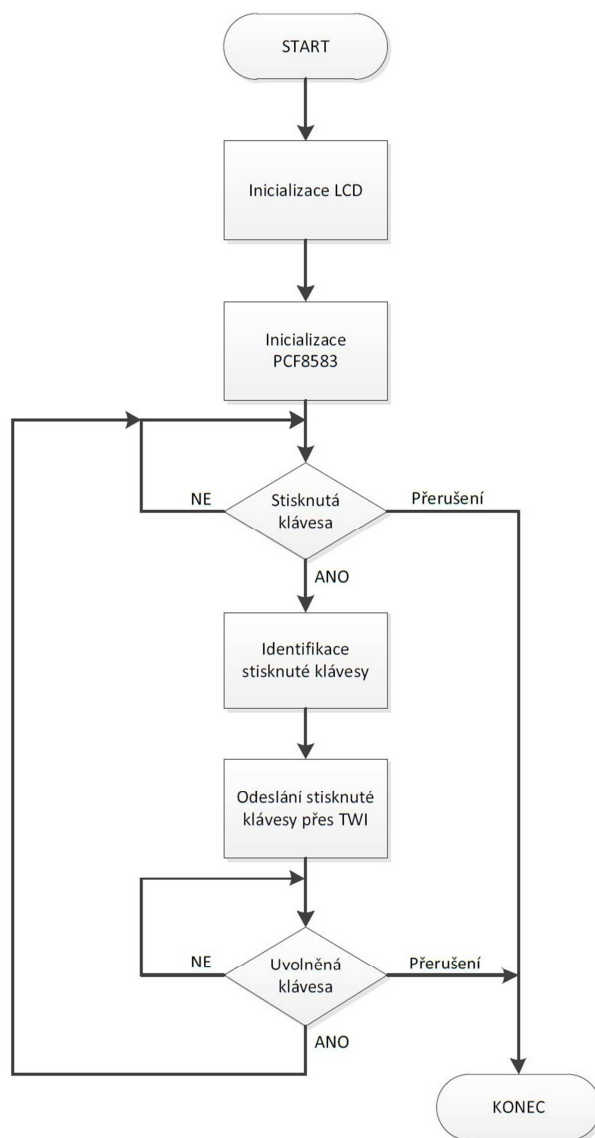


Obrázek 42: Vývojový diagram hlavní části algoritmu zabezpečovací jednotky

Zadáním servisního kódu, dochází k zakázání zmíněného přerušení INT1, což umožňuje otevřít víko krabice ústředny a provést např. údržbu, či konfiguraci nových parametrů. V tomto tzv. servisním módu je možné připojit USB kabel ke komunikačnímu modulu a provést příslušnou konfiguraci, prostřednictvím zmíněného GUI. Přijetí dat sběrnice UART způsobí přerušení, v jehož obslužné rutině dochází k uložení přijatého konfiguračního pole dat do paměti EEPROM, následuje resetování mikroprocesoru, které je vyvoláno softwarově, pomocí časovače watchdog, který přeteče a vyvolá RESET, a tím dojde k načtení nových konfiguračních dat. Druhou funkcí sběrnice UART je odeslání dat událostí, uložených také v paměti EEPROM. Při změně stavu dochází k uložení času, data a samotného stavu do paměti a tyto události je poté možné číst pomocí GUI. V klidovém stavu je mikroprocesor uveden do tzv. STANDBY režimu, hlavním důvodem je snížení celkového odběru zařízení. K probuzení mikroprocesoru, dojde při všech možných asynchronních událostech, jako je poplach, nebo komunikace přes některou z používaných sběrnic.

9.2 Softwarové řešení ovládací klávesnice

Ovládací klávesnice slouží k zadávání kódů a zobrazování současných stavů zabezpečovací jednotky na LCD. Nekonečná smyčka algoritmu, začíná čekací smyčkou, která čeká, dokud uživatel nestiskne libovolnou klávesu. Po stisknutí klávesy, dochází ke spuštění algoritmu, který zjistí klávesu stisknutou uživatelem. Jedná se o klávesnici maticovou, takže algoritmus identifikující stisknutou klávesu pracuje tak, že jednotlivé sloupce kláves jsou připojeny na vstupní piny mikroprocesoru a jednotlivé řádky jsou připojeny na piny výstupní. Na výstupních pinech jsou zapnuty vnitřní PULL-UP rezistory, v klidovém stavu je tedy na těchto pinech logická 1. Tento algoritmus pracuje tak, že čte logickou hodnotu ze všech vstupních pinů, přičemž logická hodnota na pinech výstupních se za běhu algoritmu mění tak, že v každém okamžiku je na pouze jednom výstupním pinu logická 0, ostatní mají hodnotu logické 1. Při stisknutí klávesy dojde na příslušném vstupním pinu ke shoení úrovně na logickou 0, vlivem spojení příslušného výstupního pinu, na kterém je hodnota logické 0. Mikroprocesor musí být tedy natolik rychlý, aby dokázal při stisknutí libovolné klávesy, přečíst logickou hodnotu ze všech vstupních pinů.



Obrázek 43: Vývojový diagram hlavní části algoritmu ovládací klávesnice

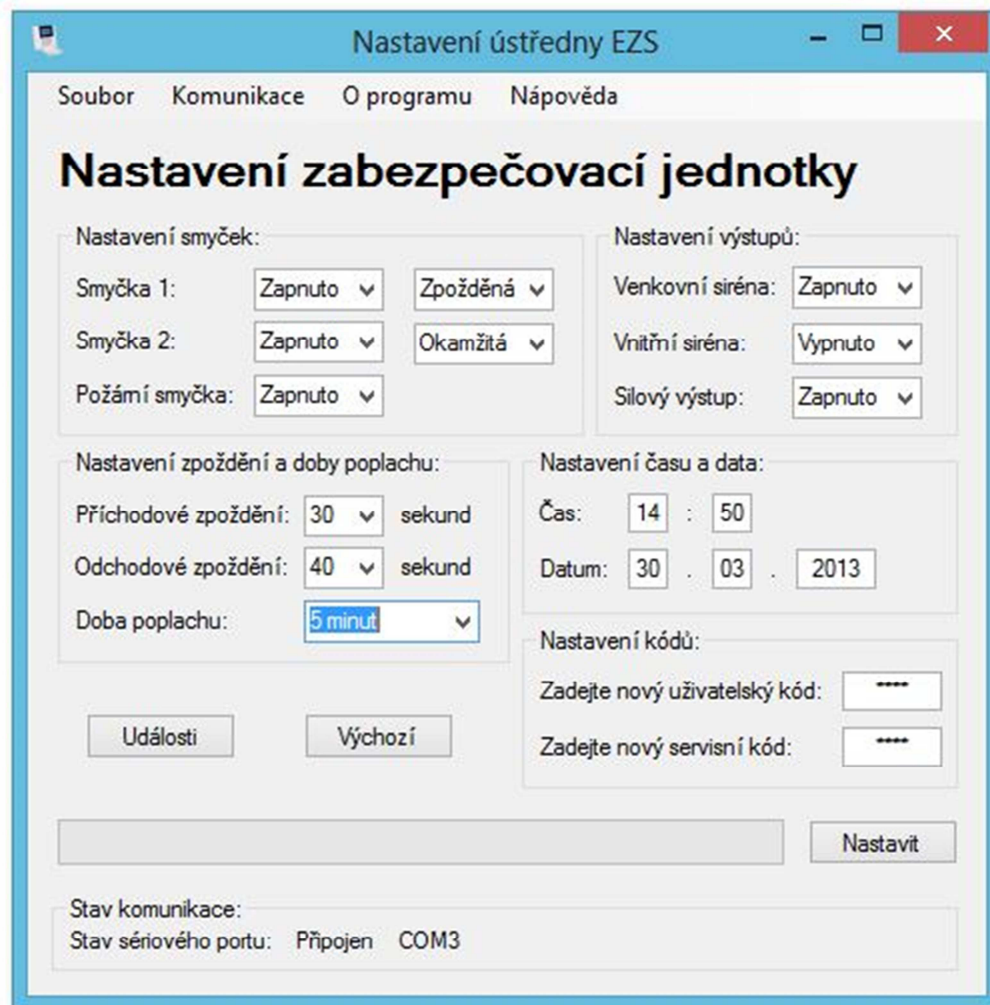
Po identifikaci stisknuté klávesy, dochází k nastavení ovládací klávesnice na zařízení typu MASTER, jako je tomu u zabezpečovací jednotky a odeslání příslušné hodnoty pomocí I²C sběrnice. Z důvodu rychlosti zpracování instrukcí mikroprocesoru, následuje další čekací smyčka, která čeká na uvolnění klávesy, což je nutné, aby došlo k identifikaci stisknuté klávesy a komunikaci po sběrnici pouze jednou, při konkrétním stisknutí. Výchozí nastavení ovládací klávesnice je zařízení typu SLAVE, aby bylo možné přijímat stavy od zabezpečovací jednotky a zobrazovat je na LCD. Předávání stavů pomocí I²C sběrnice je vyřešeno pomocí rezervovaných kombinací, z nichž každá odpovídá příslušnému stavu.

9.3 Softwarové řešení GUI

Nejdůležitější funkcí tohoto GUI je komunikace pomocí sériové linky, která umožňuje konfiguraci zabezpečovací jednotky a čtení událostí, uložených v paměti EEPROM. Pro řešení této komunikace, nabízí programovací jazyk C#, třídu s názvem SerialPort, obsahující metody, jak pro zápis dat na sériovou linku, tak i čtení dat ze sériové linky. Při spuštění GUI dochází k načtení všech sériových portů, které jsou na daném počítači k dispozici a přidání jejich jmen do příslušného combo boxu, pomocí metody GetPortNames. Konfigurační data pro odeslání po sériové lince jsou ve formě pole, jehož prvky jsou tvořeny indexy položek combo boxů jednotlivých parametrů, které se nastavují. Pole konfiguračních dat dále obsahuje konstanty, nastavující časovač na příslušný čas, které jsou závislé na indexu combo boxu, nastavujícího příslušnou funkci. Nastavení času, data a kódů je převedeno z datového typu string, získaného z textového pole, na datový typ byte, pomocí metody Parse, kterou nabízí třída Byte, poté je možné uložit tyto hodnoty do konfiguračního pole dat. K rozdělení datového typu string, na jednotlivé číselné cifry je použita metoda Remove, kterou nabízí třída String. Přenos pole dat přes sériový port, může nastat pouze v okamžiku, že je příslušný sériový port otevřen, což zabezpečí metoda s názvem Open. Pro přenos pole dat přes sériovou linku je k dispozici metoda Write, jejímž parametrem je samotné pole, počáteční index a koncový index, určující, které prvky pole se mají přenést. Po skončení komunikace je možné příslušný sériový port uzavřít, což umožňuje metoda Close, která je součástí již zmíněné třídy SerialPort.

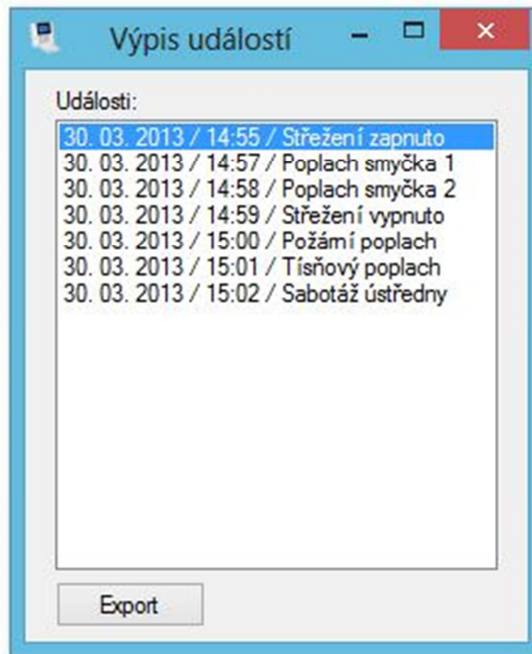
Tabulka 2: Tabulka konfiguračních možností zabezpečovací jednotky

<i>Parametr</i>	<i>Konfigurační možnosti</i>			
Smyčka 1	Zapnuto	Vypnuto	Okamžitá	Zpožděná
Smyčka 2	Zapnuto	Vypnuto	Okamžitá	Zpožděná
Požární smyčka	Zapnuto		Vypnuto	
Venkovní siréna	Zapnuto		Vypnuto	
Vnitřní siréna	Zapnuto		Vypnuto	
Silový výstup	Zapnuto		Vypnuto	
Příchodové zpoždění	10, 20, 30, 40, 50, 60, 70, 80, 90 s			
Odchodové zpoždění	10, 20, 30, 40, 50, 60, 70, 80, 90 s			
Doba poplachu	10 s, 1, 2, 3, 4, 5, 6, 7, 8, 15 min			



Obrázek 44: GUI sloužící k nastavení parametrů zabezpečovací jednotky

Jak bylo řečeno dříve, zabezpečovací jednotka ukládá při změně stavu čas, datum a kód stavu, na který přešla. Tyto události je možné zpětně číst pomocí tohoto GUI. Při stisknutí tlačítka Události v hlavním okně GUI, dochází k odeslání pole dat událostí, uložených v paměti EEPROM mikroprocesoru. Tato data jsou přijata pomocí metody s názvem ReadByte, kterou nabízí třída SerialPort. Protože je známo, kolik bytů mikroprocesor odešle, je možné s výhodou využít cyklus typu for, v jehož těle je použita zmíněná metoda. Přijaté jednorozměrné pole, je převedeno na pole dvourozměrné, jehož každý řádek, obsahuje data příslušné události, která jsou pomocí metody ToString převedena na řetězec a zobrazena, jako položka list boxu, který se otevře v novém okně. Načtené události je možné exportovat do textového souboru, pomocí metody WriteLine, kterou nabízí třída StreamWriter, umožňující práci se soubory v programovacím jazyce C#.



Obrázek 45: Okno s výpisem událostí

10 Testování a možná rozšíření

Prvním zařízením, které bylo vyrobeno a částečně otestováno, byla zabezpečovací jednotka. Při oživení tohoto zařízení, nevznikly žádné problémy, které mohou nejčastěji vzniknout chybou ve schématu zapojení, či plošném spoji. Ovládací klávesnice byla nejprve nahrazena vývojovým kitem s mikroprocesorem ATmega32, ke kterému byla připojena maticová klávesnice a LCD. Tímto postupem, vznikl prostor pro vytvoření optimálního návrhu hardwaru i softwaru ovládací klávesnice. Zabezpečovací jednotka byla optimálně hardwarově navržena, aby ji bylo možné, bez vlivu na funkčnost, uvést do STAND BY režimu, který podstatně sníží odběr mikroprocesoru v klidovém stavu. Hardware ovládací klávesnice, umožňuje vypnutí podsvícení LCD v klidovém stavu, pomocí spínacího tranzistoru, což také vede k podstatnému snížení spotřeby. Odběr obou napájených zařízení, byl měřen ve stavu klidu i v poplachovém stavu, při sepnutí všech poplachových výstupů. Tento odběr byl změřen na 260 mA, přičemž se jedná pouze o odběr samotného zařízení, bez připojených čidel a signalizačních zařízení. Odběr v klidovém stavu byl pochopitelně menší, hlavně z důvodu vypnutí podsvícení LCD a uvedení mikroprocesoru zabezpečovací jednotky, do zmiňovaného STAND BY režimu, v tomto případě dosahoval odběr pouze 150 mA. Komunikace mezi zabezpečovací jednotkou a ovládací klávesnicí, probíhá po I²C sběrnici, na kterou lze snadno paralelně připojit další zařízení, kterému je možné přidělit libovolnou adresu, z daného adresního

rozsahu. Tento fakt, by bylo možné s výhodou využít, k možnosti přidání nových zařízení. Novými zařízeními je myšleno např. více ovládacích klávesnic, či jiných ovládacích, nebo zapisovacích zařízení, jako je rádiový komunikační modul, RFID čtečka, či paměťové zařízení, ukládající události, nezávisle na datové paměti mikroprocesoru. Zabezpečovací jednotka postrádá přenosové zařízení, pro možnost dálkové komunikace s uživatelem střeženého objektu. Tento nedostatek, by bylo možné nejjednodušším způsobem vyřešit, pomocí mobilního telefonu s „rychlou“ volbou, tzn., hovorem na telefonní číslo, nastavené na libovolnou číselnou klávesu, při „dlouhém“ stisku této klávesy. Připájením vývodů na kontaktní plošky, tvořící kontakt příslušné klávesy, je možné vyvolat zmiňovaný „dlouhý“ stisk, např. sepnutím relé, při poplachovém stavu zabezpečovací jednotky.

Závěr

Tato práce byla zaměřena na elektronickou ostrahu budov a standardy, které se v tomto odvětví používají. Konstrukce zabezpečovací jednotky, byla provedena tak, aby bylo umožněno připojení klasických, běžně vyráběných detektorů, jejichž výstupní obvod tvoří relé, rozepínané v poplachovém stavu. Zapojením kontaktů, těchto detektorů, do proudových smyček, které slouží pro přenos informace o narušení střeženého objektu, vznikají tzv. zabezpečovací smyčky. Použitý návrh vstupních obvodů, sloužících k detekci rozpojení těchto smyček, se osvědčil jako velmi dobrý. V těchto obvodech je jako hlavní prvek použit optočlen, který se jeví z funkčního i bezpečnostního hlediska, jako ideální řešení, protože proudové smyčky jsou méně náchylné na rušení, než napěťové úrovně. Smyčka sabotážního kontaktu je řešena stejným způsobem, čímž bylo dosaženo, využití všech optočlenů, které jsou dva v jednom pouzdře. Požární smyčka je řešena totožným způsobem, s tím rozdílem, že dochází k detekci jejího uzavření, oproti ostatním smyčkám. Funkčnost těchto smyček, byla nejprve zkoušena na nepájivém poli, což přineslo možnost jemných úprav parametrů, před návrhem plošného spoje.

Problémy přineslo navržení optimálního algoritmu, pro detekci stisknuté klávesy na ovládací klávesnici. Při zvoleném taktovacím kmitočtu mikroprocesoru, je doba jednoho taktu, přibližně 67 ns, tento fakt, detekci stisknuté klávesy původním algoritmem znemožňoval. Důvodem byl nepříznivý tvar impulzu, vzniklého při stisknutí libovolné klávesy, který při rychlosti mikroprocesoru znemožňoval detekci. Tento nedostatek byl vyřešen, přidáním zpoždění, mezi změnu logické úrovně na příslušném řádku a podmínku vyhodnocující, která z kláves v příslušném řádku je stisknutá. Za toto zpoždění se logická úroveň dostatečně překlopí a je možná bezproblémová detekce.

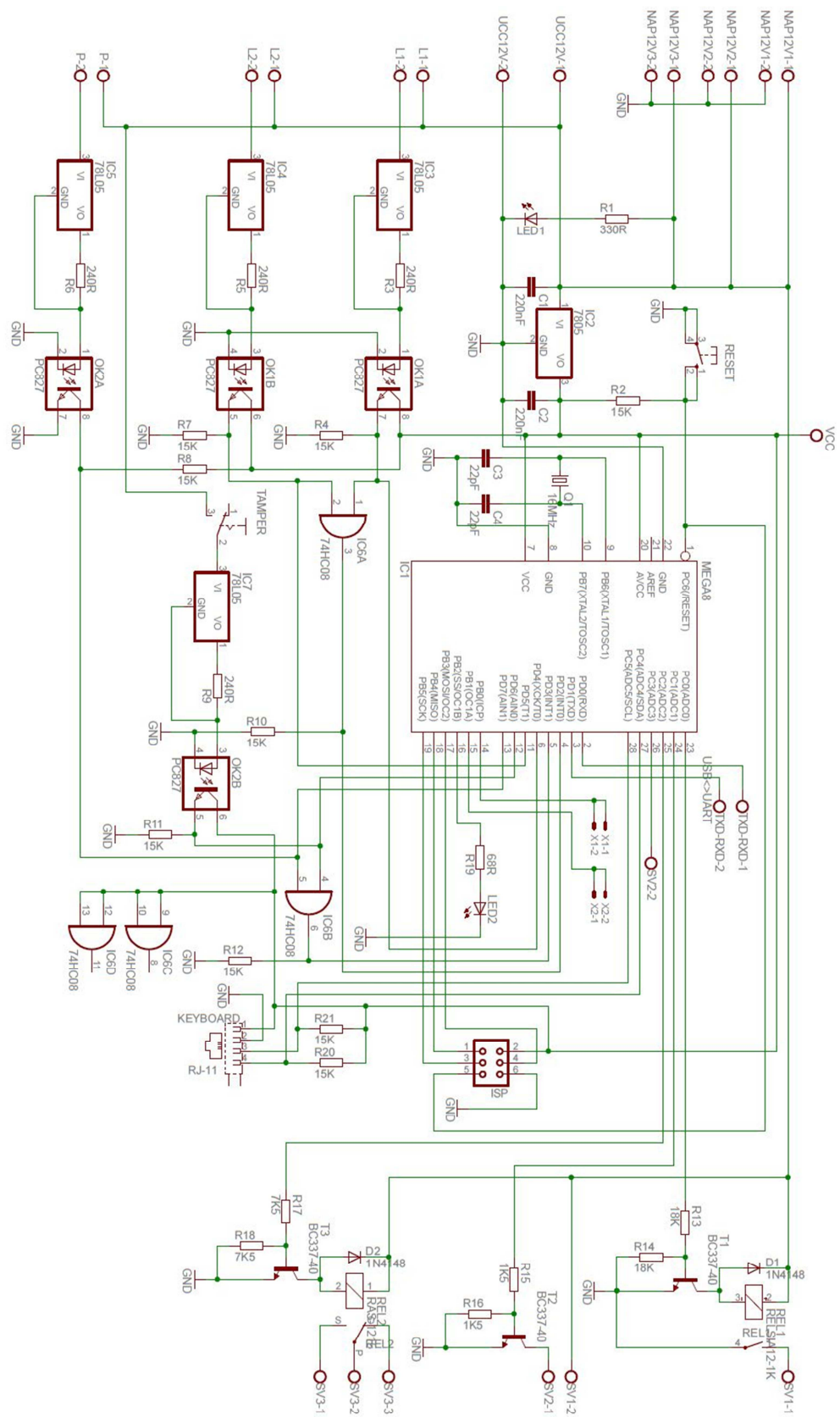
Hotové zařízení, bylo dlouhodobě testováno a dosáhlo se vysoké spolehlivosti v komunikaci, mezi zabezpečovací jednotkou a ovládací klávesnicí a především detekci poplachového stavu, při aktivaci některého z připojených detektorů. Grafické rozhraní pro konfiguraci parametrů zabezpečovací jednotky, se jeví jako dostatečně intuitivní a uživatelsky příjemné.

Literatura

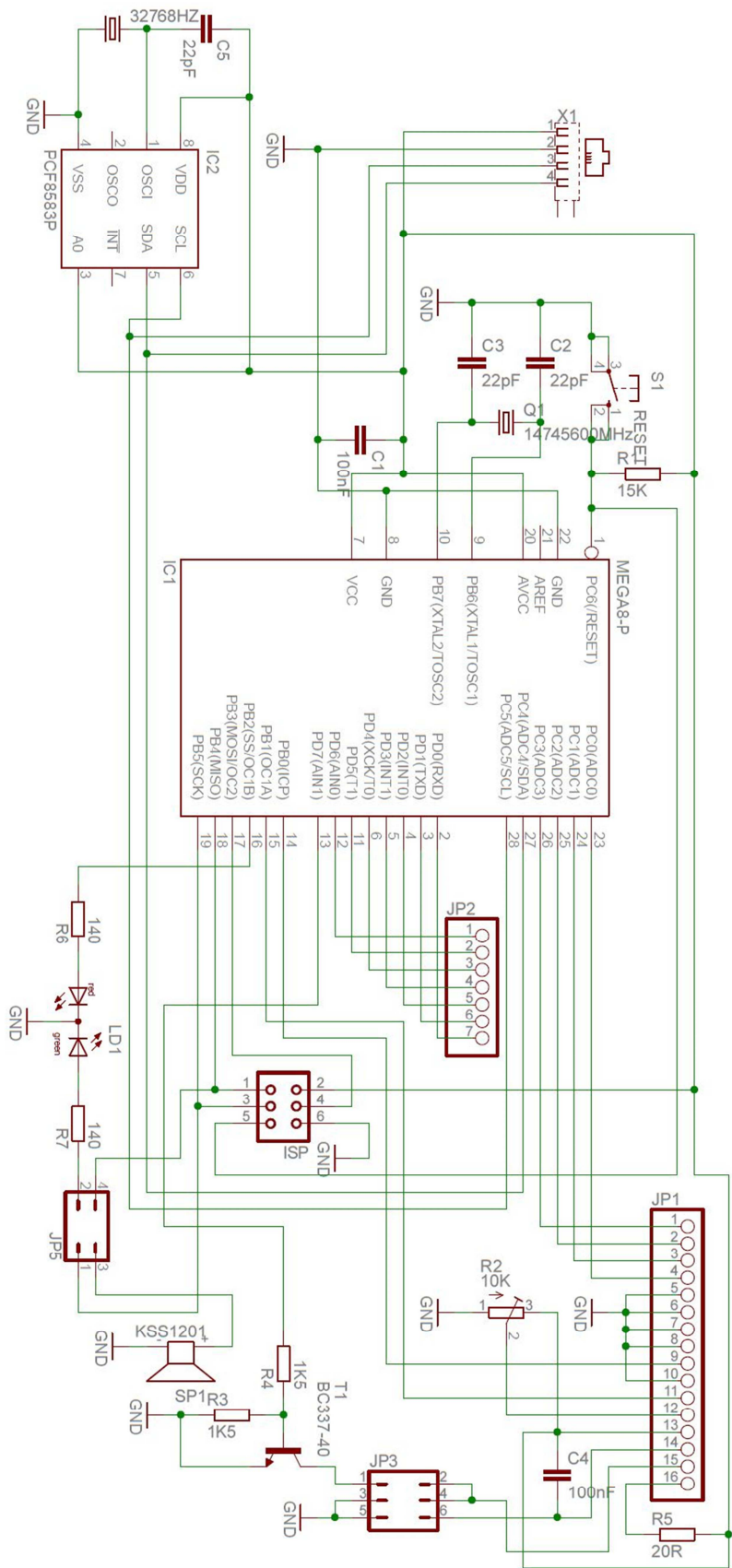
- [1] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. vyd. Blatná: Blatenská tiskárna, s. r. o., 2006. ISBN 80-902938-2-4.
- [2] JA-81F-RGB bezdrátová klávesnice, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/klavesnice/ja81frgb+bezdratova+klavesnice/>
- [3] JA-80A bezdrátová vnější siréna, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/sireny/ja80a+bezdratova+vnejsi+sirena/>
- [4] JA-82Y GSM Komunikátor, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/komunikace/ja82y+gsm+komunikator/>
- [5] Detektor SA-201-A magnetický dveřní kontakt mini, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/detektory/magneticke+detektory/detektor+sa201a+magneticky+dverni+kontakt+mini/>
- [6] JA-85B bezdrátový detektor rozbití skla, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/detektory/ja+85b+bezdratovy+detektor+rozbiti+skla/>
- [7] JA-83P bezdrátový PIR detektor pohybu osob, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/detektory/ja83p+bezdratovy+pir+detektor+pohybu+osob/>
- [8] JA-63S-80 Bezdrátový kombinovaný detektor kouře s teplotním snímačem, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/detektory/ja63s80+bezdratovy+kombinovany+detektor+koure+s+teplotnim+snimacem/>
- [9] JA-83K ústředna zabezpečovacího systému OASiS, Jablotron. [online]. [cit. 2013-03-14]. Dostupné z: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/ustredny/ja83k+ustredna+zabezpecovaciho+systemu+oasis/>

- [10] PCF8583 datasheet. [online]. s. 18 [cit. 2013-03-20]. Dostupné z:
http://www.nxp.com/documents/data_sheet/PCF8583.pdf
- [11] ATmega8 datasheet. [online]. s. 133 [cit. 2013-03-20]. Dostupné z:
http://www.atmel.com/Images/Atmel-2486-8-bit-AVR-microcontroller-ATmega8_L_datasheet.pdf
- [12] *Elektuur electronics*. Deutschland: Elektuur B.V., 2007, 7-8. ISSN 0013-5895.
- [13] VÁŇA, Vladimír. *Mikrokontroléry Atmel AVR: popis procesoru a instrukční soubor*. Praha: BEN - technická literatura, 2003. ISBN 80-7300-083-0.
- [14] HEROUT, Pavel. *Učebnice jazyka C*. 6. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-383-8.
- [15] SELS, Chris. *C# a WinForms: programování formulářů Windows*. Brno: ZONER software s. r. o., 2005. ISBN 80-86815-25-0.

Příloha A: Schémata zapojení

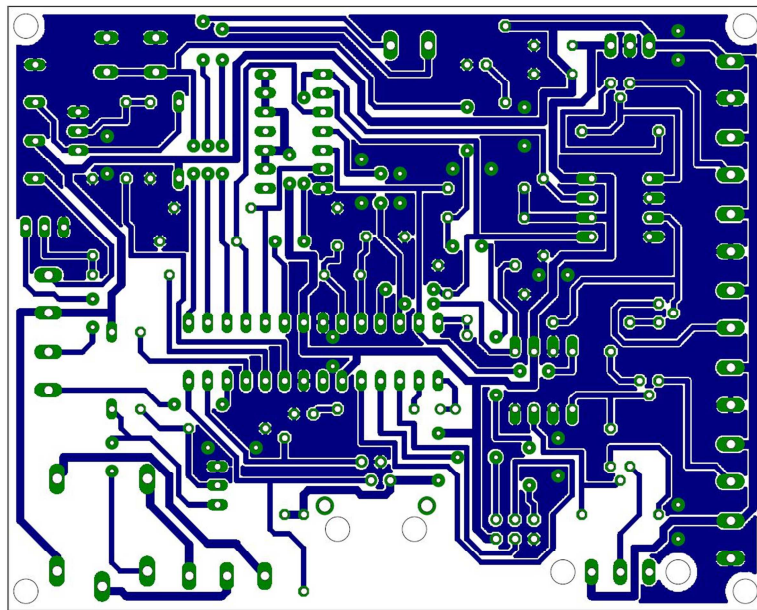


Obrázek 46: Schéma zapojení zabezpečovací jednotky

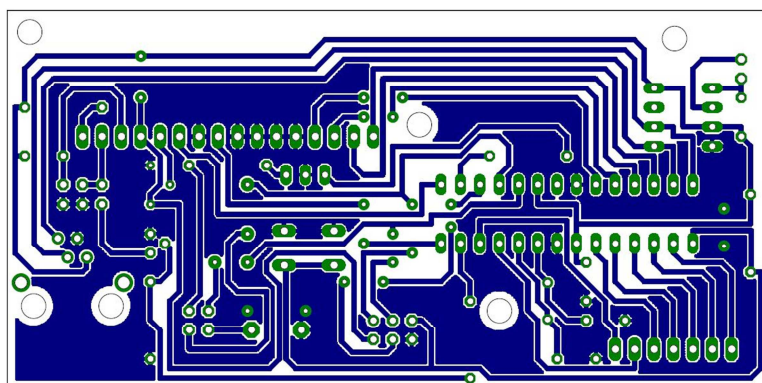


Obrázek 47: Schéma zapojení ovládací klávesnice

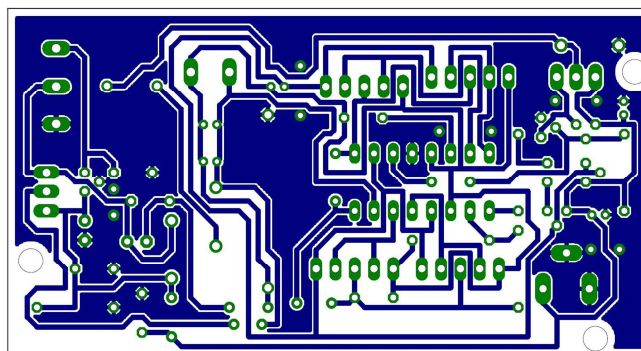
Příloha B: Návrhy plošných spojů



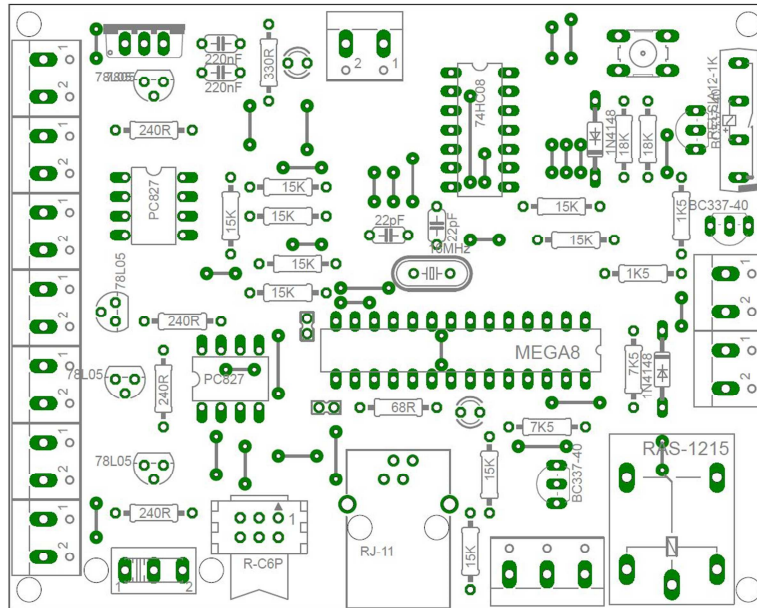
Obrázek 48: Návrh plošného spoje zabezpečovací a monitorovací jednotky



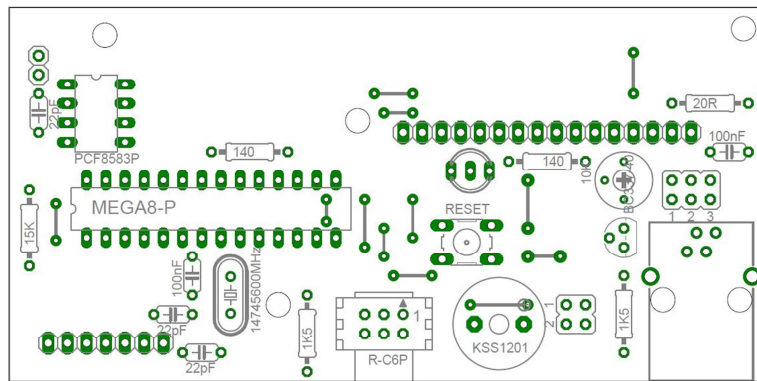
Obrázek 49: Návrh plošného spoje ovládací klávesnice



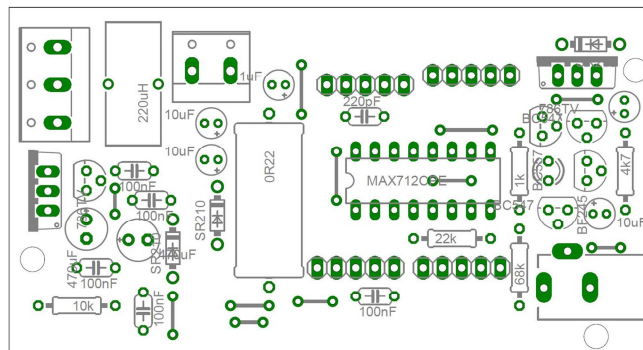
Obrázek 50: Návrh plošného spoje zálohovaného napájecího zdroje



Obrázek 51: Osazovací schéma zabezpečovací jednotky

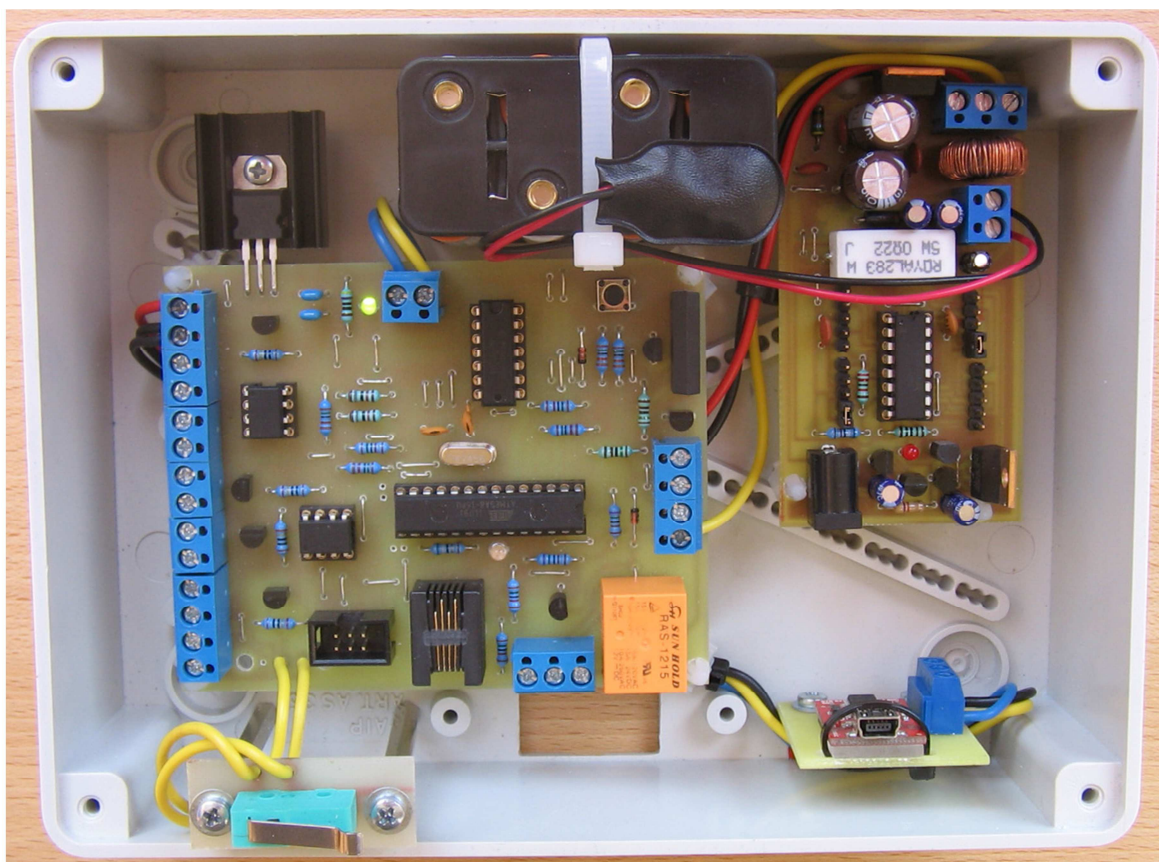


Obrázek 52: Osazovací schéma ovládací klávesnice

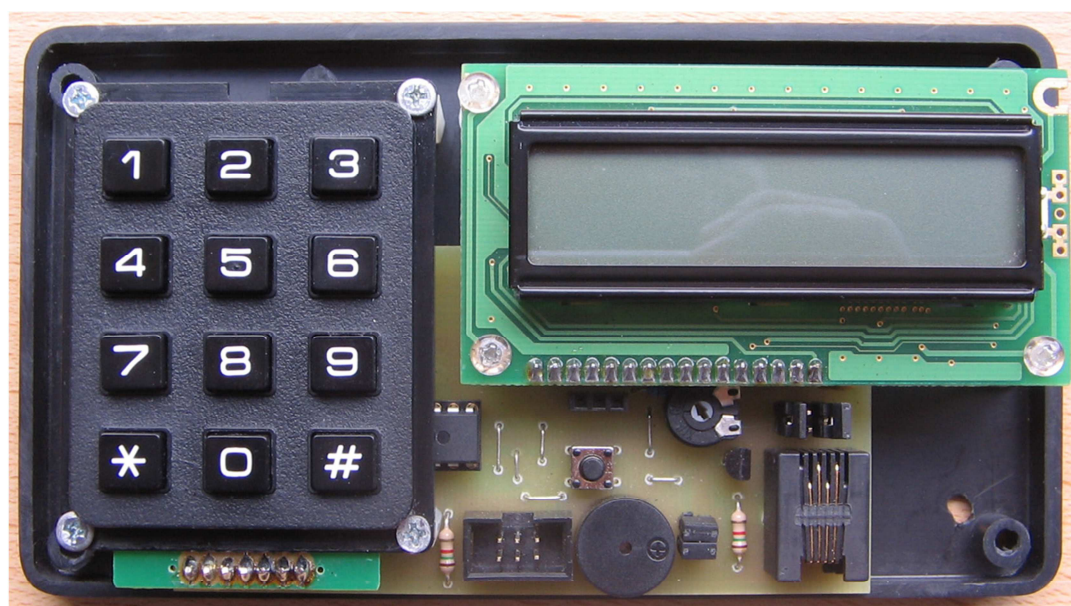


Obrázek 53: Osazovací schéma zálohovaného napájecího zdroje

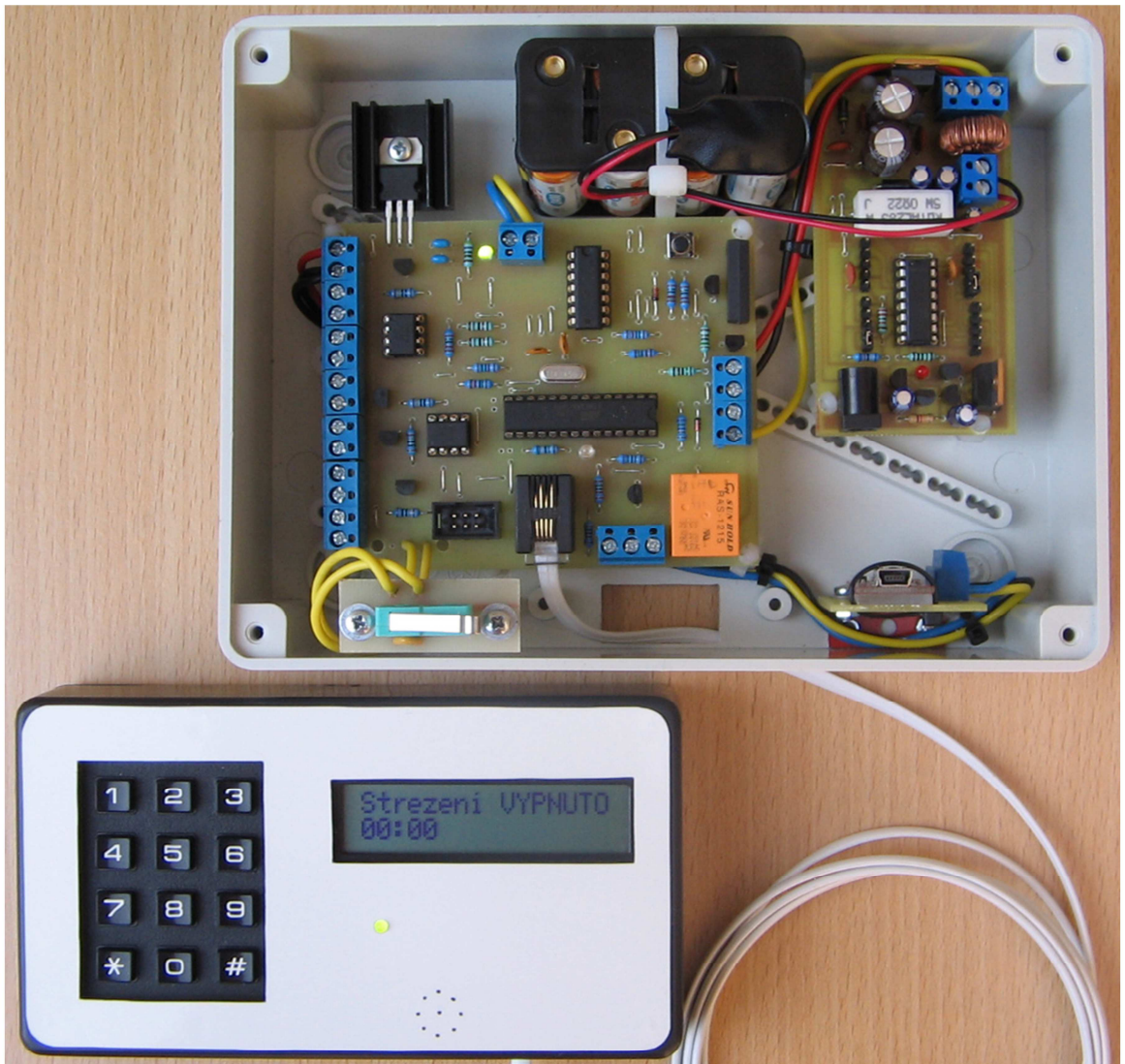
Příloha C: Kompletní zařízení



Obrázek 54: Zabezpečovací jednotka



Obrázek 55: Ovládací klávesnice



Obrázek 56: Obě zařízení