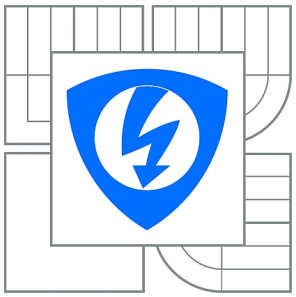


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MODUL ELEKTRICKÉ ZABEZPEČOVACÍ ÚSTŘEDNY S KOMUNIKÁTOREM ETHERNET

MODULE OF ELECTRONIC SECURITY CENTRAL WITH ETHERNET COMMUNICATOR

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

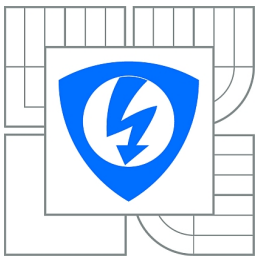
AUTOR PRÁCE — Bc. IVO STRAŠIL

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. KAREL BURDA, CSc.

SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Ivo Strašil	***ID:***	78418
Ročník:	2	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Modul elektrické zabezpečovací ústředny s komunikátorem Ethernet

POKYNY PRO VYPRACOVÁNÍ:

Stručně popište problematiku ústředen elektrické zabezpečovací signalizace (EZS). Na tomto základě navrhněte koncepci a obvodové řešení malé modulární elektrické zabezpečovací ústředny s důrazem na možnost propojení ústředny s počítačovou sítí typu Ethernet. Svůj návrh prakticky zrealizujte a ověřte.

DOPORUČENÁ LITERATURA:

[1] Martin T.: The Insider's Guide To The Philips ARM 7 Based Microcontrollers. Hitex, Coventry 2006.
[2] Křeček S. a kol.: Příručka zabezpečovací techniky. Blatenská tiskárna, Blatná 2003.

Termín zadání:	29.1.2010	***Termín odevzdání:***	26.5.2010

Vedoucí práce: doc. Ing. Karel Burda, CSc.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

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

ABSTRAKT

Diplomová práce se zabývá návrhem ústředny elektrické zabezpečovací signalizace, vybavené rozhraním Ethernet.

Jsou rozebrána současná řešení ústředen elektrické zabezpečovací signalizace a současné způsoby využití komunikace pomocí standardů Ethernet, resp. TCP/IP, v zabezpečovací technice. Na základě ekonomické rozvahy byla následně zavržena možnost přímého připojování čidel EZS do sítě Ethernet.

Pro dosažení co nejvyšší flexibility řešení byla zvolena nová koncepce ústředny elektrické zabezpečovací signalizace s volně programovatelným chováním pomocí sady skriptů v jazyce C, schopné samostatné práce i spolupráce více zařízení v síti LAN, kdy je funkce jednotlivých ústředen koordinována softwarově realizovanou nadřazenou ústřednou.

Ústředna uvedené koncepce byla realizována a její funkce byla úspěšně odzkoušena.

ABSTRACT

This diploma thesis deals with a design of a burglar alarm control panel, equipped with an Ethernet interface.

The thesis contains a discusson of present solutions of control panels and of present usage of Ethernet communication. An idea of sensors, directly connected to LAN, was discarded on basis of a component price survey.

Finally, a new concept of the panel has been chosen. This concept allows a free definition of internal logic using a C-like scripting and provides a possibility to create a network of these panels in a LAN network, using a software-only supervising main control panel.

A new control panel following this concept was designed and succesfully tested.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma *Modul elektrické zabezpečovací ústředny s komunikátorem Ethernet* jsem vypracoval samostatně pod vedením vedoucího práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené práce dále prohlašuji, že jsem v souvislosti s vytvořením této práce neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb.,včetně možných trestněprávních důsledků vyplývajících z ustanovení §152 trestního zákona č. 140/1961 Sb.

V Brně dne 22.5.2010 _____

PODĚKOVÁNÍ

Děkuji vedoucímu práce doc. Ing. Karlu Burdovi, za velmi užitečnou pomoc a cenné praktické rady při zpracování této práce.

V Brně dne 22.5.2010 _____

Obsah

Úvod....4
1. Ústředny elektrické zabezpečovací signalizace....5
1.1. Postavení ústředny v systému EZS....5
1.2. Základní typy ústředen....5
1.2.1. Kabelové ústředny....5
1.2.1.1. Smyčková ústředna a smyčky EZS....5
1.2.1.2. Sběrnicové ústředny....8
1.2.2. Smíšené (hybridní) ústředny....9
1.2.3. Bezdrátové ústředny....9
1.3. Komunikační možnosti současných ústředen....10
1.3.1. Rozhraní pro vnější komunikaci....10
1.3.2. Telefonní a GSM komunikátory....10
1.3.2.1. Přenos zpráv uživateli systému....10
1.3.2.2. Datový přenos na PCO....11
Protokol Ademco Contact ID....11
1.3.3. Propojení pomocí sítí standardu IP....11
1.3.3.1. GSM/GPRS systém: Jablotron GSMlink....12
1.3.3.2. Systémy založené na připojení k místní síti LAN....12
1.3.3.3. Protokoly pro spojení s pulty centrální ochrany pomocí sítí IP....13
Protokol IP Contact ID....13
Protokol SIA IP Events Reporting....13
1.3.3.4. Normativní požadavky na komunikátory IP/Ethernet....14
1.3.3.5. Připojení čidel pomocí Ethernet/IP řešení....14
2. Návrh ústředny s komunikátorem Ethernet....16
2.1. Základní koncepce ústředny....16
2.1.1. Požadavky pro samostatný provoz....18
2.1.2. Požadavky pro řízený provoz....20
2.1.3. Požadavky pro využití v systémech domovní automatizace....23
2.2. Obvodové řešení....24
2.2.1. Řídicí obvody....25
2.2.1.1. Architektura ARM7TDMI....26
2.2.1.2. Mikrokontrolér LPC2368....27
2.2.1.3. Skutečné zapojení bloku řízení....29
2.2.2. Obvody komunikace....30
2.2.2.1. Ethernet....30
Obvod PHY....31
Blok MAC....32
2.2.2.2. Sériová asynchronní rozhraní....32
RS-232....32
RS-485....33
2.2.2.3. Rozhraní přídavných modulů....33
2.2.3. Obvody vstupů a výstupů....37
2.2.3.1. Drátové smyčky....37
2.2.3.2. Tranzistorové a reléové výstupy....39
2.2.3.3. Místní servisní ovládání....39
2.2.4. Rozhraní paměťové karty....41
2.2.5. Obvody napájení....42
2.2.5.1. Měnič pro napájení systémem PoE....42
Systém Power over Ethernet....42

Měnič pro napájení systémem PoE....42
2.2.5.2. Měnič napájení logiky systému....43
2.2.5.3. Napájení obvodů příslušenství....44
2.3. Plošný spoj a mechanická konstrukce hlavního modulu ústředny....46
2.3.1. Návrh plošného spoje ústředny....46
2.3.2. Mechanická konstrukce ústředny....46
2.4. Softwarové řešení....47
2.4.1. Přenosy dat sítí Ethernet....48
2.4.1.1. WWW konfigurační a diagnostické rozhraní....48
2.4.1.2. Protokol pro komunikaci s nadřazenou ústřednou....49
2.4.1.3. Zasílání zpráv protokolem UDP....51
2.4.2. Softwarové řešení, použité softwarové moduly....52
2.4.2.1. Operační systém FreeRTOS....52
2.4.2.2. Knihovny IP komunikace uIP....53
2.4.2.3. Kryptografická knihovna....53
2.4.2.4. Souborový systém – knihovna EFSL....53
2.4.2.5. Skriptovací jazyk – interpreter PicoC....53
2.4.3. Struktura software ústředny....54
2.4.3.1. Inicializace zařízení....54
2.4.3.2. Úlohy, běžící v rámci FreeRTOS....55
Úloha komunikace rozhraním Ethernet....55
Vyhodnocení stavu smyček v úloze IOman....56
2.4.3.3. Zajištění spolehlivého běhu zařízení....56
2.4.3.4. Ladění běhu ústředny a skriptů....57
3. Realizace a zkoušky prototypu....58
3.1. Realizace prototypu, použité vývojové prostředky....58
3.2. Výsledky zkoušek a měření na prototypu hlavního ústředny....59
3.2.1. Funkční zkoušky ústředny....59
3.2.2. Měření....59
4. Dodatky....61
4.1. Volba a popis bezdrátové technologie Keeloq....61
Závěr....63
Seznam použité literatury....64
Seznam zkratek a definicí....66
Přílohy....68
A Doplňující informace k programování ústředny skripty....68
A.1.Systémové proměnné ústředny....68
A.2.Funkce a omezení skriptů....70
A.3.Přehled sledovaných událostí a jimi spouštěných skriptů....71
B Ukázky skriptů....72
B.1.Sada skriptů pro základní funkci ústředny....72
B.2.Ukázka autentizace uživatele pomocí RS-485 klávesnice a vzdáleného serveru....74
B.3.Ukázka programování funkcí jednoduché domovní automatizace....75
C WWW rozhraní, obsah paměťové karty....77
C.1.Obsah paměťové karty....77
C.2. Konfigurační soubor ctrl.ini....77
C.3. Ukázky WWW rozhraní....78
D Návrh přídavného modulu bezdrátového přijímače 433 MHz....79
E Obsah přiloženého CD....80

F Rozpiska materiálu....81
G Výkresová dokumentace hlavního modulu ústředny....85

Seznam obrázků

Obr. 1: Zapojení tří aktivních čidel v systému s jednoduše nebo s dvojitě vyváženými smyčkami....6
Obr. 2: Sběrnicová ústředna....8
Obr. 3: Systém s hybridní ústřednou a třemi koncentrátory....9
Obr. 4: Navrhovaná ústředna EZS jako centrální prvek jednoduchého systému....18
Obr. 5: Užití komunikace Ethernet při použití ústředny jako centrálního prvku malé instalace....19
Obr. 6: Struktura bezpečnostní sítě LAN ve velké instalaci....20
Obr. 7: Zapojení navrhované ústředny EZS ve větší instalaci s napájením PoE....21
Obr. 8: Navrhovaná ústředna EZS v roli přístupového systému....22
Obr. 9: Využití podřízené ústředny jako součásti zařízení domovní automatizace....23
Obr. 10: Blokové schéma hardwarového řešení hlavního modulu navrhované ústředny....24
Obr. 11: Zapojení obvodů mikrokontroléru (výřez z celkového schématu zapojení, viz příloha A)....29
Obr. 12: Hardwarová struktura rozhraní Ethernet....30
Obr. 13: Obvody rozhraní Ethernet navržené ústředny....31
Obr. 14: Schéma zapojení obvodů rozhraní RS-232 a RS-485....32
Obr. 15: Zapojení konektoru přídavných modulů na hlavním modulu navrhované ústředny....34
Obr. 16: Princip obvodu drátové smyčky....37
Obr. 17: Zapojení vstupů drátových smyček a výstupů napájení příslušenství....38
Obr. 18: Schéma zapojení obvodů digitálních výstupů....39
Obr. 19: Schéma bloku uživatelského rozhraní a rozhraní SD karty....40
Obr. 20: Schéma zapojení měniče pro napájení PoE....42
Obr. 21: Schéma zapojení měniče 12/3,3 V....43
Obr. 22: Pomocné napájecí obvody....45
Obr. 23: Softwarová struktura navrhované ústředny EZS....47
Obr. 24: Komunikační možnosti navrhované ústředny a jejich zařazení v softwarové struktuře zařízení....48
Obr. 25: Příjem příkazu nebo dotazu z nadřazené ústředny....50
Obr. 26: Odpověď na dotaz nebo příkaz nadřazené ústředny....51
Obr. 27: Graf stavů smyček v závislosti na poměru napětí na vstupní svorce smyčky k napájecímu napětí…56
Obr. 28: Fotografie prototypu ústředny....58
Obr. 29: Užití přenosu Keeloq v zabezpečovací technice a v technice domovní automatizace....61

Seznam tabulek

Tabulka 1: Srovnání cenové a energetické náročnosti rozhraní čidel....15
Tabulka 2: Charakteristiky vybraných mikrokontrolérů. 25
Tabulka 3: Celková kapacita vodiče SDA nebo SCL na jeden připojený přídavný modul....35
Tabulka 4: Přehled událostí a jimi spouštěných skriptů....71
Tabulka 5: Využití systémových proměnných a časovačů....72
Tabulka 6: Využití systémových proměnných a časovačů....76

Úvod

Diplomová práce se zabývá návrhem malé zabezpečovací ústředny, schopné komunikace pomocí IP sítě rozhraním Ethernet.

První část práce uvádí stručný přehled problematiky ústředen elektrické zabezpečovací signalizace se zaměřením na datové komunikační schopnosti těchto zařízení.

V druhé části je představen vlastní návrh zabezpečovací ústředny od koncepce po detailní popis zapojení a softwarového řešení.

Třetí část práce popisuje výsledky, dosažené při realizaci prototypu navržené ústředny.

Koncepce zařízení vychází ze snahy o dosažení co nejuniverzálnějšího a přitom ekonomického řešení. Z tohoto důvodu je logika ústředny definována sadou skriptů, kterou může technik upravit při instalaci zařízení a tím změnit nebo doplnit chování ústředny o další funkce.

Ústředna je navržena tak, aby byla použitelná jak v malých aplikacích, kde je rozhraní Ethernet využito pro dálkový dohled pultem centrální ochrany a případně i pro dálkové ovládání a servis, i ve větších sestavách, kde zařízení slouží jako inteligentní koncentrátor, spojený datovou sítí založenou na standardech IP a Ethernet s nadřazenou softwarovou ústřednou.

1. Ústředny elektrické zabezpečovací signalizace

1.1. Postavení ústředny v systému EZS

Jádro systému elektrické zabezpečovací signalizace tvoří *ústředna*, specializované zařízení, které přijímá signály z čidel (detektorů), na jejichž základě vyhodnocuje narušení objektu a ovládá signalizační zařízení, typicky sirénu nebo zařízení pro dálkový přenos dat na pult centrální ochrany.

Ústředna dále umožňuje oprávněným uživatelům ovládat a nastavovat systém, například jej zastřežit či odstřežit. Ústředna rovněž trvale kontroluje funkční připravenost systému a zajišťuje zálohované napájení všech komponent systému.

1.2. Základní typy ústředen

Publikace [1] a [2] rozdělují ústředny podle způsobu komunikace s ostatními součástmi systému zabezpečovací signalizace. V následující části se přidržíme tohoto rozdělení a doplníme informace o některých konkrétních řešeních.

1.2.1. Kabelové ústředny

Kabelové ústředny jsou propojeny s ostatními komponenty systému, zejména s čidly, pomocí zpravidla metalických kabelů.

1.2.1.1. Smyčková ústředna a smyčky EZS

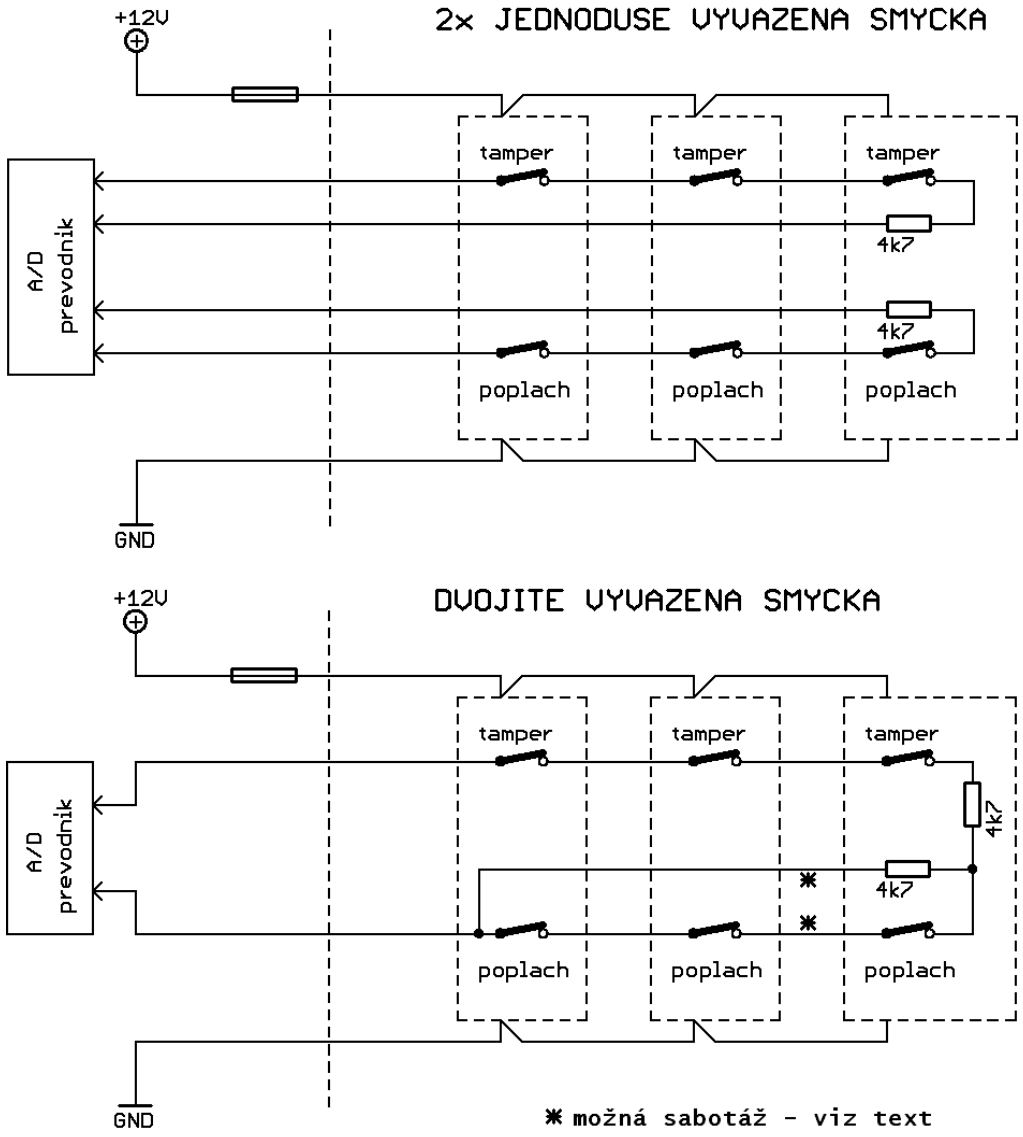
Základním a nejstarším typem kabelové ústředny je *smyčková ústředna*, vyhodnocující stav jedné nebo více *smyček.*

Smyčka je obvod, do kterého je připojeno jedno či více čidel. Podle nastaveného chování ústředny mohou být smyčky *okamžité, zpožděné* či *24 hodinové*. Aktivace *okamžité* smyčky vyvolá v zastřeženém stavu ústředny bezprostředně poplach, zatímco *zpožděná* smyčka vyvolá *předpoplach*, tedy časovou prodlevu před zahájením poplachu, během které může uživatel odstřežit hlídaný prostor. *24 hodinové* smyčky vyvolávají okamžitý poplach i v odstřeženém stavu ústředny, a užívají se například pro připojení tísňových tlačítek či požárních hlásičů.

Koncept smyček také umožňuje rozdělení sledovaného prostoru na více *sekcí (zón),* které mohou být individuálně zastřeženy či odstřeženy.

Technické řešení smyčky kabelové ústředny se postupně vyvíjelo od jednoduché proudové smyčky se sériově zapojenými čidly, přerušujícími v poplachovém stavu obvod.

Zřejmou nevýhodou tohoto zapojení byl snadný útok zkratováním vodičů smyčky v libovolném místě kabeláže, a proto bylo vyvinuto zapojení *jednoduše vyvážené smyčky* (SEOL, *Single End-of-line)*.



Obr. 1: Zapojení tří aktivních čidel v systému s jednoduše nebo s dvojitě vyváženými smyčkami

V tomto zapojení má smyčka, tvořená v klidovém stavu sepnutými výstupními kontakty čidel, definován nenulový odpor zařazením rezistoru do koncového místa smyčky tak, aby zkrat vodičů smyčky v libovolném místě kabeláže způsobil pokles odporu smyčky na nulovou hodnotu.

Ústředna měří odpor smyčky a porovnává jej se známou hodnotou zakončovacího rezistoru. Je-li odpor smyčky výrazně nižší, je smyčka náhodně nebo úmyslně zkratována, je-li odpor smyčky výrazně vyšší, je smyčka přerušena aktivací jednoho z čidel nebo sabotáží.

Jediným místem, kde je možné provést útok zkratováním svorek, jsou připojovací svorkovnice ústředny a čidel, která chráníme *sabotážními spínači*, označovanými také jako *tamper*. Tyto spínače

rozepnou při sejmutí krytu příslušného prvku a umožní zařízení upozornit obsluhu na možné poškození systému. Tento stav musí být možné sledovat i v odstřeženém stavu ústředny, kdy poplachové výstupy čidel spínají podle pohybu osob uvnitř objektu, a proto zřizujeme samostatnou smyčku pro vyhodnocení stavu sabotážních spínačů.

Toto zapojení je uvedeno na obr. 1 spolu s jeho logickou evolucí, zapojením *dvojitě vyvážené smyčky (*DEOL – Double *End-of-line).*

Dvojitě vyvážená smyčka zjednodušuje kabeláž systému tím, že umožňuje rozeznávat hned tři stavy: klidový stav, kdy je v obvodu smyčky zařazen jeden zakončovací rezistor, poplachový stav, kdy jsou v obvodu zařazeny dva zakončovací rezistory v sérii, přerušení smyčky v případě rozepnutí sabotážního spínače nebo přerušení vodičů a zkrat – poruchu či záměrný útok na vedení smyčky.

Zapojení na obr. 1 je odolné i proti ztrátě napájení čidel vlivem přerušení napájecích vodičů nebo přepálením pojistky napájení, jsou-li aktivní čidla osazena v klidu přitaženými výstupními relé. Při přerušení napájení čidla tato relé odpadají, přerušují smyčku a vyvolávají tak poplachový stav.

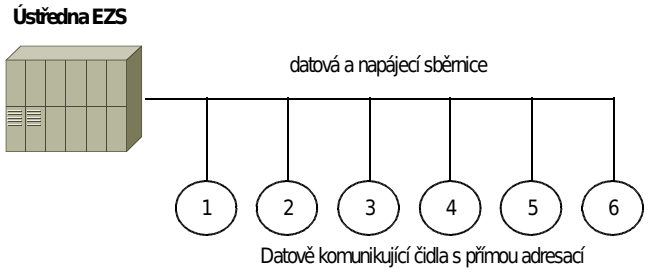
I jednoduše a dvojitě vyvážené smyčky je možné s příslušnými technickými prostředky sabotovat, má-li útočník přístup ke kabeláži.

Například v případě, že ústředna používá měření odporu smyček stálým stejnosměrným proudem a vyhodnocuje-li napětí na smyčce podle Ohmova zákona, může útočník změřit stejnosměrné napětí na vodičích smyčky mezi ústřednou a prvním detektorem a paralelně připojit tvrdý zdroj napětí se stejným svorkovým napětím, čímž bude pro ústřednu simulovat neměnný odpor smyčky bez ohledu na její skutečný stav.

V zapojení dvojitě vyvážené smyčky, uvedeném na obr. 1, může útočník zkratováním bodů, označených hvězdičkou, vyřadit první dvě čidla zleva.

1.2.1.2. Sběrnicové ústředny

Jako *sběrnicová ústředna* nebo také *ústředna s přímou adresací čidel* se označuje ústředna, komunikující s čidly pomocí zvláštní *datové sběrnice*.



Obr. 2: Sběrnicová ústředna

Datová sběrnice je společná pro všechna připojená čidla. Obvykle se užívá standard RS-485 pro svou velkou odolnost proti rušení, nízkou cenu hardwarových prvků, jednoduchou realizaci zapojení (ústředna je se všemi zařízeními na sběrnici spojena paralelně jedním krouceným párem pro přenos dat a jednou dvojicí napájecích vodičů) a dostupné komunikační rychlosti v řádech desítek kb/s na vzdálenosti až několika stovek metrů. Dostupná komunikační rychlost a povolená proudová zátěž datových vodičů sběrnice připojenými prvky omezuje počet připojených zařízení na desítky až stovky, například 127 u ústředen Paradox Digiplex EVO 48 [3].

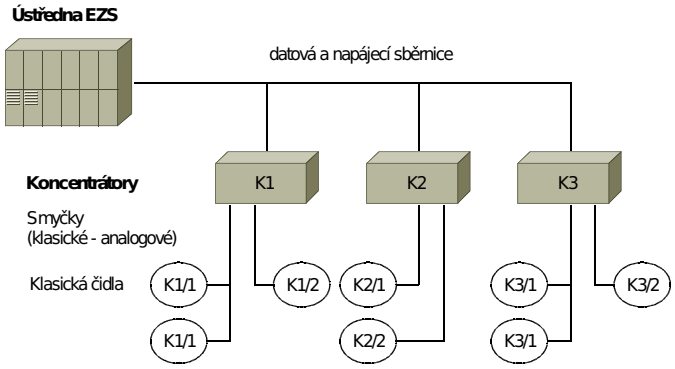
V roli *mastera* sběrnice vystupuje ústředna, která se cyklicky dotazuje připojených čidel na jejich stav.

Každé čidlo má nastavenu unikátní adresu v rámci sběrnice, a tak je možné z tabla ústředny sledovat stav jednotlivých čidel, vyhodnocovat jednoduše falešné poplachy či dálkově nastavovat parametry čidel, pokud tuto funkci podporují.

Výhodou řešení je velká odolnost proti překonání, protože veškerý přenos dat mezi ústřednou a čidly je datový a není možné jednoduchými prostředky přemostit připojenou soustavu čidel.

Naopak nevýhodou sběrnicových ústředen je nutnost užití speciálních čidel, schopných komunikovat se zvolenou ústřednou, která jsou nákladnější a dostupná jen v omezeném sortimentu. Z tohoto důvodu bývají ústředny vybaveny i klasickými vstupy drátových smyček.

1.2.2. Smíšené (hybridní) ústředny



Obr. 3: Systém s hybridní ústřednou a třemi koncentrátory

Hybridní ústředny jsou kombinací smyčkové ústředny s ústřednou s přímou adresací čidel. Datová sběrnice nevede přímo k jednotlivým čidlům, ale je zakončena na *koncentrátorech*, které pracují jako převodníky mezi smyčkovým a sběrnicovým zapojením.

Ke každému koncentrátoru je připojena jedna nebo více smyček. Na každou z nich je možné připojit jedno nebo více čidel; jsou-li na jednotlivé smyčky připojena čidla pouze po jednom, získáváme část výhod sběrnicové ústředny – i z tabla ústředny můžeme sledovat stav systému s přesností na jednotlivé detektory.

1.2.3. Bezdrátové ústředny

Ústředny tohoto typu využívají bezdrátového přenosu dat zpravidla v bezlicenčních pásmech *ISM* (Industrial, scientific and medical band) 433 MHz, 868 MHz nebo 2,4 GHz.

Zřejmé zjednodušení výstavby a úprav systému EZS, kdy není nutné provádět výrazné stavební zásahy typu frézování kabelových drážek do zdí, je vykoupeno některými aspekty specifickými pro bezdrátové systémy:

- čidla jsou napájena z baterie, která má životnost maximálně několik let, a je nutné ji pravidelně měnit. Stav baterie je obvykle přenášen do ústředny zařízení, která obsluze sdělí nutnost její výměny.
- Zařízení je citlivé na rušení v použitém přenosovém pásmu. Trvalé rušení přenosu dat může být vyhodnoceno a signalizováno jako sabotáž; moderní systémy jsou schopny dynamicky měnit používaný kanál v rámci užitého pásma tak, aby byl docílen co nejúspěšnější přenos dat.
- Zařízení musí být chráněno proti náhradě naučených bezdrátových prvků jinými, například identifikací čidel unikátními výrobními čísly, zasílanými jako součást datového rámce.

Starší a jednoduchá bezdrátová zařízení používají simplexní přenos, kdy čidlo pravidelně vysílá informace o svém stavu bez toho, aby mělo informaci, zda je hlídaný prostor zastřežený či odstřežený. Novější zařízení komunikují s čidly obousměrně a umožňují tak čidla pro prodloužení životnosti baterií přepnout do úsporného režimu, je-li systém odstřežen, a kontrolovat provozní stav všech čidel v okamžiku zastřežení systému.

Pro obě řešení platí, že pravidelné přenosy dat za běhu systému jsou uskutečňovány pouze jednou za několik minut a je-li čidlo na začátku této prodlevy zneškodněno například zastíněním antény, ústředna může jeho absenci zjistit nejdříve po uplynutí této prodlevy. Autor si sám vyzkoušel, že pokud v ústředně Jablotron JA-63KR odpojíme v zastřeženém stavu celý modul bezdrátové komunikace a tím ji znemožníme, zařízení v některých případech zareaguje až za 3 minuty. Tento pokus musíme samozřejmě provádět s přemostěným sabotážním spínačem ústředny.

Na závěr je nutno upozornit na značně neustálenou terminologii: například firma Jablotron označuje ve svých firemních manuálech drátové smyčky někdy jako smyčky, jindy jako vstupy, termín *hybridní ústředna* je často užíván pro kombinované ústředny s drátovými i bezdrátovými vstupy a termín *smyčka* se někdy užívá i pro logickou skupinu bezdrátových nebo datově komunikujících čidel.

1.3. Komunikační možnosti současných ústředen

1.3.1. Rozhraní pro vnější komunikaci

Většina moderních ústředen EZS je vybavena *přenosovým zařízením*, schopným přenášet informaci o poplachu majiteli objektu a/nebo na pult centrální ochrany.

Stejné technologie, jaké budou dále popsány, se užívají i pro ústředny elektrické požární signalizace EPS a přístupové systémy: například níže zmíněný protokol Contact ID umožňuje přenos asi 30 různých informací o stavu požárních zařízení.

1.3.2. Telefonní a GSM komunikátory

1.3.2.1. Přenos zpráv uživateli systému

Telefonní hlásič (hlasový komunikátor) je schopen na povel ústředny EZS informovat odpovědnou osobu předem uloženou hlasovou zprávou. Hlásič je připojen do telefonní sítě (k veřejné síti nebo k pobočkové ústředně objektu) a po své aktivaci postupně vytáčí uložená telefonní čísla a přehrává krátkou hlasovou zprávu.

Pokročilejším řešením je GSM komunikátor, který využívá mobilní sítě k předání zprávy o poplachu formou SMS nebo prozvonění. GSM komunikátory obvykle umožňují i ovládání

ústředny pomocí speciálních SMS zpráv nebo prozvoněním z autorizovaného telefonního čísla.

1.3.2.2. Datový přenos na PCO

Kromě hlasového oznámení poplachu jsou některé telefonní komunikátory schopné předat datovou zprávu o stavu zařízení na pult centrální ochrany.

Protokol Ademco Contact ID

Jeden z užívaných protokolů je Ademco Contact ID, který zasílá zprávy vytáčenou telefonní linkou ve formě série DTMF tónů. Specifikace protokolu je dostupná v lit. [5].

Přenáší se celkem 16 DTMF číslic:

•2 znaky udávají verzi protokolu,

•4 znaky jsou identifikací volající ústředny (*subscriber ID*),

•3 znaky udávají *kvalifikátor události*, například *poplach 24 hodinové smyčky*, *porucha sirény*, *požár*, *vypnutí systému*, a jeden znak upřesňuje *stav* dané události, např. vznik události daného typu, ukončení události (např. ukončení výpadku proudu),

•v pěti znacích jsou přenášena čísla zóny a čidla, které vyvolalo poplach, a

•posledním znakem zprávy je kontrolní součet.

Vysílač má v paměti uloženo telefonní číslo jednoho nebo více přijímačů, umístěných na pracovištích pultu centrální ochrany. Vysílač vždy iniciuje spojení; sestavení spojení ani přenos dat směrem od přijímače není možné.

Přijímač protokolu Contact ID potvrzuje navázání spojení dvojtónem *(handshake tone)* a úspěšný přenos zprávy signalizačním tónem (tzv. *kissoff tone*). V rámci jednoho telefonního spojení je možné postupně přenést více zpráv.

Kromě spojení formou telefonního hovoru se užívá i přenos dat prostřednictvím SMS zpráv (např. proprietární systém firmy Jablotron), přenos vyhrazenou linkou a přenos prostřednictvím sítě Internet, popisovaný níže.

1.3.3. Propojení pomocí sítí standardu IP

Možnosti sítí paketových standardů TCP/IP využívají komunikátory, připojené buď k lokální síti objektu (LAN), připojené do internetu, nebo pomocí GPRS spojení k mobilní síti GSM.

Vysoká kapacita sítí a komfortní ovládání pomocí počítače dovoluje rozšířit komunikátory o plné dálkové ovládání a nastavování ústředen a tak nahradit dosluhující rozhraní RS-232, užívané

u starších systémů pro nastavování parametrů ústředny pomocí místně připojeného přenosného počítače servisního technika.

1.3.3.1. GSM/GPRS systém: Jablotron GSMlink

Firma Jablotron vyvinula systém GSMlink [4] pro dálkové nastavení parametrů ústředen vybavených GSM komunikátorem. Uživatel systému přistupuje běžným WWW prohlížečem na server firmy Jablotron, který zadaná nastavení zašle šifrovaným GPRS datovým spojením GSM komunikátoru.

1.3.3.2. Systémy založené na připojení k místní síti LAN

Běžnou součástí moderních staveb je rozvod strukturované kabeláže, která umožňuje připojení ústředny EZS k místní síti LAN. Komunikátory pro síť LAN pracují zpravidla s rozhraním Ethernet 10Base-T nebo 100Base-TX, autorovi nejsou známa žádná přenosová zařízení pro připojení do bezdrátové sítě typu Wi-Fi nebo jiných standardů sítí LAN.

Firma Jablotron vyrábí kombinované komunikátory JA-80V [7] pro Ethernet a telefonní linku, určené pro vestavbu do ústředen Oasis. Komunikátory umožňují kromě běžných funkcí přenosu poplachu uživateli a na PCO i dálkové ovládání a programování ústředny speciálními SMS zprávami nebo pomocí zmíněného systému GSMlink.

Komunikátor zajímavě řeší práci s SMS zprávami: místo integrace GSM přenosového zařízení si zařízení předává texty zpráv přes internet se serverem firmy Jablotron, který řeší jejich odesílání a příjem ve formě SMS včetně účtování.

Firma Paradox vyrábí IP moduly IP-100 [8] pro své ústředny Digiplex, Spectra a Magellan. Tento modul byl původně navržen jako IP prodloužení původní servisní linky RS-232 zmíněných ústředen, ale s aktuální verzí firmware již pracuje jako vestavěný konfigurační WWW server ústředny. Oproti systému firmy Jablotron toto zařízení nevyžaduje spolupráci se servery svého výrobce[1] a umožňuje 128 bitové šifrování přenášených dat, naopak neumožňuje spojení s pulty centrální ochrany.

Mnoho dalších vestavěných komunikátorů ústředen nemá více funkcí než jejich původní telefonní předlohy. V některých případech je nutné užívat různé převodníky datových formátů, například rozšířit starší ústřednu o IP přenos dat na pracoviště PCO je možné komunikátorem, který simuluje telefonní ústřednu původnímu telefonnímu komunikátoru EZS, pracujícímu s protokolem 4/2 nebo Contact ID, a přenáší data dále po internetu na specializovaný přijímač (například systém firmy HaSaM).

Pro doplnění funkcí vzdálené správy do stávajících ústředen se na trhu objevily komunikační

1 Nicméně firma Paradox nabízí službu Paradox My Home, která umožňuje webový přístup k ústřednám, které jsou umístěny za firewally, blokujícími přímý přístup, nebo na připojení s dynamickou IP adresou.

převodníky RS-232/SSH, které umožňují dálkové šifrované připojení k RS-232 rozhraní ústředny pomocí internetu, například čtyřnásobný bezpečnostní konzolový server Lantronix SCS100.

1.3.3.3. Protokoly pro spojení s pulty centrální ochrany pomocí sítí IP

Jedinými novými veřejně dostupnými protokoly pro systémy s přenosem informací o poplachu pomocí sítí IP jsou specializované protokoly pro přenos stavových informací z ústředen EZS na pracoviště pultů centrální ochrany. Všechny ostatní funkce komunikátorů užívají buď standardní protokoly internetu, zejména HTTP, HTTPS, SSL/TLS a SMTP, nebo proprietární protokoly výrobců.

Protokol IP Contact ID

Rozšíření a jednoduchost protokolu Contact ID (CID) vedla ke vzniku jeho IP modifikace, která pracuje nad protokolem transportní vrstvy UDP nebo TCP a přenáší formou otevřeného textu sérii číslic, přenášených původním protokolem CID [9]. Potvrzení úspěšného přenosu zprávy na PCO se provádí odesláním zprávy s původním zněním zpět ústředně EZS.

Protokol neumožňuje žádnou kontrolu autenticity přenášených dat ani zajištění jejich důvěrnosti.

Protokol SIA IP Events Reporting

Protokol *SIA Internet Protocol Events Reporting*, označovaný často pouze zkratkou SIA, je jednoduchý protokol pro přenos stavových zpráv z ústředen EZS na pracoviště pultů centrální ochrany. Protokol je standardizovaný dokumentem skupiny SIA (*Security Industry Association*, jejímiž členy jsou například Honeywell, Tyco, AT&T a General Electric) *ANSI/SIA DC09* [10].

Pomocí TCP nebo UDP spojení se přenáší zprávy třech typů. Jde o:

•*zprávy o události* (event message), informující PCO o změně stavu zařízení EZS,

•*kontrolní zprávy* (supervision message) odesílá zařízení EZS a slouží pro periodickou kontrolu spojení, a

•*potvrzení* (ACK message), kterými PCO potvrzuje přijetí zprávy.

Je zřejmé, že přenos užitečných dat je pouze jednosměrný ve směru k PCO.

Protokol umožňuje volitelné šifrování přenášených dat pomocí symetrické šifry AES. Dokument [10] dále definuje chování zařízení při poruše přenosového kanálu.

1.3.3.4. Normativní požadavky na komunikátory IP/Ethernet

Evropská norma ČSN EN 50136-1-5 z února 2009 [6] stanovuje požadavky na poplachové přenosové systémy užívající paketově spínané datové sítě, tedy i sítě IP resp. LAN – Ethernet.

Norma stanovuje ve velmi obecné rovině požadavky na zajištění spolehlivosti přenosové sítě, zejména je požadována odolnost proti zablokování přenosu poplachových informací ostatním provozem na síti a odolnost přenosových zařízení proti zablokování příjmem záludných dat nebo přetížením spojení.

Poměrně zajímavé je, že norma nevyžaduje zálohování napájení prvků přenosové sítě (např. DSL modemů nebo přepínačů v síti Ethernet), přestože soubor norem ČSN EN 50136-1 zmiňuje nutnost zálohovaného napájení komunikátorů, ačkoliv přesné požadavky zatím nejsou známé – mají být obsaženy v normě ČSN EN 50136-4, která je zatím ve stádiu příprav. Je pochopitelné, že může snadno vzniknout situace, kdy při výpadku nebo záměrném přerušení dodávky elektrické energie útočníkem nebude datové spojení dostupné, přestože bude komunikátor napájen.

1.3.3.5. Připojení čidel pomocí Ethernet/IP řešení

Na tomto místě je vhodné naznačit, proč se běžně nesetkáváme se sběrnicovými ústřednami, kde by byla sběrnice realizována rozvodem paketové IP sítě, tedy čidla EZS bychom připojovali k ústředně pomocí rozhraní Ethernet nebo bezdrátově pomocí WiFi 802.11.

Podle názoru autora existují tři roviny, ve kterých stále prohrává IP řešení proti klasickému systému drátových smyček, sběrnicovému systému založenému na RS-485 nebo proprietárnímu bezdrátovému řešení v pásmech ISM.

1. *Cenová rovina* – ceny prvků EZS jsou relativně nízké a rozhraní IP/Ethernet by je zdražilo o desítky až stovky procent (viz tab. 1). Struktura sítě Ethernet je navíc hvězdicová a tak každému připojenému zařízení (čidlu, siréně, klávesnici) musíme vyhradit i zásuvku na přepínači nebo obdobném zařízení.
2. *Proudová spotřeba* – prvky sítí IP/Ethernet mají obecně vyšší spotřebu oproti klasickým řešením, což se týká zejména bezdrátových sítí WiFi, které jsou zcela nepoužitelné pro dlouhodobě napájená bateriová zařízení.
3. *Bezpečnostní problémy* – provoz zařízení EZS, integrovaný do sítě LAN objektu, může být lehce monitorován a nebudou-li použity fyzicky či virtuálně oddělené sítě, je možné na zařízení útočit z libovolné pracovní stanice v síti LAN. Zařízení EZS proto musí být vybaveno možností rozpoznání záludné změny přenášených dat, například s využitím standardních kryptografických nástrojů na principu elektronického podpisu.

Rozhraní čidla	*Drátové*	*RS-485*	*Proprietární 433 MHz*	*Ethernet (bez PoE)*	*WiFi*
Příklad provedení	jazýčkové relé	budič 75LBC176 + zakončení	semiduplexní modul HopeRF RFM12	řadič ENC28J60 + ethernetový transformátor	modul LSR WiFlex03
Kusová cena obvodů rozhraní (odběr 100 ks)	9 Kč	13 Kč	38 Kč	59 Kč + výkonnější mikrokontrolér	510 Kč + výkonnější mikrokontrolér
Trvalá spotřeba obvodu rozhraní (bezdrátová rozhraní trvale na příjmu, bez vysílání)	150 mW	5 mW	< 0,5 mW	500 mW	300 mW

Jako příklad konkrétního provedení byl zvolen nejlevnější vhodný typ zařízení podle zkušeností autora, ceny jsou kalkulovány z nabídek pro odběr 100 kusů, generovaných vyhledávačem Octopart. Konektory nejsou započteny v ceně.

Tabulka 1: Srovnání cenové a energetické náročnosti rozhraní čidel

Sítě IP/Ethernet je ale vhodné využít vždy, můžeme-li profitovat z jejich vlastností, jako je propojení s internetem, vysoká přenosová kapacita a dostupnosti kabeláže sítě v téměř každé místnosti moderní budovy.

2. Návrh ústředny s komunikátorem Ethernet

2.1. Základní koncepce ústředny

Vývoj ústředen EZS vede ke stále větší flexibilitě a nastavitelnosti chování zařízení. Například středně velké ústředny Jablotron řady Oasis mají více než 50 nastavitelných parametrů, ale i přes velký rozsah možných nastavení je možné nalézt situace, kdy je nutné realizovat některé speciální funkce externími prostředky nebo zařízením, určeným pro podstatně větší instalace.

Další rozvoj funkčního komfortu zařízení EZS je podle mého názoru stále omezen nedostatečnou integrací zařízení EZS do systémů budov. Ústředna s pevnou logikou, byť se stovkami nastavitelných parametrů, nemůže v méně typických případech nikdy plně vyhovovat požadavkům uživatelů. Typickým příkladem integrace funkcí jednotlivých systémů je požadavek na otevření garážových vrat, odjištění systému EZS a rozsvícení osvětlení stiskem jednoho tlačítka dálkového ovladače v automobilu.

Navrhovaná ústředna je vybavena komunikačním rozhraním Ethernet, které umožní poměrně komfortní ovládání přístroje pomocí počítače, a tak můžeme použít poněkud odlišný přístup od běžného řešení: ústředna nebude mít pevnou logiku, ale její chování bude zadáno sadou skriptů, napsaných v jednoduchém skriptovacím jazyce.

Toto řešení umožní plnou programovatelnost ústředny včetně možnosti realizace poměrně složitých úloh domácí automatizace, jinak řešených například PLC kontrolérem nebo systémem inteligentní elektroinstalace. Stejně tak bude implementace jednoduchých protokolů typu IP SIA možná pouhým zadáním příslušných příkazů skriptu.

Současně bude zachována základní uživatelská nastavitelnost parametrů ústředny pomocí jejího WWW rozhraní. Složitější změny chování ústředny bude možné zadat ruční úpravou skriptů nebo instalací předpřipravené sady skriptů pro danou funkci ústředny.

Změnou nainstalované sady skriptů bude možné změnit i množinu parametrů, nastavitelných pomocí WWW rozhraní, a chování komunikátoru sítě Ethernet.

De facto tedy vytváříme spíše **specializovaný volně programovatelný průmyslový počítač** s vybavením pro realizaci zabezpečovacích systémů (tedy s vhodnými komunikačními rozhraními, šifrováním, vstupy drátových smyček atd.) než klasickou ústřednu s pevně definovaným chováním.

Sada skriptů a všech nastavení bude uložena na paměťové kartě microSD, vložené v patici, umístěné na desce ústředny.

V případě hardwarové poruchy ústředny postačí paměťovou kartu z vadné ústředny vložit do nové ústředny a nebude nutné novou ústřednu zdlouhavě konfigurovat; stejně tak pro několik ústředen se shodným nastavením, například v jednotlivých patrech objektu, postačí zkopírovat obsahy paměťových karet a tím i všechna nastavení zařízení, a rozlišit ústředny pouze nastaveným identifikátorem nebo IP adresou.

Další kapitoly práce se zabývají návrhem hardwarového a softwarového vybavení ústředny uvedené koncepce.

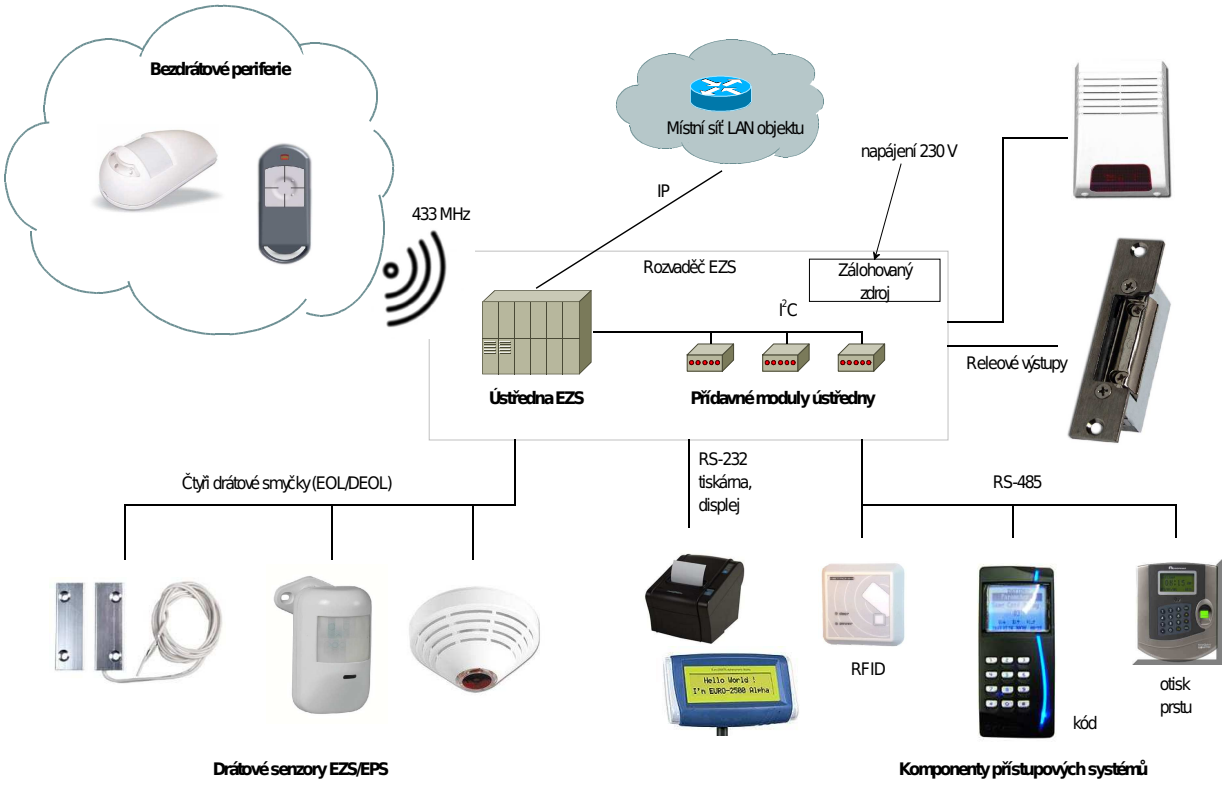
Pro co největší flexibilitu řešení bude navrhovaná ústředna EZS umožňovat rozšíření systému co do počtu vstupů a výstupů pomocí *přídavných modulů*, instalovaných v jeho těsné blízkosti. V sestavě s *přídavnými moduly* budeme navrženou desku ústředny označovat jako *hlavní modul.*

Jako příklad *přídavného modulu* je v příloze práce uveden ideový návrh modulu přijímače Keeloq 433 MHz.

Zařízení bude připraveno pro provoz v instalaci s větším počtem ústředen v síti LAN, kde se předpokládá nasazení řídící *softwarové ústředny*, tedy serveru, který bude komunikovat s jednotlivými podřízenými ústřednami navrženého provedení a provádět společné řídící funkce (například přenos příkazů odstřežení či zastřežení mezi podřízenými ústřednami, generování dat tabla ústředny pro počítačový terminál ostrahy atd.). Jednotlivé *podřízené ústředny* mohou podle konkrétního řešení *softwarové ústředny* pracovat jako samostatné ústředny, předávající softwarové ústředně pouze souhrnné informace typu vyhlášení poplachu, nebo jako pouhé koncentrátory, jejichž vstupy a výstupy budou přímo řízeny softwarovou ústřednou.

V následující části textu rozebereme typická nasazení navrhované ústředny.

2.1.1. Požadavky pro samostatný provoz



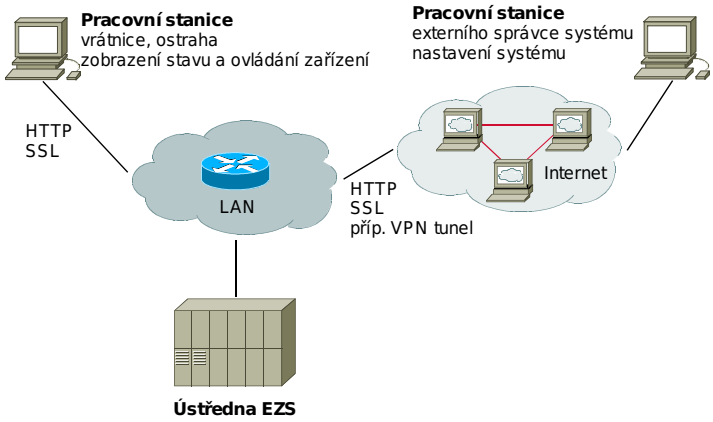
Obr. 4: Navrhovaná ústředna EZS jako centrální prvek jednoduchého systému

Zapojení ústředny v jednoduché instalaci EZS například v rodinném domku nebo malém kancelářském objektu je naznačeno na obr. 4.

Ústředna je umístěna v rozvaděči EZS, který současně obsahuje i zálohovaný zdroj s akumulátorem. Zajištění a odjištění objektu se provádí bezdrátovým ovladačem standardu Keeloq nebo autentizačním zařízením, připojeným sběrnicí RS-485, například klávesnicí nebo snímačem otisků prstů. Na sběrnici RS-232 může být připojen například informační displej nebo GSM terminál.

Hlavní modul ústředny je vybaven čtveřicí drátových smyček, čtyřmi reléovými výstupy a trojicí tranzistorových výstupů.

Pro menší rodinný domek budou rozděleny smyčky například takto: jedna zpožděná smyčka pro dveřní spínač vstupních dveří a PIR čidlo v prostoru chodby, kde je umístěno autentizační zařízení, dvě okamžité smyčky pro PIR čidla a detektory tříštění skla a jedna 24 hodinová smyčka pro požární hlásiče. Reléové výstupy mohou samostatně spínat exteriérovou a interiérovou sirénu, další relé může například ovládat garážová vrata nebo signalizovat zastřežení ovládací skříní venkovních rolet.



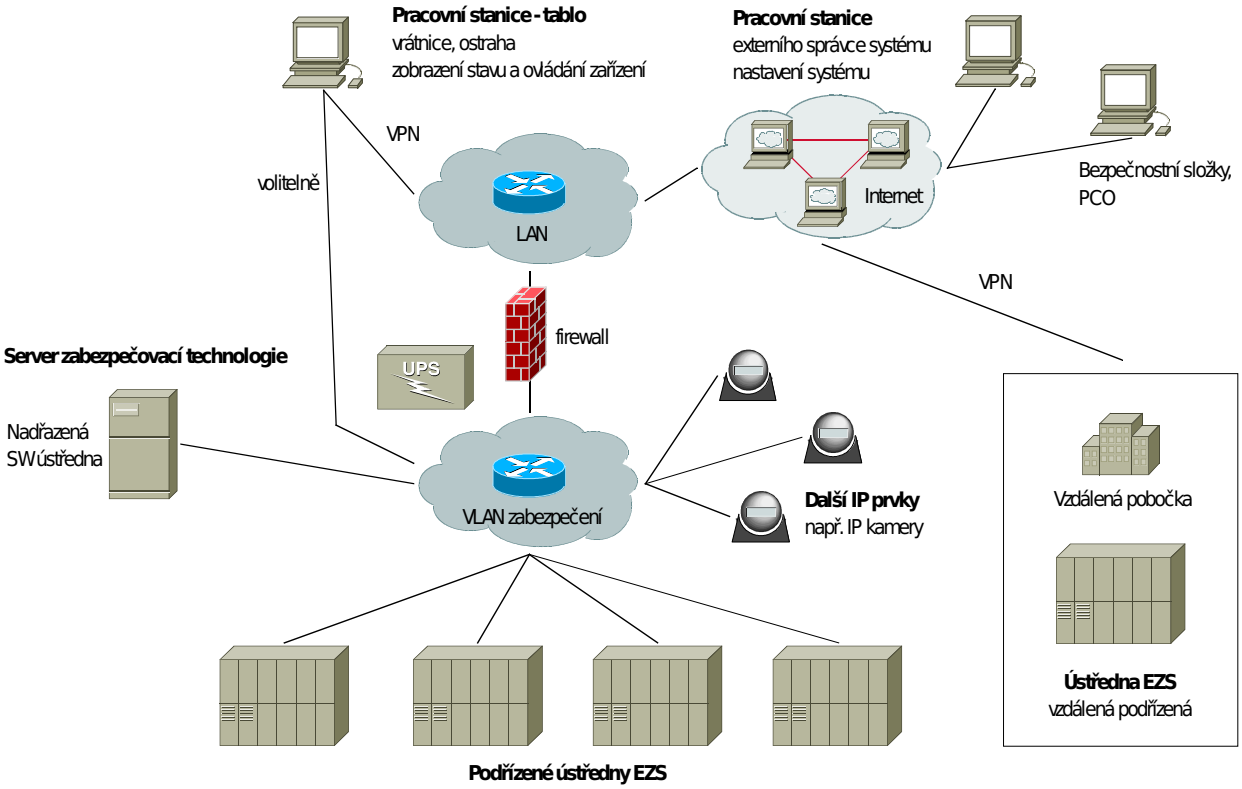
Obr. 5: Užití komunikace Ethernet při použití ústředny jako centrálního prvku malé instalace.

Komunikátor Ethernet bude v této roli ústředny sloužit zejména pro dálkové ovládání ústředny, kontrolu stavu a vzdálenou správu systému, jak je naznačeno na obr. 5.

I v malé instalaci bude samozřejmě možné použít funkce ústředny pro domovní automatizaci, popsané v oddílu 2.1.3.

2.1.2. Požadavky pro řízený provoz

V instalacích většího rozsahu, kdy bude instalováno více ústředen navrhovaného typu spolu s nadřazenou softwarovou ústřednou, je struktura systému poněkud odlišná.



Obr. 6: Struktura bezpečnostní sítě LAN ve velké instalaci

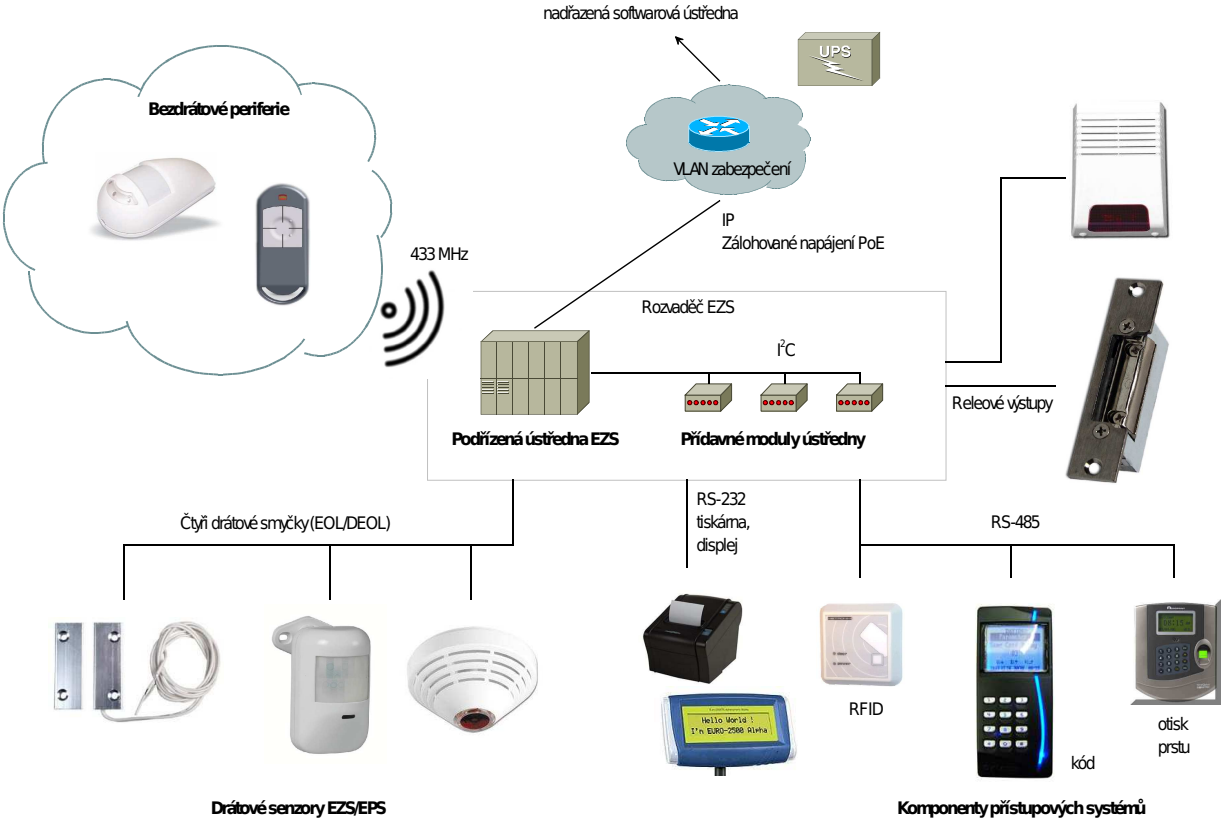
Na obrázku 6 je znázorněno spojení mezi ústřednami v objektu pomocí technologie Ethernet. Pro spojení je využita separátní síť LAN zabezpečení, která může být současně využita například i pro připojení IP kamer CCTV. Přenos dat mezi sítí LAN zabezpečení a internetem, případně běžnou vnitřní sítí LAN objektu, je omezen firewallem.

Několik podřízených ústředen EZS předává datovou sítí informace o svém stavu centrální softwarové ústředně, běžící na *serveru zabezpečovací technologie*. Softwarová ústředna může zpětně podřízeným ústřednám zasílat příkazy pro ovládání výstupních zařízení, například pro zapnutí sirény nebo otevření elektrických zámků.

Klasické tabló ústředny nahrazují obrazovky počítačů, připojených k zabezpečovací síti LAN objektu buď přímo, nebo pomocí virtuální privátní sítě VPN. VPN může být využita i pro komunikaci softwarové ústředny s podřízenou ústřednou EZS, umístěnou mimo rozsah vnitřní sítě objektu kdekoliv v dosahu sítě Internet *(Vzdálená pobočka* na obr. 6*)*.

Místo separátní sítě je možné užít i virtuální síť VLAN, která také oddělí datový provoz

bezpečnostních systémů od jiných datových toků, případně je možné za cenu poněkud menší odolnosti systému proti útoku použít i stávající, neoddělenou síť LAN. Taková síť je ovšem zranitelnější vůči útokům typu DoS, man-in-the-middle / ARP poisoning atd., které je možné provést z libovolné stanice v síti.



Obr. 7: Zapojení navrhované ústředny EZS ve větší instalaci s napájením PoE

Rozhraní Ethernet bude nyní sloužit jako hlavní a jediný spoj, kterým může ústředna zpravit obsluhu o poplachu nebo poruše, a při výpadku tohoto spojení je podřízená ústředna pouze "němé", bezcenné zařízení. Proto můžeme přesunout zálohovaný napájecí zdroj až k nadřazené softwarové ústředně nebo do její technologické místnosti a napájet ústřednu systémem Power over Ethernet (viz odd. 2.2.5.1, dále jen PoE). Současně si ušetříme náročnou kontrolu a výměny zálohovacích akumulátorů jednotlivých podřízených ústředen.Centralizované napájení tedy umožní existenci jediného záložního zdroje, napájejícího PoE injektory v technologické místnosti či serverovně objektu (na obr. 7 značen jako UPS). Podřízené ústředny jsou pomocí PoE napájeny napětím 48 V, z něhož si vytváří měničem potřebná vnitřní napájecí napětí a napětí 12 V pro napájení aktivních čidel a dalšího připojeného příslušenství.

Obvod napájení 48 V je galvanicky oddělený od okruhů 12 V, což přispívá ke zvýšení odolnosti proti rušení a přepětím.

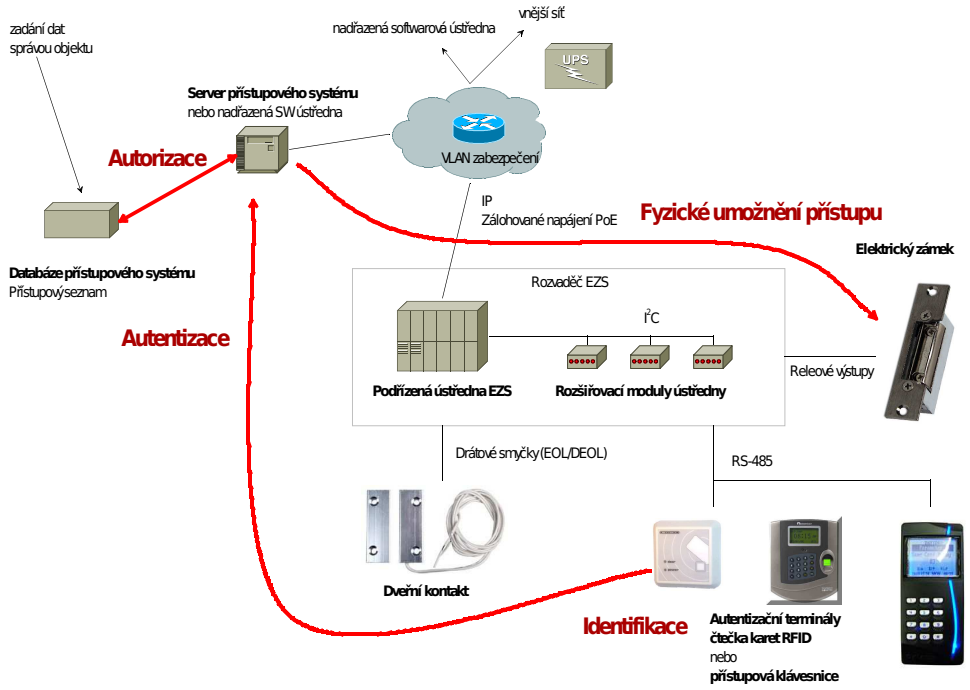
Vhodné umístění podřízené ústředny bude v kancelářských a výrobních budovách takové, aby

jedna ústředna hlídala jednu či dvě spojené místnosti, počet vstupů a výstupů na jednotce odpovídá jedné kanceláři nebo kanceláři s předsíňkou. Pro snadnou vzdálenou diagnostiku budou smyčky užívány přednostně pouze jedním čidlem, například jedno PIR čidlo, jeden detektor tříštění skla, jeden dveřní spínač a jeden požární hlásič obsadí všechny čtyři smyčky navrhované ústředny. V případě, že nebude počet smyček dostatečný, bude možné rozšířit zařízení přídavným modulem o další smyčky.

K rozhraní RS-485 bude připojen zpravidla autentizační terminál, například RFID čtečka.

Výstupy ústředny mohou spínat elektrický zámek, interiérovou sirénu, signalizaci zastřežení prostoru; některé výstupy je možné ve smyslu odd. 2.1.3. využít pro funkce domovní automatizace, například sepnutí stykače, který aktivuje elektrický rozvod v místnosti (typické pro hotelové pokoje), nebo na základě signálu od nadřazené ústředny, stavu zastřežení místnosti a času vypíná elektrický ventil nebo stykač topení.

V roli podřízené ústředny můžeme zařízení efektivně využít i jako součást přístupového systému, kdy podřízená ústředna oznamuje nadřazené softwarové ústředně nebo zvláštnímu serveru přístupového či docházkového systému údaje z připojeného autentizačního zařízení a svými výstupy uvolňuje mechanickou zábranu, například elektrický dveřní zámek (viz obr. 8).



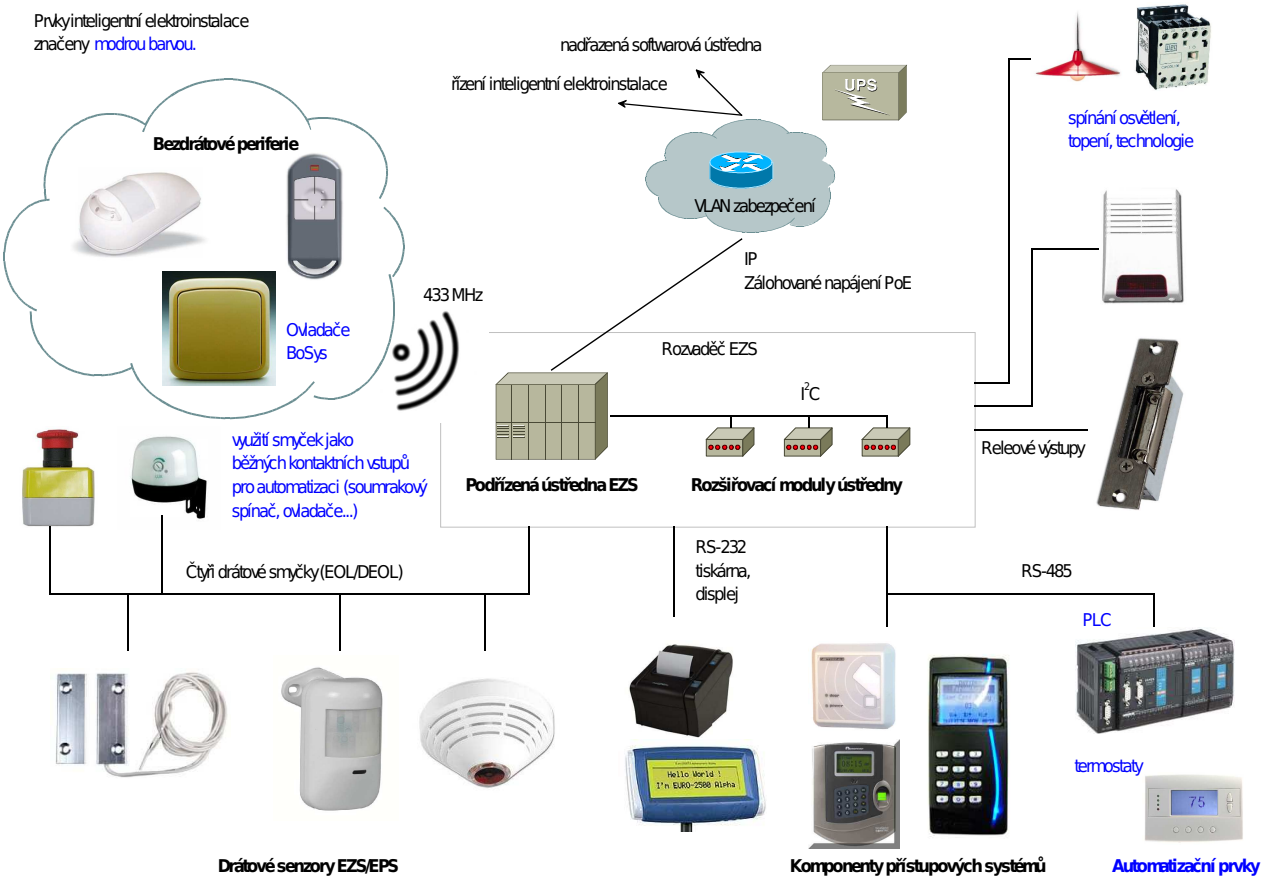
Obr. 8: Navrhovaná ústředna EZS v roli přístupového systému

Takto zapojený přístupový systém bude navíc plně funkční i při výpadku elektrické sítě: všechny prvky jsou zálohovány z centrálního záložního zdroje.

2.1.3. Požadavky pro využití v systémech domovní automatizace

Volně programovatelnou ústřednu můžeme využít i pro realizaci některých úkolů domovní automatizace – od spínání osvětlení v závislosti na stavu připojených PIR snímačů po složitější aplikace typu automatického ovládání topení podle stavu zastřežení jednotlivých místností, PIR snímači zjištěného skutečného pohybu osob, času a okolní teplotě, kterou může ústředně poskytnout vnější snímač.

Na obrázku č. 9 jsou naznačeny možnosti propojení navrhované ústředny s prostředky domovní automatizace.

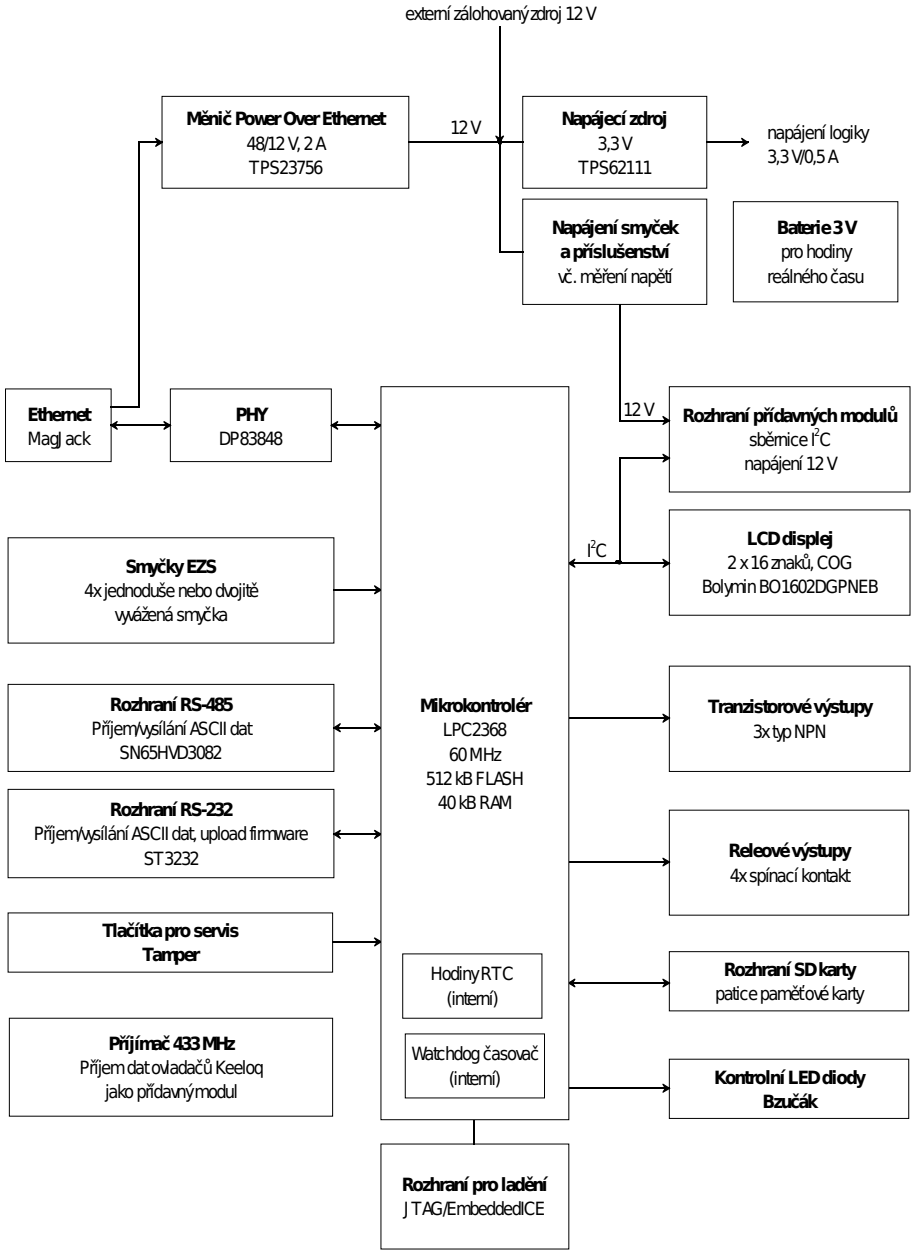


Obr. 9: Využití podřízené ústředny jako součásti zařízení domovní automatizace.

2.2. Obvodové řešení

Obvodové řešení hlavního modulu ústředny EZS je podřízeno maximální jednoduchosti a nízké ceně zařízení při současném splnění požadavků pro provoz v roli samostatné i podřízené ústředny.

Blokové schéma hardwaru hlavního modulu navrhované ústředny je uvedeno na obr. 10.



Obr. 10: Blokové schéma hardwarového řešení hlavního modulu navrhované ústředny

Vzhledem k omezenému rozsahu práce je popis v následujících částech práce zestručněn tam, kde to není na úkor výkladu principu funkce zařízení.

2.2.1. Řídicí obvody

Volba vhodného mikropočítače (mikroprocesoru, mikrokontroléru) jako řídicího prvku ústředny je podmíněna trojicí kritérií: výpočetnímu výkonu, možnosti připojení komunikace Ethernet a ceně použitých obvodů.

Pro pohodlnou a rychlou komunikaci rozhraním Ethernet si stanovíme minimální reálnou propustnost rozhraní 250 kb/s, umožňující přenesení jedné WWW stránky o velikosti 5 kB za přibližně 0,2 sekundy. Stránku této velikosti musíme rovněž stihnout v rozumné době (řádově desetin sekundy) vygenerovat, což v našem případě obnáší načtení příslušného skriptu z paměťové karty a jeho vykonání při stálém běhu rutin sledujících stav vstupů a ostatních komunikačních rozhraní.

Charakteristiky některých mikrokontrolérů, vhodných pro malé ethernetové aplikace, uvádí tabulka 2. Uvedené výkonové charakteristiky jsou uvedeny v Dhrystone MIPS, aby bylo možné porovnat výkon jednotlivých architektur [40, 41, 42].

Uvedená výkonnostní kritéria zjevně vyřazují z výběru levné osmibitové mikrokontroléry s nízkým výkonem (řádově do 5 DMIPS), které navíc zpravidla neobsahují hardwarovou podporu přenosu dat rozhraním Ethernet a používající externí řadič sítě Ethernet, připojený obvykle pomalým synchronním sériovým rozhraním typu SPI (např. Microchip ENC28J60).

Typ	*Jádro*	*RAM [kB]*	*FLASH [kB]*	*Výkon [DMIPS]*	*Cena Kč/ks odběr 100 ks*
ATMEL ATMega644P (ext. SPI řadič)	AVR 8 bitů	4	64	4,83	119,5
Rabbit Semicond. Rabbit 3000 (ext. RMII řadič)	Rabbit 8 bitů	externí	externí	3,73	376,2
NXP LCP2368 (ext. RMII řadič)	ARM7TDMI 32 bitů	58	512	64,8	137,6
NXP LPC1768 (ext. RMII řadič)	Cortex-M3 32 bitů	64	512	125	144

Ceny v Kč bez DPH přepočteny podle nejlevnější nabídky distributorů Farnell, Newark, Future Electronics a AVNET z prosince 2009.

Tabulka 2: Charakteristiky vybraných mikrokontrolérů.

Dostatečný výkon poskytují malé třicetidvoubitové mikrokontroléry, které mají často implementovánu hardwarovou podporu rozhraní MII/RMII, umožňujícího připojení řadiče

fyzické vrstvy Ethernetu (tzv. obvodu PHY).

Jedním z nejrozšířenějších typů jader takových mikrokontrolérů je jádro ARM7TDMI nebo novější a výkonnější Cortex-M3. Na základě poměru dobré hardwarové výbavy, dostupnosti volně šiřitelných vývojových prostředků a ceny byl zvolen mikrokontrolér firmy NXP (bývalá součástková divize Philips) LPC2368 s jádrem ARM7TDMI, popsaný podrobně v následujícím oddílu.

Možnost zvýšení výkonu bez podstatných změn hardwaru nabízí pinově kompatibilní mikrokontrolér stejného výrobce LPC1768, vybavený jádrem Cortex-M3. Tento obvod bohužel není vybaven rozhraním pro přístup k SD kartě, které by muselo být emulováno softwarově, a byl uveden na trh v únoru 2009, takže jeho podpora volně šiřitelnými nástroji, např. balíkem nástrojů win-arm, je prozatím v plenkách.

Další možností realizace je užití jednoduchého mikrokontroléru spolu se specializovaným modulem, obsahujícím řadič sítě Ethernet spolu s mikrokontrolérem, na kterém běží software TCP/IP stacku. Tomuto modulu je možné například pouze předat příkaz obsahující IP adresu, port a užitečná data, a vlastní přenos dat IP sítí včetně navázání TCP spojení zařídí mikrokontrolér modulu. Příkladem takových modulů jsou zařízení Lantronix XPort nebo ConnectOne LanReach. Výkon tohoto řešení by byl pravděpodobně dostatečný (autor realizoval s prvním ze zmíněných modulů přenos zvukových dat rychlostí 400 kb/s), nicméně celková cena řešení by byla více než trojnásobná oproti navrhované kombinaci ARM7+PHY.

Na trhu jsou i specializované osmibitové mikroprocesory pro ethernetové aplikace s rozsáhlou softwarovou podporou, jako je například obvod Rabbit 3000 [45] společnosti Rabbit Semiconductor, který umožňuje připojení vnějších pamětí dat i programu. Jeho velmi nízký výkon (viz tab. 2) ovšem nepostačuje pro realizaci aplikací, vyžadujících složité zpracování a šifrování dat.

Poslední zvažovanou možností bylo použití mikropočítače s operačním systémem Linux, který by ale výrazně zvýšil cenu koncového produktu.

2.2.1.1. Architektura ARM7TDMI

Autorem architektury ARM7TDMI [11], [12], užité ve zvoleném mikrokontroléru, je britská společnost ARM – Advanced RISC Machines, vyvíjející jádra mikroprocesorů a mikrokontrolérů již od 80. let 20. století, tehdy pod jménem Acorn Computers.

Politikou ARM je prodej licencí jádra a vývojových prostředků – samotné mikroprocesory a mikrokontroléry vyrábí několik známých výrobců integrovaných obvodů ve vlastních závodech.

V současné době jsou nejpoužívanějšími verzemi jádra ARM typ ARM7 a typy z něj odvozené, užívané pro nízkou spotřebu a dostatečný výkon v přístrojích spotřební elektroniky, například

MP3 přehrávačích (např. iPod), a výkonnější verze jádra ARM9 a vyšší (např. XScale), nacházející uplatnění v zařízeních PDA, routerech, WiFi zařízeních a moderních mobilních telefonech.

Vlastnosti ve zvoleném mikrokontroléru užitého jádra ARM7TDMI můžeme shrnout v těchto bodech:

- šířka instrukčního slova, datové i adresové sběrnice je 32 bitů,
- většina instrukcí je jednocyklových, 4 bity instrukčního slova slouží k zadání podmínky – podmínka je tedy přímo součástí výkonné instrukce,
- k dispozici je 32 bitový adresní prostor (4 GB), je užita von Neumannova architektura.

Oproti staršímu jádru ARM7 je jádro ARM7TDMI doplněno o následující čtveřici vylepšení:

- **T**humb – zvláštní alternativní instrukční soubor, který užívá jen 16-bitová instrukční slova, a tak spoří paměť programu na úkor pomalejší práce mikrokontroléru,
- **D**ebug-interface – rozhraní JTAG pro ladění programu přímo v aplikaci,
- Multiplier – hardwarovou násobičku,
- Interrupt – podpora rychlých přerušení.

Na jádra ARM7/ARM7TDMI vývojově navazují jádra Cortex-M3, lišící se zejména užitím harvardské architektury[2], hardwarové děličky a některých optimalizací přístupu k paměti [13]. Velká část programů je nicméně podle údajů firmy ARM přenositelná na jádra Cortex-M3 i na úrovni strojového kódu.

2.2.1.2. Mikrokontrolér LPC2368

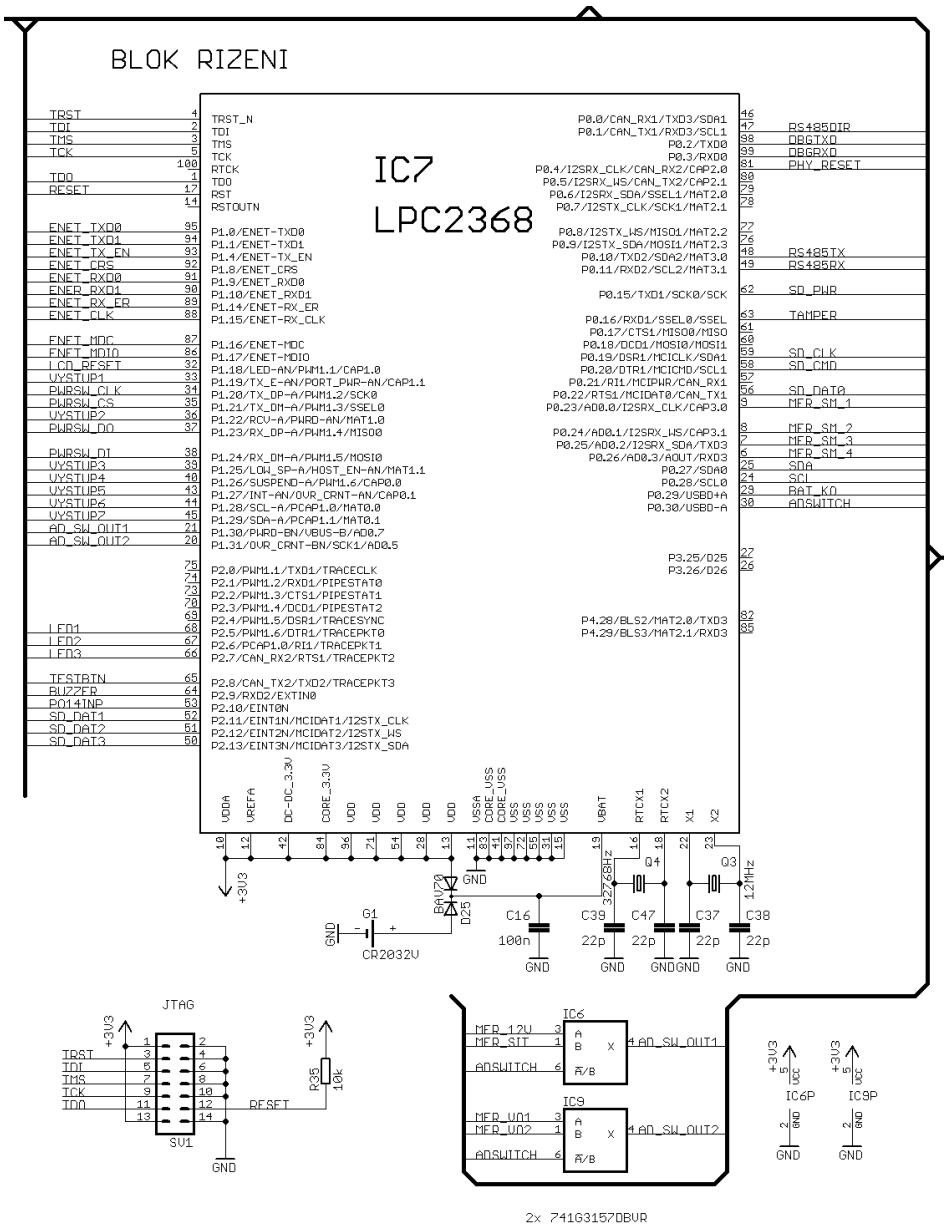
Mikrokontrolér LPC2368 [48] se vyznačuje následujícími vlastnostmi:

- 32-bitové jádro ARM7TDMI-S s podporou režimu Thumb a hodinovou frekvencí až 72 MHz,
- integrovaná paměť Flash 512 KB, paměť SRAM celkem 58 KB,
- rozhraní ISP/IAP pro programování v aplikaci, rozhraní JTAG pro debugging,
- integrovaný A/D a D/A převodník s šesti vstupy a jedním výstupem, rozlišení 10 bitů,

2 Nejde ovšem o klasické pojetí harvardské architektury – paměťový prostor je stále pouze jeden [14], ale je odstraněno nejužší místo: pokud je to možné, užije jádro Cortex dvě datové sběrnice (datovou a programovou) pro přístup k paměti (typicky RAM a FLASH) namísto jediné sdílené sběrnice von Neumannovy architektury. Rovněž cache je rozdělena na datovou a programovou; navenek se ovšem jádro chová jako von Neumannovské včetně možnosti spuštění programu z paměti RAM. Toto řešení se někdy označuje jako *Modified hardware architecture* [15].

- čítač reálného času (hodiny, RTC) s minimální spotřebou a zvlášť vyvedeným napájením,
- integrovaná komunikační rozhraní: port USB 2.0 OTG, rozhraní RMII, čtveřice asynchronních sériových rozhraní, synchronní sériové rozhraní SPI pro přenos rámců s délkou 8 až 16 bitů, dvě synchronní sériové rozhraní SSP pro přenos rámců o délce 4 až 16 bitů, sběrnice I^2S a dvojice sběrnic I^2C.

2.2.1.3. Skutečné zapojení bloku řízení



Obr. 11: Zapojení obvodů mikrokontroléru (výřez z celkového schématu zapojení, viz příloha A)

Hodinová frekvence mikrokontroléru LPC2368 (IC7, viz detail schématu na obr. 11) je řízena krystalem Q3 (12 MHz). Kmitočet krystalu se násobí vnitřním fázovým závěsem pěti na 60 MHz.

IC6 obsahuje i vnitřní obvod reálného času (RTC), který užívá pomaloběžný oscilátor s krystalem Q4. Tato část IC6 je napájena z pinu VBAT přes diodový přepínač, tvořený dvojitou diodou D25, z napájecího napětí 3,3 V mikrokontroléru nebo z lithiové zálohovací baterie typu CR2032 (G1), která vystačí na přibližně roční běh RTC při výpadku hlavního napájecího napětí.

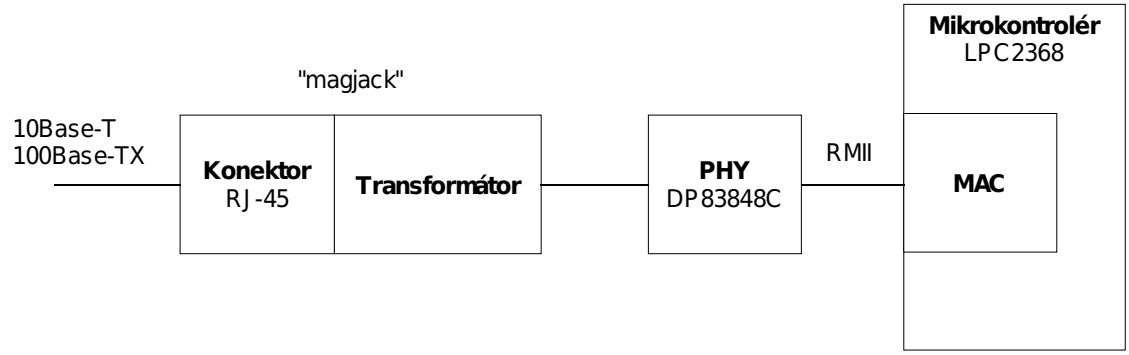
Na konektor SV1 je vyvedeno programovací a ladící rozhraní JTAG. Druhou možností programování je programování pomocí rozhraní RS-232, popsané níže. Programováním zde máme na mysli prvotní nahrání firmwaru do zařízení, nikoliv ve smyslu nastavení parametrů ústředny.

Mikrokontrolér je dále vybaven časovačem watchdog a vnitřním generátorem resetu při zapnutí napájení nebo podpětí (BOD reset), proto není nutné použít externí obvody zajišťující tyto funkce, naopak program mikrokontroléru zajišťuje reset dalších prvků, vyžadujících inicializaci po poklesu nebo výpadku napájení – v našem případě jde o LCD displej a o obvod PHY.

IC7 je vybaven desetibitovým A/D převodníkem s interním multiplexerem se šesti vstupy. Pro funkci zařízení potřebujeme měřit osm napětí a tedy musíme mít k dispozic osm vstupů. Z toho důvodu jsou osazeny dva analogové přepínače (integrované obvody IC6 a IC9 v pouzdru SOT23/6), které multiplexují čtyři vstupní analogové signály MER_12V s MER_SIT a MER_VO_1 s MER_VO_2 na dva vstupy A/D převodníku IC7. Přepínání řídí IC7 vodičem ADSWITCH.

2.2.2. Obvody komunikace

2.2.2.1. Ethernet



Obr. 12: Hardwarová struktura rozhraní Ethernet

Standardní hardwarová struktura rozhraní Ethernet, užívaná u této třídy embedded zařízení, je uvedena na obr. 12.

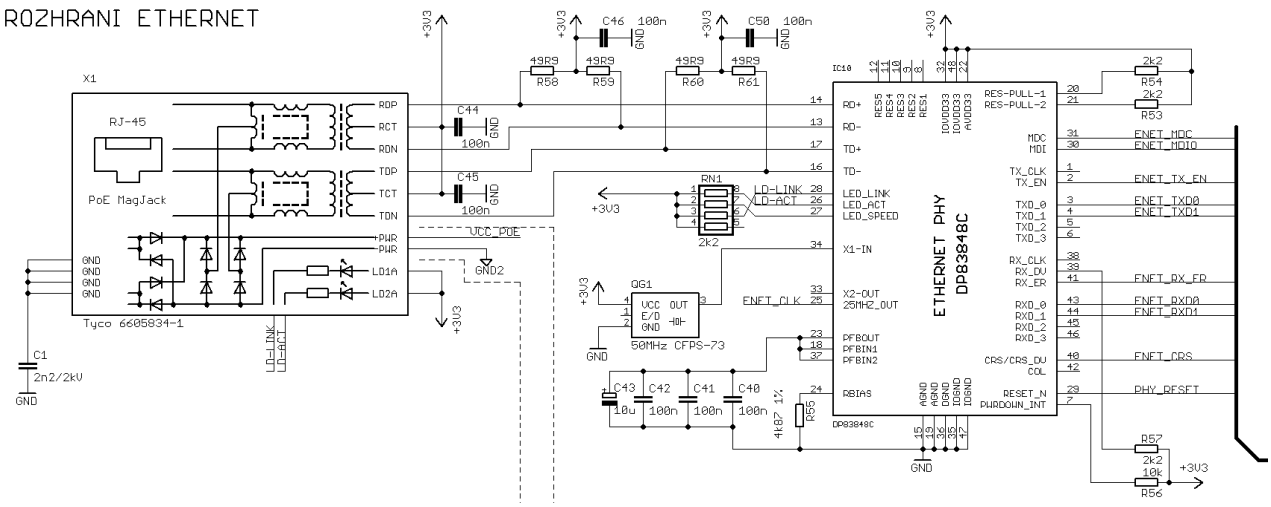
Patch kabel sítě Ethernet je zasunut do konektoru RJ-45. K signálovým vodičům je připojen impulsní transformátorek, který galvanicky odděluje ethernetový kabel od napájecích obvodů zařízení. Transformátorek má dvě oddělená jádra, jedno pro vysílání a druhé pro příjem dat, a bývá někdy vestavěn do stíněného tělesa konektoru – tento celek se označuje v angličtině jako Magjack (původně jde o registrovanou obchodní značku společnosti BEL Fuse, nicméně nyní užívanou jako obecné označení tohoto druhu součástek).

Obvod PHY

Sekundární vinutí transformátorku jsou připojena k obvodu fyzické vrstvy PHY (*PHYsical Interface*) [46], který zajišťuje převod proudu dat pro přenos sítí do vhodných signálů pro buzení vysílacího jádra transformátorku a zpětný převod signálů ze sekundárního vinutí přijímacího jádra transformátorku. Přesněji řečeno, provádí A/D a D/A převod, časování přenosu jednotlivých signálových prvků a převod kódování, tedy ve směru vysílání postupně kóduje data převody 4B5B, NRZI a MLT-3 (při provozu 100Base-TX). Moderní obvody PHY, jako je použitý IO DP83848C [47] firmy National Semiconductor, umožňují i další funkce, například automatické rozpoznání rychlosti sítě Ethernet a možnost připojení kříženým i standardním kabelem.

Nastavení obvodů PHY se provádí dvouvodičovým sériovým rozhraním MIIM *(Media Independent Interface Management).*

Jako rozhraní mezi obvodem PHY a obvodem MAC (*Media Access Controller*), tedy řadičem linkové vrstvy, se užívá jedno ze standardizovaných rozhraní MII *(Media Independent Interface*), RMII (*Reduced Media Independent Interface*) nebo proprietární rozhraní výrobců obvodů PHY.



Obr. 13: Obvody rozhraní Ethernet navržené ústředny

Ze schématu navrženého provedení obvodů rozhraní Ethernet (obr. 13) je zřejmé vnitřní zapojení konektoru Magjack (X2) a jeho propojení s obvodem PHY (IC2). Rezistory R1 až R4 slouží jako impedanční zakončení linky.

Obvod PHY dále spíná LED diody, umístěné v těle konektoru X2.

Z nevyužitých párů ethernetového kabelu a ze středů vinutí tlumivek, zapojených mezi datové vodiče rozhraní Ethernet, je pomocí diodových můstků, vestavěných v konektoru, odvozeno vstupní napětí (VCC_POE) pro měnič pro napájení ústředny podle standardu Power over Ethernet (PoE).

Blok MAC

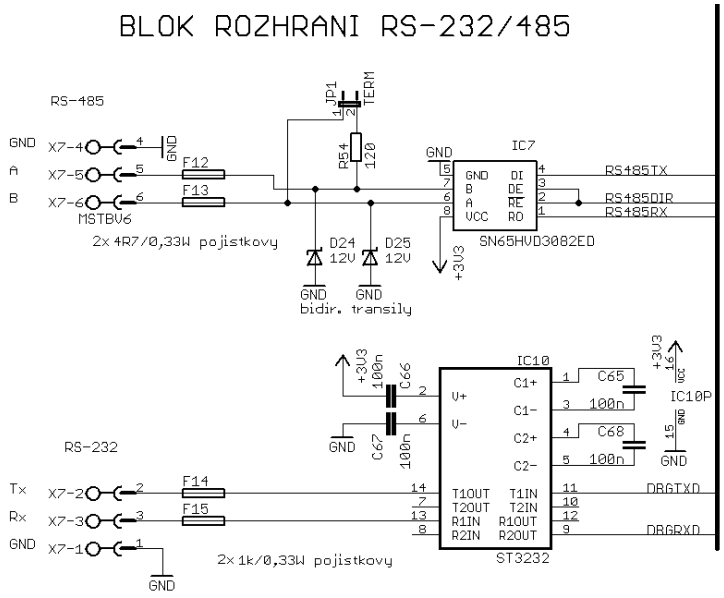
Blok MAC zajišťuje hardwarově některé funkce fyzické a linkové vrstvy rozhraní Ethernet: serializaci/deserializaci dat a přenos do vyrovnávací paměti pomocí DMA, filtrování přijatých dat podle MAC adresy zařízení a výpočet a kontrolu CRC kódů v rámci.

Mikrokontrolér IC7 je vybaven integrovaným blokem MAC, vybaveným rozhraním RMII [47] (*Reduced Media Independent Interface*) pro připojení k obvodu PHY.

Rozhraní RMII je synchronní rozhraní, pracující s hodinovou frekvencí 50 MHz a přenášející vždy paralelně dva datové bity v každém směru přenosu. Hodinový kmitočet rozhraní RMII je současně i referenčním kmitočtem pro časování přenosu obvodem PHY, a proto musí být zajištěna jeho přesnost: příslušný krystalový oscilátor (QG1 na obr. 13) musí mít odchylku nižší než 50 ppm.

Vodiče rozhraní RMII jsou na obr. 13 značeny názvy, začínajícími ENET.

2.2.2.2. Sériová asynchronní rozhraní



Obr. 14: Schéma zapojení obvodů rozhraní RS-232 a RS-485

RS-232

Rozhraní RS-232 bylo do návrhu ústředny doplněno spíše jako rozhraní pro základní ladění systému a nahrávání firmware do mikrokontroléru – jeho praktická využitelnost v systémech EZS je poměrně nízká, ačkoliv existují například GSM terminály, čtečky RFID karet, autentizační terminály, displeje nebo panelové tiskárny komunikující tímto rozhraním.

Nahrávání firmware do mikrokontroléru je možné pomocí rozhraní JTAG (konektor SV1) a pomocí asynchronního sériového portu 0 mikrokontroléru. Je-li při resetu mikrokontroléru uveden

pin P2.10 do logické nuly (zde stiskem tlačítka S2, vodič P014INP), nespustí se uživatelský program, ale z výroby předprogramovaný bootloader, komunikující po zmíněném sériovém portu 0. Počítač, připojený na tento port, je poté schopen pomocí speciálního programu (například NXP FlashMagic) programovat či verifikovat data v paměti FLASH mikrokontroléru.

Na obr. 14 je uvedeno elektrické zapojení rozhraní, které využívá převodník ST3232 (IC10) v katalogovém zapojení. Za zmínku stojí použití pojistkových rezistorů F14, F15, které do jisté míry spolu s vnitřní ESD ochranou IC10 omezují možnost poškození zařízení úmyslným přivedením přepětí na datové vodiče za cenu omezení maximální přenosové rychlosti portu.

RS-485

Rozhraní RS-485 umožňuje připojení až několika stovek zařízení (s užitým typem budiče až 320), komunikujících některým z protokolů, založených na tomto standardu. Typicky se jedná o čtečky RFID karet, biometrické čtečky, přístupové klávesnice a zařízení domovní automatizace, například teplotní čidla nebo průmyslové počítače (PLC).

Vzhledem k tomu, že k rozhraní může být připojena relativně dlouhá sběrnice, je použit kvalitní budič Texas Instruments SN65HVD1780 (IC7), který je vybaven ESD ochranou do 16 kV, vnitřními odpory pro zajištění polarity neaktivní sběrnice („fail-safe“) a budiči s omezením strmosti hran. Komunikační rychlost je maximálně 115 Kb/s.

Obvod je zajímavý povoleným přepětím na datových pinech A, B až +/– 70 V proti zemi; spolehlivá komunikace je nicméně možná jen při dodržení rozsahu napětí – 5 až + 12 V na obou vývodech.

Odolnost proti přepětí je zvýšena použitím obousměrných transilů D24, D25 a pojistkových rezistorů F12, F13, a to tak, aby linka RS-485 odolala i jednoduchému záměrnému útoku: v případě připojení datového vodiče A nebo B a země rozhraní přímo na napětí 230 V rozvodné sítě poteče obvodem proud kolem 30 A, který přeruší pojistkový rezistor podle [16] do 0,02 s, přičemž transil by neměl být nevratně poškozen (povolené přetížení transilu SMBJ 12 V je 200 A jednou půlvlnou [17] nebo 97 A impulsně v poměru 10:1000). Napětí na transilu nepřekročí zmíněnou přepěťovou odolnost budiče IC7.

Budič je připojen k asynchronnímu sériovému portu 2 IC7; přepínání směru komunikace je řízeno softwarově IC7 vodičem RS485DIR.

2.2.2.3. Rozhraní přídavných modulů

Navržený hlavní modul ústředny je vybaven rozhraním pro připojení přídavných modulů, které rozšiřují jeho vstupní a výstupní možnosti. Zejména jde o modul bezdrátového příjmu dat (viz ideový návrh v přílohze), dále prozatím neřešené moduly rozšiřující počet smyček, vstupů a výstupů, modul pro připojení interní klávesnice ústředny a modul GSM komunikátoru, jako který by měla být použitelná po úpravě firmwaru malá ústředna s GSM komunikátorem, kterou vyvinul

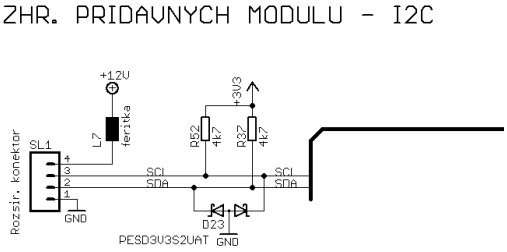
Bc. Zdeněk Dokulil (UTKO, FEKT) jako svou diplomovou práci.

Pro připojení přídavných modulů je definováno jednoduché specializované rozhraní, sestávající ze sběrnice I^2C a rozvodu napájení 12 V/300 mA na šestipinovém konektoru typu Molex IDC QF50.

Sběrnice I^2C (viz specifikace [18]) je jednoduchá dvouvodičová synchronní sériová sběrnice, umožňující adresování až 127 paralelně připojených zařízení (v rozšířeném módu 1023) a přenos dat rychlostí 100 kb/s v nejpomalejším módu sběrnice, který použijeme. Vodiče sběrnice pracují jako tzv. montážní součin: výstupy připojených zařízení (integrovaných obvodů) jsou v provedení s otevřeným kolektorem a klidovou úroveň log. 1 na sběrnici zajišťují pull-up rezistory. Sběrnice umožňuje spolupráci obvodů, napájených napětím 5 V a 3,3 V.

Pro tuto sběrnici rovněž existují hotové vstupní a výstupní moduly pro montáž na DIN lištu, které vyrábí firma MITE Hradec Králové, s r.o.

Na hlavním modulu ústředny je umístěn jeden konektor, na přídavných modulech je umístěna dvojice paralelně spojených konektorů tak, aby bylo možné zřetězeně připojovat další moduly. Konektory modulů ve vzniklé sestavě jsou propojeny kabelem o délce 15 cm, zakončeném samořeznými konektory. Plochý kabel by měl mít uspořádané vodiče tak, aby byly datové vodiče sběrnice vždy z obou stran obklopeny vodiči země nebo napájení 12 V, což přispívá ke snížení přeslechů.



Obr. 15: Zapojení konektoru přídavných modulů na hlavním modulu navrhované ústředny

Skutečné zapojení konektoru na hlavním modulu je uvedeno na obr. 15. Napájení přídavných modulů je jištěno vratnou polykrystalickou pojistkou 300 mA. R37 a R52 tvoří pull-up rezistory sběrnice.

Jako ESD ochrana sběrnice slouží dvojitý transil typu PESD5V0U2BT firmy NXP (D23) v miniaturním pouzdru SOT-23. Jde o poměrně inovativní prvek, vyznačující se sníženou kapacitou transilů na pouhých 2,9 pF [19] – běžné hodnoty u srovnatelných transilů se pohybují ve stovkách pF a znemožnily by funkci sběrnice.

Maximální počet modulů v sestavě je omezen celkovou parazitní kapacitou sběrnice I^2C a odporem napájecích vodičů.

Vysoká kapacita sběrnice způsobuje zkreslení hran, zejména z důvodu časové konstanty RC členu pull-up rezistoru a kapacity sběrnice, a tedy vznik chyb při přenosu dat. Specifikace [18] stanovuje maximální povolené kapacity sběrnice pro různé hodnoty pull-up rezistorů a pro různá napájecí napětí. V návrhu (obr. 16) užité pull-up rezistory 2,2 kΩ podle [18] dovolují práci s kapacitou sběrnice do 350 pF.

Kapacita datového vodiče sběrnice proti zemi se skládá z kapacity kabelu, konektorů, spojů na DPS a vstupních kapacit připojených součástek.

Na plochém kabelu AWG28 o délce 15 cm, osazeného zvolenými konektory, byla měřením zjištěna kapacita mezi vodičem, připojeným na dutinku 3 konektoru, a zkratovanými ostatními vodiči 12 pF (měřeno LC můstkem BM509 při 1 kHz).

Kapacita 10 cm dlouhého spoje na čtyřvrstvém plošném spoji proti zemní ploše je 7,9 pF (vypočteno programem TraceSim pro materiál FR4 a šířku spoje 0,3 mm), vstupní kapacity pinů sběrnice integrovaných obvodů s podporou I^2C se pohybují v rozmezí 7 až 15 pF: budeme uvažovat nejnepříznivější hodnotu.

Tabulka 3 shrnuje součásti celkové kapacity datového vodiče sběrnice pro jeden přídavný modul.

Položka	***Kapacita [pF]***
Kabel sběrnice s konektorem	12
Spoj na DPS (10 cm)	7,9
Vstupní kapacita IO	15
Kapacita přepěťové ochrany (transilu)	2,9
Součet	**38**

Tabulka 3: Celková kapacita vodiče SDA nebo SCL na jeden připojený přídavný modul

V případě hlavního modulu nemusíme uvažovat kabel sběrnice, zato je na sběrnici připojen LCD displej (viz oddíl 2.2.3.3) s měřením zjištěnou kapacitou vývodů sběrnice a svého konektoru 10 pF.

Kapacita vodiče sběrnice na hlavním modulu je tedy 36 pF.

Budeme-li uvažovat 50 % rezervu oproti povolené kapacitě sběrnice 350 pF, můžeme podle jednoduše vypočítat maximální počet přídavných modulů na sběrnici rovnicí

$$N = \frac{C_{\max}/1{,}5 - C_{\mathrm{HM}}}{C_{\mathrm{PM}}} = \frac{350/1{,}5 - 36}{38} = 5{,}19 \Rightarrow N = \underline{5} \qquad [-;\mathrm{pF},\mathrm{pF},\mathrm{pF}] \qquad (1)\ ,$$

kde N je počet modulů, C_{max} je povolená kapacita sběrnice, C_{HM} a C_{PM} jsou kapacity na jeden hlavní, resp. přídavný modul.

Na sběrnici můžeme tedy připojit celkem 5 přídavných modulů, pro další prodloužení by bylo nutné použít opakovač.

Pro kontrolu ještě vypočteme odpor kabeláže sběrnice, je-li celková délka kabelu 1 m. Při katalogem [20] udaném průřezu 0,087 mm^2 je odpor jednoho vodiče

$$R_\mathrm{v} = \rho \frac{l}{S} = 0{,}0178.10^{-6} \frac{1}{(0{,}087.10^{-6})} = \underline{\underline{0{,}2\,\Omega}} \qquad [\Omega\,;\Omega\,\mathrm{m}^{-1,}\,\mathrm{m}\,,\mathrm{m}^{-2}] \qquad (2)\ .$$

Úbytek napětí na zdvojených napájecích vodičích bude při maximálním proudu 300 mA podle Ohmova zákona jen

$$\Delta U = R\,I = \frac{R_\mathrm{v}}{2} I = \frac{0{,}2}{2} 0{,}3 = 0{,}03\,\mathrm{V} \qquad [\mathrm{V}\,;\Omega\,,\mathrm{A}] \qquad (3)\ .$$

Přes poměrně nízký průřez vodičů tedy neohrožuje hodnota napěťových úbytků správnou funkci připojených přídavných modulů a je hluboce pod šumovou imunitou sběrnice I^{2}C (0,33 V podle [18]).

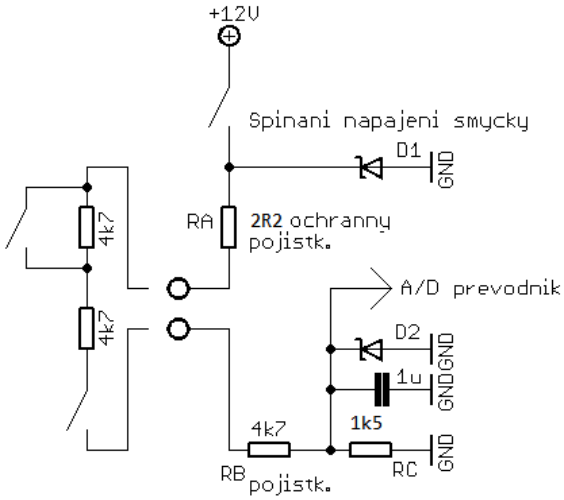
Překročen není ani maximální proud plochým kabelem, který je například pro kabel Belden AWG28 1,1 A pro oteplení o 10 K [21].

2.2.3. Obvody vstupů a výstupů

2.2.3.1. Drátové smyčky

Mikrokontrolér IC7 obsahuje desetibitový A/D převodník s integrovaným přepínačem s šesti vstupy. Čtyři z těchto vstupů vyhodnocují čtyři vstupy drátových smyček.

Obvod každé smyčky je zapojen jako odporový dělič podle obr. 17.



Obr. 16: Princip obvodu drátové smyčky

Účelem bylo navrhnout takové zapojení, které bude účinně chráněno proti zničení výkonného jádra ústředny záměrně přivedeným přepětím a které bude schopno detekovat jednoduchou sabotáž kabeláže, například zkrat vodičů smyček navzájem nebo v oddílu 1.2.1.1. naznačenou sabotáž vnějším zdrojem.

Napájení každé smyčky je spínáno polovodičovým spínačem, který je softwarově řízen tak, aby s periodou přibližně 50 ms spínal a rozpínal. Na konci tohoto času bude vyhodnoceno, zda byl přerušen průchod proudu smyčkou – nestane-li se tak, je smyčka napájena z obvodu jiné smyčky (spínání napájení jednotlivých smyček je asynchronní) nebo cizího zdroje a je nutné ji považovat za vadnou či sabotovanou. Výstupní impulsy běžných čidel mají šířku minimálně 200 ms, takže nedojde k případné ztrátě informace o narušení objektu. Tento mechanismus je v dalším textu označován jako *protisabotážní ochrana.*

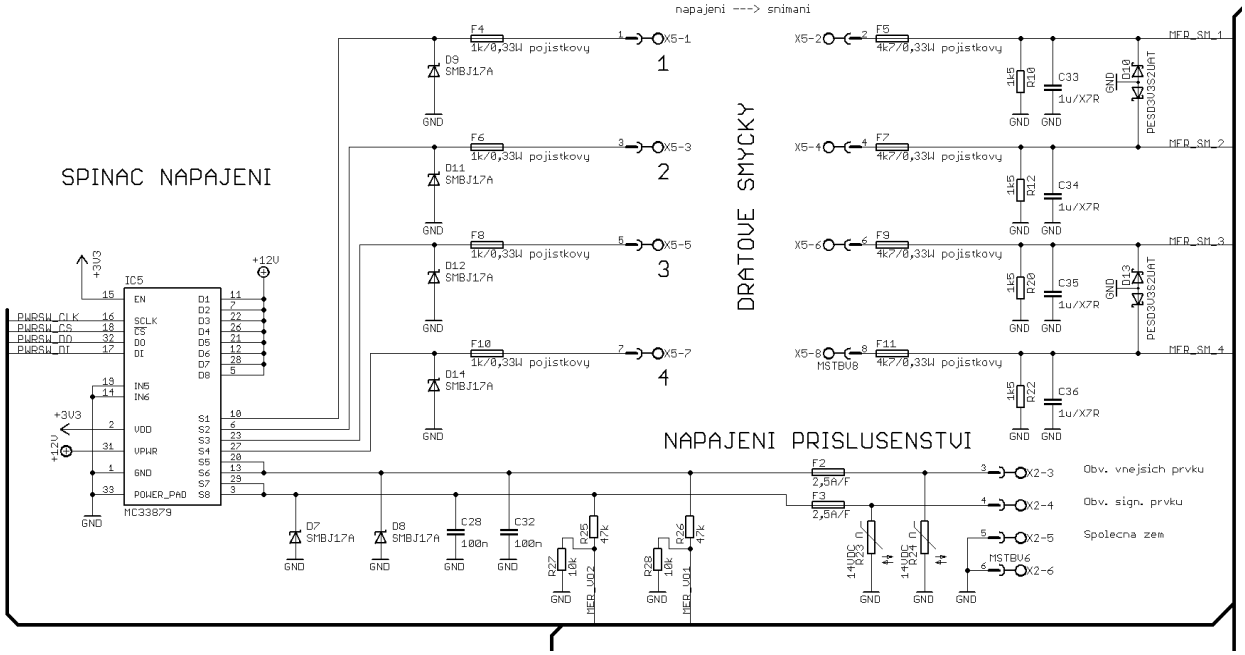
Není-li smyčka zcela rozpojena, prochází všemi rezistory v obvodu ústředny proud, který vyvolává úbytek na rezistoru R_C. Tento úbytek je snímán A/D převodníkem IC7 a se znalostí aktuální hodnoty napájecího napětí ústředny ve větvi +12 V, jehož měření je popsáno v oddílu 2.2.5.3, může být vyhodnocen stav smyčky.

Jako ESD i klasická přepěťová ochrana obvodů smyček slouží dva transily. Transil D1 je

dimenzován na napětí 17 V a slouží jako ochrana výstupu elektronického spínače. Při déletrvajícím vnějším přepětí na napájecí svorce smyčky se přepálí pojistkový rezistor R_A, který je jinak zvolen tak, aby zkratuvzdornost výstupu napájení smyčky proti zemi zajišťovala elektronická pojistka v elektronickém spínači napájení smyčky (IC5) bez toho, aby se rezistor R_A přepálil.

Transil D2 má závěrné napětí 3,3 V a chrání vstup A/D převodníku. Pojistkový rezistor R_B se rovněž při dlouhotrvajícím přepětí přepálí, aby uchránil A/D převodník a D2 před přetížením.

Kondenzátor 1 μF slouží spolu s vnitřním odporem děliče jako RC filtr s časovou konstantou $\tau = 1{,}3$ ms. Vzhledem k tomu, že postačí relativně pomalé vyhodnocování průměrováním posledních výstupních vzorků A/D převodníku a že vstupní signál je téměř stejnosměrný, není nutné používat složitější antialiasingové filtry.



Obr. 17: Zapojení vstupů drátových smyček a výstupů napájení příslušenství

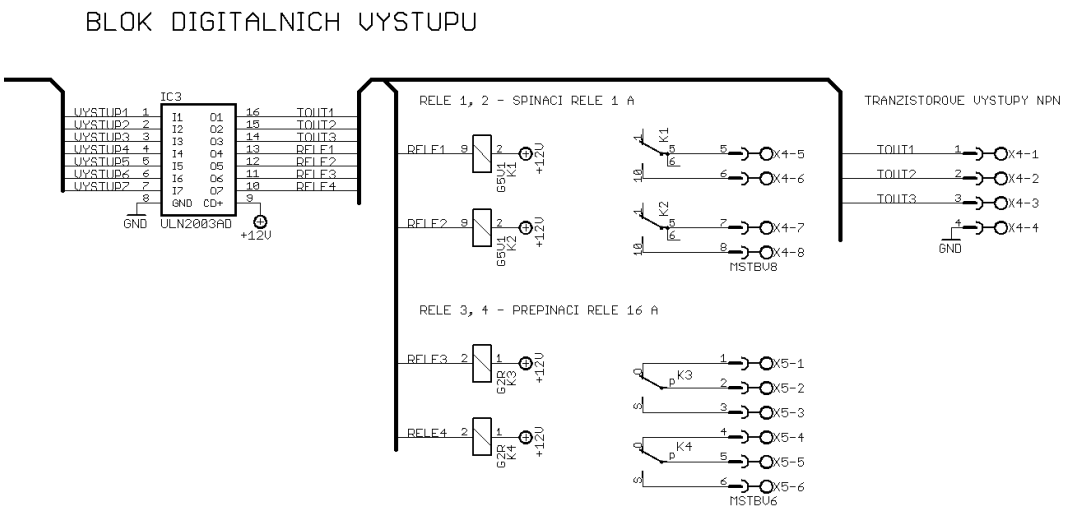
Na obr. 17 je uvedeno skutečné zapojení obvodů drátových smyček. Jako elektronický spínač je využit obvod Freescale MC33879 [22], osminásobný elektronický spínač s elektronickou pojistkou a detekcí rozpojení obvodu a zkratu, řízený sériovou sběrnicí SPI mikrokontrolérem IC7. Jeho první čtyři sekce spínají napájení smyček, výstupy zbývající čtveřice slouží jako elektronická pojistka obvodů napájení příslušenství, popsaných v oddílu 2.2.5.3. Výhodou obvodu je mimo jiné i omezení strmosti změn výstupního napětí (slew-rate limiting), snižující úroveň rušení, emitovaného vodiči smyček.

Vlastní obvod smyčky je osazen čtyřikrát zcela shodně, popíšeme tedy smyčku č. 1. Elektronický

spínač IC5 přivádí napětí větve +12 V na pojistkový rezistor F4 a první svorku konektoru X5. Proud prochází smyčkou a vrací se na druhou svorku X5 a přes pojistkový rezistor F5 vstupuje uzlu s R10, C33, anodou jedné poloviny dvojitého transilu D10 a jako vodič MER_SM_1 pokračuje na vstupní vývod A/D převodníku IC7.

2.2.3.2. Tranzistorové a reléové výstupy

Sedm vývodů portu 1 IC7 ovládá vodiči VYSTUP1 až VYSTUP7 tranzistorové a reléové výstupy zařízení.



Obr. 18: Schéma zapojení obvodů digitálních výstupů

Úrovně CMOS 3,3 V z vodičů VYSTUP jsou proudově posíleny pomocí IO ULN2003 (IC2 na obr. 18). ULN2003 je sedminásobný výkonový spínač typu NPN s povoleným výstupním proudem 200 mA z každého výstupu. Obvod je vybaven diodami pro ošetření napěťových špiček od indukční zátěže, připojenými na společný vývod CD+.

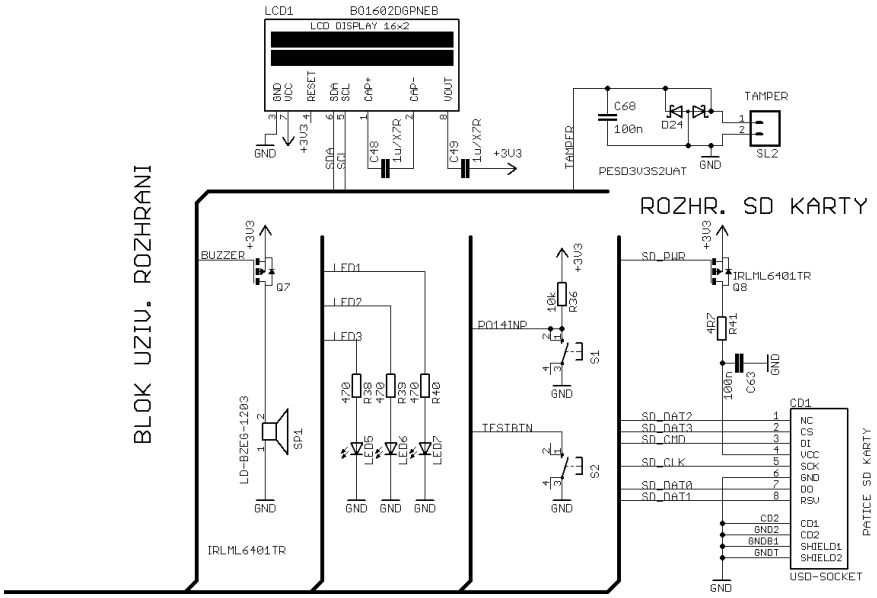
Čtyři výstupy obvodu IC2 spínají elektromechanická relé, dvě signálová s vyvedeným spínacím kontaktem a dvě výkonová, která mají vyveden spínací i rozpínací kontakt. Zbylá trojice výstupů IC2 je vyvedena na svorkovnici X4 jako tranzistorové výstupy. Tyto tranzistorové výstupy by neměly být nechráněně zapojovány do vnějších obvodů ústředny, nemají nadproudovou ani přepěťovou ochranu. Případné přepětí může projít přes strukturu IC2 do větve + 12 V napájení.

2.2.3.3. Místní servisní ovládání

Ústředna je vybavena jednoduchým místním ovládáním: jde o dvojici tlačítek, trojici LED diod a pozicí pro případné osazení LCD displeje.

Dvojice tlačítek je připojena přímo k pinům mikrokontroléru vodiči P014INP a TESTBTN.

Tlačítko S2, ovládající pin P014INP, slouží také k aktivaci bootloaderu mikrokontroléru IC7 pro nahrávání firmware prostřednictvím rozhraní RS-232 (viz odd. 2.2.1.2). Toto tlačítko nemůže využívat interní pull-up rezistor portu mikrokontroléru IC7 pro definici klidového stavu vodiče PO14INP jako tlačítko S1, protože pull-up rezistory nejsou při resetu IC7 aktivní a mohlo by dojít k nechtěnému spuštění bootloaderu.



Obr. 19: Schéma bloku uživatelského rozhraní a rozhraní SD karty

Součástí hlavního modulu je i připravená pozice pro alfanumerický LCD displej. Byl zvolen typ Bolymin DO1602DGPNEB (LCD1) v provedení COG bez podsvětlení a umožňuje zobrazit celkem 32 znaků textu na dvou řádcích. Displej může servisního technika informovat o stavu zařízení (např. přiřazené IP adrese nebo stavu smyček) a bude montován přímo na desce ústředny – nejde tedy o rozhraní pro uživatele. Data jsou displeji zasílána rozhraním I^2C, společným s rozhraním přídavných modulů. Současná verze softwaru ústředny prozatím s LCD displejem nepočítá.

Tranzistor Q7, řízený vodičem BUZZER z mikrokontroléru IC7, spíná miniaturní sirénku, osazenou na plošném spoji.

LED diody jsou na plošném spoji označeny jako ACT, RUN a COMM. LED dioda ACT je ovládána softwarově skripty ústředny, dioda RUN blikáním indikuje správnou funkci operačního systému a dioda COMM svítí, přenáší-li WWW server data.

Sabotážní kontakt ústředny (například při zavřené skříni ústředny sepnutý mikrospínač) je připojen do konektoru *TAMPER* (SL2).

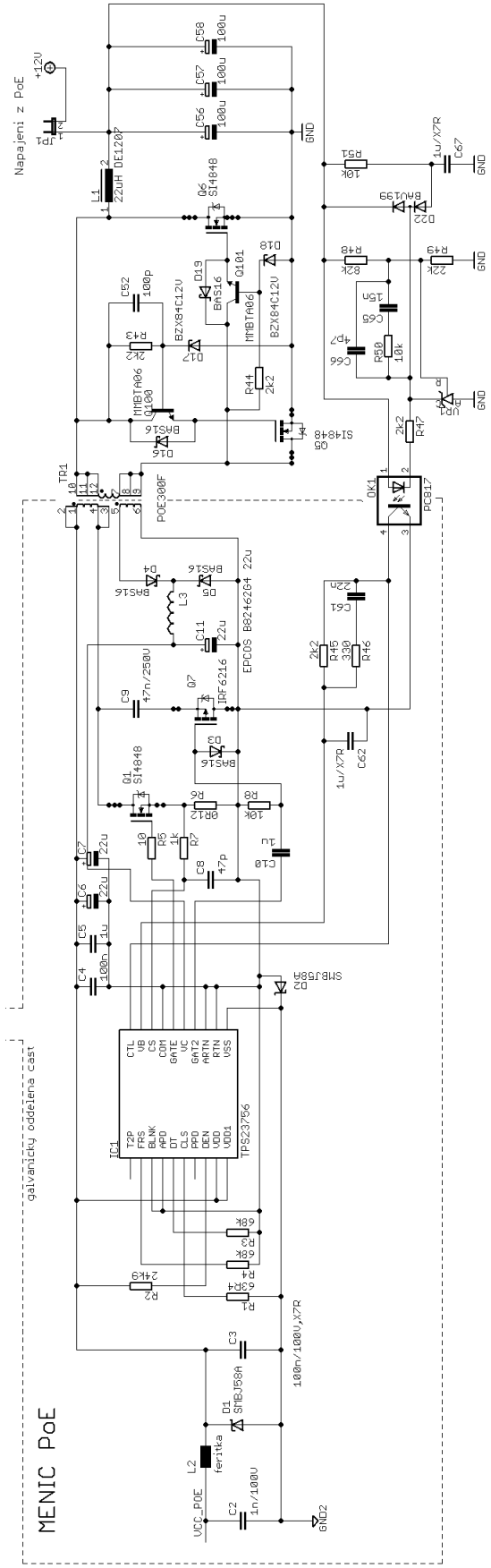
2.2.4. Rozhraní paměťové karty

Paměťová karta typu mikroSD je vložena v patici CD1.

Karta je připojena čtyřbitovým paralelním rozhraním [23] k řadiči SD karty, integrovanému v mikrokontroléru IC7. Toto rozhraní umožňuje vyšší rychlost přenosu dat oproti často využívanému rozhraní SPI, vhodnému zejména pro jednoduché aplikace a pro mikrokontroléry, které nemají vestavěný řadič.

Karty typu mikroSD sice podporují nízkospotřebový režim i softwarový reset karty, nicméně i oficiální dokumentace rozhraní karty doporučuje zařadit elektronický spínač do napájecího obvodu karty, aby bylo možné kartu hardwarově odpojit, resp. vyresetovat. Proto spíná napájení karty na pokyn mikrokontroléru tranzistor Q8.

Rezistor R41 omezuje proudovou špičku při jeho sepnutí, vyvolanou nabíjením kondenzátoru C63 a blokovacího kondenzátoru o kapacitě až 1 μF, který je součástí paměťové karty. Pokud by nebyla velikost proudové špičky omezena, by při sepnutí tranzistoru Q8 vzniknout krátkodobé podpětí napájecího napětí 3,3 V, schopné způsobit BOD reset mikrokontroléru.



Obr. 20: Schéma zapojení měniče pro napájení PoE

2.2.5. Obvody napájení

Hlavní modul ústředny umožňuje napájení ze sítě Ethernet podle standardu PoE nebo přímým připojením zdroje 12 V do svorkovnice ústředny. Jako vnější zdroj může být použit zálohovaný napáječ, například výrobek 2N Energy Bank nebo Jablotron BP-12.

2.2.5.1. Měnič pro napájení systémem PoE

Systém Power over Ethernet

Technologie Power over Ethernet slouží k přenosu elektrické energie spolu s daty strukturovanou kabeláží sítě Ethernet. Užívají se kabely kategorie 5 nebo vyšší.

Původní standard IEEE 802.3af umožňoval přenos výkonu 12,95 W, nově schválený standard IEEE 802.3at *(Power over Ethernet Plus)* ze září 2009 již dovoluje přenos výkonu až 30 W [24].

Pro přenos elektrické energie se užívá buď nevyužitých párů v kabelu sítě Ethernet, nebo fantomového napájení datovými páry. Použité napětí je 42 – 57 V.

Napájené zařízení musí být vybaveno obvody, které umožní napáječi (tzv. injektoru) PoE rozpoznat *třídu* zařízení, která udává maximální odebíraný proud. Teprve poté může začít napájené zařízení odebírat výkon z injektoru.

Měnič pro napájení systémem PoE

Navržený měnič (obr. 20) poskytuje napájecí napětí 12 V pro obvody ústředny a vnějších částí systému, například čidel nebo sirén.

Použité zapojení měniče je založeno na obvodu TPS23756 firmy Texas Instruments [25], který již implementuje standard IEEE 802.3at, a je téměř beze změn založeno na zapojení firemního demonstračního

kitu pro výstupní napětí 12 V a proud 2 A s deklarovanou účinností překračující 85 % (v lit [26]). Měnič je galvanicky oddělený a používá zatím vcelku málo rozšířenou propustnou topologii s aktivní demagnetizací (*active-clamp forward*), která umožňuje dosáhnout dobré účinnosti s menšími rozměry transformátoru než klasická topologie propustného měniče s demagnetizačním vinutím nebo blokujícího měniče (*flyback*).

Napájecí napětí, usměrněné můstkovými usměrňovači, vestavěnými v Magjack konektoru (viz obr. 13) je vedeno vodiči VCC_POE a GND2 na vstup měniče.

Vestavěný spínač s tranzistorem N-MOSFET v integrovaném obvodu TPS23756 (IC1) připojí výkonový obvod měniče k napájení až po úspěšné identifikaci se injektoru (norma používá termín *classification*). Zajímavé je, že se odpojují i vstupní elektrolytické kondenzátory měniče (C6, C7).

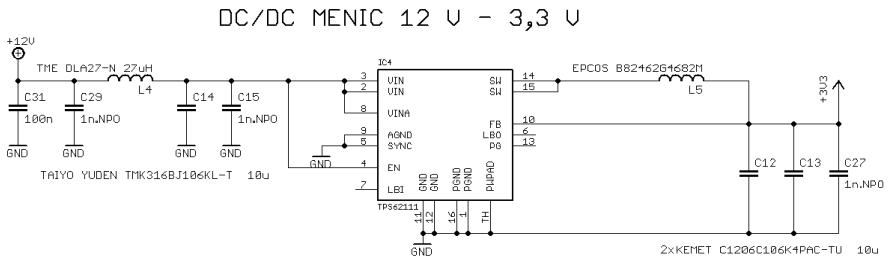
Vlastní měnič užívá externí tranzistory typu MOSFET, hlavní spínač Q1 je N-MOSFET s povoleným napětím U_{DS} 150 V a odporem kanálu v sepnutém stavu 85 mΩ.

Transformátorek POE300 (L1, [27]) je výrobek britské firmy Coilcraft s rozměry 21 x 11 x 25 mm, schopný přenášet výkon až 30 W. Sekundární strana měniče používá aktivní usměrňovač, rovněž s tranzistory MOSFET.

Regulační smyčka měniče užívá programovatelnou napěťovou referenci TL431 (VR1). Obvod C67, D22 a R51 zajišťuje plynulý náběh výstupního napětí měniče.

2.2.5.2. Měnič napájení logiky systému

Všechny obvody logiky hlavního modulu ústředny jsou napájeny napětím 3,3 V, které vytváří měnič s IO TPS62111 firmy Texas Instruments.



Obr. 21: Schéma zapojení měniče 12/3,3 V

Tento obvod (obr. 21, IC4) je základem step-down měniče s pracovní frekvencí 1 MHz a účinností kolem 82 % při výstupním proudu 300 mA [28]. Maximální výstupní proud měniče je 1 A.

Vysoká pracovní frekvence umožnila návrh zapojení tohoto měniče bez elektrolytických

kondenzátorů, které jsou v dlouhodobém provozu častou příčinou poruch.

2.2.5.3. Napájení obvodů příslušenství

Obvody, napájející vnější prvky ústředny, jsou kromě samozřejmé možnosti zkratu vlivem poruchy ohroženy i případným záměrným útokem, spočívajícím v přivedení přepěťového impulsu, který může poškodit i elektroniku ústředny.

Obvody vnějších prvků navrhované ústředny jsou rozděleny na dvě sekce:

•obvod signalizačních prvků, napájející sirénu či sirény, a

•obvod vnějších prvků, napájející ostatní součásti systému, zejména aktivní čidla.

Tyto obvody jsou napájeny napětím 12 V a každý z nich umožňuje odebírat proud až 1,2 A (celkový maximální odebíraný proud závisí na použitém napájecím zdroji).

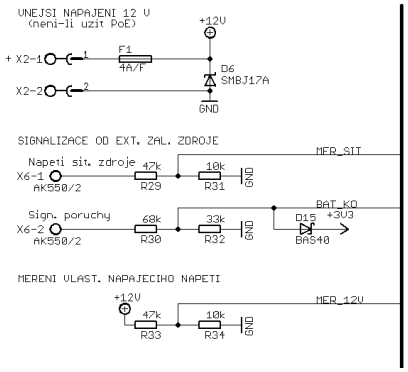
Oba obvody jsou jištěny samostatně: o*bvod signalizačních prvků* musí být vzhledem k možnosti připojení nezálohované sirény schopen práce i v případě, kdy je *obvod vnějších prvků* v poruše. (Jako hlavní siréna se v instalacích EZS někdy užívá poměrně nákladná *zálohovaná siréna*, která je napájena z vlastního záložního akumulátoru a spouští se odpojením napájení, je tedy odolná proti sabotáži odpojením napájení z ústředny, resp. zničením napájecího zdroje ústředny.)

Obvody jsou jištěny elektronickou pojistkou – součástí spínačů v obvodu Freescale MC33879 (IC5, viz schéma zapojení na obr. 17). Tato pojistka odepíná výstup od napájení, je-li překročen proud typicky 0,6 A, pro použitou paralelní kombinaci dvou výstupů je tedy vypínací proud typicky 1,2 A. Příslušné elektronické spínače v IC5 jsou trvale sepnuté, jsou tedy užity jen jejich elektronické pojistky.

Řešení elektronické pojistky v IC5 je poměrně zajímavé: obvod nejdříve omezuje proud na hodnotu vypínacího proudu a teprve po několika sekundách je výstup odpojen na základě snímání lokálního přehřátí čipu IO [25]. Po odstranění zkratu se napájení příslušného výstupu automaticky obnoví.

Aktivaci elektronické pojistky může mikrokontrolér zjistit čtením stavového registru IC5 po sběrnici SPI, ale hlavním signálem o selhání jednoho z okruhů napájení je pro software zařízení naměřená skutečná hodnota napětí na výstupech napájení. Vodiče MER_VO1 a MER_VO2, připojené k A/D převodníku IC7 přes elektronický přepínač IC6, snímají přes odporové děliče napětí na obou výstupech.

Výstupy jsou dále vybaveny ochranou transily D7, D8, varistory R23, R24 a tavnými pojistkami F2, F3. Tyto pojistky se za normálního provozu nemohou přepálit, protože dříve vybaví pojistka v obvodu IC5, ale uplatní se při přivedení vnějšího přepětí.



Obr. 22: Pomocné napájecí obvody

Na obr. 22 jsou uvedeny dosud nepopsané pomocné obvody napájení: svorky X2 slouží pro připojení napájecího zdroje, není-li užito napájení systémem PoE.

Případný vnější zálohovaný zdroj je možné monitorovat analogovým vstupem pro měření výstupního napětí jeho síťového zdroje a jedním digitálním vstupem (oba jsou vyvedeny na svorkovnici X6).

Dělič R33/R34 slouží pro měření vlastního napájecího napětí ve větvi +12 V, zejména pro vyhodnocování selhání napájecího zdroje a stavu drátových smyček. Střední bod tohoto děliče a děliče analogového vstupu měření napětí síťového zdroje je zaveden do elektronického přepínače IC6 a z něj do vstupu integrovaného A/D převodníku mikrokontroléru IC7.

Transil D6 tvoří přepěťovou ochranu větve napájení + 12 V.

2.3. Plošný spoj a mechanická konstrukce hlavního modulu ústředny

2.3.1. Návrh plošného spoje ústředny

Prototyp hlavního modulu ústředny byl realizován v jednodeskovém provedení na oboustranném prokoveném plošném spoji o rozměrech 160 x 107 mm v 7. konstrukční třídě s šířkou spojů a mezer minimálně 0,18 mm.

Je užita kombinovaná montáž vývodových součástek i součástek v provedení SMD ze strany součástek plošného spoje. Ze strany spojů je osazeno pouze několik blokovacích kondenzátorů v provedení SMT.

Návrh plošného spoje byl proveden v souladu s pravidly pro dosažení dobré elektromagnetické kompatibility (zejména šlo o rozmístění blokovacích kondenzátorů, a užití ploch „rozlité mědi“ na obou stranách plošného spoje), nicméně měření vyzařování ani odolnosti nebyla provedena.

Povrchové cesty – vzdálenosti mezi spoji od svorkovnice X3 ke kontaktům výkonových relé jsou zvoleny v souladu s požadavky normy ČSN EN 60950-1 na spoje, připojené k síti 230 V.

Plošný spoj je navržen tak, aby bylo možné osadit SMD součástky osazovacím automatem, zapájet přetavením a následně doosadit klasické součástky a zapájet stranu spojů pájecí vlnou.

Návrh plošného spoje byl proveden v systému Eagle 5.6 bez použití autorouteru.

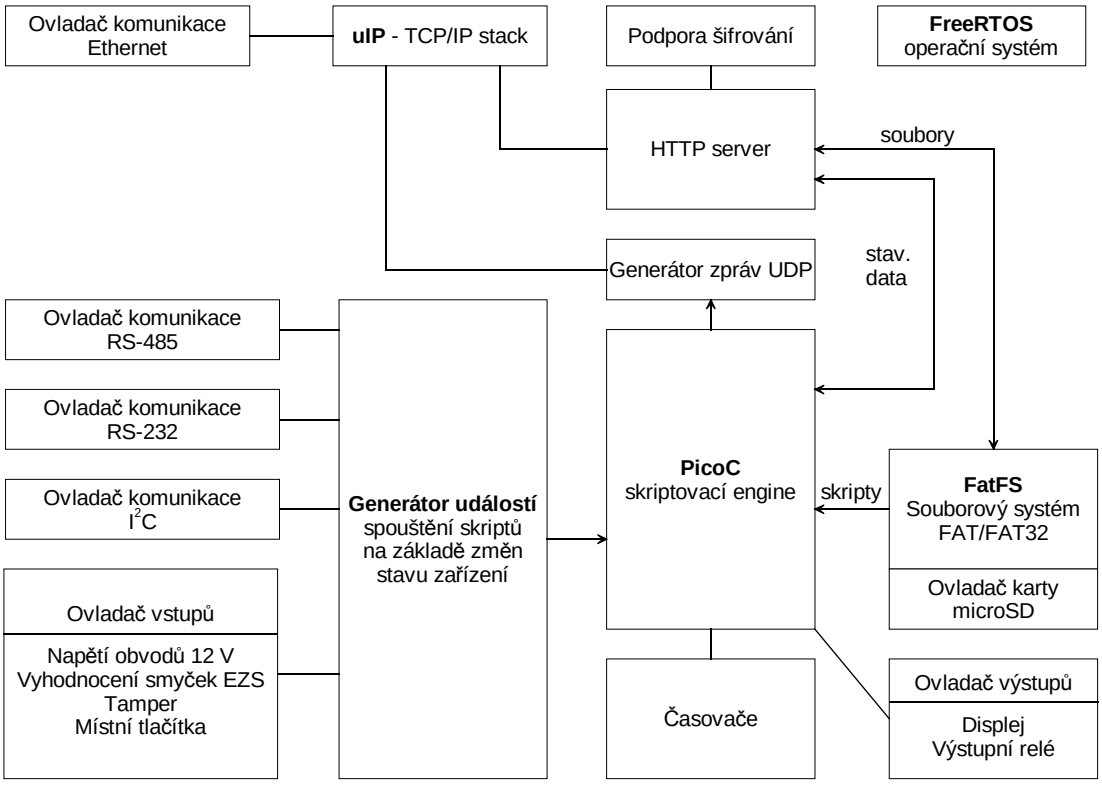
Plošný spoj je opatřen potiskem ze strany součástek.

2.3.2. Mechanická konstrukce ústředny

Deska hlavního modulu ústředny je vložena do sestavy držáku Italtronic E107CM. Držák je možné vybavit úchytkou pro montáž na DIN lištu nebo nožkami pro uchycení na montážní desku rozvaděče.

Celkové rozměry hlavního modulu včetně držáku jsou 164 x 126 x 47 mm.

2.4. Softwarové řešení



Obr. 23: Softwarová struktura navrhované ústředny EZS

Softwarové řešení logiky ústředny za pomoci skriptování (viz oddíl 2.1) vyžaduje následující následující programové celky:

•operační systém, umožňující současný běh procesů pro komunikaci sítí Ethernet a vlastní logiky zabezpečovacího zařízení,

•modul, zajišťující bezpečný přenos dat sítí Ethernet a skládající se z ovladače linkové vrstvy Ethernet, TCP/IP stacku, HTTP serveru a podpory šifrování,

•ovladače jednotlivých vstupních a výstupních periferií systému, například komunikačních linek RS-232, RS-485, výstupních relé a vstupů drátových smyček,

•engine skriptovacího jazyka a *generátor událostí*, tedy proces, zajišťující spouštění skriptů na základě změn stavů vstupů a dalších vnějších událostí,

•podpůrné součásti systému, zejména ovladač souborového systému s možností čtení a zápisu na paměťovou kartu a časovače, zajišťující zpožděné nebo periodické spouštění vybraných skriptů, například vypnutí sirény po uplynutí stanoveného času.

Vzájemnou spolupráci těchto bloků naznačuje schéma na obr. 23.

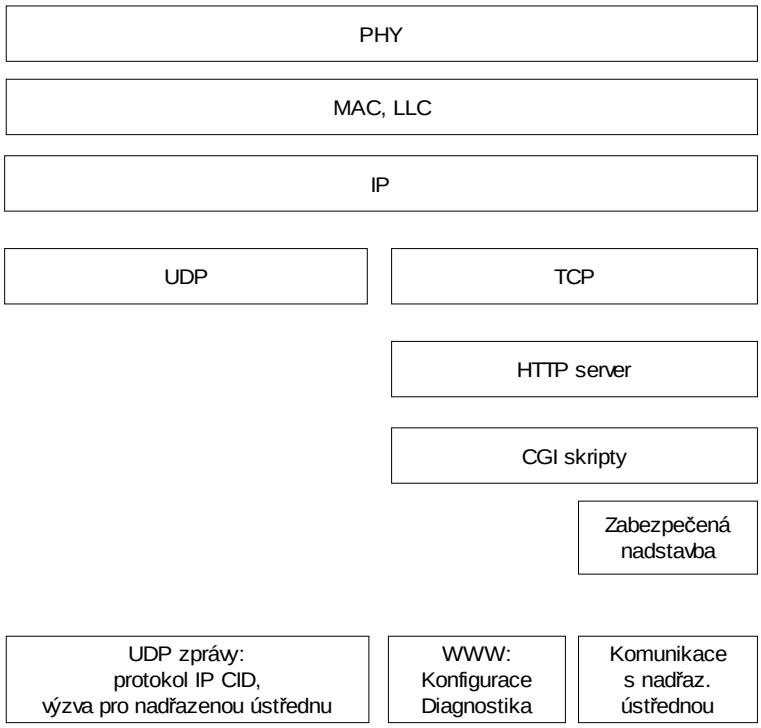
2.4.1. Přenosy dat sítí Ethernet

Navržená ústředna umožňuje komunikaci těmito metodami:

•pomocí vestavěného WWW serveru – protokolem HTTP pro konfiguraci a diagnostiku stavu zařízení,

•specializovaným protokolem pro zabezpečený přenos dat mezi zařízením a nadřazenou ústřednou a

•protokolem UDP pro zasílání krátkých informačních zpráv, generovaných skripty.



Obr. 24: Komunikační možnosti navrhované ústředny a jejich zařazení v softwarové struktuře zařízení

Vzhledem k požadavku na dodržení nízké výrobní ceny zařízení byl zvolen mikrokontrolér s relativně malou pamětí RAM, který neumožňuje implementaci protokolů HTTPS/ TLS – WWW rozhraní pro konfiguraci ústředny tedy používá nezabezpečený přenos dat, nicméně pro bezpečnostně náročnější aplikace v sestavě s nadřazenou ústřednou je možné využít jednoduchý specializovaný zabezpečený protokol.

2.4.1.1. WWW konfigurační a diagnostické rozhraní

Pro základní konfiguraci a diagnostiku zařízení běží na portu TCP/80 zařízení WWW server, který umožňuje zobrazení stavu zařízení (zejména napájecích obvodů a stavů smyček), operačního systému a výpis aktivních TCP spojení. Jednotlivé WWW stránky jsou uloženy na SD kartě jako soubory; soubory s příponou .sht WWW server před odesláním protokolem HTTP prochází a

hledá příkazy, které nahrazuje za volání funkcí, napsaných v jazyce C, které do výsledné WWW stránky doplňují on-line generované informace, například výpis běžících úloh operačního systému.

Pomocí WWW rozhraní je možné i uživatelsky modifikovat parametry zařízení změnou *systémových proměnných* - k dispozici je 128 proměnných typu int v systémovém poli CVals[], které jsou uloženy v baterií zálohované oblasti paměti RAM.

Přístup do WWW rozhraní je chráněn heslem, které vyhodnocuje jeden ze skriptů a podle zadaného hesla zasílá cookie uživateli a přiděluje uživatelská práva (jde o skript *ethauth.s*, viz příloha A).

V příloze C jsou uvedeny příklady stránek, generovaných WWW rozhraním ústředny.

2.4.1.2. Protokol pro komunikaci s nadřazenou ústřednou

Pro zajištění bezpečného přenosu systémových dat (tedy informací o stavu ústředny a příkazů ústředně) mezi navrhovanou ústřednou v roli podřízené ústředny a nadřazenou softwarovou ústřednou byla navržena jednoduchá nadstavba protokolu HTTP.

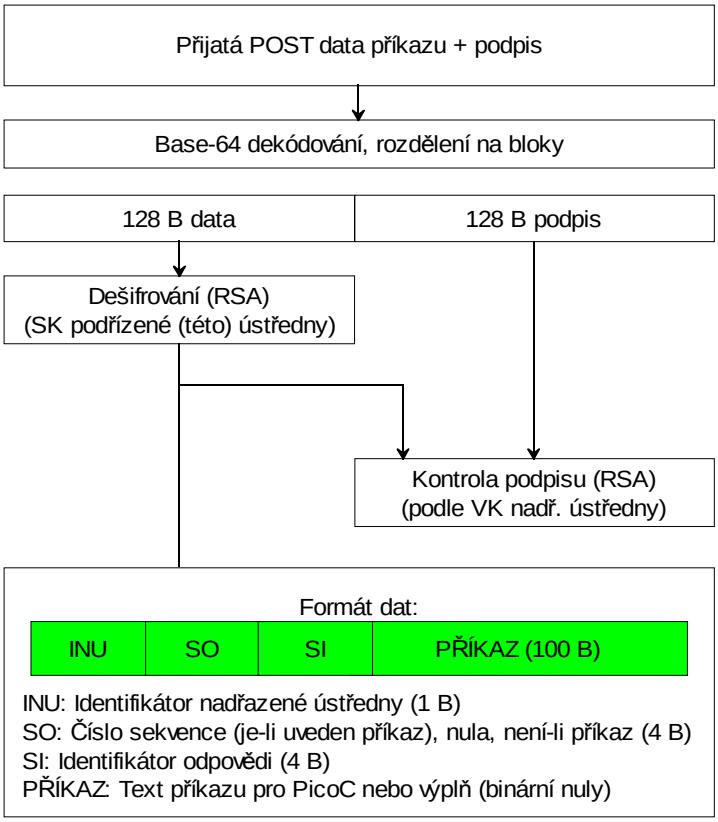
Požadujeme zajištění důvěrnosti, integrity i autenticity. Cizí útočník nesmí být schopen sledovat přenášená data (spojem mohou být v závislosti na konkrétní implementaci zasílána například přístupová hesla), nesmí být schopen data narušit (například změnit příkaz „odepři přístup“ na „povol přístup“) a nesmí mít možnost provádět útok typu man-in-the-middle nebo nahradit nadřízenou ústřednu falešným zařízením.

Poměrně omezené paměťové prostředky použitého mikrokontroléru nedovolují realizaci standardního TLS spojení s autentizací obou stran prostřednictvím certifikátů. Na druhou stranu jádro užitého procesoru umožňuje relativně rychlý běh běžných šifrovacích algoritmů.

Pro dosažení dostatečné úrovně zabezpečení byla zvolena asymetrická kryptografie: nadřazená ústředna, vystupující zde v roli klienta WWW serveru podřízené ústředny, zasílá svůj *dotaz* nebo *příkaz* podřízené ústředně. Příkaz, resp. dotaz, je podepsaný soukromým klíčem nadřazené ústředny a šifrovaný veřejným klíčem podřízené ústředny – může jej tedy dešifrovat pouze ta podřízená ústředna, pro kterou byl přenos určen, a podpis zaručuje, že jej vytvořila právě ta nadřazená ústředna, jejíž veřejný klíč byl nahrán na paměťovou kartu ústředny.

Zařízení odpovídá nadřazené ústředně zprávou - *odpovědí*, zašifrovanou jejím veřejným klíčem.

Vzhledem k tomu, že mezi nadřazenou a podřízenou ústřednou je přenášeno pouze velmi malé množství dat, nezpůsobuje výhradní užití asymetrické kryptografie výkonnostní problém.



Obr. 25: Příjem příkazu nebo dotazu z nadřazené ústředny

Obr. 25 popisuje příjem dat příkazu nebo dotazu z nadřazené ústředny. Nadřazená ústředna si vyžádá POST dotazem, nesoucím data, WWW stránku *cmd.sht* od podřízené ústředny.

Datová část POST dotazu obsahuje Base-64 kódovaná data, které firmware podřízené ústředny nejprve dekóduje, zkontroluje, zda bylo přijato 256 byte, a přijatá data rozdělí na dvě části po 128 B.

První blok obsahuje RSA-1024 šifrovaná užitečná data:

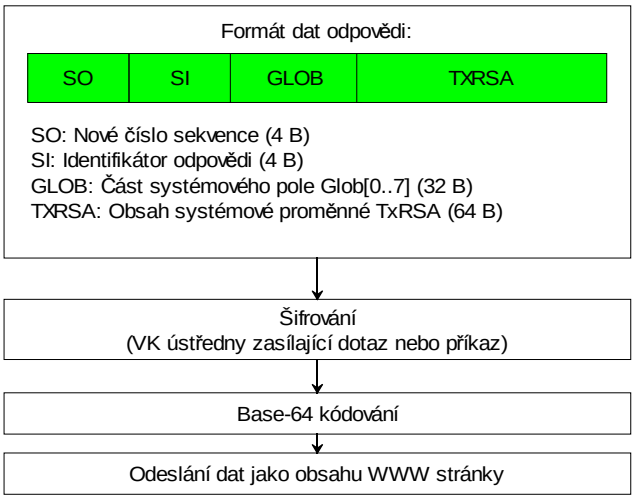
•hodnota INU – identifikátor nadřazené ústředny – umožňuje volbu jednoho veřejného klíče z maximálně 8 uložených klíčů na paměťové kartě zařízení a tedy práci v systému s více nadřazenými ústřednami, například vzájemně se zálohujícími,

•hodnota SO – číslo sekvence – je-li hodnota SO nulová, jde o *dotaz* a zařízení nereaguje na data v bloku PŘÍKAZ, v opačném případě jde o *příkaz* a zařízení kontroluje, zda poslední odeslaná odpověď pro ústřednou s tímto INU obsahovala hodnotu SO stejnou, jako je nyní přijaté SO,

•hodnota SI – identifikátor odpovědi – je náhodné číslo, které generuje nadřazená ústředna a podřízená ústředna jej zasílá beze změny zpět. Hodnota slouží pro identifikaci odpovědi a zamezení falšování odpovědí na *dotazy*,

•řetězec PŘÍKAZ je předán interpretu PicoC, který jej vykoná jako standardní příkaz jazyka C. Nejčastějším využitím bude pravděpodobně volání jiného skriptu nebo změna hodnoty některé systémové proměnné.

Je-li detekována chyba zabezpečení (neplatné pole SO nebo neplatný podpis), je volán skript *etherr.s*, který může například inkrementovat počítadlo chyb zabezpečení a při dosažení hraniční hodnoty změnit logiku skriptů podřízené ústředny do režimu, kdy nebude komunikovat s nadřazenou ústřednou a případně vyhlásí poplach.



Obr. 26: Odpověď na dotaz nebo příkaz nadřazené ústředny

Odpověď na každý příkaz či dotaz má vždy stejný formát, uvedený na obr. 26. Blok dat obsahuje nové číslo SO (byla-li předchozí zpráva *dotaz*, je jako SO užito vygenerované náhodné číslo), číslo SI, stav několika systémových proměnných z pole Glob[] a 64 B z proměnné TxRSA, jejíž hodnotu mohou běžící skripty libovolně ovládat.

2.4.1.3. Zasílání zpráv protokolem UDP

Poslední komunikační možností je zasílání krátkých zpráv protokolem UDP v uživatelem (skriptem) volně definovaném formátu, například v protokolu IP CID (je možné pouze odeslat zprávu). Tento přenos není zabezpečený, ale je velmi rychlý, minimálně zatěžuje mikrokontrolér zařízení a zasílání zpráv protokolem UDP může sloužit kromě možnosti přímého spojení na PCO i jako výzva nadřazené softwarové ústředně ke stažení informací o stavu ústředny zabezpečeným protokolem. Skriptem je samozřejmě možné implementovat jednoduché šifrování, například minimalistickou symetrickou šifru XTEA [43].

2.4.2. Softwarové řešení, použité softwarové moduly

Software (firmware) hlavního modulu ústředny je kompletně vytvořen v jazyce C s výjimkou několika optimalizovaných pasáží v assembleru. Vzhledem k rozsahu softwaru byly v maximální míře využity volně šiřitelné knihovny pro realizaci operačního systému, TCP/IP stacku, šifrování, skriptování a dalších funkcí.

V této části práce jsou uvedeny údaje o vnitřní struktuře a funkci softwarového vybavení zařízení. Stručné informace pro případné uživatele zařízení jsou předmětem příloh A až C.

2.4.2.1. Operační systém FreeRTOS

Popisované řešení ústředny EZS vyžaduje současný běh více programových procesů, například procesu WWW serveru, procesu sledování vstupů zařízení a procesů skriptovacího jazyka.

Klasickým řešením pro malé systémy je postupný běh jednotlivých procesů v nekonečné smyčce, jakási obdoba předem pevně naprogramovaného kooperativního multitaskingu. Programátor v tomto případě musí omezovat trvání běhu každého procesu tak, aby nedošlo k zablokování celého zařízení.

Využití operačního systému s preemptivním multitaskingem umožní kromě zjednodušení programování i lepší kontrolu běhu aplikace a využití prostředků. Při chybě vedoucí k selhání nebo dočasnému přetížení jednoho z procesů mohou ostatní procesy s nastavenou vyšší prioritou dále pracovat – v našem případě to znamená, že například přetížení procesu HTTP(S) serveru útokem DoS nepovede k selhání celého systému, ale pouze k výpadku komunikačních funkcí.

Operační systémy pro aplikace, pracující v reálném čase, se nazývají RTOS (*Real Time Operating systém*) a vyznačují se některými úpravami v oblasti časování procesů, které zajišťují, že budou dodrženy maximální reakční časy systému (podrobněji viz např. [29]). RTOS se dělí na soft-realtime a hard-realtime systémy, kde první typ pracuje na principu nejlepší snahy (*best effort)* a ve výjimečných případech může být časování narušeno, a druhý typ zaručuje zpravidla za cenu vyšší režie systému stoprocentní dodržení časování.

FreeRTOS [30] je operační systém reálného času typu soft-realtime, vyvinutý pro zařízení s omezenými prostředky. *FreeRTOS* je portován pro 23 platforem včetně v této aplikaci použitého jádra ARM7TDMI a podporuje preemtivní i kooperativní multitasking včetně běžných mechanismů pro zajištění současného běhu více procesů, například zámků kritických sekcí, front a semaforů.

FreeRTOS potřebuje pro svůj běh v konfiguraci s 15 procesy přibližně 1 kB RAM a 5 kB paměti FLASH.

FreeRTOS je distribuován pod licencí GPL s výjimkou, umožňující použití operačního systému v komerčních zařízeních s uzavřeným zdrojovým kódem za podmínky, že budou zveřejněny

případné změny v jádru operačního systému.

2.4.2.2. Knihovny IP komunikace uIP

Na Internetu je možné nalézt několik volně šiřitelných knihoven pro komunikaci v sítích založených na standardech Ethernet a TCP/IP. Tyto knihovny se zpravidla poněkud nepřesně označují jako TCP/IP stack, i když současně zapouzdřují i ovladač linkové vrstvy Ethernet a některé protokoly aplikační vrstvy, například SMTP a HTTP.

Mezi rozšířené knihovny tohoto typu, užívané na platformě ARM7TDMI, patří uIP, lwIP a komerční InterNiche stack.

Na základě nejmenších udávaných paměťových nároků a existence ukázkových řešení implementace *uIP* na operačním systému *FreeRTOS* byla zvolena knihovna *uIP*.

uIP [31] obsahuje kompletní implementaci linkové vrstvy Ethernet, síťové vrstvy IP a transportních protokolu UDP a TCP spolu s dalšími pomocnými protokoly (ARP, ICMP, DHCP, DNS). Součástí distribuce jsou i implementace WWW serveru a klienta a přenosu souborů pomocí FTP.

Celý stack *uIP* zpravidla běží v jediné úloze operačního systému – *uIP* má vlastní podporu kooperativního multitaskingu, tzv. *protothreads*.

Knihovnu *uIP* vyvíjí Švédský institut počítačových věd, nezisková organizace zabývající se výzkumem v oblasti aplikované informatiky a šíří ji pod licencí BSD, umožňující komerční využití tohoto produktu.

2.4.2.3. Kryptografická knihovna

Jako modul pro realizaci kryptografických funkcí je použita volně šiřitelná knihovna *PolarSSL* [32], kterou bylo možné bez problémů portovat na architekturu ARM7TDMI.

Z široké nabídky funkcí knihovny jsou užity sady funkcí pro asymetrickou kryptografii podle standardu RSA, hešovací funkci SHA-256 a funkce pro kódování a dekódování Base-64.

2.4.2.4. Souborový systém – knihovna EFSL

Knihovna *EFSL* [33] je velmi známá volně šiřitelná knihovna pro práci s paměťovými kartami typu SD a se souborovými systémy FAT/FAT32.

Knihovna podporuje SD a SDHC karty s velikostí do 16 GB a umožňuje současnou práci s více otevřenými soubory.

2.4.2.5. Skriptovací jazyk – interpreter PicoC

Původním úmyslem autora bylo nasadit jako interpreter skriptů jazyk a stejnojmenný engine LUA. Vzhledem k poměrně velké paměťové i časové náročnosti inicializace engine LUA, a

poměrně nešťastnému způsobu distribuce její vývojové větve eLUA určené pro embedded zařízení [34], kdy je v balíčku obsažen engine nakonfigurovaný pro všechny periferie konkrétního mikrokontroléru a využívající plně jeho možnosti tak, že je poměrně obtížné extrahovat samotný engine a portovat jej na jiný typ mikrokontroléru.

Nakonec byl zvolen interpreter PicoC [54], vytvořený svými autory původně pro skriptování v robotech a autopilotech leteckých modelů. PicoC neimplementuje všechny možnosti jazyka C, ale pro užití v popisovaném zařízení nepředstavují tato omezení (např. absence preprocesoru) výrazný problém.

Engine PicoC je napsán v jazyce C a ze zdrojového kódu v jazyce C je možné do konkrétní implementace jazyka doplňovat speciální funkce a proměnné, sdílené mezi nativním kódem a kódem skriptů PicoC. V našem případě pomocí těchto speciálních proměnných (nazývaných *systémové proměnné,* přehled viz příloha A.1), umožňujeme skriptům vyčítat a měnit stav zařízení.

Běh programů v jazyce PicoC je na poměry interpretovaných jazyků relativně rychlý: na prototypu ústředny byl za současného běhu ostatních úloh operačního systému naměřen čas inicializace interpreteru 8,2 ms, načtění zdrojového kódu o délce 1 kB pod 1 ms a vykonání 100 přiřazovacích příkazů 9 ms.

Zajímavou vlastností engine PicoC je jeho vlastní správa paměti, umožňující umístit haldu, užívanou pro dynamickou alokaci paměti pro proměnné skriptů a vlastního interpreteru, do oddělené paměťové oblasti mikrokontroléru. Takto byla využita 8 kB „USB RAM“ IC7, která je umístěna mimo lineárně adresovaný prostor základní paměti RAM mikrokontroléru a je tedy poměrně špatně využitelná.

2.4.3. Struktura software ústředny

Software ústředny využívá možností operačního systému *FreeRTOS*. Operační systém, distribuovaný jako sada zdrojových kódů v jazyce C, je přímo zkompilován se zdrojovými kódy softwaru ústředny a běží z paměti Flash mikrokontroléru.

Pro vývoj software bylo použito prostředí *Rowley CrossStudio for ARM*, překladač *arm-gcc* a JTAG adaptér, kompatibilní se standardem „*Wiggler*“.

2.4.3.1. Inicializace zařízení

Po připojení napájecího napětí k ústředně nejprve proběhne inicializace zařízení: tedy inicializace HW periferií (portů, rozhraní RS-232, RS-485) a souborového systému a knihovny EFSL.

Následně ústředna načítá nastavení z hlavního konfiguračního souboru (*ctrl.ini,* viz příloha C), ověří self-testem správnou funkci kryptografických funkcí RSA, inicializuje úlohy operačního

systému a nakonec je spuštěn plánovač operačního systému.

2.4.3.2. Úlohy, běžící v rámci FreeRTOS

Běh ústředny zajišťují čtyři souběžně běžící úlohy:

•úloha uIP, zajišťující komunikaci rozhraním Ethernet,

•úloha IOMan, zajišťující měření a kontrolu stavů smyček, tlačítek a rozhraní RS-232 a RS-485; úloha dále ovládá výstupy ústředny na základě požadavků skriptů,

•úloha Timers, zajišťující programovatelné časování běhu skriptů,

•úloha Scripts, v jejímž rámci běží skripty v jazyce PicoC.

Pro komunikaci mezi skripty v jazyce PicoC a úlohami uIP, IOMan a Timers je využit koncept sdílených proměnných, společných pro nativní program v jazyce C a PicoC skripty.

Úloha IOMan s periodou cca. 20 ms vyhodnocuje stav vstupů ústředny, nastavuje na základě jejich stavů hodnoty systémových proměnných *Inp* a *Cflg* a podle hodnot systémové proměnné *Out* nastavuje stavy výstupů ústředny. Úloha dále vyhodnocuje změny stavů vstupů a je-li to nutné, zavolá prostřednictvím mechanismu *událostí* obslužný skript. Podrobněji je mechanismus událostí a sdílených proměnných popsán v příloze A.

Jednotlivé skripty v jazyce PicoC spouští postupně úloha Scripts. Spouštěný skript je nejprve načten z paměťové karty do paměti RAM mikrokontroléru a teprve poté spuštěn, aby neblokoval ostatním úlohám přístup na paměťovou kartu.

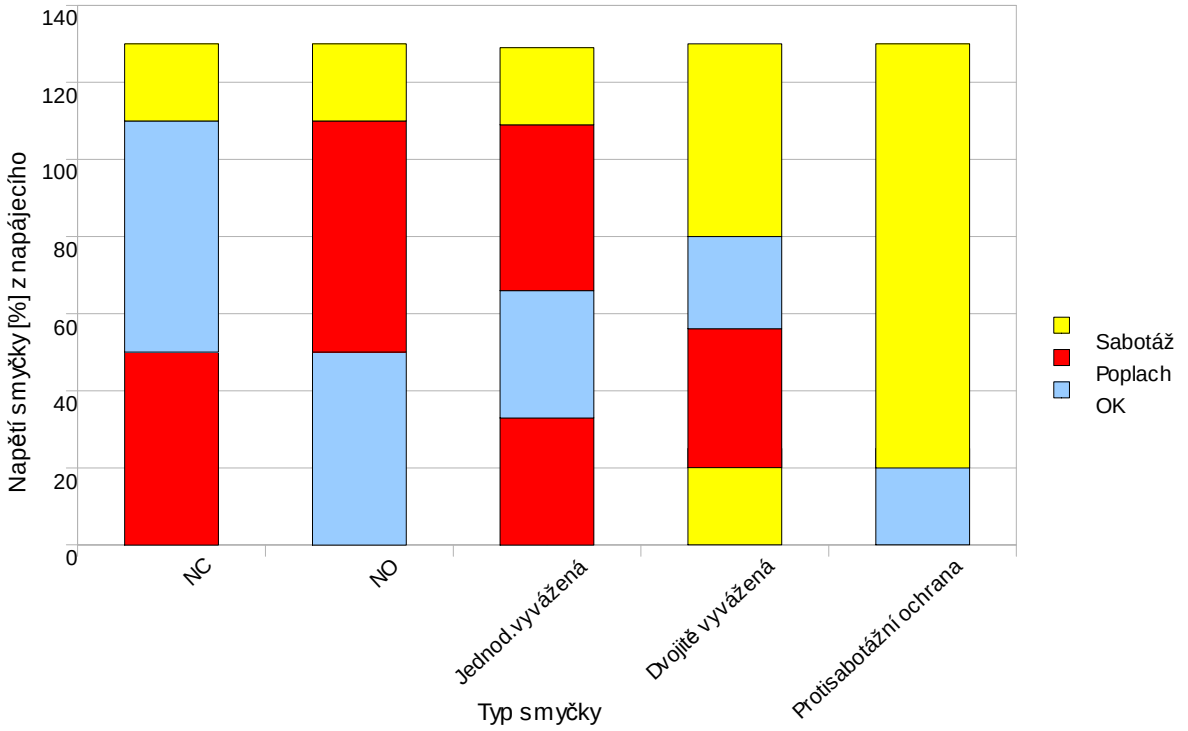
Úloha Timers zajišťuje přesné časování chodu skriptů s využitím systémového pole *Timer* – osmice časovačů. Úloha Timers je spouštěná periodicky jednou za sekundu s nejvyšší prioritou, dekrementuje nenulové hodnoty v poli *Timers* a dosáhne-li některá z hodnot nuly, přidá do fronty událostí požadavek na spuštění skriptu *tmrX.s*, kde X je číslo časovače (index pole *Timer*).

Komunikace mezi skripty je zajištěna pomocí front zpráv, a pomocí atomicky modifikovaných proměnných, sloužících jako semafory.

Úloha komunikace rozhraním Ethernet

Úloha uIP zajišťuje veškerou komunikaci rozhraním Ethernet. Na začátku běhu úlohy je z konfiguračního souboru *ctrl.ini* načteno nastavení rozhraní IP, inicializován obvod PHY a MAC interface IC7 a spuštěn proces IP stacku.

Úloha je většinu času pozastavená, a spouští se pouze v případě, že obvod PHY signalizuje přijetí rámce linkové vrstvy Ethernet, při požadavku na odeslání UDP zprávy nebo pro zpracování časovačů (např. vyprázdnění ARP cache, opakované vysílání TCP segmentu atd.).



Obr. 27: Graf stavů smyček v závislosti na poměru napětí na vstupní svorce smyčky k napájecímu napětí

Vyhodnocení stavu smyček v úloze IOman

Graf na obr. 27 popisuje způsob vyhodnocení stavů drátových smyček pro jednotlivé volitelné režimy NC (v klidovém stavu sepnutá), NO (v klidovém stavu rozpojená) a pro jednoduše a dvojitě vyvážené smyčky. Na základě znalosti vnitřního odporu vstupu ústředny (6,2 kΩ) můžeme podle požadovaných hodnot napětí na vstupech ústředny odvodit požadované hodnoty zakončovacích rezistorů smyček. Triviální rovnice odvození hodnot těchto rezistorů podle Ohmova zákona nebudeme uvádět, pouze uvedeme výsledné hodnoty: zakončovací rezistor jednoduše vyvážené smyčky by měl mít hodnotu 6,2 kΩ, pro dvojitě vyváženou smyčku vyhoví rezistory 3,9 kΩ.

Poslední sloupec grafu na obr. 27 („Protisabotážní ochrana“) ukazuje rozmezí povolených napětí na vstupu smyčky v době, kdy je cyklem protisabotážní ochrany (viz odd. 2.2.3.1) odpojeno napájení smyčky.

2.4.3.3. Zajištění spolehlivého běhu zařízení

Spolehlivý běh zařízení zajišťuje časovač watch-dog (WDT), který hlídá běh úloh IOMan, Timers a Scripts. Při chybě komunikace s SD kartou jsou prováděny pokusy o opětovné navázání komunikace a jsou-li déle než několik sekund neúspěšné, dojde k resetu zařízení watch-dog časovačem.

Úloha uIP běží trvale na pozadí s nejnižší prioritou tak, aby případný DoS útok na ethernetové

rozhraní nezablokoval ostatní funkce ústředny. Skripty ústředny mohou sledovat, zda probíhá periodická komunikace s nadřazenou ústřednou (je volán skript *ethcmd.s)* a pokud ne, spustit například lokální poplach nebo přejít do takového režimu práce, který počítá s výpadkem komunikace s nadřazenou ústřednou. Selhání úlohy uIP záměrně nevyvolává reset mikrokontroléru. Rozhodnutí, zda je nutné restartovat ústřednu, je ponecháno na programátorovi skriptů.

2.4.3.4. Ladění běhu ústředny a skriptů

Volbou *dbgintf* v hlavním konfiguračním souboru ústředny je možné zvolit, zda budou informace pro ladění chodu ústředny (např. názvy požadovaných WWW stránek, chybová hlášení interpreteru PicoC) zahazována, odesílána portem RS-232 nebo odesílána prostřednictvím rozhraní JTAG do okna terminálu IDE CrossStudio.

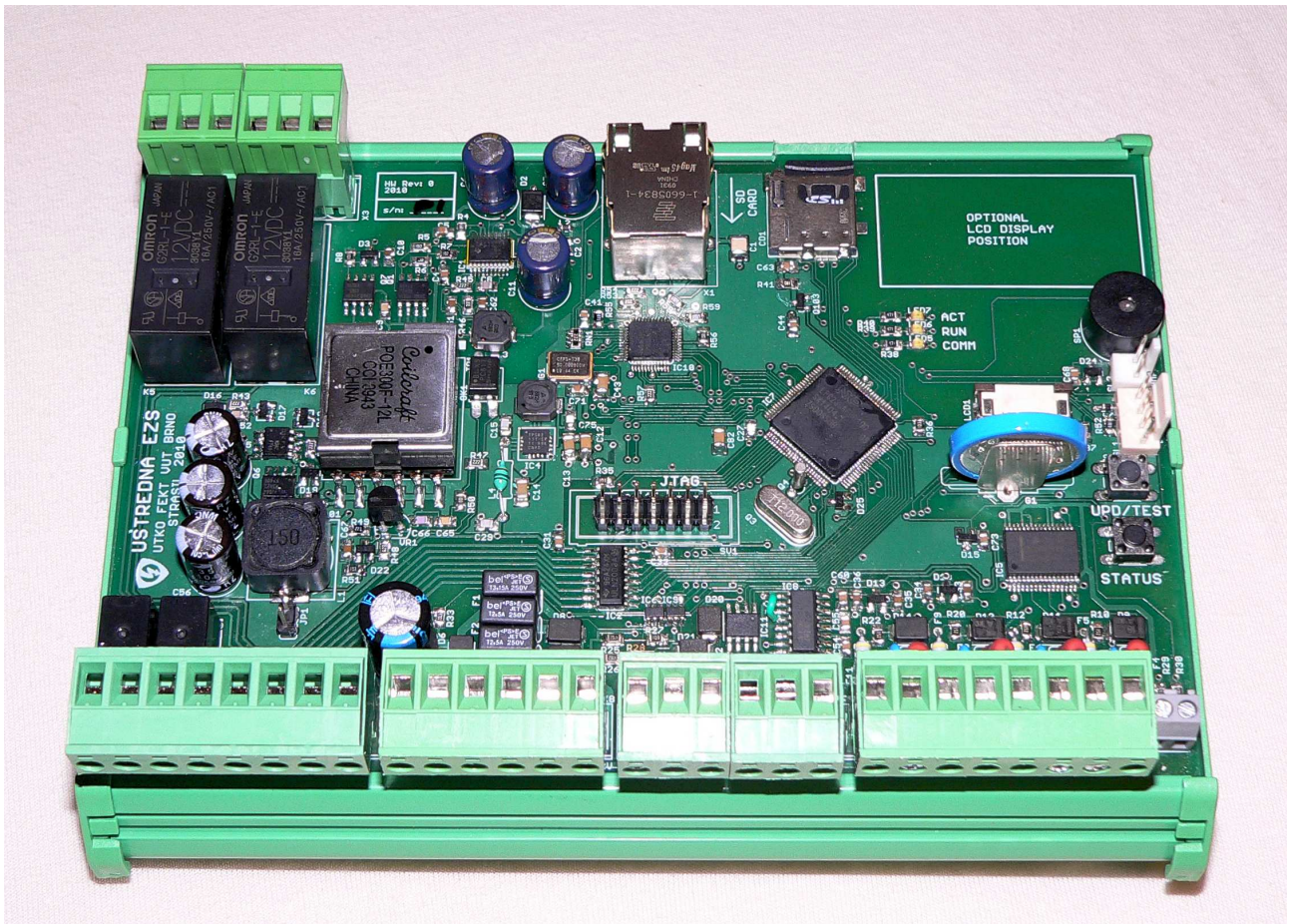
3. Realizace a zkoušky prototypu

Uvedený návrh ústředny byl prakticky ověřen realizací jednoho prototypu. Vzhledem k omezeným časovým i finančním možnostem nebylo možné navrhnout a otestovat i sadu rozšiřujících modulů či naprogramovat ukázkovou aplikaci emulující nadřazenou softwarovou ústřednu.

3.1. Realizace prototypu, použité vývojové prostředky

Prototyp byl osazen ručně a částečně přetavením v konvekční reflow peci. Dvě drobné chyby, které se vyskytly při oživování hardwaru (zkrat napájení prokovkou, který z nepochopitelných důvodů nehlásila kontrola návrhových pravidel v systému Eagle, a přehozený vývod obvodu ST3232), byly na prototypu i v dokumentaci opraveny.

Prvotní ověření funkce prototypu (konkrétně IC7 a rozhraní Ethernet) bylo provedeno zavedením ukázkové distribuce FreeRTOS [30], na jejímž základě byl následně vytvořen finální software zařízení.



Obr. 28: Fotografie prototypu ústředny

Software hlavního modulu ústředny v současné verzi obsazuje 190 KB z 512 KB paměti Flash a 37 KB z celkem 42 KB dostupné pameti RAM mikrokontroléru.

Podle rozpisky materiálu (viz příloha F) byla vytvořena hrubá cenová kalkulace pro výrobu desek v sérii 200 ks. Cena materiálu včetně plošného spoje a držáku je pro 1 ks ústředny přibližně 950 Kč bez DPH (720 Kč bez DPH, pokud nebude osazen PoE měnič).

3.2. Výsledky zkoušek a měření na prototypu hlavního ústředny

3.2.1. Funkční zkoušky ústředny

Pro praktickou ukázku funkcí ústředny byla vytvořena a odladěna sada ukázkových skriptů, uvedených v příloze B. Tyto skripty sloužily spolu s jednoduchými zkušebními skripty pro odzkoučení jednotlivých rozhraní ústředny, mechanismu *událostí* a spolehlivosti běhu celého zařízení.

Krátkodobě byla testována spolehlivost běhu software ústředny: během 50 hodin nepřetržitého chodu, kdy byl celkem 180 000x spuštěn skript *tick.s*, odesílající data rozhraními RS-485 a RS-232 a manipulující se stavy výstupních relé ústředny, a 36 000x načtena WWW stránka diagnostiky ústředny, nedošlo k odeslání chybných dat nebo přerušení komunikace s WWW serverem ústředny.

Vzhledem k tomu, že prozatím neexistuje nadřazená softwarová ústředna, byla funkce protokolu pro zabezpečenou komunikaci s nadřazenou ústřednou otestována pouze pomocí jednoduché konzolové aplikace, vytvořené úpravou příkladu, dodávaného s knihovnou *polarSSL*.

Funkce WWW rozhraní byla odzkoušena v běžných WWW prohlížečích (Internet Explorer 7, Firefox 3, Opera 9). Funkce UDP přenosu dat byla sledována programy Wireshark a Netcat.

3.2.2. Měření

Na prototypu ústředny bylo provedeno několik orientačních měření, jejichž výsledky jsou stručně uvedeny níže:

- proudová spotřeba ústředny kolísá mezi 60 a 80 mA při napájecím napětí 13,8 V; při odpojení rozhraní Ethernet klesá na 40 mA,
- výkonné jádro ústředny – mikrokontrolér, SD karta a WWW rozhraní – běží až do poklesu napájecího napětí na 4,7 V (užitečná funkce ústředny je limitována napětím cca. 8 V, kdy přestanou spínat výstupní relé),
- výstupní napětí měniče PoE se při vstupním napětí 55 V pohybuje v rozsahu 11,6 až 12,2 V při odběru 0 – 2 A.

Pro ověření elektrické bezpečnosti byla provedena zkouška izolace napětím 2 500 V, 50 Hz mezi vodiči od svorkovnice X3 k výkonovým relé a mezi kontakty svorkovnice X3 a cívkami výkonových relé.

Programem Wireshark byla zběžně změřena rychlost jednotlivých funkcí rozhraní Ethernet při připojení ústředny kříženým kabelem k síťové kartě počítače.

- WWW rozhraní ústředny přenáší soubory z SD karty rychlostí 320 kb/s (65 KB JPEG; brzdou propustnosti je zde pomalé načítání souborů z SD karty po jednotlivých sektorech),
- doba odezvy na ICMP PING (Echo Request / Echo Reply) je v rozsahu 1 – 3 ms,
- doba odezvy na běžný HTTP GET požadavek kolísá v rozmezí 20 – 80 ms,
- doba odezvy na šifrovaný podepsaný dotaz (simulovaný dotaz nadřazené ústředny) kolísá v rozmezí 300 – 450 ms.

Doba běhu kryptografických rutin knihovny polarSSL (měřeno osciloskopem po úpravě softwaru tak, aby bylo možné podle logických úrovní na pinech mikrokontroléru identifikovat běh jednotlivých kryptografických podprogramů) při současném běhu ostatních úloh je:

- RSA-1024 verifikace klíčů: 15 ms,
- RSA-1024 šifrování: 19 ms,
- RSA-1024 dešifrování: 221 ms,
- RSA-1024 podepsání 32 B dat (SHA-1): 221 ms (neužíváme),
- RSA-1024 ověření podpisu 32 B dat (SHA-1): 13 ms.

(použité měřící přístroje: osciloskop Rigol DS1042CD, multimetr HP 34401A, čítač HP 5334A)

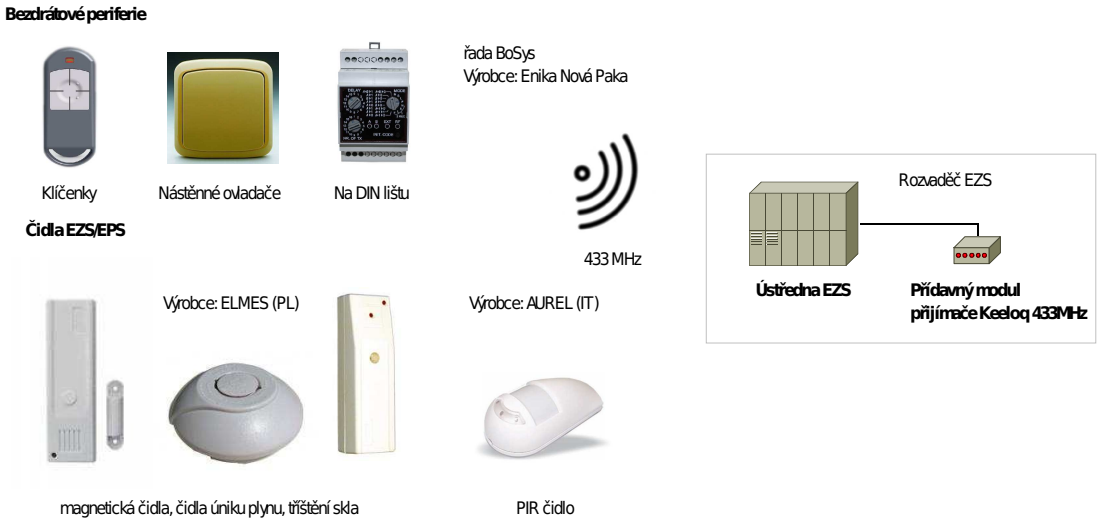
4. Dodatky

4.1. Volba a popis bezdrátové technologie Keeloq

Jako možná technologie pro připojení jednoduchých bezdrátových čidel a pro příjem signálů z ovládacích klíčenek byl zvolen simplexní systém Microchip Keeloq [38] s přenosem dat na frekvenci 433 MHz.

Volba užitého systému byla podmíněna dostupností zařízení (čidel a klíčenek), pracujících s uvedeným standardem a umožňující výrobu bezdrátové ústředny bez nutného vývoje bezdrátových čidel. Jejich příklady jsou uvedeny na obrázku 24. Jinými bezdrátovými čidly, dostupnými na trhu EU i s dokumentací přenosového protokolu, jsou pravděpodobně pouze bezdrátová simplexní PIR čidla bez jakéhokoliv zabezpečení nebo plovoucího kódu (!), která vyrábí italská firma AUREL.

Z důvodů, uvedených v oddílu 1.2.3, by bylo poněkud výhodnější užití čidel s duplexní komunikací (například s datovými bezdrátovými moduly HopeRF 433 MHz v ceně kolem 45 Kč/ks při 1000 ks odběru), nicméně pro praktické užití ústředny by bylo nutné vyvinout celý sortiment čidel a klíčenek, což je pro kusovou nebo malosériovou výrobu nepraktické. Systém je nicméně schopen doplnění o jiné nebo druhé rádiové rozhraní formou přídavného modulu.



Obr. 29: Užití přenosu Keeloq v zabezpečovací technice a v technice domovní automatizace

Vysílač Keeloq je zpravidla řadiče s vestavěným šifrovacím kontrolérem, pracujícím s proprietární blokovou šifrou s pseudonáhodným generátorem, založeným na nelineárním posuvném registru (*NLFSR*); někdy je doplněno dodatečné šifrování šifrou XTEA. Příkladem IO řadiče je obvod HCS201 [39] v ceně 0,83 $/1000 ks. Tento řadič spíná velmi jednoduchý vysílač – oscilátor 433 MHz se SAW rezonátorem a tím vytváří modulovaný signál ASK 433 MHz s

výkonem do 10 mW, aby byly splněny podmínky pro užití v pásmu ISM.

Pro příjem se zpravidla užívá běžných hybridních přijímacích modulů a softwarového ověření správnosti kódu mikrokontrolérem – firma Microchip poskytuje příslušné knihovny v jazyce C. Po podpisu licenčního ujednání jsou k dispozici i knihovny pro realizaci vysílačů, ale vzhledem k cenové politice firmy jsou obvykle užívány integrované vysílače.

Dosah tohoto spojení je 80 – 120 metrů v závislosti na citlivosti přijímače a konstrukci antén.

Při užití systému Keeloq pro dálkové ovládání a snímání se s každým přenosem přenáší 32 bitů dat plovoucího kódu, odvozeného od počítadla přenosů a tajného klíče. V těchto datech je obsaženo dva až pět bitů užitečných dat, například stavů tlačítek klíčenky. Keeloq je využíván i pro obousměrné přenosy v RFID aplikacích nebo ověření pravosti akumulátorů.

Pro použití v zabezpečovacích zařízení jsou vhodné ovládací klíčenky a bezdrátové PIR snímače standardu Keeloq. V systémech integrovaných s domovní automatizací může být zajímavé i užití bezdrátových spínačů a vysílačů Keeloq pro montáž do rozvodných skříní, které vyrábí česká firma Enika Nová Paka (viz obr. 29).

Závěr

Předložený návrh ústředny podle názoru autora plně splňuje zadání práce.

Zvolená koncepce ústředny umožňuje téměř neomezenou programovatelnost systému pomocí jednoduchých skriptů v jazyce blízkém jazyku C – ústřednu můžeme tedy považovat spíše za volně programovatelný řídicí počítač, uzpůsobený svými rozhraními přednostně pro řešení úloh v zabezpečovací technice. To dovoluje užití ústředny i jako prvku v systémech domovní automatizace.

Ústředna umožňuje samostatný provoz i provoz v síti, řízené plně softwarovou nadřazenou ústřednou (serverem). Pro vzájemnou komunikaci ústředen je užit zabezpečený protokol, založený na protokolové sadě TCP/IP.

Zařízení je vybaveno možností napájení po síti Ethernet, čtveřicí vstupů pro připojení čidel smyčkou s jednoduchým nebo dvojitým vyvážením se základní ochranou proti sabotáži kabeláže, sedmi digitálními výstupy a rozhraními RS-485 a RS-232.

Na vyrobeném prototypu zařízení byly úspěšně otestovány všechny funkce a odladěny ukázkové skripty, tvořící logiku jednoduché ústředny.

Výsledná materiálová cena výrobku je relativně nízká (720 až 950 Kč při sérii 200 ks) a použitý mikrokontrolér stále disponuje dostatkem paměti pro implementaci dalších funkcí; jediným výrazným ústupkem nižší ceně zařízení je implementace vlastního paměťově úspornějšího zabezpečeného protokolu na místo užití standardního řešení, založeného na SSL/TLS.

Navržená ústředna EZS je schopna dalšího rozšiřování prostřednictvím přídavných modulů, které mohou doplňovat další komunikační rozhraní nebo navýšit počet vstupů a výstupů zařízení. V příloze práce je naznačeno řešení bezdrátového přijímače pro ovladače a čidla, užívající komunikaci standardem Keeloq.

V rámci dalšího rozvoje systému by bylo vhodné vytvořit serverovou aplikaci – nadřazenou ústřednu, komunikující s podřízenými ústřednami navrženého typu. Dále by bylo vhodné vytvořit aplikaci, umožňující automatickou tvorbu skriptů definujících logiku ústředny na základě například grafického zadání diagramu požadovaného chování.

Seznam použité literatury

[1] KŘEČEK Stanislav a kol.: *Příručka zabezpečovací techniky*. Blatenská tiskárna, Blatná 2003.

[2] BURDA Karel: *Zabezpečovací systémy*. Přednáškové texty, VUT Brno 2009 [online] [cit. 2009-12-01] Dostupné z WWW: <www.vutbr.cz/elearning/course/view.php?id=87063>

[3] PARADOX SECURITY SYSTEMS: *Digiplex and Digiplex EVO* [online] [cit. 2009-11-28] Dostupné z WWW: <http://www.paradox.com/Products/default.asp?CATID=7>

[4] JABLOTRON ALARMS, A. S.: *GSMLink.cz (prezentace)*. [online] [cit. 2009-12-10] Dostupné z WWW: <www.jablotron.cz/component.php?cocode=download&doid=12>

[5] ADEMCO GROUP: *Ademco ® Contact ID Protocol for Alarm System Communications*, SIA Virginia, USA 1999. Dostupné z WWW: <http://www.smartelectron.ru/files/DC-05_Contact_ID.pdf>

[6] ČSN EN 50136-1-5. - Poplachové systémy - Poplachové přenosové systémy a zařízení - Část 1-5: Požadavky na paketově přepínanou síť PSN. [s.l.] : [s.n.], 2009. 8 s.

[7] JABLOTRON ALARMS, A. S.: JA-80V kombinovaný komunikátor LAN a telefonní linka (návod). [online] [cit. 2009-12-10] Dostupné z WWW: <http://old.jablotron.cz/docs/manualy/ja-80/JA-80V_CZ_MKA51101.pdf>

[8] PARADOX SECURITY SYSTEMS: IP-100 User Manual [online] [cit. 2009-11-28] Dostupné z WWW: <www.alarmtec.ee/doc.php?3071 >

[9] ICT, INC.: Armor IP Internet Monitoring Application [online] [cit. 2009-11-28] Dostupné z WWW: <http://www.integratedcontroltechnology.com/pdfloader.php?LK=13799158&FT=specs&FE=PDF&FN=CRX-ARMORIP_ArmorIP_Internet_Monitoring_Application_Brochure_En.pdf>

[10] SECURITY INDUSTRY ASSOCIATION: SIA Digital Communications Standard – Internet Protocol Events Reporting. SIA Virginia, USA 2007. Dostupné z WWW: <http://www.hacker-soft.net/tools/Assessment/dc09_20070319.pdf>

[11] Martin T.: The Insider's Guide To The Philips ARM 7 Based Microcontrollers. Hitex, Coventry 2006.

[12] ARM Architecture [online]. 2002- , [cit. 2009-12-11]. Dostupný z WWW: <http://en.wikipedia.org/wiki/ARM_architecture>.

[13] ADVANCED RISC MACHINES: ARM Cortex-M3 [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.arm.com/products/CPUs/ARM_Cortex-M3.html>

[14] ADVANCED RISC MACHINES: What is the difference between a von Neumann architecture and a Harvard architecture? [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.arm.com/products/CPUs/ARM_Cortex-M3.html>

[15] Modified Harvard architecture [online]. 2007- , [cit. 2009-12-11]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Modified_Harvard_architecture>

[16] Royal Ohm NFR Fusible Resistor. 2009. [cit. 2009-11-04] Dostupný z WWW: <http://zefiryn.tme.pl/dok/a07/nfr1w.pdf>.

[17] STMicroelectronics: SMBJ Transil [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.st.com/stonline/products/literature/ds/5616/smbj.pdf>

[18] NXP: I2C Specification [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.nxp.com/acrobat_download2/literature/9398/39340011.pdf>

[19] NXP: PESD5V0U2BT Data Sheet [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.nxp.com/documents/data_sheet/PESD5V0U2BT.pdf >

[20] SOS Electronic: Online katalog [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.soselectronic.cz>

[21] BELDEN: Current Ratings for Flat Cable [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.belden.com/pdfs/TechInfo/TechFlatCurrent.htm>

[22] FREESCALE SEMICONDUCTOR: MC33879 Data Sheet [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.freescale.com/files/analog/doc/data_sheet/MC33879.pdf>

[23] SD CARD ASSOCIATION: Simplified SD Card Physical Layer Specification [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.sdcard.org/developers/tech/sdcard/pls/Simplified_Physical_Layer_Spec.pdf>

[24] IEEE COMPUTER SOCIETY: IEEE Standard 802.3at [online]. [cit. 2009-12-11]. Dostupný z WWW: <http://www.ieee.org>

[25] Texas Instruments: TPS23756 Data Sheet [online].[cit. 2009-12-11]. Dostupný z WWW: <http://www.ti.com/lit/gpn/tps23756>

[26] Texas Instruments: TPS23756EVM User Manual [online].[cit. 2009-12-11]. Dostupný z WWW: <http://www.ti.com/litv/pdf/slvu329>

[27] Coilcraft: POE 300 Data Sheet [online].[cit. 2009-12-11]. Dostupný z WWW: <http://colilcraft.com/pdfs/poe300.pdf>

[28] Texas Instruments: TPS62111 Data Sheet [online].[cit. 2009-12-11]. Dostupný z WWW: <http://www.ti.com/lit/gpn/tps62111>

[29] Operační systém reálného času. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 25.4.2010 [cit. 2010-05-24]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Operační_systém_reálného_času>.
[30] The FreeRTOS Project [online]. 2010 [cit. 2010-05-24]. The FreeRTOS Project. Dostupné z WWW: <www.freertos.org>.
[31] uIP TCP/IP stack [online]. 2010 [cit. 2010-05-24]. Dostupné z WWW: <http://www.sics.se/~adam/uip/index.php/Main_Page>.
[32] polarSSL [online]. 2010 [cit. 2010-05-24]. Dostupné z WWW: <http://www.polarssl.org>.
[33] EFSL, Embedded Filesystems Library[online]. 2010 [cit. 2010-05-24]. Dostupné z WWW: <http://www.efsl.be>.
[34] ELUA Project [online]. 2010 [cit. 2010-05-24]. Dostupné z WWW: <http://www.eluaproject.net>.
[35] ELUA Demo Scripts[online]. 2010 [cit. 2010-01-20]. Dostupné z WWW: <http://lua-users.org/wiki/DemoScripts>.
[36] WILLIAMS, Tim. EMC for product designers. 3rd ed. Oxford : Newnes, 2001. 360 s. ISBN 0750649305.
[37] BURDA, K. Bezpečnost informačních systémů. 1. Brno: FEKT VUT Brno, 2005. s. 1-104.
[38] Microchip Technology, Inc. website [online]. 2007 [cit. 2010-05-24]. Keeloq code hopping devices. Dostupné z WWW: <http://ww1.microchip.com/downloads/en/devicedoc/41172a.pdf>.
[39] Microchip Technology, Inc. website [online]. 2001 [cit. 2010-05-24]. HCS201 KEELOQ Code Hopping Encoder Data Sheet. Dostupné z WWW: <ww1.microchip.com/downloads/en/devicedoc/41098c.pdf>.
[40] Rabbit Semiconductor [online]. 2009 [cit. 2010-05-24]. Benchmark Study Results. Dostupné z WWW: <http://www.rabbit.com/products/benchmarks/index.shtml>.
[41] Dhrystone. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2010-05-24]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Dhrystone>.
[42] ECROS Technology [online]. 2005 [cit. 2010-05-24]. Dhrystone Benchmark for MCUs. Dostupné z WWW: <http://www.ecrostech.com/Other/Resources/Dhrystone.htm>.
[43] XTEA. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2010-05-24]. Dostupné z WWW: <http://en.wikipedia.org/wiki/XTEA>.
[44] IETF: RFC2812: HTTP over TLS. [online]. 2000 [cit. 2010-05-24]. Dostupné z WWW: <http://tools.ietf.org/html/rfc2818>.
[45] Rabbit Semiconductor [online]. 2009 [cit. 2010-05-24]. Rabbit 3000. Dostupné z WWW: <http://www.rabbit.com/products/rab3000/>.
[46] National Semiconductor. DP83848C. 2008. 84 s. Dostupný z WWW: <http://cache.national.com/ds/DP/DP83848C.pdf>.
[47] National Semiconductor. RMII 2 ™ Specification. 1998. 17 s. Dostupný z WWW: <http://www.national.com/appinfo/networks/files/rmii_1_2.pdf>.
[48] NXP Semiconductors. *LPC2368 User Manual*. 2nd edition. 2009. 285 s. Dostupný z WWW: <http://www.standardics.nxp.com/support/documents/microcontrollers/pdf/user.manual.lpc2368.pdf>.
[49] Coilcraft: *POE 300 Data Sheet* [online].[cit. 2009-12-11]. Dostupný z WWW: <http://colilcraft.com/pdfs/poe300.pdf>
[50] NXP Semiconductors. *LPC2368 ERRATA SHEET*. 2009. 8 s. [cit. 2009-11-04] Dostupný z WWW: <http://www.standardics.nxp.com/support/documents/microcontrollers/pdf/errata.lpc2368.pdf>.
[51] HOROWITZ, Paul, WINFIELD, Hill. *The Art of Electronics*. 2nd enl. edition. Cambridge : Cambridge University Books, 1989. 1152 s. ISBN 0521370957.
[52] JOHNSON, Howard, GRAHAM, Martin. *High-speed Digital Design : A Handbook of Black Magic*. [s.l.] : Prentice Hall, 1993. 446 s. ISBN 0-13-395724-1.
[53] THOMAS, Martin. *Interfacing ARM controllers with Memory-Cards* [online]. 2006- , Last mod.: Thursday, 20-Sep-2007 [cit. 2009-10-20]. Dostupný z WWW: <http://www.siwawi.arubi.uni-kl.de/avr_projects/arm_projects/efsl_arm/index.html>.
[54] SALEBA, Zik. *PicoC: A Very Small C Interpreter.* [cit. 2009-5-10] Dostupný z WWW: <http://code.google.com/p/picoc/>.

Seznam zkratek a definicí

ADC	Analog Digital Converter A/D převodník
ARM	Advanced RISC Machines firma vyvíjející stejnojmenná jádra 32-bitových RISC mikroprocesorů
AWG	American Wire Gauge stupnice průřezů vodičů
BOD	Brown Out Detector detektor podpětí (zde součástí mikrokontroléru, vyresetuje mikrokontrolér, poklesne-li jeho napájecí napětí pod nejnižší povolenou mez).
COG	Chip On Glass technologie výroby řadiče LCD, kdy je čip umístěn přímo na skleněné ploše displeje a není nutná samotná DPS s řadičem
DMA	Direct Memory Access přímý přístup k paměti – zejména pro kopírování bloků dat bez účasti jádra procesoru
DPS	Deska plošných spojů
Engine	Zde ve smyslu *skriptovací motor*, program, který vykonává (interpretuje) kód skriptu. Příkladem skriptovacího enginu je například *Java Virtual Machine*.
FAT	File Allocation Table alokační tabulka souborů, také typ souborového systému založený na tabulce FAT, vyvinutý firmou Microsoft
GPL	General Public Licence volná licence pro software s otevřeným zdrojovým kódem
I^2C	Inter-integrated Circuit sběrnice firmy Philips (dnes NXP) pro komunikaci mezi integrovanými obvody v rámci desky nebo jednoho zařízení
ISM	Industrial, Scientific and Medical veřejná pásma pro datovou rádiovou komunikaci s malým dosahem
LDO	Low Drop-Out nízký úbytek napětí (na stabilizátoru, také označení pro stabilizátory s nízkým úbytkem napětí)
Poplachový stav čidla	Stav, kdy čidlo detekuje útok a vytváří příslušnou odezvu (signál) na svém výstupu
RTC	Real Time Clock (v některé literatuře Real Time Counter) hodiny reálného času
SPI	Serial Peripheral Interface synchronní sériová datová sběrnice pro komunikaci mezi integrovanými obvody, někdy také označení přijímače/vysílače pro tuto sběrnici

SSP	Synchronous Serial Port označení přijímače/vysílače pro synchonní sériové sběrnice, integrovaného v mikrokontrolérech řady LPC2xxx firmy NXP
UART	Universal Asynchronous Receiver – Transmitter přijímač/vysílač pro asynchronní sériový přenos
WDT	Watch-dog Timer časovač watchdog – vyvolává restart mikroprocesorového systému, pokud není periodicky nulován

Přílohy

A Doplňující informace k programování ústředny skripty

V této příloze jsou uvedeny některé doplňující informace k programování ústředny v jazyce Pico C.

A.1.Systémové proměnné ústředny

Komunikaci mezi skripty v jazyce Pico C a pevným programem ústředny zprostředkovávají mezi všemi skripty sdílené globální proměnné, nazývané jako *systémové proměnné*. Pro jednodušší rozpoznání těchto speciálních proměnných je první písmeno jejich názvu oproti běžným zvyklostem velké.

Proměnná	*Datový typ*	*Význam*
Out[8]	int **pro zápis i čtení**	Pole pro ovládání výstupních signálů ústředny: Out[0] .. Out[3] odpovídá relé 1 až 4, Out[4] .. Out[6] odpovídá tranzistorovému výstupu 1 až 3 (hodnota 1 = sepnuto, hodnota 0 = rozepnuto) Out[7] ovládá bzučák ústředny a LED diodu „ACT“ (hodnota 0 = vypnut, hodnota 1/2/3 zapne bzučák s trvalým / rychle / pomalu přerušovaným tónem; přičtení hodnoty 4 rozsvítí LED)
Inp[8]	int **pouze pro čtení**	Pole pro čtení stavů vstupů zařízení: Inp[0] .. Inp[3] odpovídají stavům smyček 1 až 4. Výstupní hodnoty jsou: 0 smyčka v klidovém stavu 1 smyčka v poplachovém stavu 2 smyčka ve stavu sabotáž (rozpojená dvojitě vyvážená sm.) 3 smyčka ve stavu sabotáž (přepětí na smyčce) K této hodnotě je přičtena hodnota 4, je-li vybavena protisabotážní ochrana – systém detekuje zkrat mezi smyčkami nebo připojení cizího zdroje. Protisabotážní ochrana musí být povolena v poli Stp[]. Další prvky pole udávají stav kontaktních vstupů zařízení (1 = aktivní vstup, 0 = neaktivní) Inp[4] tlačítko 1 Inp[5] tlačítko 2 Inp[6] sabotážní kontakt ústředny Inp[7] externí vstup „signalizace poruchy zál. zdroje“
Rtc[6]	int **pouze pro čtení**	V poli je uložen systémový čas takto: Rtc[0] sekundy Rtc[1] minuty Rtc[2] hodiny Rtc[3] dny v měsíci Rtc[4] měsíce Rtc[5] kalendářní rok (dvojciferně)

Volt[8]	int **pouze pro čtení**	V poli jsou uloženy hodnoty měřených napětí na svorce: Volt[0] .. Volt[3] smyčky 1 až 4 (je-li zapnuta protisabotážní ochrana, jde o napětí měřená v době, kdy je smyčka napájená) Volt[4] napájecí napětí 12 V systému (vodič +12V) Volt[5] napájecí napětí obvodu vnějších prvků Volt[6] vstup pro externí měření napětí Volt[7] napájecí napětí obvodu signalizačních prvků Hodnoty napětí jsou uloženy jako celá čísla v milivoltech.
Stp[8]	int **pro zápis i čtení**	Pole pro nastavení zařízení: Stp[0] .. Stp[3] nastavují režim smyček 1 až 4. Hodnoty jsou: 0 jednoduchá smyčka, NC 1 jednoduchá smyčka, NO 2 jednoduše vyvážená smyčka 3 dvojitě vyvážená smyčka Přičtením čísla 4 k výše uvedeným hodnotám se aktivuje protisabotážní ochrana. Hodnota Stp[4] obsahuje v podobě 32-bitového čísla cílovou IP adresu pro komunikaci protokolem UDP. Hodnota Stp[5] obsahuje cílový port pro komunikaci protokolem UDP. Hodnoty Stp[6] a Stp[7] nejsou v současnosti využity.
Glob[128]	int **pro zápis i čtení**	Pole 128 globálních proměnných typu int, vhodných pro předávání dat mezi skripty. Data jsou uložena v baterií zálohované oblasti paměti RAM IC7.
CVals[128]	int **pro zápis i čtení**	Pole 128 globálních proměnných typu int, nastavitelných pomocí WWW rozhraní koncovým uživatelem. Data jsou uložena v baterií zálohované oblasti paměti RAM IC7.
UR	int **pro zápis i čtení**	Hodnota proměnné určuje aktuální nastavení zabezpečení ústředny pro nepřihlášené uživatele: 0 WWW server nedostupný 1 WWW server přístupný pouze pro zabezpečenou komunikaci s nadřazenou ústřednou 2 navíc jsou přístupné WWW stránky pro sledování stavu zařízení 3 jsou přístupné WWW stránky pro nastavení koncovým uživatelem 4 jsou přístupné všechny WWW stránky
Auth	int **pro zápis i čtení**	Při volání skriptu ethauth.s pro kontrolu hesla pro přístup na WWW rozhraní ústředny je v proměnné předáno heslo; skript do proměnné uloží hodnotu 0/2/3/4 odpovídající hodnotám proměnné UR.
Rd232	char[32] **pouze pro čtení**	Poslední rámec, přijatý rozhraním RS-232
Rd485	char[32] **pouze pro čtení**	Poslední rámec, přijatý rozhraním RS-485
Cflg	int[8] **pro zápis i čtení**	Pole obsahuje stavové příznaky, vážící se ke komunikačním rozhraním ústředny.

		Hodnota Cflg[0] je nenulová, je-li v poli Rd232 uložen přijatý rámec. Vynulováním hodnoty uvolníme další příjem dat rozhraním RS-232. Hodnota Cflg[1] je obdobou Cflg[0] pro rozhraní RS-485 a pole Rd485. Hodnota Cflg[2] je obdobou Cflg[0] pro šifrovaný kanál a pole RdRSA.
TxIO	char[256] **pro zápis i čtení**	Výstupní buffer pro odesílání dat (null-terminated string) RS-232, RS-485 a UDP.
TxRSA	char[64] **pro zápis i čtení**	Data z tohoto pole jsou vkládána do odpovědí, zasílaných šifrovaným kanálem.
TxDir	int	Nastavením proměnné zahájíme přenos dat – po ukončení přenosu zařízení proměnnou vynuluje. Hodnota 1: odesílání rozhraním RS-232 Hodnota 2: odesílání rozhraním RS-485 Hodnota 3: odesílání protokolem UDP (emulace IP Contact ID)
Timer[8]	int **pro zápis i čtení**	Osm časovačů Timer[0] až Timer[7] umožňuje měření časových úseků. Hodnota každého časovače s hodnotou vyšší než nula je jednou za sekundu dekrementována a dosáhne-li nuly, je spuštěn skript *tmrX.s,* kde *X* je číslo časovače v rozsahu 0 až 7.
ScJump	char[8] **pro zápis i čtení**	Není-li po ukončení běhu skriptu řetězec prázdný, zařízení pokračuje spuštěním skriptu *X.s*, kde *X* je obsah proměnné *ScJump*.

A.2.Funkce a omezení skriptů

Pro usnadnění práce programátora ústředny zařízení vyhodnocuje některé změny stavu zařízení, tzv. *události* (přehled viz sekce B.4). *Událost* je pokynem pro spuštění skriptu, který její vznik vhodným způsobem ošetřuje (např. *událost* sabotáž krytu ústředny je *pokynem* pro spuštění skriptu *ctrltamp.s,* který bude pravděpodobně obsahovat sadu příkazů pro vyvolání poplachu).

Ústředna nepodporuje současný běh více skriptů. Jednotlivé pokyny pro spuštění skriptů jsou proto postupně řazeny do *fronty spouštění skriptů* typu FIFO (realizované jako fronta OS FreeRTOS), a pokud aktuální skript skončí nebo žádný skript neběží, je spuštěn další požadovaný skript. Maximální délka fronty FIFO je 16 pokynů.

Alternativní metodou vyhodnocování událostí může být užití jediného trvale běžícího skriptu, který bude vyhodnocovat stav zařízení analýzou hodnot systémových proměnných: v tomto případě vůbec nemusíme využít mechanismus událostí a *fronty spouštění skriptů* ústředny.

Délka zdrojového kódu jednoho skriptu je omezena na 4 kB. V případě potřeby je také možné zřetězit více skriptů jejich vzájemným voláním nastavením systémové proměnné *ScJump.*

Skripty si mohou alokovat maximálně 6 kB paměti RAM.

A.3.Přehled sledovaných událostí a jimi spouštěných skriptů

V následující tabulce je uveden seznam událostí, které vyvolávají spuštění odpovídajícího skriptu (přesněji řečeno generují *pokyn*, který ústředna zařadí do FIFO fronty spouštění skriptů). Není-li skript s uvedeným jménem nalezen, je událost ignorována.

Napájení systému		
Vnější napájení (externího) zálohovaného zdroje	Výpadek Obnovení Signalizace poruchy	*pwrout.s* *pwrnorm.s* *pwrfail.s*
Napájení systému	Podpětí Přepětí	*syspwuv.s* *syspwov.s*
Napájení obvodu vnějších periferií	Podpětí, přepětí, zkrat	*expwfail.s*
Napájení obvodu signalizačních prvků	Podpětí, přepětí, zkrat	*sipwfail.s*
Drátové smyčky		
Samostatně pro sm. 1 – 4 (X = číslo smyčky)	Poplach na smyčce Detekce sabotáže	*lpXalarm.s* *lpXtamp.s*
Komunikátor Ethernet		
Vzdálené spuštění skriptu	Skript podle podepsaného příkazu	
Komunikace s nadřazenou ústřednou	Pokus o komunikaci s neplatným podpisem Přijat dotaz nebo příkaz	*etherr.s* *ethcmd.s*
Autentizace uživatele WWW rozhraní	Kontrola hesla	*ethauth.s*
Komunikace RS-485, RS-232		
Příjem dat	Přijat datový rámec	*rs232in.s* *rs485in.s*
Připojitelné moduly (příprava – neimplementováno)		
Dekodér a přijímač 433 MHz Keeloq	Příjem platných dat, příjem dat s porušeným plovoucím kódem, příjem dat pro učení vysílačů, detekce trvalého rušení spektra	
Vstupní moduly	Změna stavu vstupů	
Interní zdroje dat		
Časovač	Periodicky 1x za sekundu Po vypršení časovače X	*tick.s* *tmrX.s*
Interní chyby	Náběh systému / restart systému	*init.s*
Tlačítka na desce ústředny	Stisk tlačítka 1 Stisk tlačítka 2	*btn1.s* *btn2.s*
Sabotážní kontakt ústředny	Rozepnutí	*ctrltamp.s*

Tabulka 4: Přehled událostí a jimi spouštěných skriptů

B Ukázky skriptů

V následujících ukázkách předpokládáme, že smyčky 1 a 2 jsou zpožděné, smyčka 3 okamžitá a smyčka 4 24-hodinová; výstupní relé 1 spíná sirénu. Ukázky jsou poněkud zjednodušené tak, aby byl zřejmý princip programování a variability ústředny, nejsou uvedeny například skripty pro ošetření chybových stavů napájení a sabotáže smyček a některé funkční závislosti jsou zjednodušené.

B.1.Sada skriptů pro základní funkci ústředny

Systémové pole Glob[] je v této sadě skriptů využito pro uložení stavu zastřežení ústředny (viz tabulka).

Glob[0]	0: odstřeženo, 1: zastřeženo
Tmr[0]	Odpočet odchodového zpoždění
Tmr[1]	Odpočet zpoždění zpožděných smyček
Tmr[2]	Odpočet doby poplachu

Tabulka 5: Využití systémových proměnných a časovačů

Skript **init.s**, spouštěný při zapnutí napájecího napětí nebo restartu ústředny, nastaví typy smyček v systémovém poli Stp[] a inicializuje proměnné v poli Glob[].

```
Stp[0]=Stp[1]=Stp[2]=Stp[3]=3+4; //jednoduše vyvážené smyčky s protisabotážní ochranou
```

Zdrojový kód 1: Inicializace ústředny (init.s)

Prozatím budeme ovládat zastřežení a odstřežení ústředny tlačítky na její desce. Ta spouští skripty **btn1.s** a **btn2.s**, kterými budeme řídit stav proměnné Glob[0]. Zastřežení systému je doplněno odchodovým zpožděním: během něj je zařízení de facto stále odstřežené. Pro účely naší ukázky postačí řešení, kdy pouze spustíme časovač 0 nastavený na 30 sekund, který po svém vypršení spustí skript **tmr0.s** – ten teprve zastřeží nastavením proměnné Glob[0] na hodnotu 1.

```
Glob[0]=0;              //odstřežíme
Tmr[0]=0;               //zrušíme případné běžící odchodové zpoždění
Tmr[1]=0;               //zrušíme případné běžící zpoždění zpož. smyčky
Tmr[2]=0;               //zrušíme případně běžící časovač sirény a tím zajistíme i její vypnutí (tick.s)
```

Zdrojový kód 2: Odstřežení ústředny (btn1.s)

```
Tmr[0]=30;              //nastavíme časovač pro odchodové zpoždění
```

Zdrojový kód 3: Zastřežení ústředny s odchodovým zpožděním (btn2.s)

```
Glob[0]=1;              //zastřežíme
```

Zdrojový kód 4: Zastřežení ústředny s odchodovým zpožděním (tmr0.s)

Periodicky se opakující akce soustředíme do skriptu **tick.s**, který je spouštěn jednou za sekundu. V něm budeme provádět následující akce:

- podle stavu časovače sirény sepneme nebo rozepneme výstupní relé sirény,
- podle stavu zastřežení ovládáme LED diodu „ACT“ na desce ústředny,
- běží-li odchodové zpoždění nebo časovač zpožděných smyček, sepneme signalizační sirénku na desce ústředny.

```
if (Tmr[2]) Out[0]=1; else Out[0]=0;                    //sepneme sirénu podle stavu jejího časovače
if (Tmr[0]||Tmr[1]) Out[7]|=3; else Out[7]&=~3;   //ovládání sign. sirénky při běhu zpoždění
if (Glob[0]) Out[7]|=4; else Out[7]&=~0;          //ovládání LED „ACT“
```

Zdrojový kód 5: Vyhodnocení časovačů (tick.s)

24-hodinová smyčka spouští ihned poplach, a to bez ohledu na stav zastřežení systému. Při její aktivaci tedy můžeme přímo nastavit časovač doby poplachu: při jeho běhu se pomocí skriptu **tick.s** sepne výstupní relé sirény. Obdobně můžeme ošetřit například sabotáž smyček nebo skříně ústředny.

```
Tmr[2]=60;                              //spustíme sirénu na 60 sekund
```

Zdrojový kód 6: Vyhodnocení 24-hodinové smyčky (lp4alarm.s)

Okamžitá smyčka smí spustit poplach jen tehdy, je-li systém zastřežený.

```
if (Glob[0]) Tmr[2]=60;                 //spustíme sirénu na 60 sekund, je-li zastřeženo
```

Zdrojový kód 7: Vyhodnocení okamžité smyčky (lp3alarm.s)

Zpožděné smyčky spouští časovač Tmr[1] a to jen tehdy, je-li systém zastřežený. Pokud časovač Tmr[1] již běží (byl aktivován jinou smyčkou nebo se stav smyčky mění), skript do jeho chodu již nezasahuje. Vypršení časovače Tmr[1] (**tmr1.s**) již přímo spouští časovač poplachu.

```
if (Glob[0]&!Tmr[1]) Tmr[1]=20;  //zpoždění smyčky 20 sekund spustíme, je-li zastřeženo
                                 //a časovač zpoždění neběží
```

Zdrojový kód 8: Vyhodnocení zpožděných smyček (lp1alarm.s a shodný lp2alarm.s)

```
Tmr[2]=60;                              //spustíme sirénu na 60 sekund
```

Zdrojový kód 9: Vyhodnocení zpožděných smyček (tmr1.s)

B.2.Ukázka autentizace uživatele pomocí RS-485 klávesnice a vzdáleného serveru

Předchozí ukázku doplníme o autentizaci uživatelů klávesnicí, připojenou na rozhraní RS-485 ústředny. Předpokládejme, že klávesnice zasílá přímo zadaný kód, ukončený znaky <CR><LF>.

Seznam kódů opravňujících ke vstupu bude uložen v systémovém poli Glob[] v prvcích Glob[100] až Glob[119]. Nepoužité prvky budou mít nulovou hodnotu.

Po přijetí dat z klávesnice vyvolá úloha *IOman* ústředny spuštění skriptu **rs485in.s**. Pokud bude zadán kód „#", systém se zastřeží; bude-li zadán jiný kód, je nejprve prohledán seznam kódů, uložených v poli Glob[], a je-li nalezena shoda, je systém ihned odstřežen.

V předchozím oddílu byly popsány skripty **btn1.s** pro odstřežení ústředny a **btn2.s** pro její zastřežení, které nyní budeme volat pomocí systémové proměnné scJump.

```
//prijem dat z RS-485
if (strcmp(Rd485,"#")==0) {
        strcpy(scJump,"btn2");                                  //zavoláme skript pro zastřežení ústředny
                                                                //při stisku křížku
} else {
        //pokus o odstřežení
        int i;
        int opr = 0;
        int kod = atoi(Rd485);
        for (i=100;i<120;i++) {                                 //projdeme pole Glob a hledáme
                                                                //shodu se zadaným kódem
                if (Glob[i] && Glob[i]==kod) opr = 1;
        }
        //máme shodu?
        if (opr) {
                strcpy(scJump,"btn1");                          //zavoláme skript pro odstřežení ústředny
        } else {
                //nemáme shodu, zkusíme dotaz na nadřazený systém
                strcpy(TxIO,"Neplatny kod");
                Cflg[3]=231;                                    //nastavíme UDP port 231
                Cflg[4]=192;Cflg[5]=168;Cflg[6]=1;Cflg[7]=4;    //nastavíme IP adresu 192.168.1.4
                TxDir=3;                                        //start odesílání textu „Neplatny kod"
                                                                // protokolem UDP

                //připravíme data pro odpověď na podepsaný šifrovaný dotaz
                strcpy(TxRSA,"KOD=");
                strcat(TxRSA,Rd485);
        }
}

Cflg[1]=0;      //resetujeme přijímací logiku RS-485 (povolíme příjem dalšího kódu)
```

Zdrojový kód 10: Vyhodnocení kódu, zadaného klávesnicí (rs485in.s)

Pokud nebude zadaný kód nalezen v systémovém poli, zařízení zašle protokolem UDP nešifrovanou výzvu nadřazenému systému (text „`Neplatny kod`"). Nadřazený systém následně zašle podepsaný dotaz na stav systému, na který dostane šifrovanou podepsanou odpověď se zadaným kódem (`KOD=<zadaná hodnota>`).

V případě, že bude kód vyhodnocen jako platný, zašle nadřazený systém šifrovaný podepsaný příkaz pro odstřežení systému pomocí skriptu **otevr485.s**, který současně uloží zadaný kód do pole Glob[].

```
//příjem dat ze šifrovaného kanálu

        int i;
        int kod = atoi(RdRSA);
        for (i=100;i<120;i++) {          //projdeme pole Glob a zapíšeme kód na volnou pozici
                if (!Glob[i]) {
                        Glob[i]=kod;
                        break;
                }
        }
        strcpy(scJump,"btn1");           //zavoláme skript pro odstřežení ústředny
        Cflg[2]=0;                       //povolíme další příjem dat RSA kanálem
```

Zdrojový kód 11: Příjem příkazu ze serveru a odstřežení systému (otevr485.s)

Nadřazený systém může kdykoliv smazat jeden z uložených kódů skriptem **smazkod.s**, který dálkově spustí šifrovaným podepsaným příkazem.

```
//příjem dat ze šifrovaného kanálu

        int i;
        int kod = atoi(RdRSA);
        for (i=100;i<120;i++) {          //projdeme pole Glob a uvolníme prvky, obsahující rušený kód
                if (Glob[i]==kod) {
                        Glob[i]=0;
                }
        }
        Cflg[2]=0;                       //povolíme další příjem dat RSA kanálem
```

Zdrojový kód 12: Příjem příkazu ze serveru a smazání kódu (smazkod.s)

B.3.Ukázka programování funkcí jednoduché domovní automatizace

Jednoduchou aplikaci z předchozího oddílu můžeme rozšířit o prvky automatizace budov a řízení přístupu osob.

Pro účely tohoto příkladu předpokládejme umístění zařízení v kancelářské budově. Budeme požadovat, aby zařízení po přiložení karty na čtečku, umístěnou přede dveřmi kanceláře, sepnulo na několik sekund elektrický zámek a rozsvítilo na zadanou dobu v předsíňce pokoje.

Osvětlení v předsíňce bude dále možné rozsvítit i zhasnout samostatným tlačítkem.

Dále budeme požadovat, aby blokovalo pomocí jednoho výstupního relé chod klimatizace, není-li v prostoru více než tři hodiny detekován pohyb. Pokud uživatel zastřeží systém v době mezi 16:00 a 24:00, zablokujeme chod klimatizace okamžitě, v opačném případě necháme doběhnout zmíněný tříhodinový časovač, aby se klimatizace nevypnula například během pauzy na oběd.

Využijeme výstupní relé 2 pro spínání osvětlení, výstupní relé 3 pro blokování klimatizace a výstupní relé 4 pro otvírač dveří. Na smyčku 1 připojíme místo čidel EZS tlačítko ovládání osvětlení.

Tmr[3]	Čas sepnutí elektrického zámku
Tmr[4]	Odpočet od posledního pohybu (blok. klimatizace)
Tmr[5]	Časový spínač osvětlení

Tabulka 6: Využití systémových proměnných a časovačů

Do skriptu **btn1.s**, který zajišťuje odstřežení ústředny, doplníme sepnutí elektrického zámku, osvětlení a inicializaci příslušných časovačů.

```
(doplnit)
Tmr[3]=2;               //2 sekundy chod el. zámku
Out[3]=1;               //sepnutí el. zámku
Tmr[4]=10800;           //3 hodiny timeout pro klimatizaci
Out[2]=0;               //vypneme blokaci klimatizace
Tmr[5]=30;              //30 sekund časovač osvětlení
Out[1]=1;               //sepnutí osvětlení
```

Zdrojový kód 13: Odstřežení ústředny (btn1.s)

Do skriptu **btn2.s**, který zajišťuje zastřežení ústředny, doplníme sepnutí blokace klimatizace.

```
(doplnit)
if (Rtc[2]>=16 && Rtc[2]<=23) {//je 16 - 24 hodin
        Out[2]=1;               //zapneme ihned blokaci klimatizace
}
```

Zdrojový kód 14: Zastřežení ústředny (btn2.s)

Do skriptů, které ošetřují smyčky s pohybovými čidly, doplníme příkaz pro restart časovače blokace klimatizace.

```
(doplnit)
Tmr[4]=10800;
```

Zdrojový kód 15: Doplnění příkazu pro restart časovače blokace klimatizace

Obslužný skript smyčky č. 1 nahradíme skriptem, který umožní rozsvícení osvětlení na 10 minut stiskem připojeného tlačítka. Pokud osvětlení svítí, stisk tlačítka jej vypne.

```
(tmr3.s)
Out[3]=0;               //vypni el. zámek
(tmr4.s)
Out[2]=1;               //zapni blokaci klimatizace
(tmr5.s)
Out[1]=0;               //vypni osvětlení
```

Zdrojový kód 16: Spínání osvětlení (lp1alarm.s)

Nakonec **ošetříme vypršení časovače** elektrického zámku, blokace klimatizace i osvětlení.

```
(tmr3.s)
Out[3]=0;               //vypni el. zámek
(tmr4.s)
Out[2]=1;               //zapni blokaci klimatizace
(tmr5.s)
Out[1]=0;               //vypni osvětlení
```

Zdrojový kód 17: Ošetření časovačů (tmr3.s … tmr5.s)

Doplněním několika skriptů jsme ústřednu obohatili o funkce, které by v případě užití standardních prvků vyžadovaly instalaci několika poměrně nákladných časových relé a samostatného PIR snímače, případně zapojení relativně složitého úvazku na systém EZS.

C WWW rozhraní, obsah paměťové karty

C.1.Obsah paměťové karty

Zjednodušený obsah paměťové karty:

```
\ --- ctrl.ini                    ---     hlavní konfigurační soubor
   |  tick.s                      ---     jednotlivé soubory skriptů
   |   .
   |   .


   |  HTTP                        ---     adresář souborů WWW serveru
       --- index.htm              ---     přesměrování na index.sht
         |  login.sht             ---     formulář pro zadání hesla do WWW rozhraní
         |  index.sht             ---     index WWW rozhraní - diagnostika
         |  tcp.sht               ---     diagnostika OS a spojení
         |  cfg.sht               ---     editor souborů skriptů
         |  pub.sht               ---     vrací veřejný klíč ústředny
         |   .                    ---             a další soubory, přístupné přes WWW rozhraní

         |  pub.cer               ---     veřejný klíč ústředny (předávaný WWW rozhraním)
```

C.2. Konfigurační soubor ctrl.ini

Příklad obsahu konfiguračního souboru ctrl.ini ústředny:

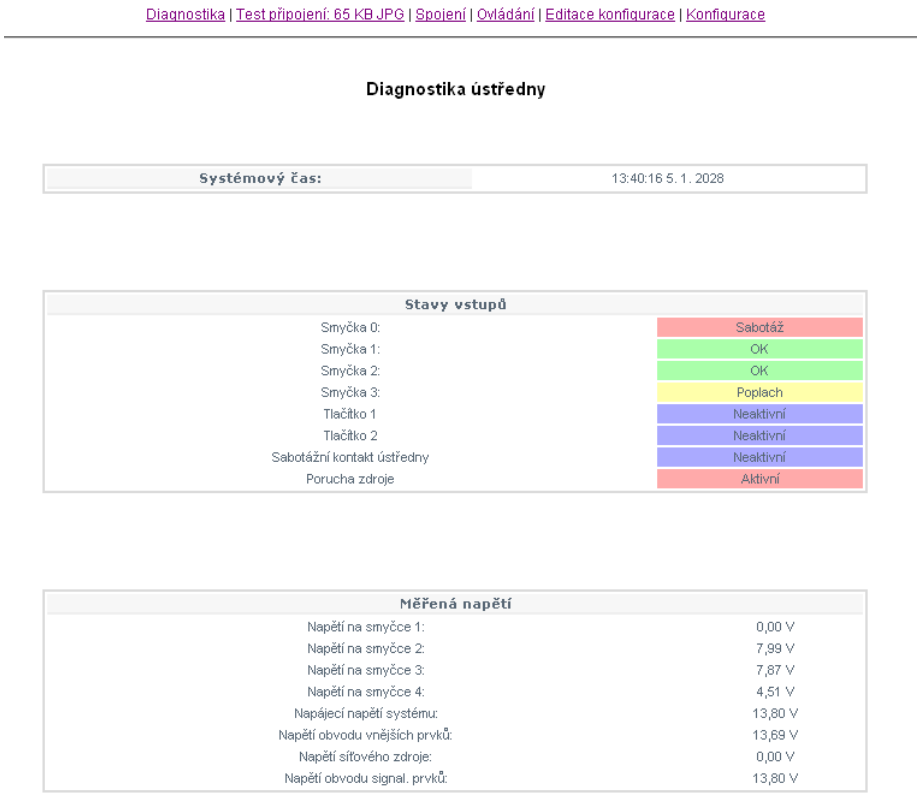
```
[IP]
;IP adresa (192.168.1.43), brána (192.168.1.1), maska sítě (255.255.255.0)
IP1=192
IP2=168
IP3=1
IP4=43
GATE1=192
GATE2=168
GATE3=1
GATE4=1
MASK1=255
MASK2=255
MASK3=255
MASK4=0

[GENERAL]
dbgintf=1       ;rozhraní pro ladění: 0 = vypnuto, 1 = RS232, 2 = JTAG

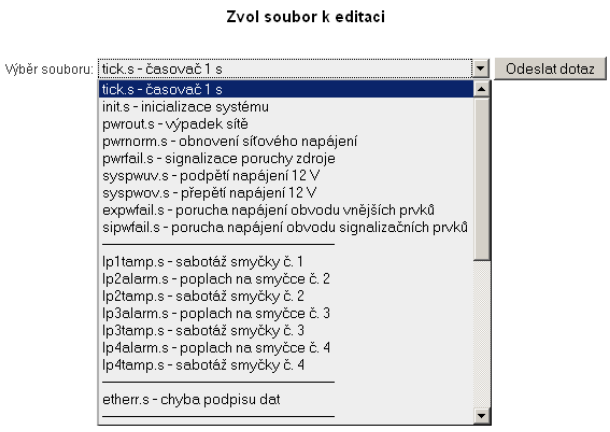
[KEY]
;privátní RSA klíč ústředny (hex)
RSA_N=9292758453063D803DD603D5E777D7888ED1D5BF35786190FA2F23EBC0848AEA...
.
. (další data)
.

[PUBK]
;veřejné klíče nadřazených ústředen č. 0 až 7
P0_N=5845305A2814AB...
P0_E=10001
P1_N=603D5777FA8AEA...
P1_E=3
P2_N=AB5ED48A7557BC...
P2_E=10001
.
.
.
```

C.3. Ukázky WWW rozhraní

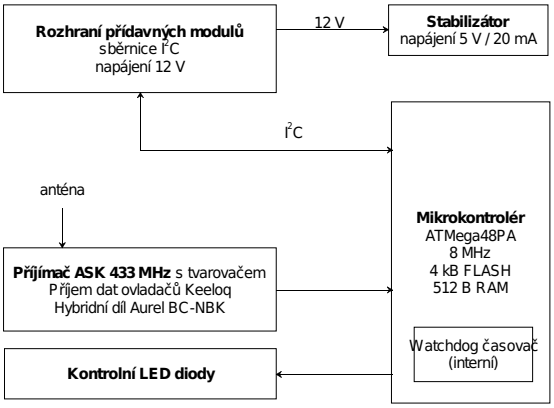


Obr. C 1: Diagnostika stavu ústředny



Obr. C 2: Editor skriptů: výběr souboru k editaci

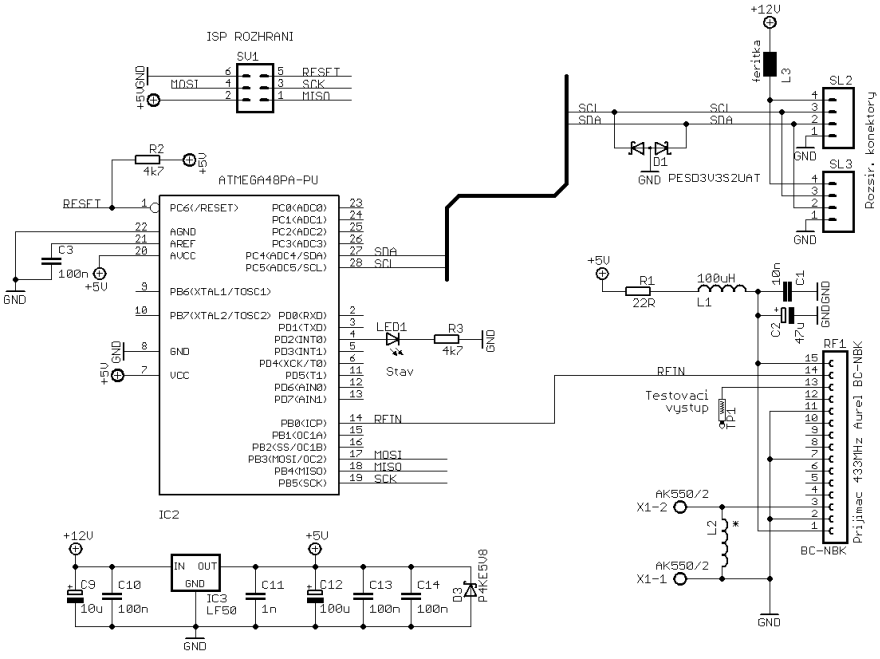
D Návrh přídavného modulu bezdrátového přijímače 433 MHz



Obr. D 1: Blokové schéma bezdrátového přijímače 433 MHz

Uvedené blokové schéma ukazuje možné zapojení přídavného modulu pro příjem dat v pásmu 433 MHz, například pro příjem vysílačů standardu Keeloq. V tomto případě je komunikace rozhraním I²C řízena softwarově použitým mikrokontrolérem, který současně řeší časování příjmu, vlastní příjem dat a jejich dekódování.

Na obr. D 2 je uvedeno netestované detailní schéma zapojení modulu s užitím přijímače Aurel BC-NBK.



Obr. D 2: Schéma zapojení modulu přijímače Keeloq

Výrobní cena modulu by při množství v řádu stovek kusů neměla překročit 120 Kč.

E Obsah přiloženého CD

- text práce,
- schémata a výkresy ve formátu Cadsoft Eagle 5.60,
- obsah paměťové karty prototypu,
- zdrojové kódy firmware mikrokontroléru včetně použitých knihoven

F Rozpiska materiálu

Počet kusů	*Součástka*	*Hodnota*	*Poznámka*	*Reference*
1	Kondenzátor	2n2/2kV	SMD 1210	C1
2	Kondenzátor	KEMET C1206C106K4PAC-TU 10u	SMD 1206	C12, C13
1	Kondenzátor	TAIYO YUDEN TMK316BJ106KL-T 10u	SMD 1206	C14
9	Kondenzátor	1nF, NP0	SMD 0805	C15, C27, C29, C74, C75, C76, C77, C78, C79
1	Kondenzátor	1nF, 100V	SMD 0805	C2
1	Kondenzátor	100n, 100V,X7R	SMD 0805	C3
1	Kondenzátor	1000µF, 25V, 105C	RM 5	C30
4	Kondenzátor	22pF	SMD 0805	C37, C38, C39, C47
23	Kondenzátor	100nF	SMD 0805	C4, C28, C31, C32, C40, C41, C42, C44, C45, C46, C50, C54, C55, C59, C60, C63, C68, C69, C70, C71, C72, C73, C80
1	Kondenzátor	10uF tantal	SMD B	C43
10	Kondenzátor	1µF, X7R	SMD 0805	C5, C10, C33, C34, C35, C36, C48, C49, C62, C67
1	Kondenzátor	100pF	C-EUC0805K	C52
3	Kondenzátor	100µF	RM 3,5	C56, C57, C58
3	Kondenzátor	22µF	RM 3,5	C6, C7, C11
1	Kondenzátor	22nF	C-EUC0805K	C61
1	Kondenzátor	15nF	C-EUC0805K	C65
1	Kondenzátor	4,7pF	C-EUC0805K	C66
1	Kondenzátor	47pF	C-EUC0805K	C8
2	Kondenzátor	10u/X7R	C-EUC1206	C81, C82
1	Kondenzátor	47n/250V	C-EUC0805K	C9
1	Patice SD karty	3M 2900		CD1
2	Transil	SMBJ58A		D1, D2
4	Transil	PESD3V3S2UAT		D10, D13, D23, D24
1	Dioda	BAS40		D15
2	Zenerova dioda	BZX84C12V		D17, D18
2	Transil	SMBJ12A		D20, D21
1	Dioda	BAV199		D22

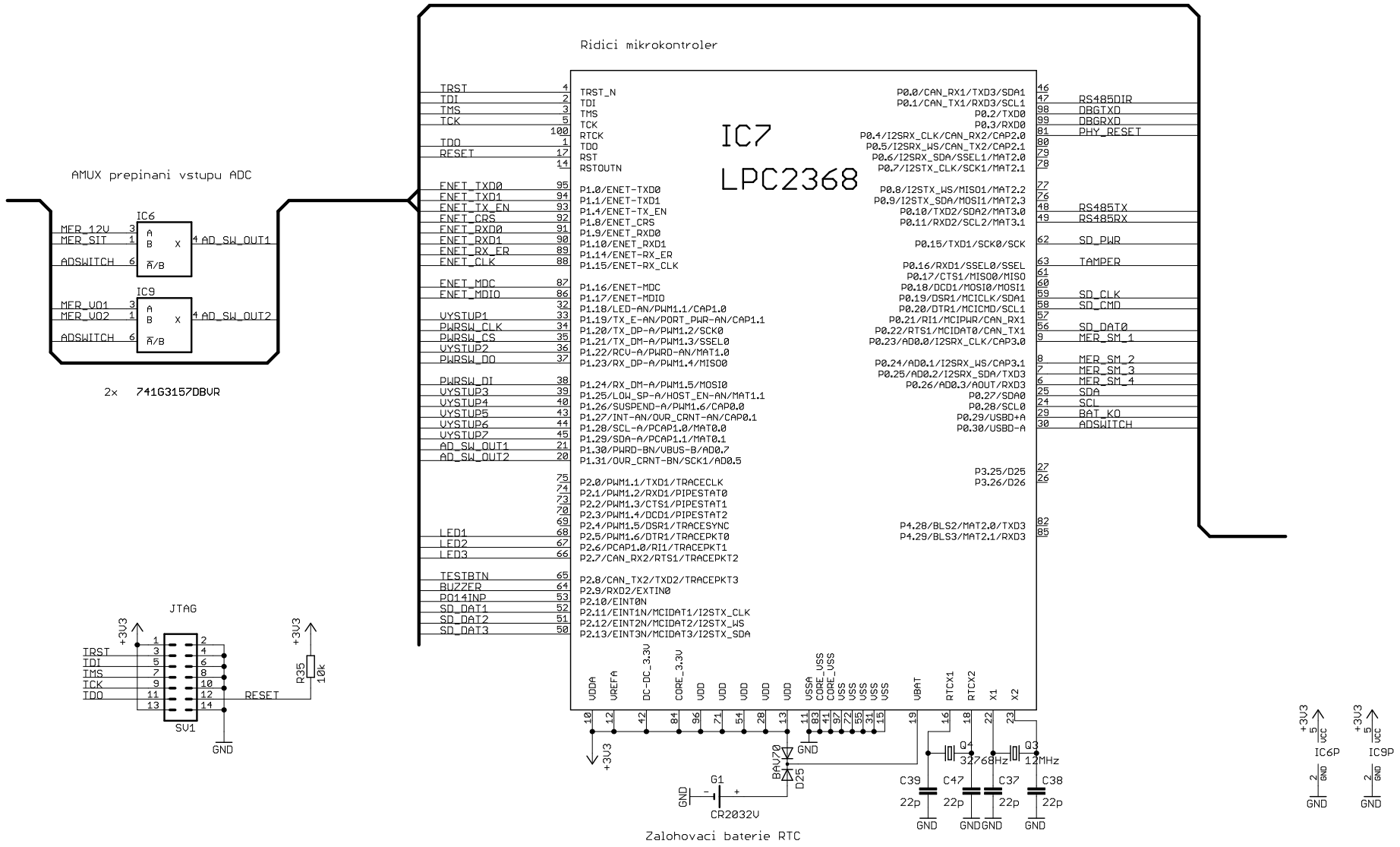
Počet kusů	*Součástka*	*Hodnota*	*Poznámka*	*Reference*
1	Dioda	BAV70		D25
5	Dioda	BAS16		D3, D4, D5, D16, D19
7	Transil	SMBJ17A		D6, D7, D8, D9, D11, D12, D14
1	Pojistka	3,15A/F	TE5	F1
2	Pojistkový rezistor	1k/0,33W		F12, F17
2	Pojistkový rezistor	4R7/0,33W		F18, F19
2	Pojistka	2,5A/F	TE5	F2, F3
4	Pojistkový rezistor	2R2/1W pojistkovy	TE5	F4, F6, F8, F10
4	Pojistkový rezistor	4k7/0,33W		F5, F7, F9, F11
1	Baterie	CR2032V	CR2032 vertik.	G1
1	IO	TPS23756		IC1
1	IO	DP83848C		IC10
1	IO	SN65HVD3082ED		IC11
1	IO	ULN2003AD		IC2
1	IO	TPS62111		IC4
1	IO	MC33879		IC5
2	IO	741G3157DBVR		IC6, IC9
1	IO	LPC2368		IC7
1	IO	ST3232	SO-16	IC8
2	Jumper 2 pin			JP1, JP2
2	Relé	Omron G5V1 12V		K1, K2
2	Relé	Omron G2R 12V		K5, K6
1	Tlumivka	22uH DE1207	DR125	L1
2	Feritka	feritka	WE-CBF_0603	L2, L7
1	Tlumivka	EPCOS B82462G4 22u	L-B84262-G4	L3
1	Tlumivka	TME DLA27-N 27uH	L-US0207/12	L4
1	Tlumivka	EPCOS B82462G4682M	L-B84262-G4	L5
1	LCD displej	BO1602DGPN	neosazen	LCD1
3	LED		SMD 0805	LED5, LED6, LED7
1	Optočlen	PC817		OK1
3	Tranzistor	SI4848	SO-8	Q1, Q5, Q6
2	Tranzistor	MMBTA06	SOT-23	Q100, Q101

Počet kusů	*Součástka*	*Hodnota*	*Poznámka*	*Reference*
1	Tranzistor	IRLML6401TR	SOT-23	Q103
1	Krystal	12MHz	HC49U-V	Q3
1	Krystal	32768Hz	TC26V	Q4
1	Tranzistor	IRF6216	SO-8	Q7
1	Krystalový oscilátor	50MHz CFPS-73	SM77H	QG1
1	Rezistor	63,4 Ω	SMD 0805	R1
4	Rezistor	820 Ω	SMD 0805	R10, R12, R20, R22
1	Rezistor	24,9 kΩ	SMD 0805	R2
4	Rezistor	47 kΩ	SMD 0805	R25, R26, R29, R33
3	Rezistor	68 kΩ	SMD 0805	R3, R4, R30
1	Rezistor	33 kΩ	SMD 0805	R32
2	Rezistor	4,7 kΩ	SMD 0805	R37, R52
3	Rezistor	470 Ω	SMD 0805	R38, R39, R40
1	Rezistor	4,7 Ω	SMD 0805	R41
1	Rezistor	100 Ω	SMD 0805	R42
7	Rezistor	2,2 kΩ	SMD 0805	R43, R44, R45, R47, R53, R54, R57
1	Rezistor	330 Ω	SMD 0805	R46
1	Rezistor	82 kΩ	SMD 0805	R48
1	Rezistor	22 kΩ	SMD 0805	R49
1	Rezistor	10 Ω	SMD 0805	R5
1	Rezistor	4,87 kΩ 1%	SMD 0805	R55
4	Rezistor	49,9 Ω	SMD 0805	R58, R59, R60, R61
1	Rezistor	0,12 Ω	SMD 0805	R6
1	Rezistor	1 kΩ	SMD 0805	R7
10	Rezistor	10 kΩ	SMD 0805	R8, R27, R28, R31, R34, R35, R36, R50, R51, R56
6	Varistor	14VDC	S05K11	R9, R11, R13, R21, R23, R24
1	Rez. síť	2k2	SMD 1206/4	RN1
2	Tlačítko	P-B1720		S1, S2
1	Konektor	PSH02-04P	M04	SL1
1	Konektor	PSH02-02P	M02	SL2
1	Bzučák	AL60P		SP1
1	Konektor	PFL14	ML14	SV1
1	Transformátor	POE300F	POE300F	TR1
1	Reference	TL431	SO-8	VR1

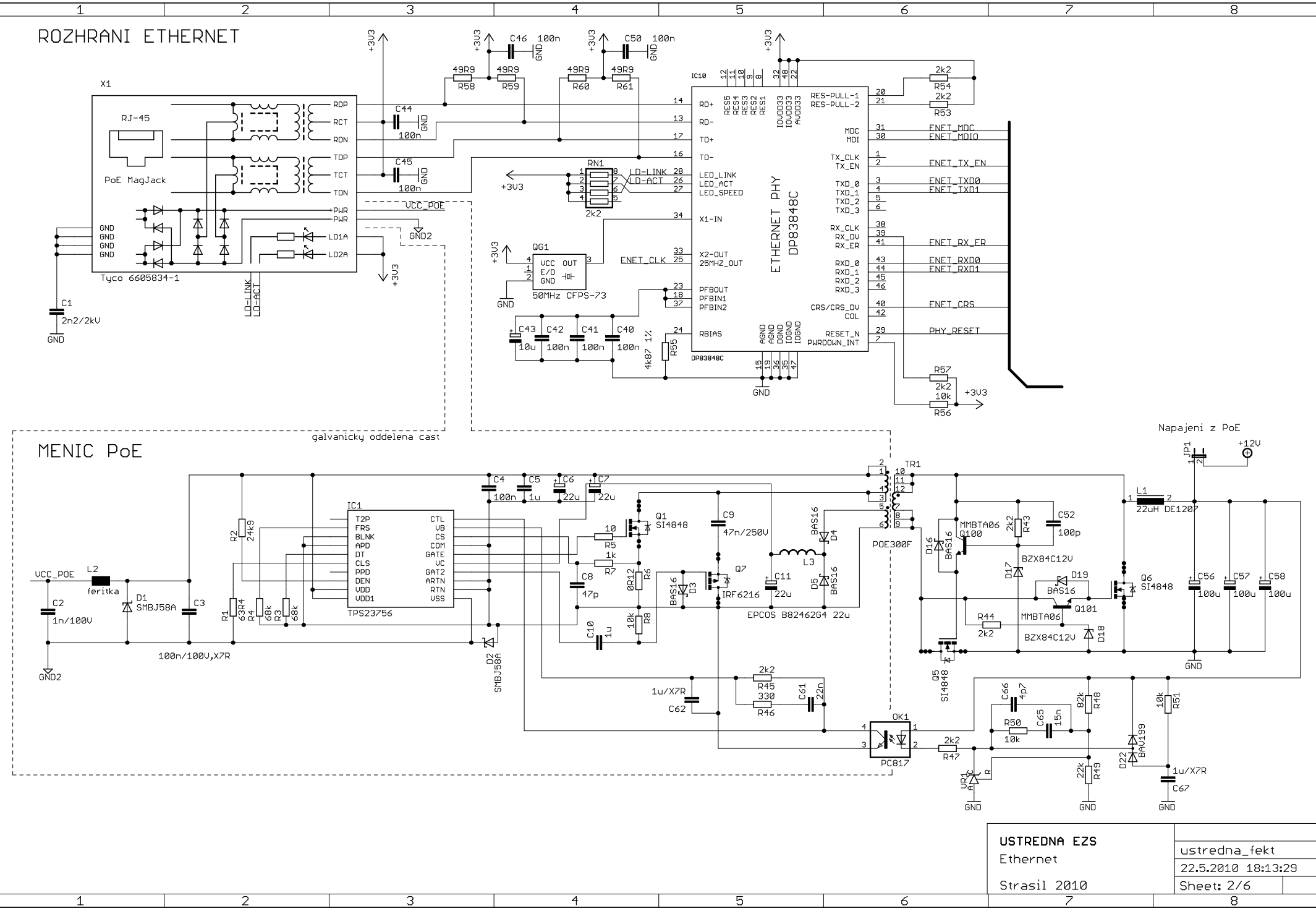
Počet kusů	*Součástka*	*Hodnota*	*Poznámka*	*Reference*
1	Konektor	Tyco 6605834-1	MAGJACK	X-10
1	Svorkovnice	AK550/2	Ninigi	X-6
3	Svorkovnice	MSTBV6	Phoenix Cnt.	X2, X3, X8
2	Svorkovnice	MSTBV8	Phoenix Cnt.	X4, X5
1	Plošný spoj			---
1	Držák	Italtronic E107	(sestava)	---

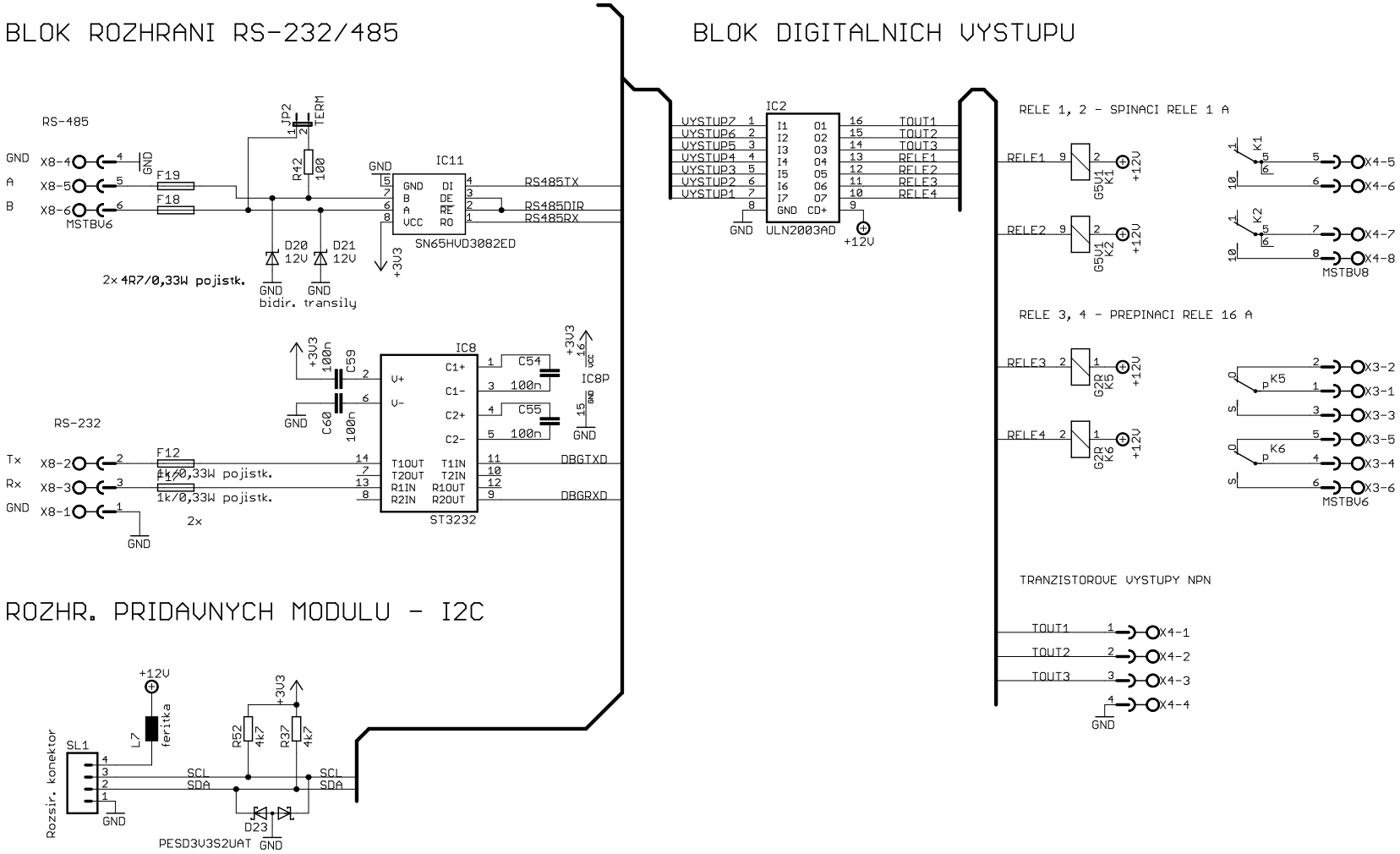
G Výkresová dokumentace hlavního modulu ústředny

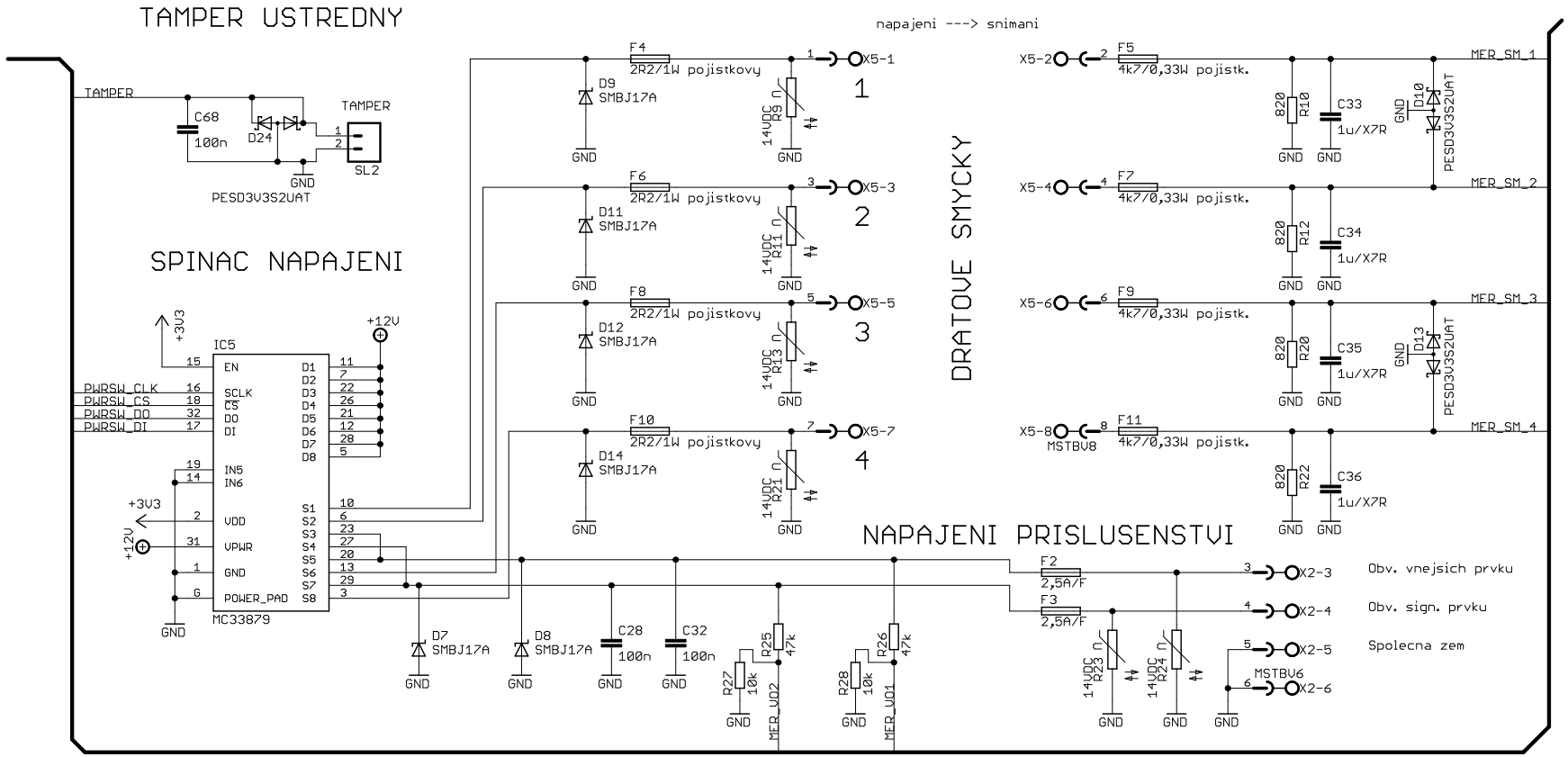
BLOK RIZENI



USTREDNA EZS	
Blok rizeni	ustredna_fekt
Strasil 2010	22.5.2010 18:13:29
	Sheet: 1/6


ROZHRANI ETHERNET
X1
RJ-45
PoE MagJack
Tyco 6605834-1
RDP
RCT
RDN
TDP
TCT
TDN
PWR
PWR
LD1A
LD2A
GND
GND
GND
GND
LD-LINK
LD-ACT
C1
2n2/2kV
C44
100n
C45
100n
VCC_POE
GND2
+3V3
C46 100n
C50 100n
49R9 R58
49R9 R59
49R9 R60
49R9 R61
IC10
ETHERNET PHY
DP83848C
RD+
RD-
TD+
TD-
LED_LINK
LED_ACT
LED_SPEED
X1-IN
X2-OUT
25MHZ_OUT
PFBOUT
PFBIN1
PFBIN2
RBIAS
RES-PULL-1
RES-PULL-2
MDC
MDI
TX_CLK
TX_EN
TXD_0
TXD_1
TXD_2
TXD_3
RX_CLK
RX_DV
RX_ER
RXD_0
RXD_1
RXD_2
RXD_3
CRS/CRS_DV
COL
RESET_N
PWRDOWN_INT
AGND
DGND
IOGND
RES5
RES4
RES3
RES2
RES1
IOVDD33
AVDD33
2k2 R54
2k2 R53
RN1
LD-LINK
LD-ACT
2k2
QG1
VCC OUT
E/D
GND
50MHz CFPS-73
ENET_CLK
ENET_MDC
ENET_MDIO
ENET_TX_EN
ENET_TXD0
ENET_TXD1
ENET_RX_ER
ENET_RXD0
ENET_RXD1
ENET_CRS
PHY_RESET
C43 10u
C42 100n
C41 100n
C40 100n
4k87 1% R55
R57 2k2
R56 10k
galvanicky oddelena cast
MENIC PoE
Napajeni z PoE
JP1
+12V
TR1
POE300F
L1
22uH DE1207
IC1
TPS23756
T2P
FRS
BLNK
APD
DT
CLS
PPD
DEN
VDD
VDD1
CTL
VB
CS
COM
GATE
VC
GAT2
ARTN
RTN
VSS
C4 100n
C5 1u
C6 22u
C7 22u
R2 24k9
R1 63R4
R4 68k
R3 68k
R5 10
R7 1k
R6 0R12
R8 10k
C8 47p
C10 1u
Q1 SI4848
Q7 IRF6216
C9 47n/250V
C11 22u
L3
D4 BAS16
D5 BAS16
D3 BAS16
D2 SMBJ58A
L2 feritka
D1 SMBJ58A
C2 1n/100V
C3 100n/100V,X7R
EPCOS B82462G4 22u
D16 BAS16
Q100 MMBTA06
R43 2k2
C52 100p
D17 BZX84C12V
D19 BAS16
Q101 MMBTA06
R44 2k2
D18 BZX84C12V
Q6 SI4848
Q5 SI4848
C56 100u
C57 100u
C58 100u
C61 22n
R45 2k2
R46 330
C62 1u/X7R
OK1
PC817
R47 2k2
C66 4p7
R50 10k
C65 15n
R48 82k
R49 22k
VR1
D22 BAV199
R51 10k
C67 1u/X7R
USTREDNA EZS
Ethernet
Strasil 2010
ustredna_fekt
22.5.2010 18:13:29
Sheet: 2/6

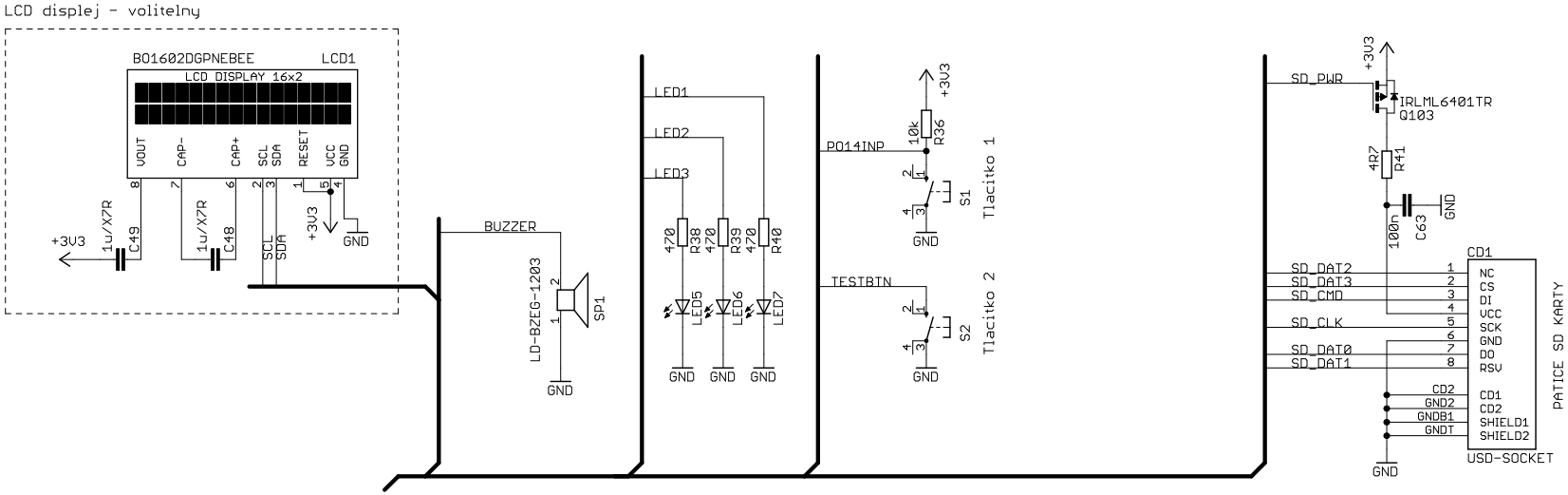

BLOK ROZHRANI RS-232/485
RS-485
GND
A
B
X8-4
X8-5
X8-6
MSTBV6
F19
F18
JP2
TERM
R42
100
IC11
GND
DI
B
DE
A
RE
VCC
RO
SN65HVD3082ED
RS485TX
RS485DIR
RS485RX
+3V3
D20
12V
D21
12V
2x 4R7/0,33W pojistk.
bidir. transily
RS-232
Tx
Rx
X8-2
X8-3
X8-1
F12
1k/0,33W pojistk.
2x
IC8
+3V3
100n
C59
C60
C54
C55
IC8P
V+
V-
C1+
C1-
C2+
C2-
T1OUT
T2OUT
R1IN
R2IN
T1IN
T2IN
R1OUT
R2OUT
ST3232
DBGTXD
DBGRXD
ROZHR. PRIDAVNYCH MODULU - I2C
+12V
ferita
L7
SL1
Rozsir. konektor
SCL
SDA
R52
R37
4k7
D23
PESD3V3S2UAT
BLOK DIGITALNICH VYSTUPU
IC2
VYSTUP7
VYSTUP6
VYSTUP5
VYSTUP4
VYSTUP3
VYSTUP2
VYSTUP1
I1
I2
I3
I4
I5
I6
I7
GND
O1
O2
O3
O4
O5
O6
O7
CD+
TOUT1
TOUT2
TOUT3
RELE1
RELE2
RELE3
RELE4
ULN2003AD
RELE 1, 2 - SPINACI RELE 1 A
G5V1
K1
K2
X4-5
X4-6
X4-7
X4-8
MSTBV8
RELE 3, 4 - PREPINACI RELE 16 A
G2R
K5
K6
X3-2
X3-1
X3-3
X3-5
X3-4
X3-6
MSTBV6
TRANZISTOROVE VYSTUPY NPN
X4-1
X4-2
X4-3
X4-4
USTREDNA EZS
Vystupy a ser.linky
Strasil 2010
ustredna_fekt
22.5.2010 18:13:29
Sheet: 3/6



USTREDNA EZS Vstupy + nap.smycek Strasil 2010	ustredna_fekt 22.5.2010 18:13:29 Sheet: 4/6

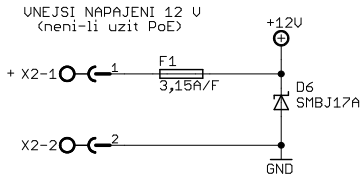
BLOK UZIV. ROZHRANI

ROZHR. SD KARTY

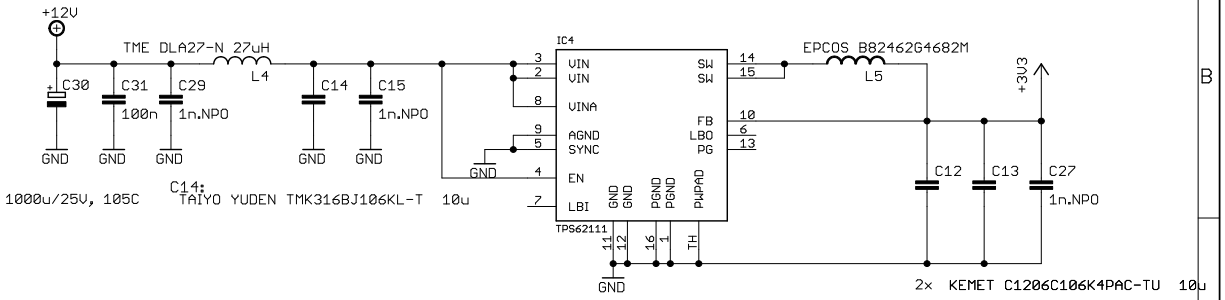


USTREDNA EZS	
Uziv.rozhr.+SD karta	ustredna_fekt
	22.5.2010 18:13:29
Strasil 2010	Sheet: 5/6

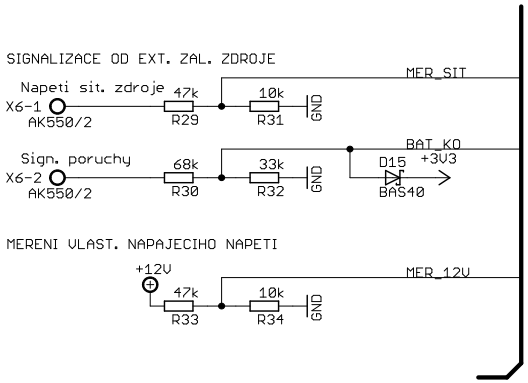
EXT. NAPAJENI

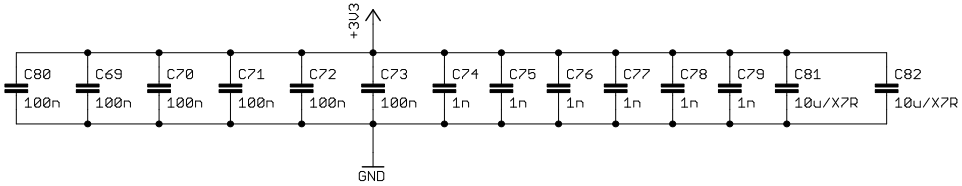


DC/DC MENIC 12 V - 3,3 V



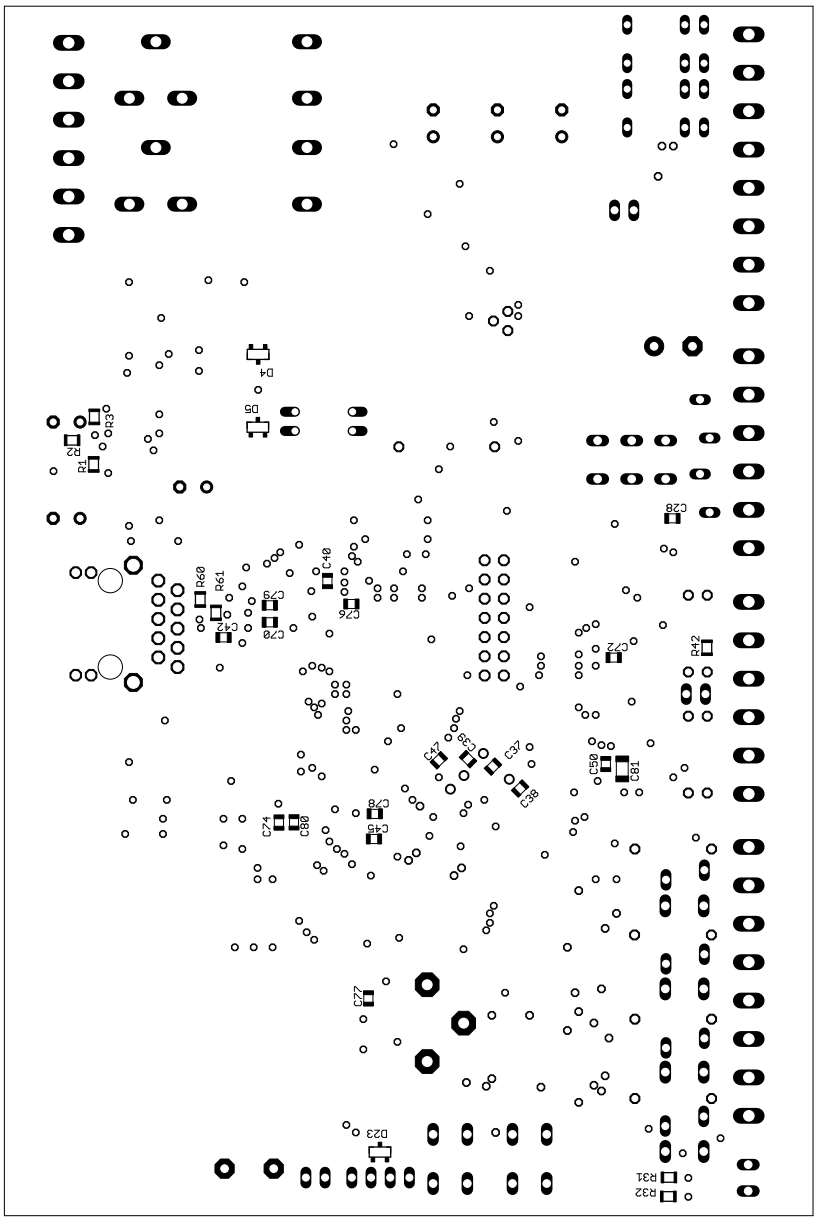
KONTROLA NAPAJENI

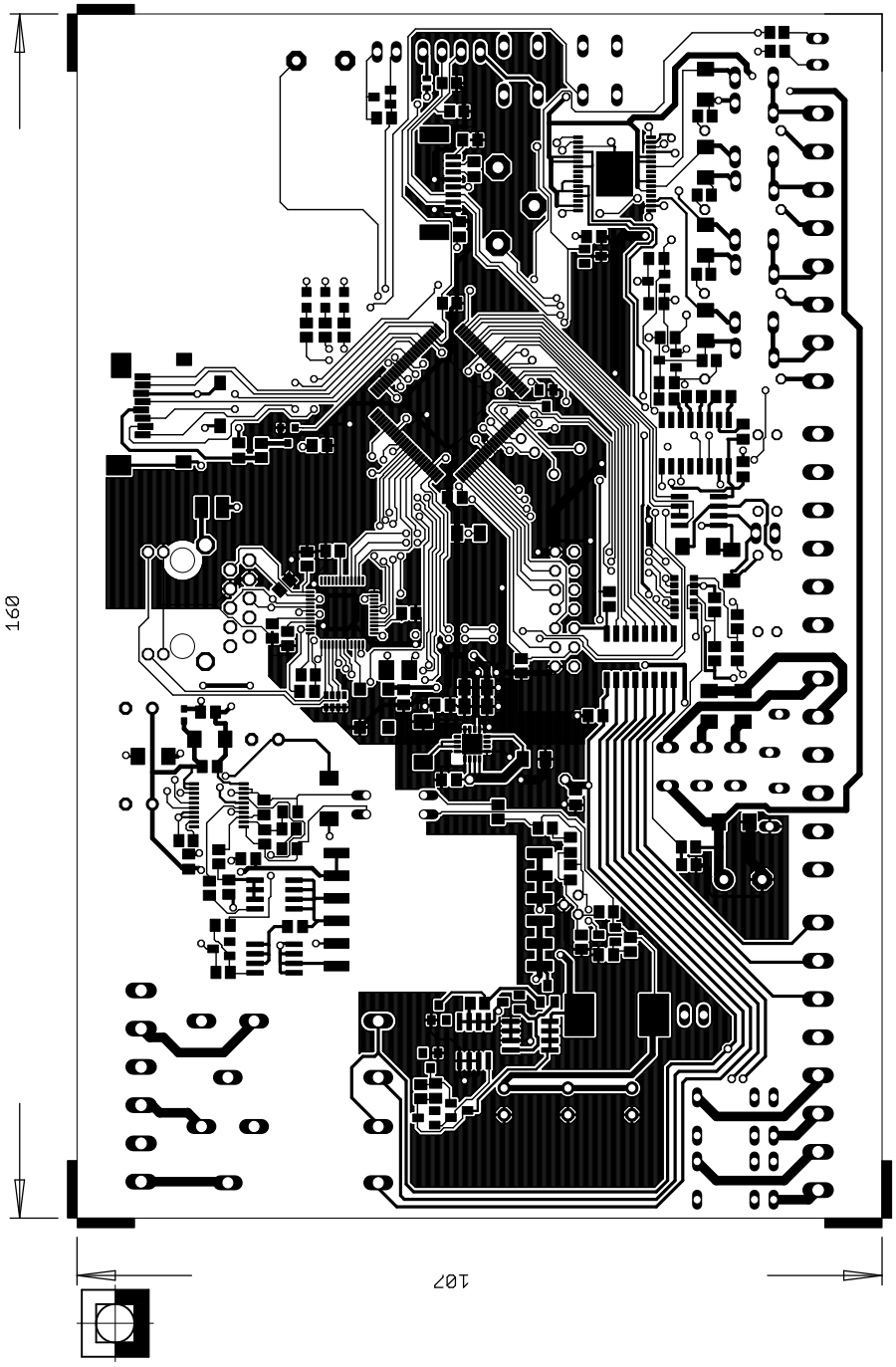


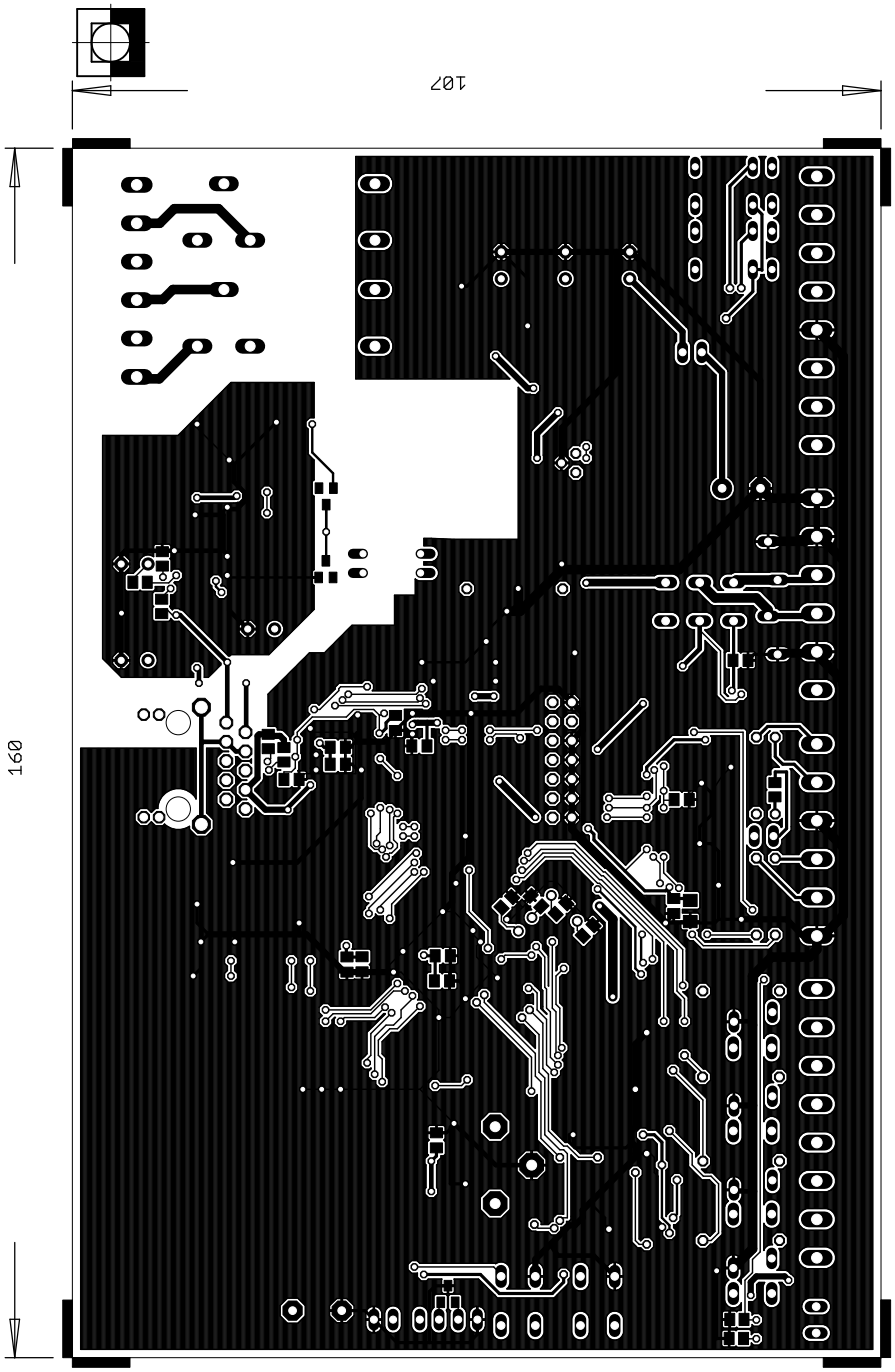


USTREDNA EZS Napajeni Strasil 2010	ustredna_fekt 22.5.2010 18:13:29 Sheet: 6/6

OPTIONAL
LCD DISPLAY
POSITION
ACT
RUN
COMM
TAMPER
EXT I2C
UPD/TEST
STATUS
SD
CARD
ETH/PoE+
JTAG
TERM
PoE SUPPLY
USTREDNA EZS
UTKO FEKT VUT BRNO
STRASIL 2010
HW Rev: 0
2010
s/n: ------
Re3: NC
C
NO
Re4: NC
Re1
Re2
TO1
TO2
TO3
GND
SIGN
VNEJ
EXT12V
RS485 A
B
RxD
TxD
L10
L11
L20
L21
L30
L31
L40
L41
Lith3V


D4
D5
R2
R1
R3
C28
C42
R42
C50
C81
C47
C39
C37
C38
C74
C80
C48
C46
C27
D23
R32
R31
C40
C76
C79
C70
C72
R60
R61


160
107


107
160