Vysoká škola Báňská – Technická univerzita Ostrava
Fakulta strojní
Katedra automatizační techniky a řízení

Návrh zabezpečovacího systému na bázi mikroprocesorů PIC

Design of security system based on microprocessors PIC

Student: Bc. Tomáš Pawlenka
Vedoucí práce: doc. Ing. Jaromír Škuta, Ph.D.

Ostrava 2017

Anotace

PAWLENKA, T. *Návrh zabezpečovacího systému na bázi mikroprocesorů PIC:* Diplomová práce. Ostrava: VŠB – Technická univerzita Ostrava, Fakulta strojní, Katedra automatizační techniky a řízení, 2017, Vedoucí práce: Škuta, J.

Práce se zabývá návrhem a realizací zabezpečovacího systému na bázi mikroprocesoru PIC firmy Microchip. Systém je tvořen senzorovými moduly pro detekci neoprávněného vstupu na bázi magnetického kontaktu, oxidu uhelnatého, pohybu, teploty a vlhkosti. Dále obsahuje řídicí jednotku, ovládací panel a vývojovou desku Arduino s ethernet rozhraním pro webový server.

Hlavním prvkem systému je centrální řídicí jednotka, která řídí a zprostředkovává veškerou komunikaci mezi jednotlivými moduly. Jejím úkolem je sbírat měřená data ze senzorových modulů a poskytovat je uživateli prostřednictvím ovládacího panelu a webového serveru. Také vyhodnocuje alarmové stavy z příchozích dat a poslouchá příkazy pro aktivaci a deaktivaci z webového serveru a ovládacího panelu. Komunikaci se senzorovými moduly a ovládacím panelem zajišťuje sběrnice RS-485. Pro komunikaci s rozhraním webového serveru je využit standard RS232. K vytvoření a programování vnitřních algoritmů byl využit programovací jazyk C a k realizaci webové aplikace byla využita technologie AJAX, která na stránce obnovuje pouze příchozí data bez nutnosti aktualizace ve webovém prohlížeči.

Klíčová slova: mikroprocesor PIC, zabezpečovací systém, komunikace, senzory inteligentní domácnosti

Obsah

1 Úvod

V dnešním světě se stále více rozvíjí a klade důraz na automatizaci, a to nejen v oblasti průmyslu, ale také v domácnostech. Takovým domácnostem se říká inteligentní a mezi hlavní přednosti těchto domácností patří kvalitní inteligentní zabezpečovací systém s velkou variací různých snímačů, např. pohybové, magnetické, teplotní, protipožární apod. Použití zabezpečovacích systémů se však neomezuje pouze na domácnosti, ale také různé průmyslové a veřejné objekty. Práce se tedy zabývá návrhem a realizací inteligentního zabezpečovacího systému s využitím mikroprocesorů řady PIC. Práce začíná samotným návrhem zabezpečovacího systému, což zahrnuje volbu snímačů, konkrétních typů jednočipových počítačů PIC dle zvolených kritérií a volbu komunikačního rozhraní. Kapitolu uzavírá návrh struktury zabezpečovacího systému. V další kapitole bude popsán komunikační protokol průmyslové sběrnice RS-485, návrh a realizace hlavní řídicí jednotky včetně řídicího algoritmu. Dále bude rozebrán návrh a realizace ovládacího panelu a dílčích modulů se zvolenými typy snímačů. Poslední kapitola se zabývá návrhem rozhraní pro vzdálený přístup uživatele k měřeným veličinám a stavům zabezpečovacího systému prostřednictvím Arduino webového serveru.

2 Návrh zabezpečovacího systému

Prvním krokem v návrhu zabezpečovacího systému je ujasnění, co vše má zabezpečovací systém obsahovat. Hlavními prvky zabezpečovacího systému jsou snímače. Systém by měl zabezpečit nejen neoprávněný vstup do hlídaného objektu, ale také by měl sledovat události uvnitř tohoto objektu. Neoprávněné vniknutí lze sledovat pohybovými senzory nebo také magnety, které mohou kontrolovat otevření dveří a oken. Jako další událost uvnitř objektu lze označit například vznik požáru, který lze kontrolovat teplotními snímači a detektory kouře, nebo prasklé vodovodní potrubí, což je možné indikovat pomocí senzorů vlhkosti. Dále by měl zabezpečovací systém obsahovat prvky, které mají sbírat a zpracovávat data o měřených veličinách a stavech a poskytovat je hlavnímu řídicímu prvku, který veškerá data zpracuje a vyhodnotí alarmové stavy. Těmito prvky budou tedy jednočipové počítače PIC a bude tedy nutno zvolit konkrétní typy tak, aby vyhovovaly daným kritériím. Moderní zabezpečovací systémy jsou také schopny údaje o měřených veličinách a hlídaných stavech poskytovat uživateli vzdáleně s využitím mobilních technologií, což může být realizováno například pomocí webového serveru.

2.1 Snímače zabezpečovacího systému

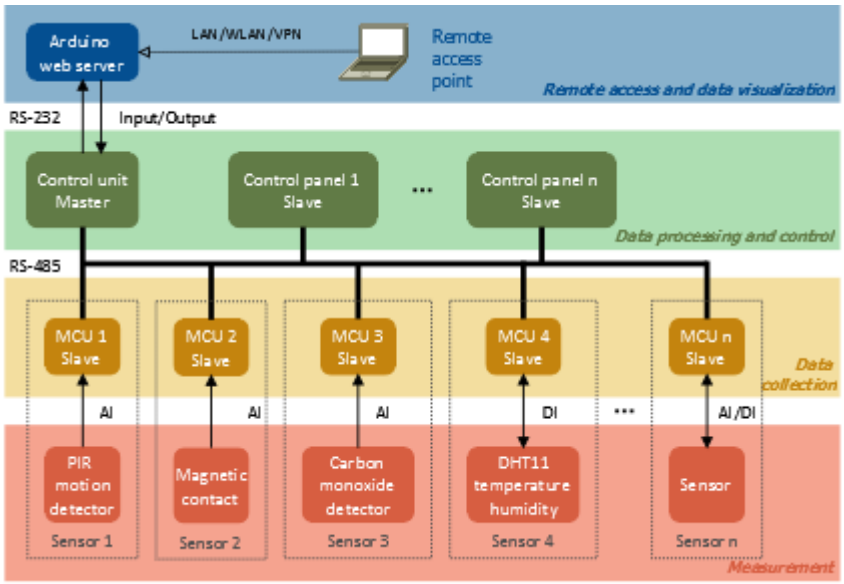
Pro detekci pohybu byl zvolen senzor PIR s označením SB00322A-1. Pro detekci oxidu uhelnatého byl zvolen inteligentní snímač MQ-9. Dále byl zvolen modul DHT11 s digitálním výstupem pro měření teploty a vlhkosti a pro hlídání dveří a oken lze využít jazýčkový kontakt P-MK472.

2.2 Návrh komunikace

Jelikož zabezpečovací systém obsahovat hlavní mikroprocesor, který bude komunikovat s mikroprocesory zpracovávající data z jednotlivých snímačů, bude se jednat o komunikaci typu Master – Slave. Komunikace by také neměla být omezená vzdáleností. Hlídaným objektem totiž nemusí být jen domácnost, ale také rozsáhlý objekt. Těmto kritériím vyhovuje průmyslová sběrnice RS-485 a bude tedy využita pro komunikaci mezi mikroprocesory PIC.

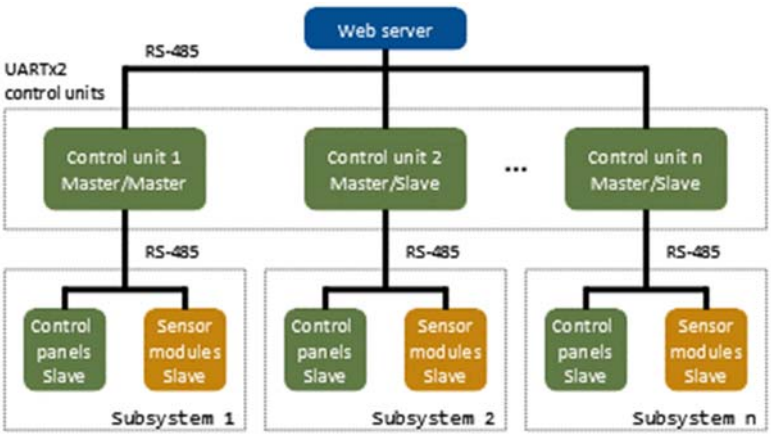
2.3 Struktura zabezpečovacího systému

Strukturu zabezpečovacího systému lze rozdělit do několika úrovní – měření dat, sběr dat, zpracování dat a řízení a vzdálený přístup a vizualizace dat. Na nejnižší úrovni měření jsou jednotlivé snímače systému, které poskytují data buď analogově nebo digitálně mikroprocesorům na úrovni sběru dat. Snímač na úrovni měření a mikroprocesor na úrovni sběru dat dohromady tvoří senzorový modul, který je přizpůsoben k poskytování dat řídicí jednotce na vyžádání v rámci průmyslové sběrnice RS-485, která tedy tvoří rozhraní mezi úrovní pro sběr dat a úrovní pro zpracování dat a řízení. Řídicí jednotka tedy zpracovává tyto data a vyhodnocuje alarmové stavy, dále tyto data poskytuje ovládacím panelům, které jsou na stejné úrovni, a také webovému serveru, který je o úroveň výše. Ovládací panely ovšem neslouží pouze pro příjem dat, ale také posílají data obsahující různé příkazy zpět řídicí jednotce. Stejně je tomu u webového serveru. Komunikační rozhraní mezi řídicí jednotkou a webovým serverem je tvořeno sériovou linkou RS232 a TTL logikou.



Obr. 1 Blokové schéma zabezpečovacího systému

Takto navržené řešení je vhodné pro menší komplexy či domácnosti, jelikož na sběrnici RS-485 lze napojit maximálně 32 zařízení bez opakovače. Pro rozsáhlejší aplikace by bylo možné využít tento návrh jako jeden subsystém z mnoha, kde však rozhraní RS232 a TTL nahradíme další sběrnicí RS485, na které by byly napojeny řídicí jednotky všech subsystémů a webový server.



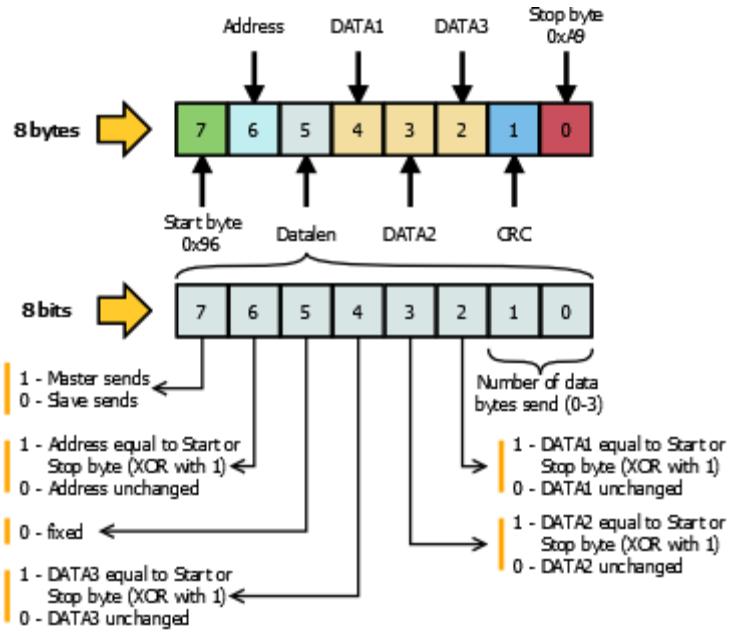
Obr. 2 Rozsáhlejší aplikace

3 Realizace zabezpečovacího systému

Zabezpečovací systém obsahuje hlavní řídicí jednotku s mikroprocesorem PIC18F46K80, který má za úkol sbírat a zpracovávat data z ostatních mikroprocesorů PIC16F88 a PIC12F1840, na které jsou přímo napojeny senzory. Dále obsahuje ovládací panel na bázi mikroprocesoru PIC18F452. Pro všechny tyto mikroprocesory je nutné vytvořit programy tak, aby byla mezi nimi zajištěna bezproblémová komunikace.

3.1 Protokol sběrnice RS-485

Pro realizaci průmyslové sběrnice RS-485 je nutno do obvodu zakomponovat integrovaný obvod LTC485, což je nízkonapěťový přijímač pro sběrnice RS-422/RS-485. Pro programování mikroprocesorů zabezpečovacího systému je používáno vývojové prostředí MikroC PRO for PIC, které má implementovánu knihovnu pro komunikaci s využitím sběrnice RS-485. Tato knihovna má jasně stanovený protokol pro komunikaci.

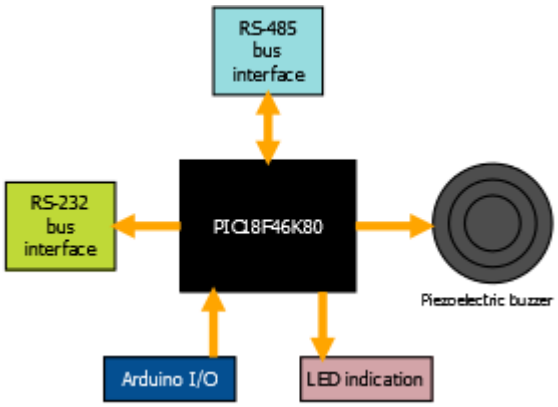


Obr. 3 Komunikační protokol sběrnice RS-485, (MikroElektronika, 1998)

Komunikace je zahájena vysláním start bytu, který má hodnotu 0x96. Další byte obsahuje cílovou adresu zařízení, na které jsou zasílána data. Následující byte obsahuje informaci o tom, zda posílá data Master nebo Slave. Také obsahuje informace o změně posílaných dat a adresy v případě, že dojde k rovnosti se start bytem nebo stop bytem. Konkrétně je zde v případě rovnosti prováděn XOR s hodnotou 1. V dalším kroku jsou zasílány samotná data ve 3 bytech a pak následuje byte s kontrolním součtem CRC. Nakonec je vyslán stop byte s hodnotou 0xA9, (MikroElektronika, 1998).

3.2 Hlavní řídicí jednotka

Jako procesor hlavní řídicí jednotky byl zvolen PIC18F46K80. Úkolem hlavní řídicí jednotky je vyžadovat data ze senzorových modulů na průmyslové sběrnici RS-485, tyto data zpracovat a následně vyhodnotit alarmové stavy. Dále má za úkol zpracované data posílat do ovládacího panelu a na zařízení, které zprostředkovává webový server, aby data mohla být poskytnuta uživateli. Z ovládacího panelu a webového serveru následně přijímá informace o tom, zda byl systém aktivován či deaktivován. Z ovládacího panelu dále přijímá zprávy, které obsahují nové heslo v případě, že bylo uživatelem změněno.



Obr. 4 Zjednodušené schéma hlavní řídicí jednotky

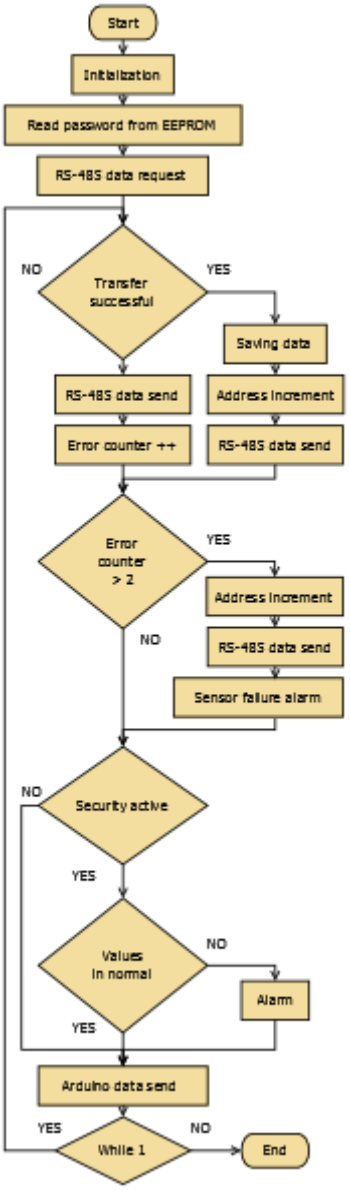
Hlavní řídicí jednotka tedy obsahuje kromě řídicího mikroprocesoru také rozhraní průmyslové sběrnice RS-485 pro komunikaci s ostatními senzorovými moduly a ovládacím panelem, dále rozhraní RS232 pro posílání dat na Arduino web server, LED indikaci pro příjem a vysílání dat, chybný paket a vypršení limitu pro příjem zprávy. Dále obsahuje piezoelektrickou sirénu, která slouží jako indikace alarmového stavu a konektory pro připojení vodičů z vývojové desky Arduino.

3.2.1 Návrh řídicího algoritmu

Před zahájením tvorby algoritmu je nutné si uvědomit, že zabezpečovací systém je založen na měření veličin v reálném čase. Proto algoritmus musí běžet pořád dokola bez ohledu na to, zda byla či nebyla provedena nějaké interakce, nebo zda se vyskytla nějaká chyba. Program se tedy nesmí za žádných okolností zastavit, což znamená, že hlavní řídicí smyčka by měla být z hlediska časového co nejkratší a nesmí obsahovat žádné prodlevy.

Hlavní cyklus programu by měl být tvořen postupným zasíláním požadavků na data na všechny senzorové moduly na sběrnici a dále obsahovat větev, která se provede v případě, že zabezpečovací systém není aktivovaný a větev, která se provede v případě, že aktivovaný je.

Program tedy začíná inicializací, pokračuje vyčtením hesla z paměti EEPROM, po kterém okamžitě posílá požadavek na data na první adresu. Jestliže přenos dat proběhl úspěšně, data jsou uložena, adresa je inkrementována a je odeslán požadavek s daty na adresu novou. V případě neúspěšného přenosu je požadavek vyslán znovu na stejnou adresu. Jestliže přenos není úspěšný dvakrát za sebou, adresa je zvýšena a jsou posílána data na novou adresu a zároveň se spustí alarm z důvodu selhání senzoru. Dále následuje větev sledování veličin systému v případě, že je systém aktivní. Jakmile některá z veličin překročí svou limitní hodnotu, je spuštěn alarm. Posledním důležitým krokem v programu je zaslání dat Arduino web serveru.



Obr. 5 Zjednodušený vývojový diagram

3.2.2 Popis zdrojového kódu programu

Program začíná deklarací a definicí proměnných, inicializací PWM modulace, dále nastavením registrů mikroprocesoru, inicializací obou modulů sériové linky a nastavením mikroprocesoru jako „Master“ sběrnice RS-485, inicializací bufferu pro posílání dat a nastavením registrů přerušení například pro příjem a vysílání. Po inicializaci a nastavení je vyslán první požadavek na data na sběrnici RS-485. Funkci, který tento požadavek zprostředkovává byl předán buffer pro přenos dat, dále parametr, který určuje kolik bytů se má poslat a adresa cílového Slave zařízení. Pro zjednodušení přenosu byl zvolen počet bytů 3 a adresa má inicializační hodnotu 160.

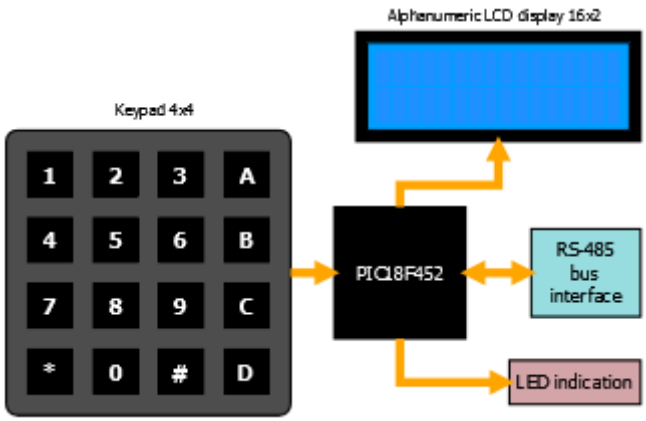
Následuje nekonečný cyklus, a tedy hlavní řídicí smyčka zabezpečovacího systému. Nejprve je testováno, zda je na pozici 5 bufferu logická jednička, což znamená, že při přenosu dat došlo k chybě a požadavek na data je vyslán znovu na stejnou adresu. Pokud k chybě nedošlo pak je splněna podmínka logické jedničky na pozici 4 bufferu. Tato větev obsahuje switch, který dle aktuální adresy ukládá příchozí data do patřičných proměnných. Po uložení je adresa inkrementována a je možno posílat požadavek na adresu novou. K tomu však dochází až po uplynutí nastaveného počtu cyklů. Důvodem je velmi krátká doba jednoho cyklu programu. Při posílání dat v každém cyklu by tedy došlo k zahlcení sběrnice a z hlediska zabezpečovacího systému není potřeba posílat data v řádech milisekund či mikrosekund. Hlavní cyklus programu dále obsahuje sledování napěťové úrovně na vstupech pro aktivaci a deaktivaci systému z webového serveru. Data na webový server jsou posílána po uplynutí poloviny z nastaveného počtu cyklů.

Aby byl zabezpečovací systém spolehlivý a bezpečný, je nutno softwarově ošetřit poruchové stavy. Může dojít například k výpadku jednoho senzorového modulu. Proto je zde tedy čítač chyb a podmínka, která se provede, dojde-li k chybě přenosu opakovaně. V tom případě je posílán požadavek na jinou adresu, ale zároveň je spuštěn alarmový stav selhání senzoru.

Hlavní smyčka obsahuje kromě obsluhy sběrnice také větev, která sleduje hodnoty měřených veličin a dle nastavených limitů vyhodnocuje alarmové stavy.

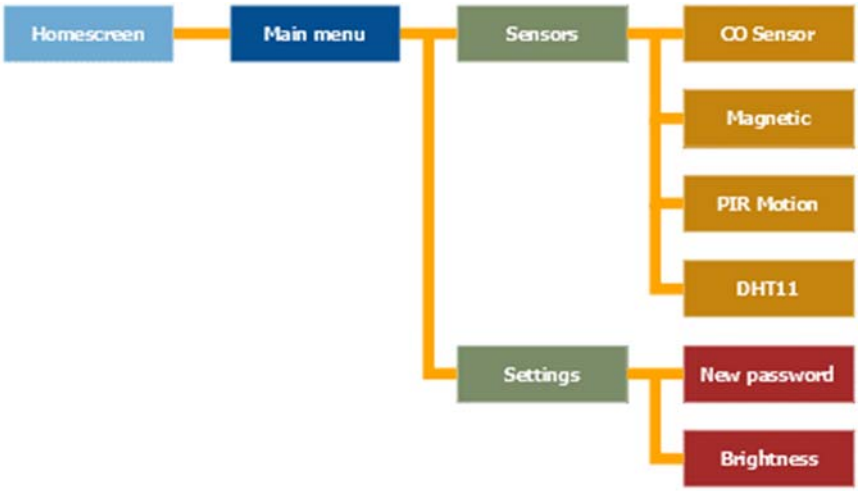
3.1 Ovládací panel

Jako procesor ovládacího panelu byl zvolen PIC18F452. Úkolem ovládacího panelu je zprostředkovat rozhraní pro komunikaci s uživatelem pomocí LCD a klávesnice. Uživatel tak může s využitím rozhraní sledovat nejen měřené veličiny systému, ale také zabezpečovací systém aktivovat a deaktivovat. Mezi další funkce ovládacího panelu patří možnost zvýšení či snížení intenzity podsvícení LCD a také změny hesla.



Obr. 6 Zjednodušené blokové schéma ovládacího panelu

Uživatelské rozhraní, které je zobrazováno na LCD a ovládáno pomocí klávesnice je rozděleno na jednotlivé sekce připomínající stromovou strukturu.



Obr. 7 Struktura uživatelského rozhraní

Po zapnutí systému se objeví na LCD úvodní obrazovka, která odkazuje na další možnosti interakce se systémem. Pro otevření menu je nutno zmáčknout na klávesnici hvězdičku. Menu obsahuje položky, které odkazují na data ze senzorů a do nastavení zabezpečovacího systému. Pro přístup do nastavení je nutno kurzorem, který je posouván pomocí kláves „2“ a „8“, najet na příslušnou položku a potvrdit vstup hvězdičkou. Pro přístup do nastavení je nutno zadat přístupové heslo. Jakmile je heslo zadáno správně, objeví se položky nastavení, které umožňují nastavit heslo nové nebo intenzitu podsvícení LCD.

Každá sekce uživatelského rozhraní představuje proceduru, kterou lze rozdělit do pěti částí. První částí je deklarace proměnných. Druhá část stanovuje rozsah nebo počet řádků aktuální sekce. Třetí část překresluje LCD v případě, že došlo k prvotnímu přechodu do sekce nebo například ke změně pozice kurzoru. Čtvrtá část funkce zachycuje odezvu uživatele v podobě stisknutí určitého znaku klávesnice, který ukládá do proměnné pro tento účel a přiřazuje mu konkrétní číselnou hodnotu znaku dle ASCII tabulky. V poslední páté části dochází k reakci na tuto odezvu.

Nastavení podsvícení LCD je realizováno s využitím pulzně šířkové modulace PWM.

Pro změnu přístupového hesla do systému byla vytvořena funkce, která ukládá příchozí zadané číselné hodnoty do pole. Jakmile pole obsahuje čtyři hodnoty, přidá se na konec pole zakončovací nula, aby byl řetězec kompletní a následně je využita řetězcová funkce strcpy(), která aktuální heslo ve formě řetězce překopíruje zadaným heslem. Poté se nastaví proměnná, která indikuje změnu hesla, na hodnotu TRUE, což způsobí platnost podmínky v hlavním cyklu programu a odeslání nového hesla do řídicí jednotky, která si nové heslo uloží do paměti EEPROM.

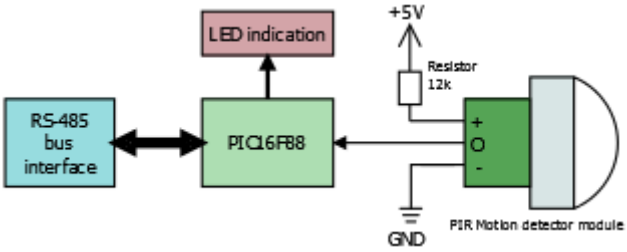
K aktivaci zabezpečovacího systému v módu plného zabezpečení dojde při stisku klávesy „A“, což lze pouze nacházíme-li se v sekci úvodní obrazovky. Následně se spustí čekací smyčka s nastaveným časem. Na obrazovce se objeví odpočet a uživatel tedy musí hlídaný objekt do uplynutí tohoto času opustit. Systém je od této chvíle zakódován. Funkce, která zajišťuje zabezpečení, hlídá alarmové stavy a také vstup klávesnice. K dekódovací proceduře dojde v případě aktivace pohybového snímače, který má pod dohledem dekódovací panel. V případě, že dekódovací panel není pod dohledem žádného

senzoru, dojde k dekódovací proceduře po stisku libovolné klávesy. K okamžitému spuštění alarmu dojde například při překročení limitní hodnoty oxidu uhličitého.

Dekódovací procedura zahrnuje časový odpočet, během kterého uživatel musí zadat dekódovací heslo a potvrdit jej hvězdičkou. Jestliže uživatel zadá špatné heslo a potvrdí ho, dojde ke spuštění alarmu. Pokud zadá heslo špatně, ale uvědomí si svou chybu před jeho potvrzením, lze zadaný řetězec anulovat bez spuštění alarmu stisknutím mřížky a zadat heslo znovu.

3.2 Modul s detektorem pohybu

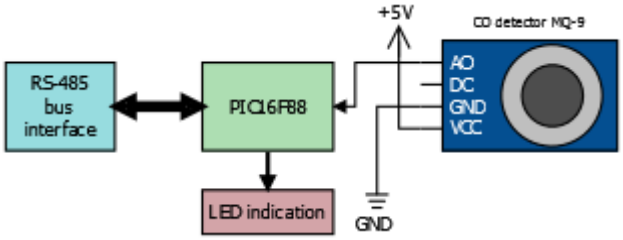
Pro modul s detektorem pohybu PIR byl zvolen jednočipový mikropočítač typu PIC16F88. Je vybaven rozhraním USART a je možno jej tedy v této aplikaci použít pro připojení k průmyslové sběrnici RS-485. Mikroprocesor čte stavy logické 1 a 0 na výstupu senzoru PIR a tyto stavy jsou indikovány pomocí LED diody. K odeslání aktuálního stavu dochází po přijetí požadavku od hlavního řídicího modulu na sběrnici.



Obr. 8 Zjednodušené schéma zapojení PIR detektoru

3.3 Modul s detektorem oxidu uhelnatého

Pro tento modul byl zvolen stejný typ mikroprocesoru jako u PIR modulu a to PIC16F88. Jelikož je výstup snímače analogový, je nutné jej připojit na kanál mikroprocesoru, který umožňuje A/D konverzi. Výsledkem konverze je číselný údaj, který představuje koncentraci oxidu uhelnatého.

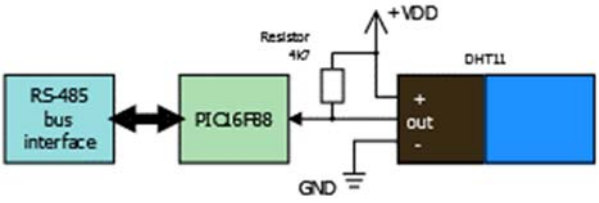


Obr. 9 Zjednodušené schéma zapojení detektoru oxidu uhelnatého

3.4 Modul s měřením teploty a vlhkosti

Jelikož je snahou vytvořit inteligentní zabezpečovací systém, který může mít uplatnění i v domácnostech, nemusí být měřeny a hlídány pouze stavy související se zabezpečením. Příkladem může být měření pokojové teploty a vlhkosti.

Pro aplikaci byl zvolen senzor DHT11, který měří vlhkost a teplotu zároveň. Jedná se o senzor se speciálním protokolem, který využívá jeden datový vodič, (UUGear 2014).



Obr. 10 Zjednodušené schéma zapojení senzoru DHT11

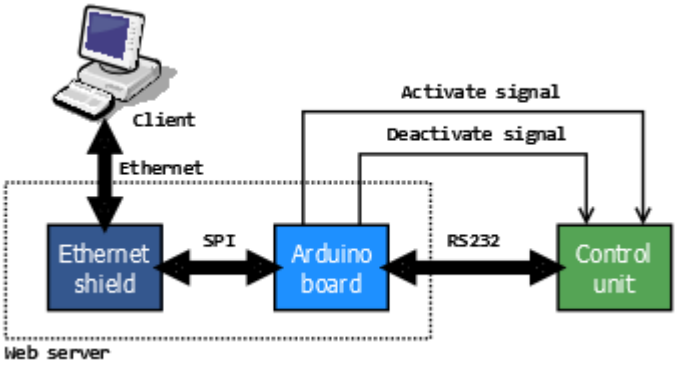
4 Návrh rozhraní pro realizaci webového serveru

Moderní zabezpečovací systém by měl umožnit uživateli sledovat data s využitím mobilních zařízení, případně systém ovládat vzdáleně. K tomu lze využít například připojení zabezpečovacího systému do sítě LAN. Uživatel by tak mohl mít přehled o dění zabezpečovacího systému mimo hlídaný objekt, za předpokladu zřízeného VPN připojení.

Pro sledování měřených veličin a stavů je nutno vytvořit webový server. K jeho vytvoření je možné využít ethernet nástavbu pro vývojové desky Arduino. Tato nástavba s vývojovou deskou komunikuje pomocí SPI rozhraní.

Cílem webového serveru je tedy vizualizace dat zabezpečovacího systému, které představují například data ze senzorů či alarmové stavy. V rámci vzdáleného ovládání bude cílem systém buď aktivovat nebo deaktivovat po zadání hesla.

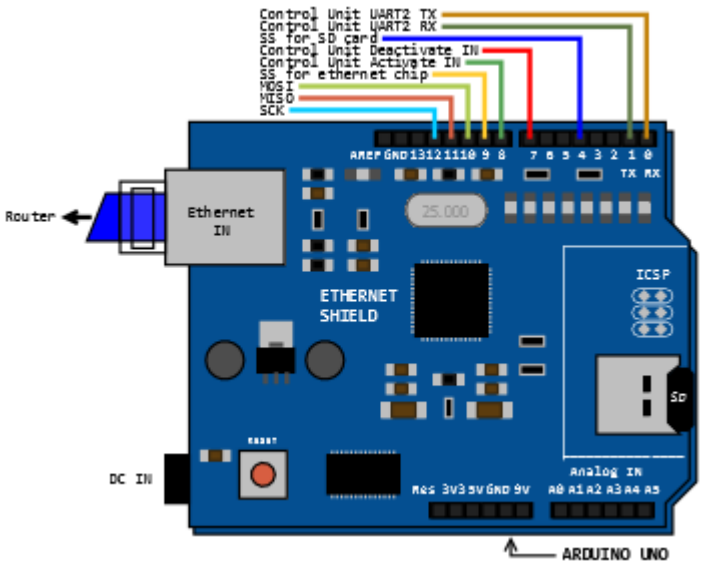
Pro vytvoření webového serveru prostřednictvím ethernet modulu je využita vývojová deska Arduino UNO. Ta přijímá data o zabezpečovacím systému z hlavního master mikroprocesoru řídicí jednotky a poskytuje je dále skrze vytvořený webový server připojenému klientovi. Ke komunikaci řídicí jednotky systému s vývojovou deskou Arduino byla navržena sériová linka RS232. K urychlení aktivace a deaktivace zabezpečovacího systému jsou vedeny signály zvlášť mimo sériovou linku, které představují logické úrovně 1 a 0.



Obr. 11 Blokové schéma realizace webového serveru

4.1 Popis hardwaru a zapojení

Tato kapitola se zabývá popisem hardwaru pro realizaci webového serveru. Arduino UNO je vývojová deska od stejnojmenné firmy, která pracuje na bázi mikroprocesoru ATMega328. Dalším zařízením je Arduino ethernet shield, což je ethernet nástavba pro vývojovou desku UNO. Obsahuje konektor RJ45 pro připojení do sítě a také kapsu pro vložení karty SD micro. Využívá digitální piny 10 až 13 pro komunikaci prostřednictvím SPI rozhraní a pin 4 je využíván SD kartou, ostatní piny jen prodlužuje, (Arduino 2017).



Obr. 12 Arduino UNO s ethernet nástavbou a popis použitých datových I/O

4.2 Realizace webového serveru

Realizace webového serveru spočívá ve vytvoření programu pro vývojovou desku Arduino UNO a dále ve vytvoření webové stránky, kterou je nutno nahrát na kartu mikro SD ethernet modulu. K vytvoření webového serveru byly zvoleny technologie HTML5, CSS a AJAX.

AJAX (Asynchronní JavaScript a XML) je technologie, která umožňuje zobrazovat data webového serveru na webové stránce bez nutnosti aktualizace celé stránky ve webovém prohlížeči. Využívá kombinaci vestavěného objektu XMLHttpRequest webového prohlížeče na vyžádání dat z webového serveru, JavaScriptu a HTML DOM, (W3Schools c1999-2017).

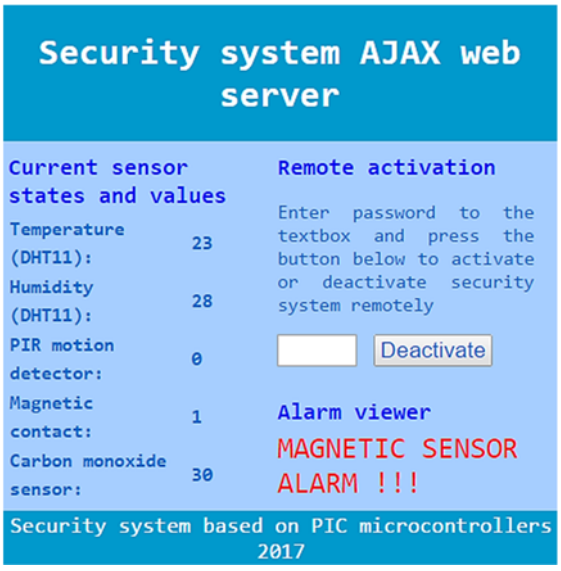
K vytvoření webové stránky byl využit značkovací jazyk ve verzi HTML5 a její vzhled byl upraven technologií CSS.

4.3 Popis vytvořené webové aplikace

Výsledná webová aplikace se skládá ze tří bloků, které slouží pro sledování stavů a měřených veličin, vzdálenou aktivaci a deaktivaci systému a sledování aktuálních alarmů.

Pro aktivaci nebo deaktivaci je zde umístěno textové pole, do kterého je nutno zapsat čtyřmístné heslo a následně zmáčknout tlačítko pro potvrzení aktivace či deaktivace.

Webová aplikace je také responsivní. Přizpůsobuje se dle rozlišení displeje daného zařízení. Je tedy dobře čitelná a ovladatelná i na mobilních telefonech a tabletech.



Obr. 13 Ukázka výsledné webové aplikace

5 Závěr

Práce na vývoji zabezpečovacího systému na bázi mikroprocesorů PIC vyžadovala úvodní seznámení s těmito jednočipovými počítači, jejich architekturou, typovými řadami, technickými parametry a také s možnostmi jejich programování.

Systémový návrh zabezpečovacího systému započal úvodním slovem, kde bylo nutno zamyslet se nad tím, co by měl zabezpečovací systém zahrnovat. Nyní bylo možno zahájit samotný návrh volbou vhodných komponent a komunikačního rozhraní. Vznikla tak výsledná hierarchická struktura zabezpečovacího systému rozdělená do několika úrovní dle činností, které jsou úkolem prvků dané úrovně.

Samotná realizace zahrnovala popis komunikačního protokolu RS-485. Dále byl navržen modul hlavní řídicí jednotky, ovládacího panelu a také dílčí senzorové moduly. komunikace. Jelikož o veškerou komunikaci na sběrnici se stará hlavní řídicí jednotka, byl navržen řídicí algoritmus s využitím vývojových diagramů. Následně bylo možné tyto moduly realizovat a sestavit model zabezpečovacího systému.

Dále bylo možné pomýšlet na další rozšíření, konkrétně ovládání a poskytování údajů o měřených veličinách a stavech uživateli vzdáleně. K tomu byla využita vývojovou desku Arduino, která prostřednictvím ethernet nástavby vytvořila webový server, ke kterému je možné se připojit prostřednictvím webového prohlížeče na jiném zařízení v síti. Rozhraním mezi uživatelem a zabezpečovacím systémem je tedy webová stránka, která umožňuje nejen sledovat měřené veličiny a stavy zabezpečovacího systému, ale také obsahuje tlačítko pro aktivaci a deaktivaci systému po zadání hesla. Dále obsahuje pole, které v případě alarmového stavu vypíše, o jaký typ alarmu se jedná.

Jako směr dalšího řešení lze navrhnout například rozšíření zabezpečovacího systému o modul GSM, který by v případě alarmového stavu kontaktoval uživatele prostřednictvím mobilního telefonu.

Závěrem lze poznamenat, že práce na toto téma byla velmi zajímavá. Zabezpečovací systém lze snadno rozšířit o další moduly se snímači, kterých je na trhu spousta a z hlediska jednočipových počítačů také není nutné omezovat se pouze na řadu PIC. Zabezpečovací systém je tedy multiplatformní.

6 Použitá literatura

Arduino [online]. Ivrea: Arduino, c2017 [cit. 2017-04-14]. Dostupné z: https://www.arduino.cc/

DHT11 Humidity & Temperature Sensor Module. *UUGear* [online]. Praha: UUGear s.r.o., 2014 [cit. 2016-06-12]. Dostupné z: http://www.uugear.com/portfolio/dht11-humidity-temperature-sensor-module/

MikroElektronika [online]. Bělehrad: MikroElektronika, 1998 [cit. 2017-02-01]. Dostupné z: https://www.mikroe.com/

W3Schools Online Web Tutorials [online]. W3.CSS, c1999-2017 [cit. 2017-04-14]. Dostupné z: https://www.w3schools.com/