Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

# Implementace poplachového tísňového zabezpečovacího systému v rámci Smart Home

# Electronic Security Systems Implementation within Smart Home

2019 Karel Fajt

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

# Zadání bakalářské práce

Student: **Karel Fajt**

Studijní program: B2649 Elektrotechnika

Studijní obor: 2612R041 Řídicí a informační systémy

Téma: Implementace poplachového tísňového zabezpečovacího systému v rámci Smart Home
Electronic Security Systems Implementation within Smart Home

Jazyk vypracování: čeština

Zásady pro vypracování:

Praktická implementace poplachového tísňového zabezpečovacího systému (PTZS) v rámci technologie Smart Home (SH).

1. Provedení rešerše současného stavu dané problematiky.
2. Seznámení se s jednotlivými druhy používaných technologií (normativní a legislativní pozadí), detailní popis zvolené technologie PTZS v SH.
3. Návrh aplikace pro realizaci PTZS v SH.
4. Provedení praktické realizace.
5. Ověření dosažených výsledků.
6. Celkové zhodnocení výsledků práce.

Seznam doporučené odborné literatury:

[1] UHLÁŘ, Jan. *Technická ochrana objektů. II. díl, Elektrické zabezpečovací systémy II.* 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-313-0.
[2] HEŘMAN, Josef a Zdeněk TRINKEWITZ. *Elektrotechnické a telekomunikační instalace: komplexní zpracování problematiky elektrotechnických a telekomunikačních instalací v budovách.* [Svazek 2]. Praha: Dashöfer, 2007. ISBN 80-86897-06-0.
[3] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* 3. aktualiz. vyd. Blatná: Blatenská tiskárna, 2006. ISBN 80-902938-2-4.
[4] CAPEL, Vivian. *Home Security.* Second Edition: Alarms, sensors and systems 2nd Edition. Oxford,UK: Newnes, 1997. ISBN-13: 978-0750635462.
[5] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.
[6] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II.* Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4.
[7] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III.* Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.
[8] VELAS, Andrej. *ELEKTRICKÉ ZABEZPEČOVACIE SYSTÉMY.* Žilina, SK: EDIS – vydavateľstvo Žilinskej univerzity v Žiline, 2010. ISBN 978-80-554-0224-6.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Jan Vaňuš, Ph.D.**

Datum zadání: 01.09.2018

Datum odevzdání: 30.04.2019


doc. Ing. Jiří Koziorek, Ph.D.
*vedoucí katedry*

prof. Ing. Pavel Brandštetter, CSc.
*děkan fakulty*

## Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou/diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: 30.4.2019

.....
podpis studenta

# Poděkování

Chtěl bych poděkovat svému vedoucímu panu Ing. Janu Vaňušovi, Ph.D za odbornou pomoci a vřelý přístup při vytváření této bakalářské práce.

# Abstrakt

Tato bakalářská práce je v první části věnována průzkumu současných trendů a nových technologií v oblasti „inteligentních domácností“ (dále: „SH“) a „poplachových zabezpečovacích tísňových systému“ (dále: „PZTS“). Dále je uveden podrobný popis systému SH spadajících pod asociaci KNX a PZTS firmy Paradox – cílem není obsáhnout všechny podrobnosti o výše zmíněných systémech, ale vytvořit obecný přehled. Jsou zde popsány základní normy a legislativy vztahující se k výše zmíněným systémům.

Praktická část práce se zabývá způsoby implementace PZTS ve SH. Jsou zde popsány dva způsoby realizace implementace PZTS ve SH. Jeden ze způsobů je prakticky realizován. Také je v rámci této práce vypracováno pět laboratorních úloh, které obsahují detailní popis pro zapojení a nastavení PZTS firmy Paradox.



# Klíčová slova

Inteligentní domácnost; poplachové zabezpečovací tísňové systémy; KNX; Paradox

# Abstract

This bachelor's thesis in its first part deals with research of current trends and new technologies in the Smart Home field (hereinafter referred to as the "SH") and emergency alert security (hereinafter referred to as the "PZTS"). Furthemore, there is detailed description of the SH system, which comes under the association KNX and PZTS of the Paradox company. The target is not to cover all particulars about the systems mentioned above, but to create common overview of them. Also, there are described basic norms and legislatives applied to the systems mentioned above.

Practical part of this thesis deals with methods of implementation PZTS into SH. There are described two ways of realization of implementation PZTS into SH. One of the methods was practically made. In addition, as a part of this piece of work, there were elaborated five laboratory tasks. That include detailed description for plugging in and setting of PZTS of the Paradox company.



# Key words

Smart Home; Security System; KNX, Paradox

# Obsah

# Seznam použitých symbolů a zkratek

| | | |
|---|---|---|
| PZTS | | poplachový zabezpečovací tísňový systém |
| EPS | | elektronický požární systém |
| SH | Smart Home | inteligentní domácnost |
| IoT | Inthernet of Things | internet věcí |
| HMI | Human Machine Interface | uživatelské rozhraní |
| ID | IDentification | identifikace |
| EKG | ElektroKardioGraf | elektrokardiografie |
| PPG | PhotoPlethysmoGram | penilní pletysmografie |
| NO | normally open | normálně otevřené |
| NC | normally close | normálně zavřené |
| ETS | Engineering Tool Software | inženýrský programovací nástroj |
| PL | Power Line | typ přenosového média KNX |
| TP | Twisted Pair | kroucený dvoupár |
| CSMA/CA | Carrier Sense Multiple Access with Collision Avoidance | vícenásobný přístup s předcházením kolizí |
| LAN | Local Area Network | lokální síť |
| HAN | Home Area Network | domácí síť |
| Ω | Ohm | jednotka elektrického odporu |

# Seznam ilustrací

# Seznam tabulek

# 1 Úvod

Lidé mají od nepaměti snahu chránit svá obydlí ať už před zloději, požárem či vandalizmem. Primitivní zámky, petlice a různé ploty v dnešní době nahradily plně elektrické zabezpečovací systémy, které souhrnně nazýváme „poplachové zabezpečovací tísňové systémy“. Ty se v dnešní době stali již jistým standardem ve vybavení domácností. Postupným zušlechťováním svých domovů, spojeným s vývojem domácích spotřebičů se vyvinuly systémy, které dnes nazýváme „inteligentní domácností“. Jak už bylo zmíněno, zabezpečovací systémy se do domácností instalují již dlouhou dobu, avšak dnes se do domácností, který již zabezpečovací systém obsahují, začínají ve velkém instalovat systémy SH. A zde vyvstává otázka, zda by se tyto dva systémy nedaly propojit a jednotně ovládat. Po jednotném, tedy i jednodušším a přívětivějším ovládání dvou výše zmíněných systémů je mezi uživateli velká poptávka.

Cílem této bakalářské práce je v prví části zmapování aktuálních trendů a nových technologií v oblasti SH a PZTS. Vytvoření obecného přehledu obou systémů, který by měl vést k jejich pochopení a základnímu seznámení s nimi. Druhá, praktická část je věnována možnostem implementace SH v PZTS. Jsou zde popsány dva způsoby řešení, a to propojení systémů binárními vstupy a propojení sběrnic systémů. Pro řešení s propojením binárních vstupů je vytvořena praktická realizace, kde jsou systémy SH a PZTS navrženy do modelu rodinného jednopatrového domu. Reálné propojení systémů bylo provedeno ve školní laboratoři. Byly při něm použity ty samé komponenty, které jsou umístěny v modelovém domě.

Závěrečná část práce je věnována popisu pěti laboratorních úloh, které byly vypracovány v rámci této práce. Každá z těchto úloh obsahuje detailní popis zapojení a oživení PZTS pro určitý druh detektorů a ústředny.

# 2 Trendy v systémech SH a PTZS

### Zabezpečení a inovace v IoT

Zařízení IoT jsou stále rozšířenější a stávají se nedílnou součástí našich životů. Stále častěji se instalují jako součást inteligentních domácností. Každý objekt IoT má vlastní speciální ID, které se využívá pro jeho identifikaci. Právě ověřování totožnosti komponentu IoT je reálným bezpečnostním rizikem. Tímto tématem se ve svém článku zabývá se svým týmem AHMED, I., A. P. SALEEL, B. BEHESHTI a Z. A. KHAN. Jejich článek pojednává o kritických otázkách souvisejících s bezpečností a ochranou soukromí v oblasti IoT [1].Výzkumná práce Manimuthu, A. a R. Ramesh prezentuje požadavky na vývoj ekonomicky efektivní IoT-HAN systému spojeného s inteligentní sítí. V jejich návrhu jsou senzory s podporou IoT použity pro zabezpečení komunikace a integritu dat uvnitř sítí HAN (Home Area Network). Vkládáním dat na cloud zpřístupňují uživateli údaje o spotřebě energie. Výsledné konstrukční schéma definuje umístění, nastavení sensorů a řídící jednotky pro energeticky efektivnější přenos dat [2].GUO, Z. M., N. KARIMIAN, M. M. TEHRANIPOOR, D. FORTE s jejich týmem navrhují, že zabezpečení IoT systémů by mělo začínat od hardwarové úrovně. Jelikož velká část IoT zařízení vyžaduje interaci s lidmi, nabízí se využití biometrie jako prvku zabezpečení v IoT aplikacích. Jejich práce popisuje kombinaci využití biometrických prvků jako EKG a PPG k přístupu k zařízením IoT a dalším elektronickým zařízením [3]. Avšak rozkvět IoT technologií má svá úskalí. Výsledkem stále vyššího počtu připojených inteligentních zařízení je zvyšující se objem dat uložených na internetu. Stále se zvyšující datové toky a nároky kladoucí se na sítě, a především zabezpečení těchto sítí jsou problémy, které je do budoucna nutno vyřešit. RADOVAN, M. a B. GOLUB se svým týmem se ve svém článku zabývají možnými řešeními tohoto problému. Dále zde shrnují a analyzují trendy v oblasti IoT a zabezpečovacích systémech [4]. Dalším problémem je zabezpečení inteligentní domácnosti a IoT zařízení proti hackerským útokům. V případě, že je dům napojen na internet, ho mohou hackeři napadnout z druhého konce světa. Shafid ur Rehman a Volker Gruhn pro řešení toho problému navrhli bezpečnou architekturu pro domy připojené k internetu. Té dosáhli přidáním sicher firewallu mezi centrální LAN rozbočovač a přípojku na internet. Tento firewall chrání systém inteligentního domu před internetovými hrozbami, jako jsou viry a hackerské útoky [5].

### Rozvoj inteligentních technologií ve zdravotnictví

IoT aplikace mají velké možnosti využití i v systémech zdravotní péče. Zde mohou sloužit jako podpora pro seniory, oběti chronických onemocnění a osoby, které vyžadují neustálý dohled. Touto problematikou se zabývá JOSHITTA, R. S. M. a L. AROCKIAM se svým týmem. Ve svém článku představují nový postup pro ověřování zdravotnických prostředků založený na speciálně navrženém algoritmu. Výsledkem je systém pro ověřování IoT zařízení, jejich zabezpečení a následné využití v systémech zdravotní péče [6]. Pro přímou podporu a kontrolu zdravotního stavu uživatelů v reálném čase slouží systém popsaný v práci autorů Bujnowska-Fedak, M. M. a U. Grata-Borkowska. Navrhují systém SH využívající Telecare, který slouží pro podporu osob se zdravotními potížemi. Tento systém je především zaměřen na starší lidi, kteří trpí chronickým onemocněním a nejsou schopni se o sebe samostatně starat. Systém sleduje v reálném čase zdravotní stav uživatele, který vyhodnocuje, a v případě zdravotních potíží je schopen zavolat pomoc. Také pomocí jednoduchého a intuitivního ovládání usnadňuje uživateli péči o sebe sama. Tím dává pocit jistoty a bezpečí a umožňuje těmto lidem žít v prostředí dle jejich výběru [7].

**Ekologie, úspora energií**

Inteligentní domácnosti by neměly sloužit pouze pro zvýšení pohodlí uživatelů. Také by měly zvýšit úsporu energií a vést k energetické nezávislosti domů. Metodu pro úsporu elektrické energie popisuje ve svém článku ALI, N., A. K. ALBANNA, M. ABU ARQOUB a G. ISSA, kteří se svým týmem představují systém využívající chytrých zařízení připojených na IoT využívajícího AWS (Amazon Web Services). Jedná se o finančně dostupný inteligentní systém snižující spotřebu elektrické energie, který zároveň automatizuje a zabezpečuje domácnost. Jejich návrh byl již úspěšně testován v laboratořích na Fakultě informačních technologií na University of Petra v Jordánsku [8]. Podporou životného prostředí se ve své práci zabývají BIN SHAHIN, F., P. TAWHEED, M. F. HAQUE a M. R. HASAN, kteří se svým týmem vyvíjí energeticky nezávislý systém domácí automatizace. Celý systém je napájen ze solárních kolektorů. Propojení mezi domem a uživatelem je realizováno přes webový server. Tento navrhovaný inteligentní systém je ekologicky šetrný, šetří energie, automatizuje domácnost a nabízí vzdálené monitorování a ovládání domácnosti [9]. Problémem u bezdrátových systémů bývá rušení způsobení silovým vedením, nebo rušení souběhem bezdrátových sítí. KHAN, M., B. N. SILVA a K. J. HAN ve svém článku použijí síť ZigBee pro řízení inteligentních domů. Návrh systému má tři části: 1) inteligentní řídící systém kontrolující rušení způsobené souběhem bezdrátových sítí; 2) inteligentní systém řízení spotřeby energie domácích spotřebičů; 3) inteligentní řídící systém, který efektivně řídí provoz elektronických zařízení. Dle počítačových simulací se ukazuje, že navrhovaný SH je méně ovlivňován rušením a jeho použití účinně snižuje spotřebu energie [10].

**Zabezpečení budov**

S rozvojem techniky se objevují nové technologie pro zabezpečení budov. Biotelemetrické údaje jsou přesným a spolehlivým nástrojem pro ověření totožnosti osob. Těchto údajů využívá ve svém návrhu zabezpečovacího systému ASLAN, E. S., O. F. OZDEMIR, A. HACIOGLU a G. INCE. Společně se svým týmem představují ve své práci přístupový systém založený na rozpoznávání tváří. Pro implementaci těchto funkcí byly použity mikrokontroléry, snímače pohybu a infračervené kamerové systémy. Výsledkem je systém zvyšující zabezpečení přístupu do budov, který je odolný vůči podvodným vniknutím do budovy více než přístupové systémy, které současně používají [10]. Stejný biometrický údaj použili ve svém návrhu i ALIM, M. A., M. M. BAIG, S. MEHBOOB a I. NASEEM. Společně navrhli elektronický zabezpečovací systém, který pro rozpoznávání tváří využívá metody lokálních binárních vzorů (LBP) pro charakterizaci tváře v texturovaném formátu. Navrhovaný systém má dvě úrovně zabezpečení, ověření ID uživatele a následné rozpoznání obličeje. Systém má výborné výsledky při rozpoznávání tváří a oproti ostatním biometrickým údajům má menší rušení. Výsledkem je spolehlivý přístupový zabezpečovací systém se dvěma úrovněmi kontroly [12]. CHEGGOU, R., E. H. KHOUMERI a K. FERHAH se ve své práci zabývá dvěma aspekty inteligentních domácností: zabezpečení domácnosti a domácí automatizace. Pro návrh inteligentních a zabezpečovacích systémů je použito vývojové prostředí Raspberry PI propojené s IoT. Tyto systémy se také dají použít pro pomoc a podporu osob žijících v těchto prostorách. Výsledkem této práce je inteligentní systém domácí automatizace, který je ovládaný přes internet a zároveň slouží jako zabezpečovací systém [13]. BODYANSKIY, Y., O. VYNOKUROVA, G. SETLAK a D. PELESHKO se svým týmem navrhli zabezpečovací systém využívající multifunkční adaptivní neurofuzzy systém, který umožňuje zpracování nestacionární informace. Tento navrhovaný systém lze použít především v průmyslových aplikacích a SH k úspoře spotřeby energie, řízení elektronických spotřebičů včetně zabezpečovacího systému [14]. LEE, C. T., T. C. SHEN a W. D. LEE vyvinuli nový elektronický zámek. Zámek je

schopen kódovat a dekódovat opticky modulované signály. Jako kodéry jsou použity komponenty emitující světlo (např. LED smartphonu). Fotorezistory s mikrokontroléry jsou použity jako dekodéry. Je vysoce odolný vůči různým světelným podmínkám prostředí. V testech se ukázala spolehlivost tohoto systému vyšší než 65 % [15]. KUSTIJA, J., K. S. N. ADILLAWATI a D. FAUZIAH představili systém SH, který je vytvořen na vývojové platformě Raspberry Pi. Jako interface slouží mobilní aplikace. Jako komunikační médium WiFi dongle. Systém je dále vybaven bezpečnostním systémem, který využívá webové kamery a PIR čidla. Pro komunikaci s uživatelem je použit GSM modul. Výsledky testů ukazují, že systém je schopný šetřit elektrickou energii, přispívá zabezpečení domu a je snadno ovladatelný [16]. Novým prvkem pro zjednodušení ovládání PZTS a SH je bezdrátová technologie Bluetooth Smart, kterou vyvinuli LODHA, R., S. GUPTA, H. JAIN a H. NARULA. Jedná se o automatickou bezdrátovou identifikaci zařízení s bluetooth. Ta je především zaměřena na inovativní aplikace ve zdravotnictví, školství a zabezpečení domácností [17]. Pro uzamykání dveří lze využít polyfonní tón vydávaný smartphonem. Tento způsob ve své práci navrhují RANGKUTI, H. A. a J. W. SIMATUPANG se svým týmem. K přijímání signálu slouží čidlo a program pracující na mikrokontorléru v Adrduinu. Pro otevírání dveří jsou použity solenoidy v zámcích dveří. Tento systém má však doposud řadu nevýhod. Především má nízkou úroveň zabezpečení, krátký rozsah citlivosti a omezený počet možných hesel [18].

**Zabezpečení stavebních materiálů**

Zabezpečení se nemusí nutně týkat pouze vnitřních a venkovních prostor budov, ale také stavby samotné. Zabezpečení, identifikace fyzických objektů se stává velmi důležitým aspektem nutným pro realizaci rozsáhlých zabezpečovacích systémů. Předpokládá se, že identifikace stavebních konstrukcí a materiálů by získala praktické využití v blízké budoucnosti při realizaci inteligentních domů či měst. Touto problematikou se zabývá ALDROUBI, S. a W. ADI. Cílem jejich práce je prozkoumat možnosti využití bezpečnostní identifikace fyzických stavebních prvků v reálných aplikacích [19].

**Inovace ve SH**

DEBABHUTI, N., S. DAS, S. DUTTA, A. SARKAR a jejich tým vytvořili inteligentní komunikaci, která pro svou činnost využívá jednoduchý mikrokontrolér. Ten vytváří bezdrátové spojení mezi uživatelem a spotřebiči, napojenými na inteligentní systém budovy. Spotřebiče jsou řízeny přijímáním SMS zpráv odesílaných uživatelem. Systém je finančně nenáročný, uživatelsky přívětivý a má široké pole využití [20].

# I. Teoretická část

## 3 Rozbor komponent PZTS

Každý PZTS systém se skládá ze základních komponentů, které jsou nezbytné pro jeho funkčnost. Jako základní prvek by se dala považovat zabezpečovací ústředna. Ta zpracovává informace z celého systému a vyhodnocuje je, avšak samotná ústředna bez detektorů, která by hlídala dění v zabezpečeném prostoru, by ke střežení nestačila. Je nutné zabezpečovací systém ovládat prostřednictvím nějakého HMI. Tuto funkci zastává klávesnice, která slouží k ovládání zabezpečovacího systému.

### 3.1.1 Zabezpečovací ústředny

Zabezpečovací ústředny jsou centrálním bodem PZTS. Vyhodnocují stav detektorů zabezpečeného systému, obsahují paměť pro historii událostí a nahráný firmware.

Technická specifikace ústředen použitých v této práci je k nahlédnutí v Příloze 1.


*Obr. 1 Deska zabezpečovací ústředny DIGIPLEX EVO192 výrobce PARADOX [29]*

Rozdělení ústředen podle typu vyhodnocování poplachu:

- Smyčkové – Detektory se zapojují na zónové svorky ústředny. Zapojený detektor tvoří proudovou smyčku. Každá zóna má vlastní vyhodnocovací obvod, který měří proud protékající touto smyčkou. Tento proud je definovaný a má určitou toleranci.
- S přímou adresací čidel – Komunikace mezi ústřednou a detektory probíhá po datové sběrnici. Každý detektor je vybaven vlastním komunikačním modulem. V takovémto systému je možné paralelně napojit více detektorů, čímž se zjednodušuje realizace celé instalace a dochází k úspoře vodičů.
- Bezdrátové ústředny – detektory jsou k ústředně připojeny radiofrekvenčním signálem. Každý detektor musí mít vlastní napájení, nejčastěji z akumulátoru.
- Smíšené – Jedná se o ústředny, které kombinují výše popsané typy.

Zabezpečovací ústředny se instalují do boxu, ve kterém je modul zabezpečovací ústředny chráněn proti napadení. Tento box také obsahuje napájecí transformátor pro ústřednu a záložní akumulátor pro případ výpadku proudu.

### 3.1.2 Klávesnice

Souží jako HMI zabezpečovacího systému. Na jejím display se zobrazuje stav jednotlivých podsystémů, narušení zón a poruchy. Zapojují se na sběrnici zabezpečovací ústředny.

Jejím prostřednictvím lze zapnout nebo vypnout zastřežení systému. Také lze jejím prostřednictvím vytvářet uživatelské kódy a provádět základní nastavení systému.

Většina klávesnic obsahuje display, a to LCD nebo LED. Dále v ní může být integrovaná čtečka karet.


*Obr. 2 Klávesnice K641+ výrobce PARADOX [30]*

### 3.1.3 Detektory PTZS

Detektor je zařízení, které monitoruje stav hlídaného prostředí. Pokud jsou splněna předem stanovená kritéria, vyhlásí narušení, které pak vyhodnotí ústředna.

Dle připojení k zabezpečovací ústředně se dělí na:

- Drátové – Jeden detektor je vždy připojen právě na jeden zónový vstup ústředny (v případě ATZ jsou dva).
- Sběrnicové – Detektory se připojují paralelně na sběrnici ústředny.
- Bezdrátové – Detektory jsou s ústřednou spojeny radiofrekvenčním signálem.

V následujícím textu jsou popsány základní detektory používané v PZTS, včetně popisu principu jejich funkce. Technická specifikace detektorů, použitých v této práci je k nahlédnutí v Příloha 1.

**Detektory pohybu**

**PIR** (pasive infrared)

Pasivní detektory snímající infračervené záření okolí.

Infrapasivní snímače pracují na principu pyroelektrického jevu. Při tomto jevu dochází k deformaci pyroelektrického materiálu při změně teploty (změně vlnové délky infračerveného záření). Každý objekt

s teplotou nad 0 °K vyzařuje teplo ve formě infračerveného záření. Vlnová délka infračerveného zářené je závislá na teplotě objektu, pro každou teplotu je přesně definována vlnová délka. Na povrch pyroelektrického materiálu je optickou soustavou promítán obraz okolí. Když v okolí dojde k tepelné změně, např. projde člověk, je materiál změnou vlnové délky infračerveného záření v části povrchu deformován a je možné detekovat indukovaný náboj na jeho povrchu.

Dle způsobu zpracování signálu se na digitální a analogové.

*Obr. 3 Vnitřní PID detektor DG75 výrobce PARADOX*

**MW** (micro wawe)

Aktivní detektor, který pro svou činnost vysílá mikrovlnné záření do okolí. Je založen na Dopplerově jevu. Obsahuje vysílač a přijímač mikrovlnného signálu (přibližně 10GHz). Při odrazu signálu od pohybujícího se předmětu se změní jeho vlnová délka. Tím dojde k tomu, že přijímačem je přijata jiná vlnová délka, než která byla přijata, tím je vyvolán poplach.

Nevýhodou těchto detektorů je časté vyvolání falešných poplachů. Vysílaný mikrovlnný signál je schopný proniknout sádrokartonem, dřevem nebo sklem, což může vést k detekci pohybu mimo střeženou oblast. Kvůli této vlastnosti se také mohou rušit vzájemně dva detektory. [21]

**Spojení PIR a MW**

U detektory s kombinací dvou výše popsaných principů je možnost falešných poplachů velmi malá. Poplach je vyhlášen pouze ve chvíli, kdy je pohyb zaznamenám oběma detektory.

*Obr. 4 PIR + MW + AM detektor pohybu NV75MW [32]*

- **Antimasking**
  Neboli ochrana proti zastínění je doplňková funkce pohybových detektorů. Slouží k ochraně detektoru proti jeho vyřazení zakrytím nebo zastříkáním ve chvíli, kdy není systém zastřežen. Tato ochrana je nejčastěji realizována vyzařováním infračerveného záření infradiodou a jeho následného snímání. V případě zakrytí detektoru nějakým předmětem dojde k odrazu tohoto záření a jeho detekci infračerveným sensorem. Doba, po kterou musí být detektor zakryt, aby došlo k poplachu, je různá. Nejčastěji však bývá 30 s. [22]

**Magnetické kontakty**

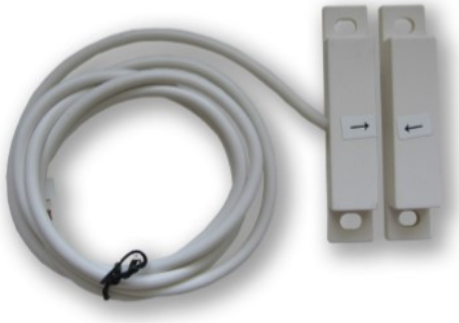
Magnetické kontakty se využívají pro střežení oken a dveří. Jedná se o pasivní detektory, nepotřebují žádné napájení. Část kontaktu, která obsahuje kabeláž, se instaluje na rám oken či dveří. Část bez kabeláže se instaluje na pohyblivou část okna či dveří.

Část kontaktu s kabeláží obsahuje jazýčkové relé. Ve druhé části je magnet. V normálním stavu je kontakt rozepnutý. Při přiblížení obou částí k sobě dojde k sepnutí jazýčkového relé vlivem magnetického pole magnetu. [27]

Jsou to prvky plášťové ochrany.

Z hlediska provedení se dělí na:

- Dvouvodičové – Obsahují pouze zatavené jazýčkové relé (NC kontakt).
- Čtyřvodičové – Kromě zataveného relé obsahují tamper. Ten je tvořen uzavřenou smyčkou, která prochází celám tělem kontaktu. Tím jsou vodiče kontaktu chráněny proti přerušení v případě, že je kontakt rozepnutý.
- Polarizované – Obsahují dvě zatavené jazýčková relé. Kontakt je chráněn proti pokusu o vyblokování magnetu kontaktu jiným magnetem. Také obsahuje tamper.



*Obr. 5 Polarizované magnetické kontakty 3G-SM-60 výrobce PARADOX [33]*

**Požární a kouřové detektory**

Tyto detektory slouží k detekci požáru. Pro svou instalaci mají dány parametry, jako je maximální výška stropu, maximální vzdálenost od zdi, maximální vzdálenost mezi detektory a maximální detekční plochu.

Pro svou činnost využívají několik způsobů [28]:

- **Teplotní detekce**
  Požár je detekován v případě, že dojde k překročení určité teploty. Měření teploty probíhá pomocí termistoru. Termistor je pasivní elektronická součástka, která vlivem změny teploty mění svůj odpor. Detektor tedy neustále měří odpor termistoru a tím vyhodnocuje teplotu v místnosti.
- **Termodiferenciální detekce**
  Je sledována křivka nárůstu teploty. Teplota je měřena termistorem. Křivky nárůstu teploty jsou definovány v normě EN 54 - 5.
- **Opticko-kouřová detekce**
  Na rozdíl od teplotních detektorů dokáže poznat požár již v počáteční stádiu. Pracuje na principu vniknutí kouře do měřící komory. Měřící komora detektoru je chráněna mřížkou proti nečistotám a hmyzu. V ní se nachází IR dioda, která prosvěcuje komoru. Při vniknutí kouře do měřící komory je část IR záření odražena částicemi prachu. Množství světla se vyhodnocuje pomocí fotoreakčního aktivního prvku.

  Měřící komora pracuje na principu Tyndallova fotoelektrického jevu. Při tomto jevu dochází k rozptylu světla při průchodu prostředím v mikroskopickými částicemi. V měřící komoře se nachází zářič a snímač infračerveného záření. Tyto dva prvky však nejsou umístěny naproti sobě, ale jsou vůči sobě posunuty. V normálním stavu tedy infračervené záření nedopadá na snímač. Pokud do měřící komory vnikne kouř, je infračervené záření rozptýleno, to začne dopadat na snímač a je inicializován požár.

  Jejich návrhem e zabývá norma ČSN EN 54-7.

  Jeden detektor v sobě může obsahovat více čidel a tím mít více způsobů detekce požáru.

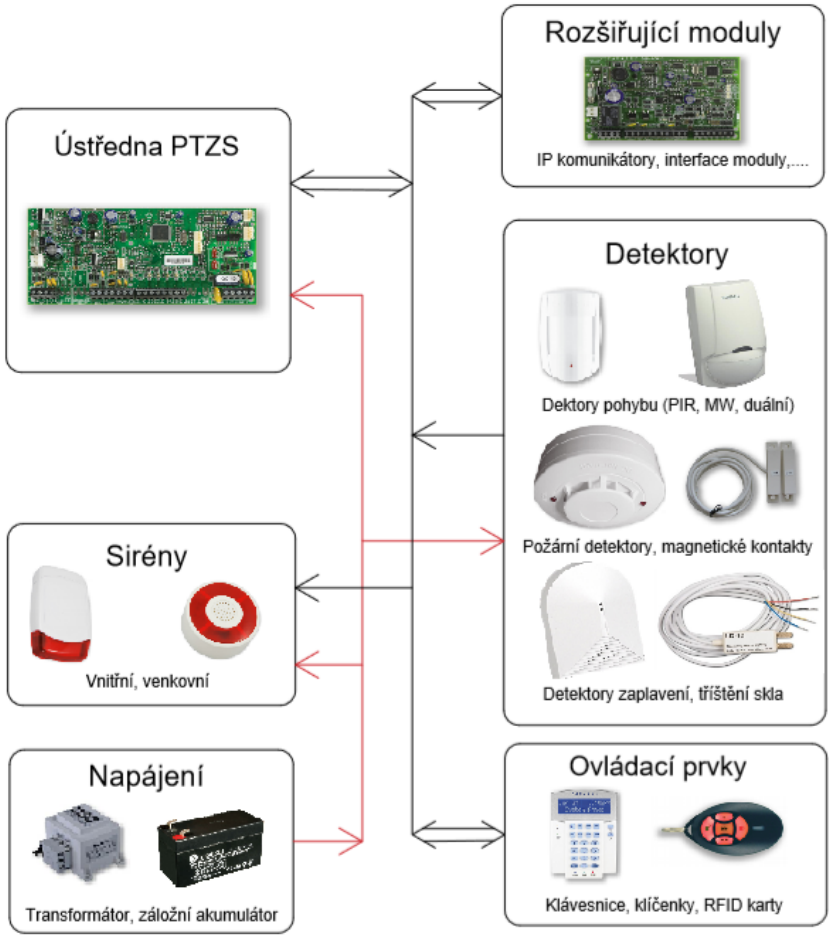

*Obr. 6 Požární detektor FDR-26-S výrobce PARADOX [34]*

# 4 Zapojení PZTS

Zabezpečovací systémy firmy Paradox jsou centralizovaný systém. Centrálním bodem je zabezpečovací ústředna, ke které se připojují detektory, klávesnice a ostatní komponenty.

Zabezpečovací ústředna je napájena ze síťového transformátoru. Jako záložní zdroj energie je k ní připojen akumulátor. Transformátor i akumulátor se napojují přímo na ústřednu. Detektory s drátovým nebo sběrnicovým připojením jsou napájeny z ústředny, vyjma detektorů pasivních, které žádné napájení pro svou činnost nepotřebují. Další rozšiřující moduly jsou ve spoustě případů napájeny z ústředny, konkrétně z její sběrnice. Moduly, které vyžadují vlastní napájecí zdroj, nesmí tento zdroj sdílet se zabezpečovací ústřednou. To znamená, že na transformátor, který napájí ústřednu, může být napojena pouze ústředna. Přídavné moduly musí mít vlastní síťový transformát.

Zapojení detektorů se provádí metalickými vodiči s pevným nebo žilovým jádrem a průměru 0,22 mm.




*Obr. 7 Blokové schéma zapojení PZTS*

## 4.1 Zapojení sběrnicových modulů

Rozšiřující moduly se připojují na sběrnici ústředny. Ústředny firmy Paradox využívají sériovou komunikaci. Zapojení sběrnice je realizováno čtyřmi vodiči. Dva jsou napájecí – GND a 12 V (černý a červený). Jedná se i napájecí výstup ústředny AUX. Další dva jsou datové vodiče (žlutý a zelený).

## 4.2 Zapojení detektorů

Základně lze rozdělit zapojení na zapojení s NO nebo s NC kontaktem detektoru. Avšak zapojení s NO kontaktem jsou spíše výjimečná a v praxi se v moc často nepoužívají. Ani já jsem je v této práci nepoužil, tudíž je zde nebudu zmiňovat.

### 4.2.1 Základní pojmy

Pro doplnění popisů zapojení, které se nachází v následující části textu, je potřeba popsat základní prvky a pojmy, které s těmito zapojeními souvisejí.

**Tamper**

Kontakt detektoru, který hlídá sejmutí krytu detektoru. Když je detektor zakrytovaný, je tamper kontakt sepnutý. Pokud by byl násilně jeho kryt odstraněn, nebo by došlo k jeho výraznému poškození je inicializován poplach. Tento kontakt se zapojuje sériově do smyčky s kontaktem detektoru.

**EOL rezistor**

Jedná se o rezistory, které jsou zapojen ve smyčce s čidle. Zapojují se do série s kontaktem detektoru. Obvykle se používají hodnota 1 KΩ. Jejich hlavní význam je ochrana zapojené smyčky proti bypassu. V literatuře a různých dokumentech se mohou nazývat zakončovací rezistory.

**Vyvažovací rezistory**

Zapojují se paralelně k výstupním kontaktům detektoru. Slouží k rozlišení stavu, kdy je spuštěn poplach inicializací detektoru nebo sabotáží. Jejich hodnota může být různá a při zapojení ATZ se jejich hodnota u každého z detektorů liší. Nejčastěji je využívají hodnoty 1 KΩ a 2,2 KΩ.

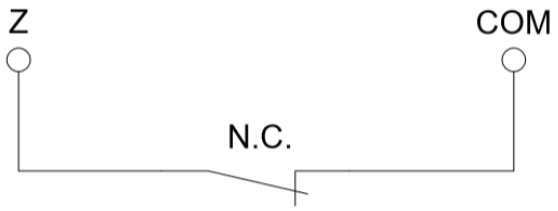
### 4.2.2 Zapojení detektorů s NC kontakty

Zapojení NC kontaktů detektorů k ústředně lze rozdělit do pěti základních zapojení:

- bez EOL a tamperu,
- se zapojením EOL rezistoru,
- se zapojením kontaktu tamper,
- se zapojeným EOL a tamperem,
- zapojení ATZ.

**Zapojení detektoru bez EOL a tamper kontaktu**

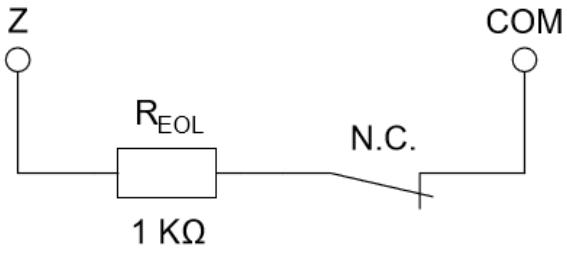
Jedná se o nejjednodušší zapojení. Hlídá se pouze rozepnutí NC kontaktu detektoru, nebo sabotáž vedení přestřižením vodičů vedoucím k detektoru z ústředny. Toto zapojení není nijak ošetřeno proti bypassu nebo odstranění krytu samotného detektoru. Je zde měřen proud tekoucí smyčkou, pokud dojde k jejímu rozpojení, je inicializován poplach. Není však nijak specifikováno, zda se jedná o poplach vyvolaný přestřižením vedení, nebo zda je poplach vyvolaný inicializací detektorem. Schéma zapojení je zobrazeno na Obr. 8.




*Obr. 8 Schématické zapojení NC kontaktu detektoru [35]*

**Se zapojením EOL rezistoru**

Toto zapojení detektoru je chráněno proti bypassu. Odpor smyčky je v klidovém stavu roven hodnotě OEL rezistoru. Pokud by byly vodiče k detektoru vyzkratovány (napadení bypassem), odpor smyčky by se změnil a byl by inicializován poplach. V tomto zapojení není zapojen tamper kontakt, tudíž detektor není chráněný proti odstranění krytu. Schéma zapojení je zobrazeno na Obr. 9.

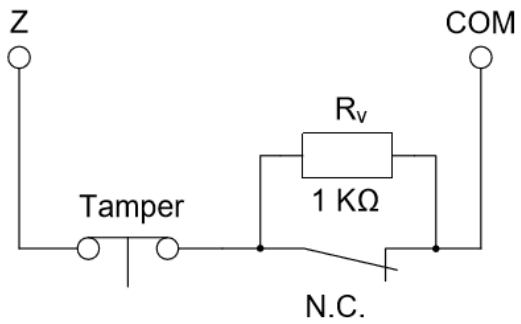



*Obr. 9 Schématické zapojení NC kontaktu a EOL rezistoru [35]*

**Se zapojením kontaktu tamper**

Zapojení chrání samotný detektor proti napadení odstraněním jeho krytu. Je hlídáno rozpojení kontaktu tamperu, který je v běžném stavu sepnutý. Toto zapojení není chráněno proti napadení bypassem.

Rozpínací NO kontakt a kontakt tamperu jsou zapojeny sériově. Paralelně ke kontaktu detektoru je zapojen rezistor. Je tu z toho důvodu, aby se rozlišil poplach inicializovaný detektorem a poplach vyvolaný sabotáží detektoru. Pokud by tedy došlo k odstranění krytu, kontakt tamperu se rozepne, přeruší se obvod a je vyvolán poplach sabotáží detektoru. Když dojde k rozpojení NC kontaktu, odpor měřené smyčky se zvýší z nulové hodnoty na hodnotu zapojeného rezistoru a tím je inicializován poplach detektoru. Schéma zapojení je zobrazeno na Obr. 10.

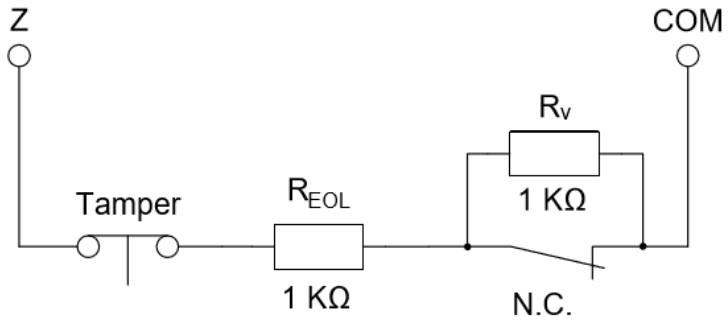



*Obr. 10 Schématické zapojení NC kontaktu a kontaktu tamper [35]*

**Zapojení s EOL a tamperem**

Jedná se o nejvíce zabezpečené zapojení, jelikož je zde chráněno odkrytování detektoru i napadení vedení bypassem. Také se mu říká trojité vyvážení.

Jak lze vidět na Obr. 11 NC kontakt, kontakt tamperu a EOL rezistor jsou zapojeny sériově. Paralelně k NC kontaktu je zapojen rezistor $R_v$, ten však nemá vliv na odpor smyčky v klidovém stavu. Odpor měřené smyčky je tedy v klidovém stavu roven hodnotě EOL rezistoru (na obrázku je to 1 KΩ). Pokud by došlo k napadení vedení vodičů mezi ústřednou a detektorem bypassem, odpor smyčky by se změnil a došlo by k poplachu vyvolaný sabotáží vedení. Kdyby byl odstraněn kryt detektoru, rozpojí se kontakt tamperu, a tím je rozpojena celá smyčka. Smyčkou přestane protékat proud a je vyvolán poplach sabotáží detektoru. Pokud by však došlo k rozpojení NC kontaktu, tak se odpor celé smyčky zvýší o hodnotu vyvažovacího odporu (na obrázku 1 KΩ) a tím je inicializován poplach vyvolaný detektorem.

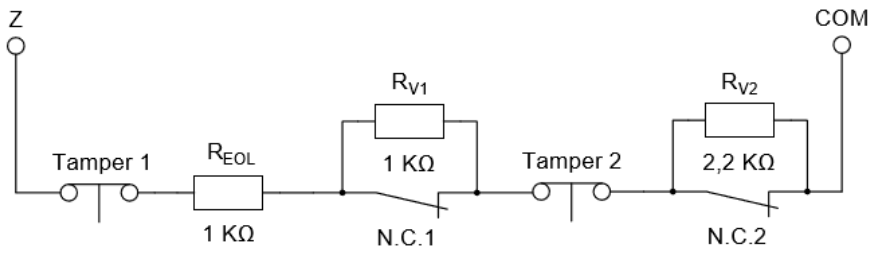



*Obr. 11 Schématické zapojení NC kontaktu detektoru s EOL rezistorem a tampererem [35]*

**Zapojení NC kontaktu detektoru a tamperu, s OEL a ATZ**

V tomto zapojení jsou na jeden vstup ústředny připojeny dva detektory. Tampery a NC kontakty obou detektorů jsou zapojeny sériově s EOL rezistorem, zobrazeno na **Chyba! Nenalezen zdroj odkazů. .** Ke každému NC kontaktu je paralelně připojen vyvažovací rezistor, každý má však jinou hodnotu. To kvůli tomu, aby se rozlišilo, jaký detektor spustil poplach.

V klidovém stavu je odpor celé smyčky roven hodnotě EOL rezistoru. Pokud by však došlo k rozpojení NC kontaktu jednoho z detektorů, je tento odpor zvýšen o hodnotu vyvažovacího rezistoru připojenému k danému detektoru.




*Obr. 12 Schématické zapojení AT [35]*

# 5 Popis technologie Smart Home KNX

Ve své práci pracuji s komponenty SH firmy Schneider elekctric, které spadají pod asociaci KNX.

Asociace KNX vznikla v roce 1990 a sdružuje výrobce komponent pro SH z celého světa. Její aktivitou je technický rozvoj a propagace standardu KNX. Cílem je standardizovat instalační systém sběrnic pro technologie SH. V dnešní době sdružuje okolo čtyř set firem.

Cílem technologií SH je zvýšit pohodlí a komfort osob, jejich bezpečnost a energetickou úsporu při provozu budovy. K tomu se využívá moderních technických řešení, konstrukce samotné budovy a systémů řízení provozu budovy. Umožňuje účelové využití i rekombinaci. Dokáže se přizpůsobit potřebám a rozmarům uživatele. Ovládání takového systému je uživatelsky přívětivé a intuitivní.

## 5.1 Instalační software KNX

Asociace KNX vyvinula vlastní software, kterým lze programovat moduly od různých výrobců, kteří vyrábí své komponenty pod standardem KNX. Software je určený pro plánování a návrh projektu KNX systému a jeho uvedení do provozu.

## 5.2 Média pro přenos informací

Standardy KNX nabízejí přenos informací celkem pěti různými způsoby:

- TP1,
- Powerline PL110,
- Radiofrekvenční přenos RF,
- KNX IP.

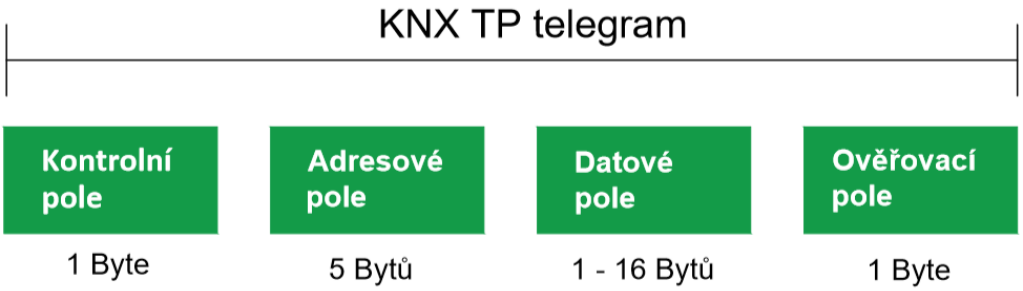
**TP1 (Twist Pare)**

Instalace KNX SH, kterou jsem použil v praktické části této práce, je zapojena právě kroucenou dvoulinkou.

Pro sběrnicové vedení se používají vodiče YCYM 2x2x0,8 nebo JYSTY 2x2x0,8. Sběrnicové vedení je možné klást souběžně se silovým vedením 230 V. Pro toto použití musí však být použit certifikovaný kabel KNX, který je testován do 4 kV. To je velkou výhodou při realizaci i návrhu instalace SH.

Pro přenos informace jsou využívány tvz. telegramy, které obsahují informace pro přenos v podobě bitů. Jeden telegram může obsahovat maximálně 23 bitů.

Napájecí moduly poskytují napětí 29 V. Avšak napětí, při kterém jsou přístroje připojené ke sběrnici schopny pracovat je od 21 V do 30 V DC. Tako rezerva napětí je z důvodů úbytků napětí na přechodových odporech a úbytku na samotném vedení. Při příliš dlouhém vedení také dochází ke zpoždění telegramů. Z těchto důvodů je délka vedení mezi napájecím zdrojem a zařízením omezena na maximální délku 350 m.

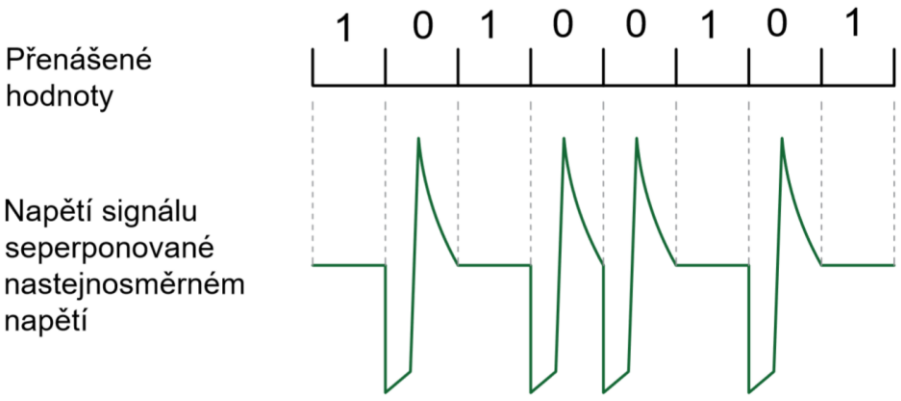



*Obr. 13 Struktura telegramu KNX TP [24]*

Obsah telegramu KNX TP:

- Kontrolní pole – jeho velikost je 1 byte. Obsahuje informaci o prioritě telegramu. Rozhoduje, zda bude odesílání telegramu opakováno v případě neúspěšného přenosu telegramu.
- Adresované pole – obsahuje informaci o individuální adrese odesílatele. Také osahuje adresu příjemce. Ta může být buď individuální adresa nebo skupinová adresa. Jeho velikost je 5 bytů.
- Datové pole – Obsahuje samotnou zprávu. Jedná se užitečnou zátěž telegramu. Jeho velikost je jeden a šestnáct bytů.
- Ověřovací pole – používá se pro ověření toho, že telegram byl úspěšně přijat příjemcem. Jeho velikost je 1 byt.

Logické úrovně jsou zde prezentovány tak, že logická jedna je rovna nulové změně napětí na vedení. Logická nula je rovna krátkému poklesu napětí o 5 V. Napájecí zdroje jsou vybaveny tlumivkou, která je nezbytná pro funkci komunikace. Je zde kvůli přepólování napětí. Doba přepólování je 104 $\mu$s, což je rovno době odeslání jednoho symbolu. Ukázka přenosu informace po KNX TP je na Obr. 14.

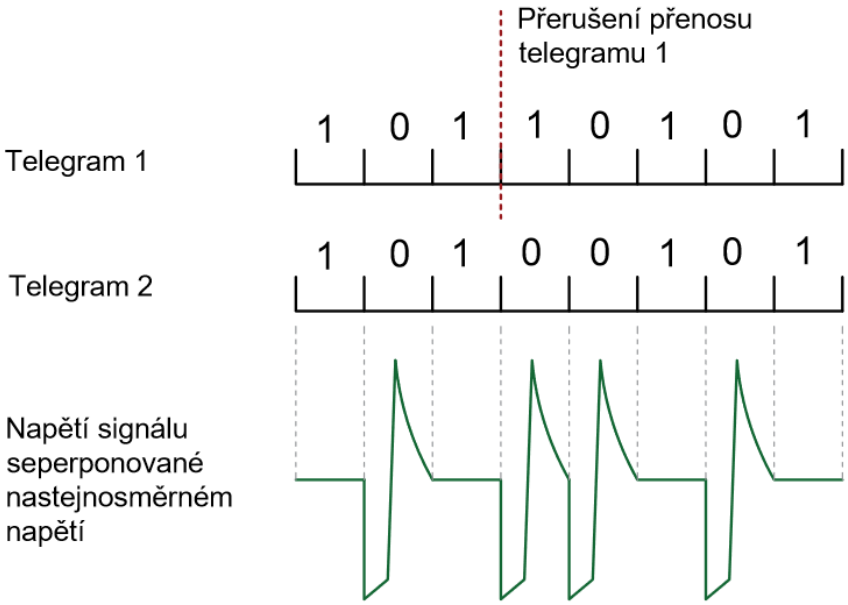



*Obr. 14 Grafické znázornění signálu v KNX TP [24]*

Přístup na s

běrnici KNX TP je náhodný a vysílání jednoho přístroje podmíněno tím, že ostatní přístroje připojené na sběrnici mlčí. K ošetření proti kolizím při vysílání na sběrnici je použit protokol CSMA/CA

(vícenásobný přenos se zabráněním kolizí). Vysílání logické hodnoty nula má přednost před vysíláním logické úrovně jedna. Pokud dojde k tomu, že jeden přístroj bude vysílat logickou hodnotu 0 a v té chvíli začne vysílat druhý přístroj logickou hodnotu 1, je druhý přístroj nucen se na několik period odmlčet a vyčkat, až bude sběrnice volná. Případ, kdy dochází ke kolizi je vyobrazen na Obr. 15.



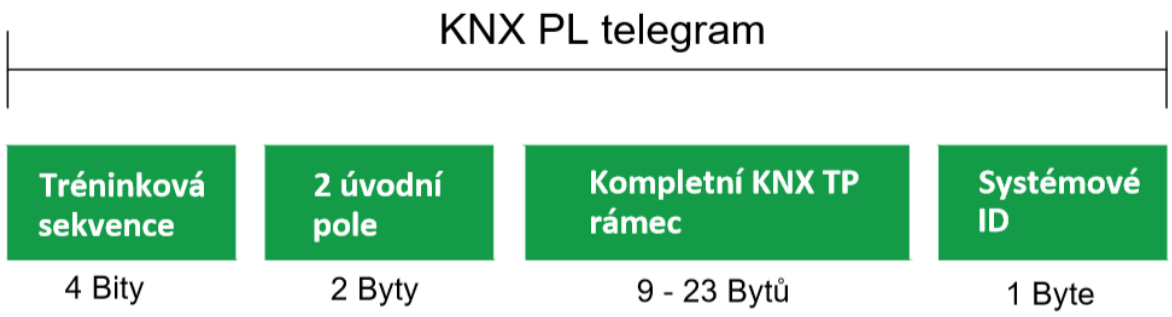

*Obr. 15 Ukázka kolize v KNX TP [24]*

### 5.2.1 Powerline-PL110

Tento typ datového přenosu nebude v praktické části této práci použit, tudíž zde bude zmíněn spíše okrajově.

Přenos datových telegramů se provádí pomocí již existující elektroinstalace (230 V). Využívá se fázový a nulový vodič, v případě třífázového vedení je použit jeden z fázových vodičů a nulový vodič. Mezifázové spojky jsou použity pro přenos dat po všech třech fázích, kdežto pásmové zádrže brání přenosu datových signálů do vnější silové sítě. Přenosová rychlost dat je 1200 bit/s. Logické úrovně, nuly a jedničky, jsou přenášeny širokým kmitočtový klíčováním. Pro logickou nulu odpovídá frekvence odeslaná vysílačem 105,6 kHz, pro logickou jedničku je to 115,2 kHz. Název PL110 je odvozen od středního kmitočtu, který je 110kHz. Signály jsou superponovány na síťové napětí a díky technice komparátorů a inteligentní korekční proceduře lze přijímané signály vyhodnotit i při přítomnosti rušení. Pro dosažení správného vyhodnocování přijímaných a vysílaných digitálních dat neustále upravuje vysílací výkon a citlivost sběrnicových přístrojů v závislosti na momentálních podmínkách v síti.

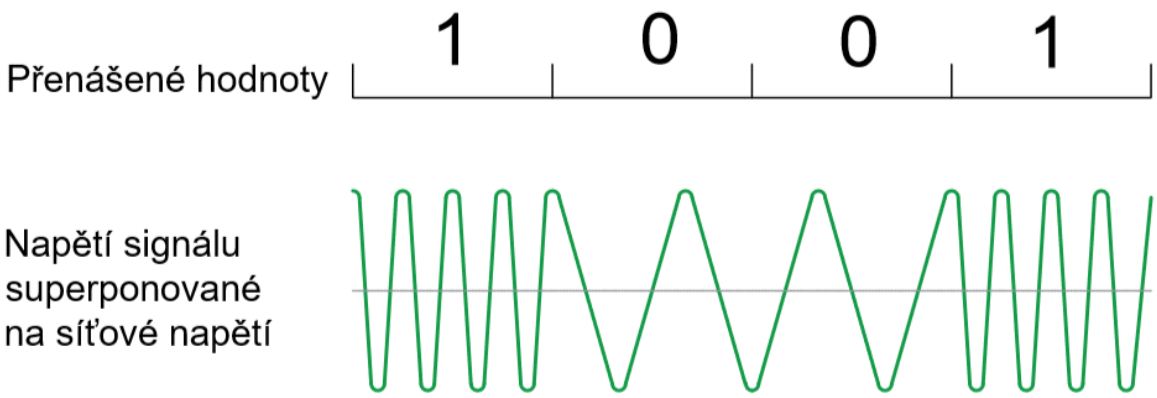
Ochrana proti kolizím je zde řešena tím způsobem, že všechna zařízení jsou v režimu přijímání. Ve chvíli, kdy chce jeden z přístrojů vysílat a nezaznamená na vedení sekvenci úvodních bitů, je mu povoleno odeslat TP telegram [24]




*Obr. 16 Struktura telegramu v KNX LP110 [24]*

Telegramy používané v KNX LP jsou v podstatě rozšířenými telegramy KNX TP a také se sestávají ze čtyř částí:

- Tréninková sekvence – synchronizuje a nastavuje vysílací a přijímací úrovně.
- Úrovní pole – řídí přístup na sběrnici a používá se při ochraně proti kolizím. Také udává zahájení přenosu.
- Třetí pole obsahuje kompletní telegram KNX TP.
- Systémové ID – používá se pro odlišení signálů dalších systémů KNX PL. Obsahuje totiž systémové ID, takže pouze systémy používající stejné systémové ID mohou vzájemně komunikovat.




*Obr. 17 Zobrazení signálu v KNX PL110 [24]*

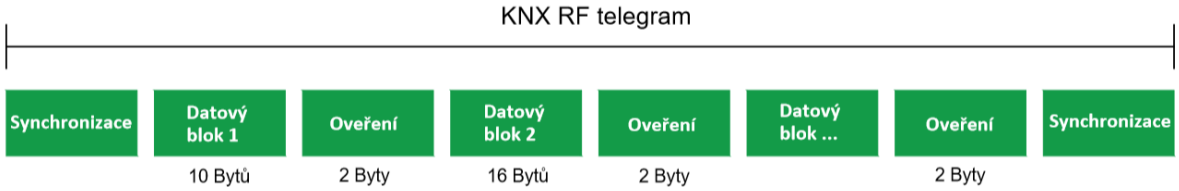
### 5.2.2 Radiofrekvenční přenos RF

Tento typ datového přenosu nebude v praktické části této práci použit, tudíž zde bude zmíněn spíše okrajově.

Napájení přístrojů se provádí připojením v síti 230 V, nebo jsou napájeny bateriemi. Přenos dat pracuje s modulací nosné vlny přenášené informace. V technologiích KNX RF se tato modulace provádí frekvenční modulací. V přístrojích, které modulovaný signál přijmou, dochází k demodulaci. Nosné kmitočty se dělí na dva druhy. KNX Ready a KNX Multi.

KNX Ready je nosný signál s kmitočtem 868,3 kHz, má pouze jeden komunikační kanál. Kvůli tomu je více náchylný na rušení od jiných spotřebičů.

KNX Ready obsahuje více kanálů. Kanály se dále dělí na rychlé a pomalé. Rychlé jsou určené pro uživatele a mají přenosovou rychlost 19,384 kb/s. Pomalé kanály jsou určeny pro přístroje, které nejsou stále v režimu příjmu. Mají poloviční přenosovou rychlost.




*Obr. 18 Struktura telegramu KNX RF [24]*

### 5.2.3 KNX IP

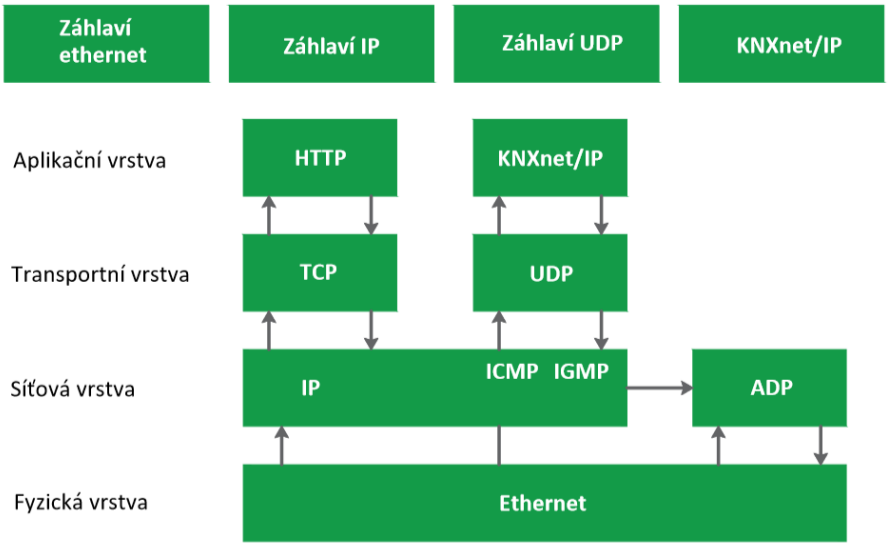
Tento typ datového přenosu nebude v praktické části této práci použit, tudíž zde bude zmíněn spíše okrajově.

Zde jsou používány dva způsoby komunikace po Ethernetu, tunnneling a routing. Oba dva způsoby používají protokol UDP. Tunneling se používá k dosažení sběrnice z místní sítě nebo internetu pro účely jako je programování KNX instalace. Routing se používá pro přenos telegramů po Ethernetové síti. Protokoly pro tyto dva způsoby se nazývají KNXnet/IP routing a KNXnet/IP tunneling.

Komunikace v IP KNX probíhá přes aplikační vrstvy, které generuje KNXnet/ IP telegram. Poté transportní vrstvy, síťové vrstvy a na závěr fyzickou vrstvu, tedy Ethernet. (viz. Obr. 19)

KNXnet/IP tunneling je potřebný ve chvíli, kdy je cílovou adresou individuální adresa. To jsou případy, kdy je programována fyzická adresa, nebo se nahrává aplikační software do přístroje KNX.

KNXnet/IP routing je používaný pro komunikace s více účastníky. Také se používá pro spojení s TP kabelem. Také se zde používají KNXnet/IP routery, které slouží jako liniová spojka na TP sběrnici. Telegramy jsou zde však odesílány na IP stranu, a to pouze v případě, že je skupinová adresa zapsána ve filtrační tabulce KNXnet/IP routeru.




*Obr. 19 OSI referenční model [24]*

## 5.3 Topologie KNX

Každé z přenosových médií má svou vlastní topologii. V praktické části je použito médium TP, tudíž se zde budu zabývat pouze topologií toho média.

### 5.3.1 Individuální adresa

Individuální adresa je jedinečné číslo, které má každý přístroj KNX systému. Je nutná pro identifikaci přístrojů a pro jeho programování. Přístroje, které mají na posledním místě číslo 0 jsou vždy liniové a oblastní spojky.

Toto číslo je složeno ze tří čísel oddělených tečkou:

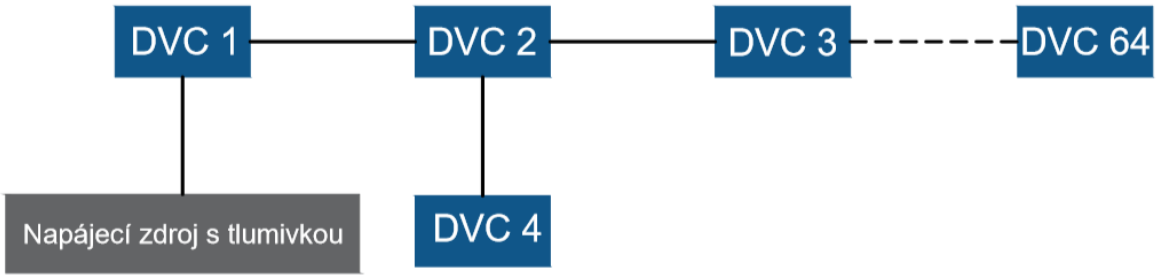
- První číslo udává číslo oblasti.
- Druhé číslo znamení číslo linie.
- Třetí číslo je pořadové číslo přístroje v linii.

### 5.3.2 Skupinová adresa

Jedná se o adresu, která zahrnuje více přístrojů.

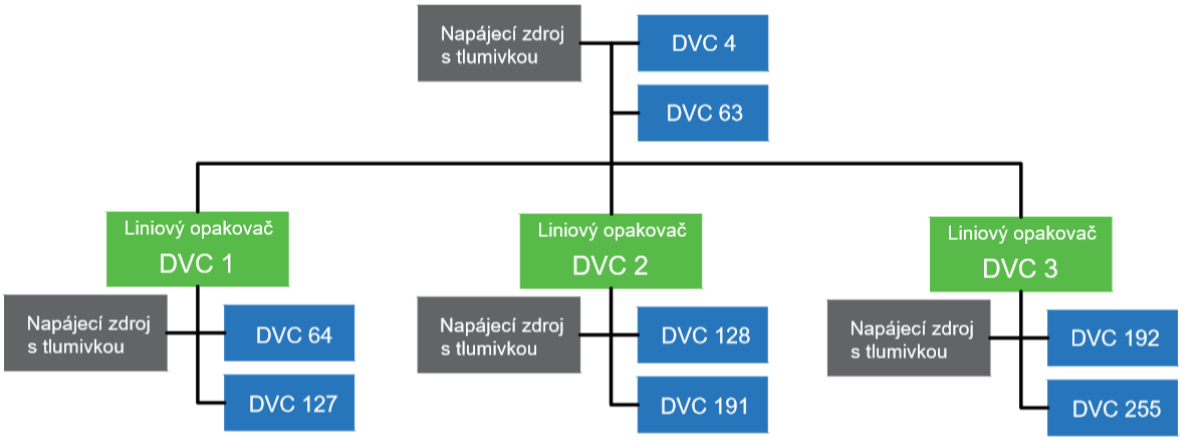
### 5.3.3 Linie

Linie je základní jednotkou topologie KNX TP. Lze na ní připojit až 64 přístrojů. Základním prvkem linie je napájecí zdroj s tlumivkou, který zajišťuje napájení přístrojů na sběrnici. Kabely krouceného páru můžou být libovolně napojovány. To umožňuje velkou flexibilitu celého návrhu instalace. [24]




*Obr. 20 Linie KNX TP [24]*

Velikost linie se dá rozšířit pomocí liniových opakovačů, a o to až o dalších 64 přístrojů. Vzniklé linie se nazývají liniovými segmenty. Každý liniový segment obsahuje vlastní liniový opakovač a zdroj s tlumivkou, přičemž se liniový opakovač počítá jako přístroj na sběrnici. V jedné linii nelze použít více než tři paralelně zapojené liniové opakovače. Tím je dán maximální počet přístrojů na 255.

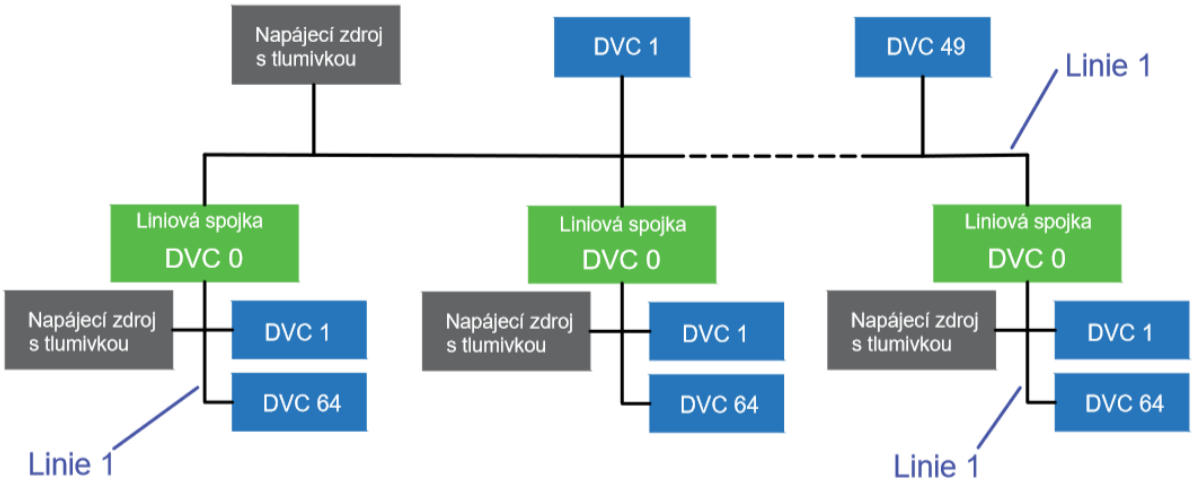



*Obr. 21 Maximální velikost linie KNX TP [24]*

### 5.3.4 Oblast

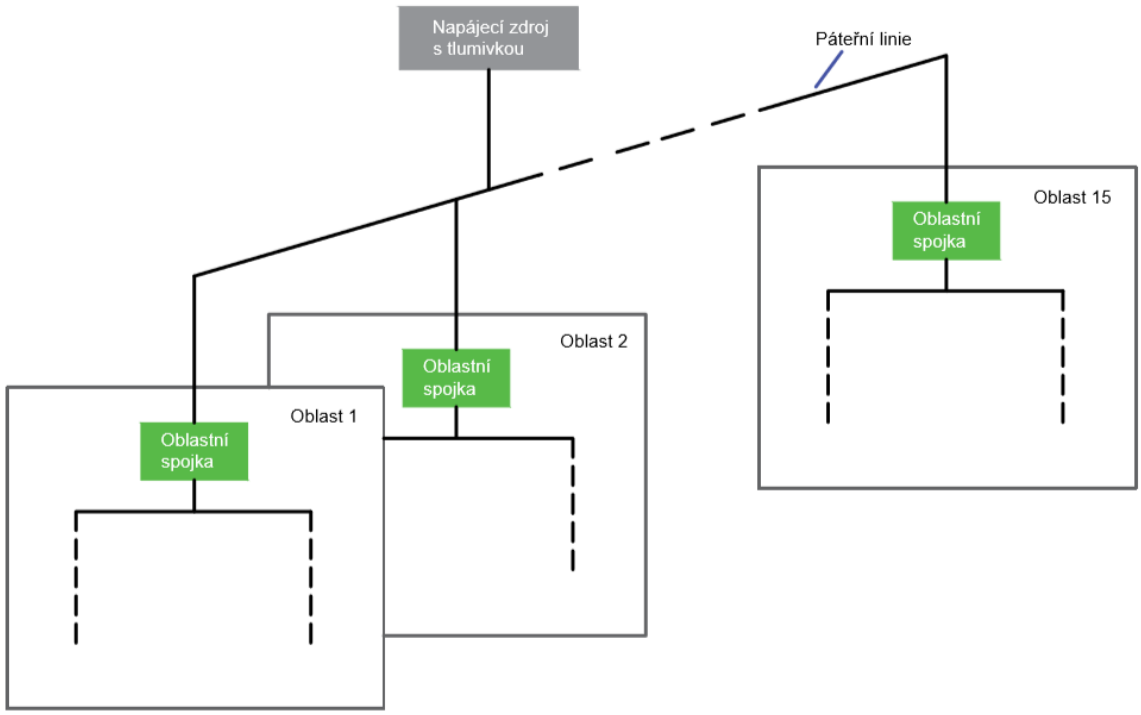
Spojením více linií pomocí liniových spojek vytváří oblast. Maximálně lze spojit 15 minií na tzv. hlavní linii. Oblasti se vytvářejí při potřebě topologického rozdělení objektu, nebo z důvodu požadavku využití více než 255 přístrojů v instalaci. [24]

Hlavní linie se dá považovat za samostatný liniový segment. Jelikož 15 míst na tomto segmentu zabírají liniové spojky, je možné na hlavní linii připojit 49 přístrojů. Topologie oblasti KNX je na obrázku Obr. 22.




*Obr. 22 Grafické znázornění oblasti KNX TP [24]*

Pomocí páteřní linie je možné propojit více oblastí a tím vytvořit ještě větší instalaci. Jednotlivé linie se připojují na páteřní linii pomocí oblastních spojek. Na páteřní oblasti může být připojeno maximálně 15 oblastí. Také je možné na ní připojit i přístroje.




*Obr. 23Maximální velikost instalace KNX TP [24]*

# 6 Legislativa PTZS

## 6.1 ČSN CLC/TS 50398 (334597)

Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace. Jedná se o českou verzi technické specifikace CLC/TS 50131-7:2010, která byla schválena Evropským výborem pro normalizaci v elektronice (CELENEC). Norma rozlišuje poplachové systémy pro detekci vniknutí a poplachové systémy pro detekci přepadení a v některých částech o těchto systémech pojednává odděleně.

Členění normy je rozloženo do sedmi hlavních kapitol, ve kterých uvádí, jak by měly osoby odpovědné za danou konkrétní činnost postupovat. [26]

Hlavní kapitoly normy:

- návrh systému,
- příprava realizace,
- montáž,
- kontrola provedení montáže, funkční zkouška a přejímka,
- dokumentace a záznam o provozu systému,
- provoz PTZS,
- údržba a opravy PTZS.

## 6.2 ČSN EN 50131-1 ed.2(33 4591)

Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky. Česká technická norma převzatá z evropských norem. Norma specifikuje požadavky poplachového tísňového zabezpečovacího systémy (PTZS) v případě, že jsou instalovány odděleně. Dále určuje požadavky na poplachové bezpečnostní a tísňové systémy určené pro vnitřní použití ve vnitřních prostorách budov. Další částí normy jsou definice tříd prostředí a stupně zabezpečení, do kterých musí být komponenty PTZS členěny. To znamená, že jednotlivé komponenty PTZS se nesmějí navzájem ovlivňovat a musí být voleny dle stupně zabezpečení a odolnosti vůči vlivům prostředí. V poslední části norma popisuje funkční požadavky na provoz, detekci, nastavování, obnovení stavu z poplachového stavu či poruchy, testování a také definuje přístupové úrovně, které udávaní možnost přístupu uživatelům ke komponentům a ovládacím prvkům PTZS. [24]

### 6.2.1 Rozdělení stupňů zabezpečení

Stupeň bezpečnosti PTZS je dán jejím komponentem s nejnižším stupněm zabezpečení.

*Tab. 1 Tabulka stupňů zabezpečení PTZS dle normy ČSN EN 50131 – 1 ed.2 (33 4591) [24]*

| Stupeň zabezpečení | Název | Popis narušitele |
|---|---|---|
| 1 | Nízké riziko | Předpokládá se, že narušitelé mají malou znalost PTZS, mají omezený sortiment snadno dostupných nástrojů |
| 2 | Nízké až střední riziko | Předpokládá se, že narušitelé mají určité znalosti PTZS, mají k dispozici základní sortiment nástrojů a přenosných systémů |
| 3 | Střední až vysoké riziko | Předpokládá se, že narušitelé jsou obeznámeni s PTZS, mají úplný sortiment nástrojů a přenosných systémů |
| 4 | Vysoké riziko | Předpokládá se, že narušitelé jsou schopni zpracovat podrobný plán narušení, nebo loupeže a mají kom pletní sortiment zařízení včetně prostředků pro náhradu PTZS |

### 6.2.2 Třídy prostředí

Každému komponentu PTZS je přiřazena třída prostředí, která uvádí, ve kterých podmínkách je možné daný komponent naistalovat, aby byla zajištěna jeho správná činnost.

*Tab. 2 Tabulka rozdělení tříd prostředí PTZS [24]*

| Třída prostředí | Název prostředí | Popis prostředí | Rozsah teplot |
|---|---|---|---|
| I | vnitřní | vnitřní prostory při stálé teplotě | +5 až +40 °C |
| II | Vnitřní - všeobecné | vnitřní prostory při nestálé teplotě (např. chodby, haly, skladiště s nestálým vytápěním) | -10 až +40 °C |
| III | Venkovní - chráněné nebo extrémní vnitřní podmínky | vlivy vně budov, kde komponenty nejsou trvale vystaveny povětrnostním vlivům (např. přístřešky) | -25 až +50 °C |
| IV | Venkovní - všeobecné | vlivy vně budov, kde komponenty jsou plně vystaveny povětrnostním vlivům | -25 až +60 °C |

# 7 Legislativa KNX

V dnešní době je KNX celosvětový systém pro řízení domů a budov. Po vzniku asociace v roce 1997 zde byla snaha o specifikaci a jasné určení celého konceptu. Ta vycházela z mateřské sběrnice EIB a v roce 2003 byla, spolu se dvěma základními přenosovými médii TP (kroucený pár) a PL (silové vedení), uznána jako evropská norma EN 50090. Systém se dále rozšiřoval za hranice Evropy, a proto vznikla potřeba jej normalizovat ve světovém měřítku. V roce 2006 byl protokol KNX schválen jako celosvětová norma ISO/IEC 14543-3. Tím se stal jedinou celosvětově uznávanou normou pro systémovou techniku budov s decentralizovanou technologií.

**EN 50090**

V roce 2003 byl standard KNX schválen v CENELEM (European Committee of Electrotechnical Standardisation) jako součást této evropské normy, elektronické systémy pro budovy. **Chyba! Nenalezen zdroj odkazů.**

**EN 13221–1**

Součástí této normy jsou přenosová média a komunikační protokoly KNX **Chyba! Nenalezen zdroj odkazů.**

**EN 13321-2**

Normalizuje komunikaci přenosem po IP síti s využitím rozhraní KNXnet/IP **Chyba! Nenalezen zdroj odkazů.**

**ISO/IEC 14543-3**

Do této celosvětové normy byly veškeré normativní požadavky zahrnuty v roce 2007 **Chyba! Nenalezen zdroj odkazů.**

# II. Praktická část

# 8 Implementace PZTS v SH

Za poslední tři desetiletí působení firmy Paradox na trhu byly v domácnostech po celém světě provedeny desetitisíce instalací zabezpečovacích systémů právě od této firmy. Zatím co instalace SH technologií v domácnostech je trendem posledního desetiletí. A právě instalace SH v domácnostech, ve kterých je již instalován zabezpečovací systém, přivádí na otázku propojení těchto dvou systému. Zákazníci si žádají jednodušší ovládání PZTS, které by bylo prováděno ovládacími prvky společnými se SH. Také zavádění SH systému v novostavbách naráží na tuto otázku. Jelikož SH KNX není certifikovaný zabezpečovací systém, je pro ochranu domu nutná také instalace certifikovaného zabezpečovacího systému.

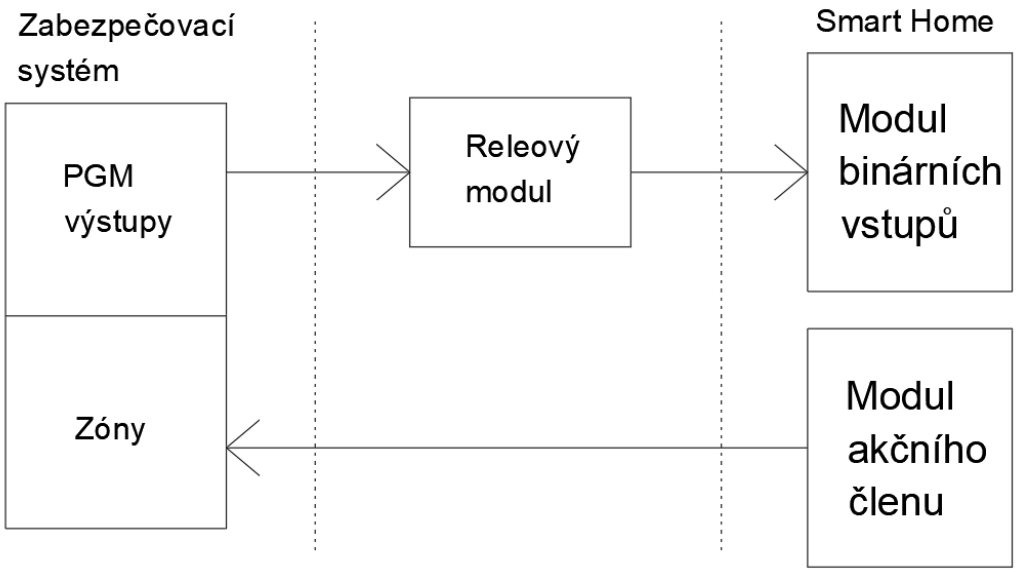
První možností pro implementaci PZTS v SH je propojení těchto dvou systémů jejich binárními vstupy a výstupy. Druhý způsob implementace je přes vzájemné spojení obou sběrnic. V této části práce se zabývám návrhem obou těchto způsobů a praktickou realizací propojení binárních vstupů.

## 8.1 Propojení PZTS a instalace SH KNX binárními vstupy

Pro vzájemné propojení PZTS a SH KNX je potřeba nalézt způsob, jak by každý z těchto systémů přijímal a vysílal binární informaci. Jako výstup binární informace lze využít jakýkoli prvek, který je možné provést sepnutí, jako reakci na určitou událost v systému. To v případě SH KNX není problém najít. Pro tuto aplikaci se hodí každý akční člen určený ke spínání. V případě PZTS je to o něco komplikovanější. Avšak pro tuto činnost lze využít PGM výstupy umístěné na zabezpečovací ústředně. U ústředen Paradox je však potíž s tím, že na každé ústředně je pouze jeden PGM výstup, který je spínaný relátkem, na nějakých ústřednách není žádný. Ostatní PGM výstupy spínají napěťový výstup. Ústředny řad MAGELLAN a SPECTRA mají pouze dva PGM výstupy. Počet PGM výstupů je možné rozšířit připojením modulu PGM4, který obsahuje čtyři PGM výstupy spínané relátky.

Pro příjem binární informace je potřeba najít prvek, který by na vstup binární informace dokázal reagovat. Ve SH KNX to opět není problém, jelikož je možné použít modul, který je přímo pro příjem binární informace vytvořen – modul binárních vstupů. Na straně PZTS se pro tuto funkce nabízí využití zapojení zónového vstupu jako keyswitch. Prostřednictvím tohoto zapojení je možné přijmout binární informaci systémem PZTS, ale pouze pro zapnutí či vypnutí zastřežení.

Tato komunikace je možná pouze v jednom směru. Tudíž jsou pro vzájemnou komunikaci vytvořeny dvě větve. Vzájemná komunikace je vyobrazena na blokovém schématu Obr. 24 Blokové schéma zapojení binárních vstupů



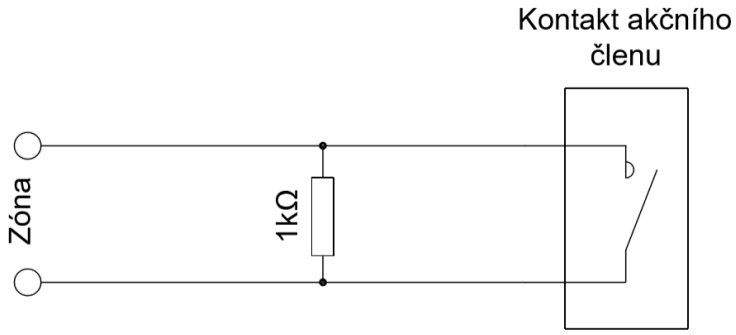

*Obr. 24 Blokové schéma zapojení binárních vstupů*

**PGM**

Jsou programovatelné výstupy ústředny. Jejich výstup je sepnut jako reakce na událost, která je nastavena. Rozepnutí tohoto výstupu může být nastaveno buď na určitou událost, nebo na časový interval.

**Keyswitch**

Zapojuje se na zónový vstup ústředny. Slouží k zapnutí a vypnutí zastřežení. Lze ho nastavit na zapnutí a vypnutí jakéhokoli typu zastřežení.




*Obr. 25 Zapojení keyswitch napojeného na akční člen*

# 9 Praktická realizace komunikace binárními vstupy

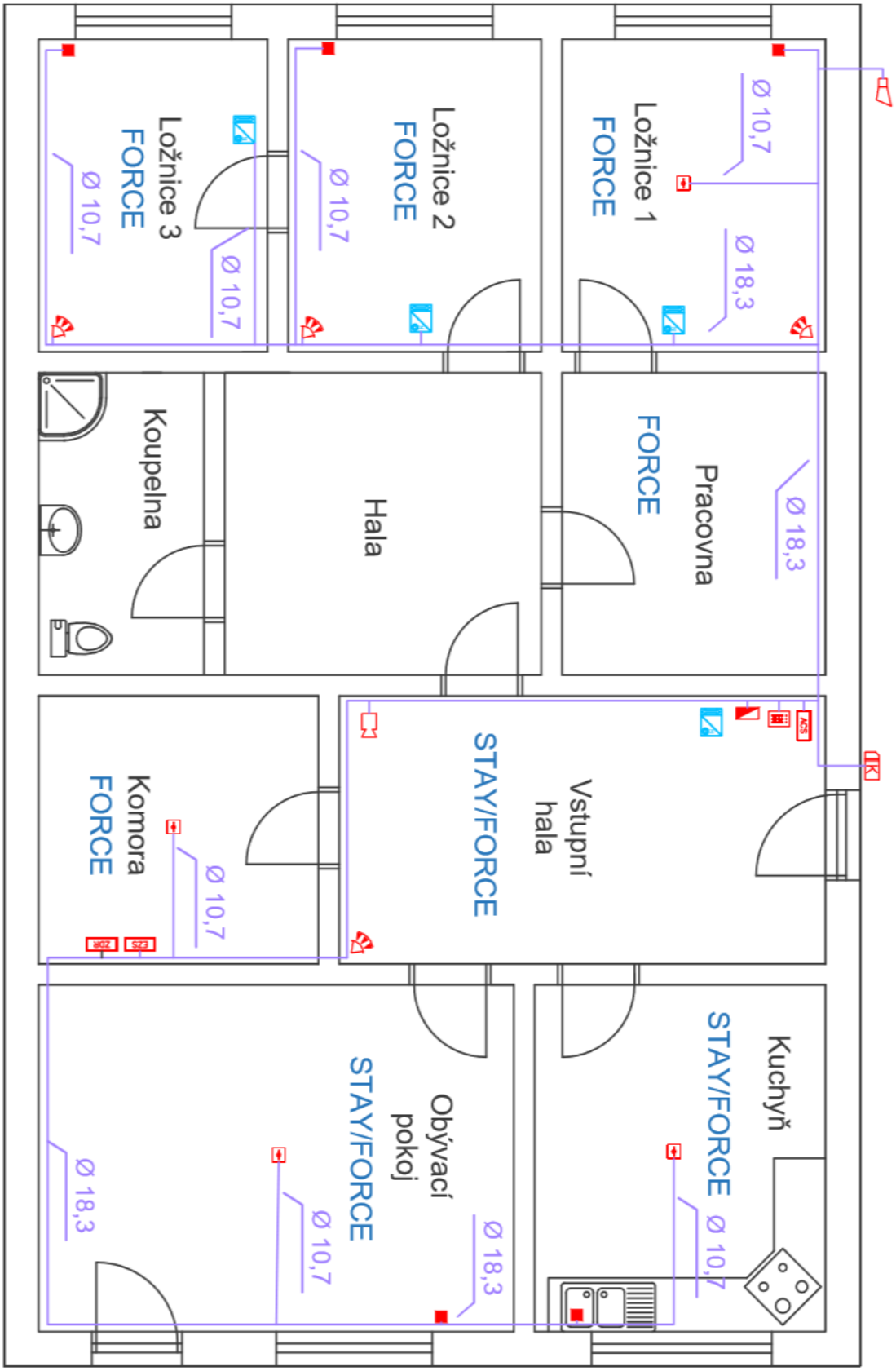
Praktické ověření řešení s propojením binárních vstupů jsem provedl ve školní laboratoři. Tato realizace je provedena tak, jako by se jednalo o instalaci v rodinném domě, ve kterém je nainstalován zabezpečovací systém firmy PARADOX a systém SH KNX. Půdorys domu s rozmístěnými přístroji je zobrazen na Obr. 26. Při této realizaci byly použity ty samé systémy a komponenty, které jsou umístěny do půdorysu domu. Situace s modelovým domem slouží pouze k názornému předvedení, jak by zde popsaný systém mohl v praxi fungovat. V modelovém domě je akorát PZTS doplněn o několik detektorů. Jedná se však pouze o rozšíření systému, který jsem zapojil ve školní laboratoři. Byly použity i stejné postupy zapojení všech komponent. V této části práce se budu zabývat popisem systému, který byl zapojen ve školní laboratoři

## 9.1 Ovládání propojených systémů

Pro ovládání zabezpečovacího systému slouží vypínače instalace SH KNX. Pomocí nich je možné zapnout a vypnout zastřežení domu. Zastřežení ovládaná těmito vypínači jsou dvě: STAY a FORCE.

Zastřežení STAY je možné zapnout a vypnout z jakékoli ze tří ložnic. Tyto vypínače jsou umístěny vedle dveří v každé z těchto místností. Jejich stisknutím dojde k zastřežení STAY bez zpoždění. Také dojde k vypnutí všech světel a stažení rolet v místnostech, kterých se zastřežení STAY týká (Rozdělení místností podle zastřežení je popsáno na Obr. 26). Stiskem jakéhokoli ze tří tlačítek je zastřežení bez zpoždění vypnuto.

Tlačítko pro zastřežení FORCE je umístěno u vchodových dveří, slouží pouze pro zapnutí zastřežení celého domu v případě odchodu z něj. Stiskem tohoto tlačítka dojde k odpočtu odchodového zpoždění a následného zastřežení celé domácnosti do režimu FORCE. Také je vyslán telegram na sběrnici TP KNX pro vypnutí všech světel. Vypnutí zastřežení je nutné provést na klávesnici zadáním přístupového kódu. Dveře lze otevřít přiložením karty na čtečku umístěnou u vchodových dveří. Po jejich otevření dojde k inicializaci pohybu PIR čidlem umístěným ve vstupní hale. Následuje odpočet vstupního zpoždění, které lze zrušit zadáním přístupového kódu na klávesnici. Toto řešení je voleno z důvodu bezpečnosti, kdy by bylo riskantní ponechat vypnutí zastřežení prázdného domu na jednom tlačítku, byť by se nacházelo uvnitř domu.



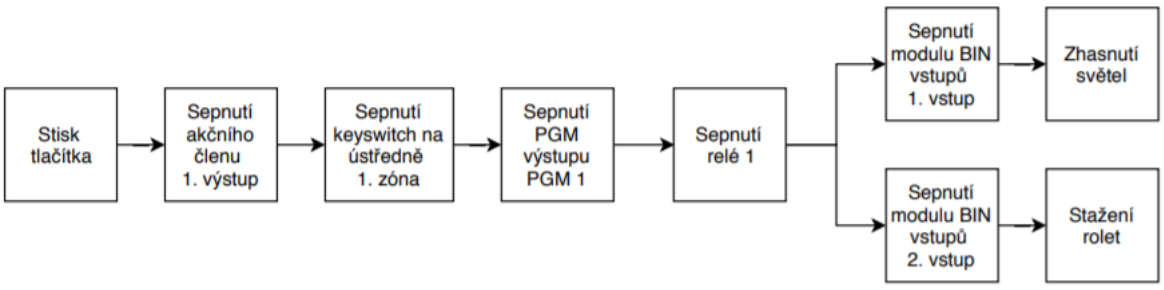

*Obr. 26 Půdorys rodinného domu s rozmístěnými přístroji*

| | |
|---|---|
| EZS | ÚSTŘEDNA PZTS |
| ZDR | PŘIDAVNÝ ZDROJ PZTS |
| | OVLÁDACÍ KLÁVESNICE PZTS |
| | INFRAPASIVNÍ DETEKTOR |
| | INFRAPASIVNÍ DETEKTOR S ANTIMASKINGEM |
| | MAGNETICKÝ KONTAKT |
| | OPTICKO-KOUŘOVÝ DETEKTOR PZTS |
| | SIRÉNA VNITŘNÍ |
| | SIRÉNA VNITŘNÍ S OPTICKOU SIGNALIZACÍ |
| | SIRÉNA VENKOVNÍ |
| ACS | ŘÍDÍCÍ JEDNOTKA PŘÍSTUPU |
| K | BEZDOTYKOVÁ ČTEČKA |
| | ELEKTRICKÝ DVEŘNÍ ZÁMEK |
| | KÓDOVÁ KLÁVESNICE |
| | VYPÍNAČ KNX |

*Obr. 27 Legenda značek PZTS a KNX*

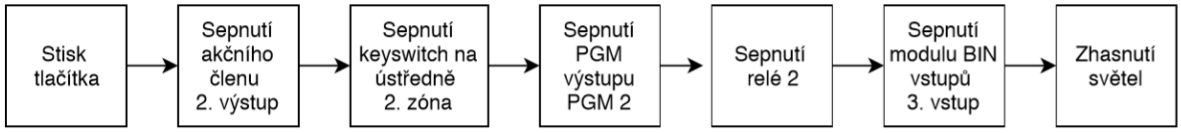
### 9.1.1 Popis funkce propojených systémů

Při stisku tlačítka pro zapnutí zastřežení STAY (MTN 617225) je vyslán na sběrnici TP KNX telegram k akčnímu členu (MTN 646991), který sepne svůj první výstup na dobu jedné sekundy. Spínacím kontaktem akčního členu je sepnut keyswitch zapojený na první zónový vstup ústředny. Ta na tuto informaci ústředna reaguje okamžitým zastřežením systému do režimu STAY bez zpoždění. Jako reakce na zapnutí tohoto režimu je sepnut PGM výstup 1 na dobu jedné sekundy. Napěťovým výstupem PGM je sepnuto první relé umístěné na releovém modulu. Na spínací kontakty tohoto relé je napojen první vstup modulu binárních vstupů (MTN 644592). Ten po sepnutí tohoto vstupu vyšle na sběrnici telegram obsahující informace o vypnutí světel a stažení rolet v místnostech, kterých se zastřežení STAY týká. Tento postup je popsán v diagramu na Obr. 28.



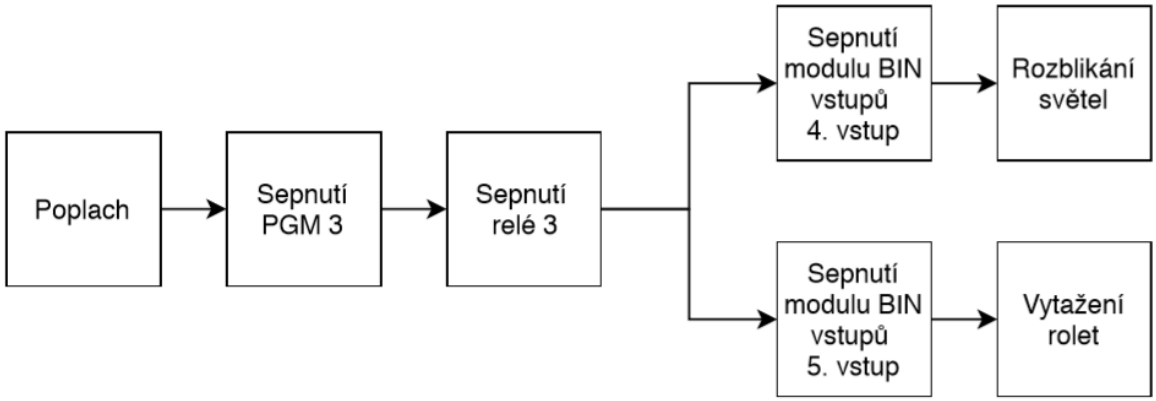

*Obr. 28 Diagram zastřežení STAY*

Stiskem tlačítka umístěného u dveří (MTN 617125) je též vyslán telegram k akčnímu členu (MTN 646991), je sepnutý jeho druhý výstup. Tím je sepnut kontakt keyswitch zapojený druhý zónový stup ústředny. Ústřednou je přijata informace o tom, že má zapnout zastřežení FORCE. Po odpočtu odchodového času je systém zastřežen do režimu FORCE. Po zastřežení je automaticky sepnut PGM výstup 2. Ten je napojen na druhé relé reléového modulu. Na spínací kontakty tohoto relé je napojen druhý vstup modulu binárních vstupů (MTN 644592). Sepnutím tohoto vstupu je vyslán telegram obsahující informaci o vypnutí všech světel v domácnosti. Diagram zastřežení FORCE je popsáno na diagramu Obr. 30.

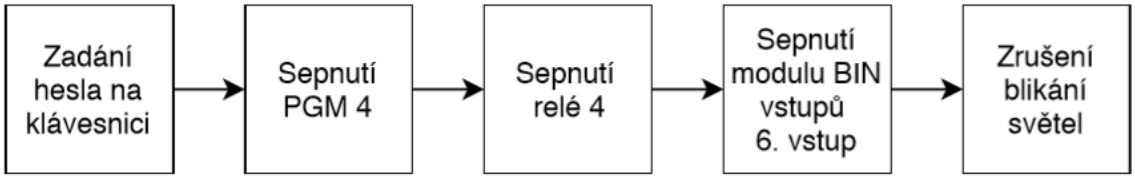



*Obr. 29 Diagram zastřežení FORCE*

Pokud by došlo k narušení zabezpečení, je ústřednou inicializován poplach. Touto událostí je sepnut třetí výstup PGM, který sepne třetí vstup modulu binárních vstupů (MTN 644592). Modul binárních vstupů vyšle na sběrnici KNX telegram a rozblikání světel a vytažení rolet. Světla začnou blikat s periodou jedné sekundy Obr. 30 Poplach lze poté vytnou pouze zadáním hesla na klávesnici. Zrušením poplachu zadáním uživatelského kódu na klávesnici je sepnu čtvrtý PGM výstup. ten sepne čtvrté relé, které předá informaci na modul binárních vstupů. Ten vyšle informaci a vypnutí blikání světel, Obr. 31.




*Obr. 30 Diagram poplachu*

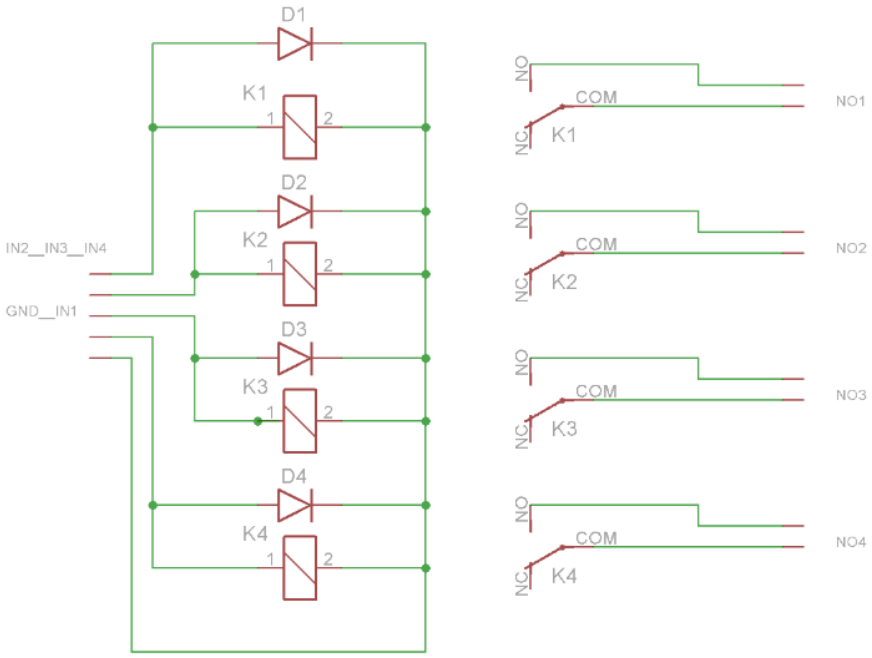



*Obr. 31 Diagram vypnutí poplachu*

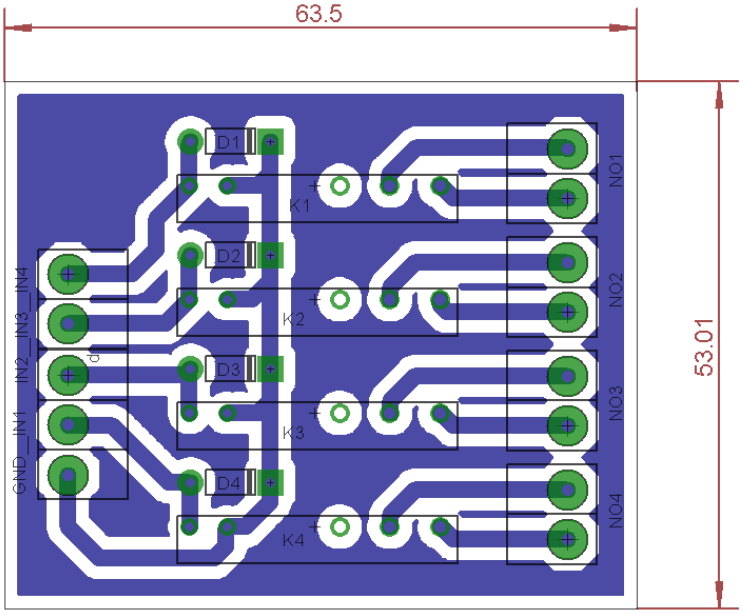
### 9.1.2 Rozšíření PGM

Při praktické realizaci jsem nepoužil rozšiřující modul PGM4 pro zvýšení počtu PGM výstupů. Místo něj jsem vytvořil releový modul, který obsahuje čtyři relé, která jsou spínána PGM výstupy ústředny. Schématické zapojení tohoto modulu je zobrazeno na Obr. 32 Releový modul je navržen speciálně pro toto použití a je součástí této práce.

K cívkám relé jsou paralelně zapojeny diody, které chrání PGM výstupy proti zpětné indukci napětí při vypnutí relé.



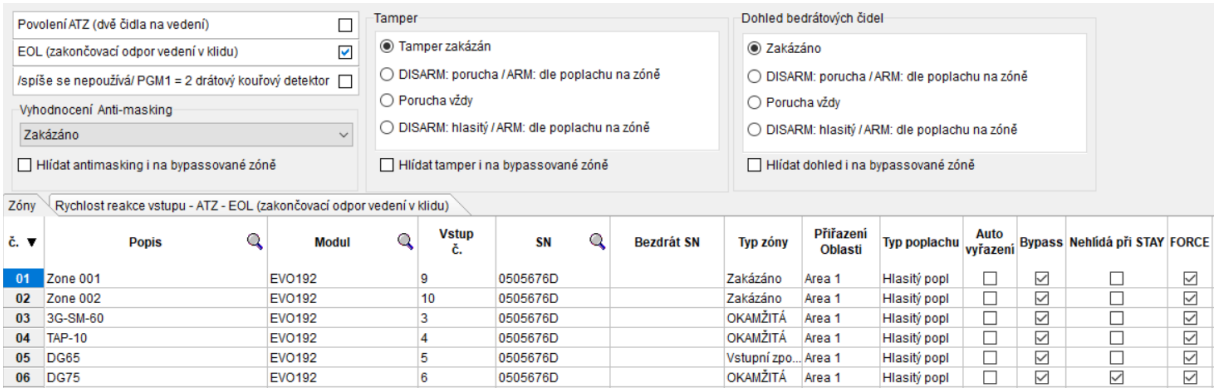

*Obr. 32 Schéma zapojení reléového modulu*




*Obr. 33 DPS reléového modulu*

### 9.1.3 Popis PZTS systému

Systém PZTS jsem nastavoval v instalačním software Babyware. PZTS systém použitý v této realizaci je postaven na zabezpečovací ústředně EVO192. Na ústřednu jsou připojeny čtyři detektory. Dva magnetické kontakty a dva PIR detektory. Jejich rozdělení je tokové, že PIR detektory nejsou aktivní při zastřežení systému do STAY. Dále je u PIR detektorů zakázána funkce antimasking. Kdyby byla tato funkce povolena, tak by nebylo možné systém v laboratoři odzkoušet, jelikož po jejich zakrytí by se zpustil poplach. V případě uvedení instalace do reálného domu by bylo hlídání antimaskingu zapnuto. Magnetické kontakty 3G-SM-60 a TAP jako prvky plášťové ochrany jsou aktivní i při zapnutí střežení STAY. Nastavení detektorů v programu Babyware je zobrazeno na Obr. 34.




| č. | Popis | Modul | Vstup č. | SN | Bezdrát SN | Typ zóny | Přiřazení Oblasti | Typ poplachu | Auto vyřazení | Bypass | Nehlídá při STAY | FORCE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | Zone 001 | EVO192 | 9 | 0505676D | | Zakázáno | Area 1 | Hlasitý popl | ☐ | ☑ | ☐ | ☑ |
| 02 | Zone 002 | EVO192 | 10 | 0505676D | | Zakázáno | Area 1 | Hlasitý popl | ☐ | ☑ | ☐ | ☑ |
| 03 | 3G-SM-60 | EVO192 | 3 | 0505676D | | OKAMŽITÁ | Area 1 | Hlasitý popl | ☐ | ☑ | ☐ | ☑ |
| 04 | TAP-10 | EVO192 | 4 | 0505676D | | OKAMŽITÁ | Area 1 | Hlasitý popl | ☐ | ☑ | ☐ | ☑ |
| 05 | DG65 | EVO192 | 5 | 0505676D | | Vstupní zpo... | Area 1 | Hlasitý popl | ☐ | ☑ | ☐ | ☑ |
| 06 | DG75 | EVO192 | 6 | 0505676D | | OKAMŽITÁ | Area 1 | Hlasitý popl | ☐ | ☑ | ☑ | ☑ |

*Obr. 34 Nastavené zóny v software Babyware*

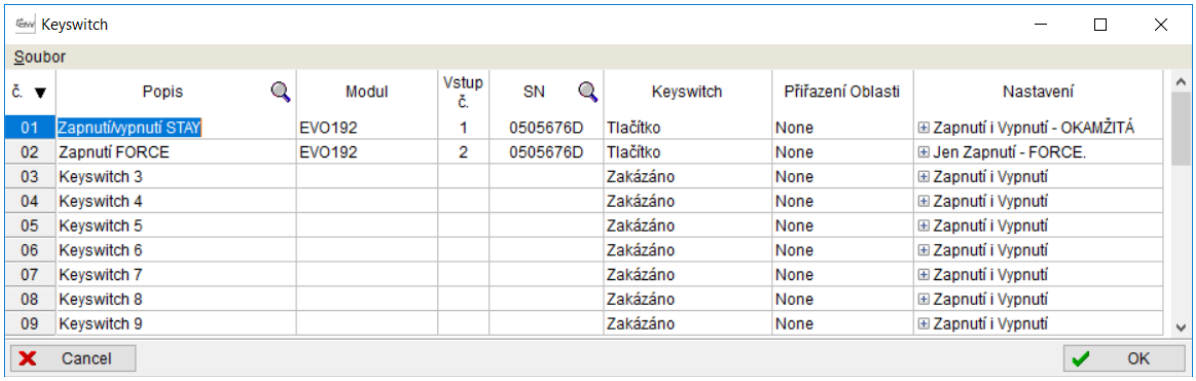
Pro ovládání systému jsou vytvořeni čtyři uživatelé, kteří mají rovnocenné oprávnění k ovládání systému. Uživatelé 1 a 2 mají přiřazenou přístupovou kartu. Jejich seznam s nastavenými uživatelskými kódy lze vidět na Obr. 35.


| č. | Popis | Jméno | Příjmení |
|---|---|---|---|
| 000 | Instalační k | | |
| 001 | User 001 | | |
| 002 | User 002 | | |
| 003 | User 003 | | |
| 004 | User 004 | | |

| No | Kód | Karta č. | Klíčenka SN | Šablony klíčenek | Area 1 | Area 2 |
|---|---|---|---|---|---|---|
| 000 | 000000 | N/A | N/A | N/A | N/A | N/A |
| 001 | 1234 | 059:51117 | 000000 | Šablona 00 | ☑ | ☑ |
| 002 | 2222 | 076:30948 | 000000 | Šablona 00 | ☑ | ☑ |
| 003 | 3333 | 000:00000 | 000000 | Šablona 00 | ☑ | ☑ |
| 004 | 4444 | 000:00000 | 000000 | Šablona 00 | ☑ | ☐ |

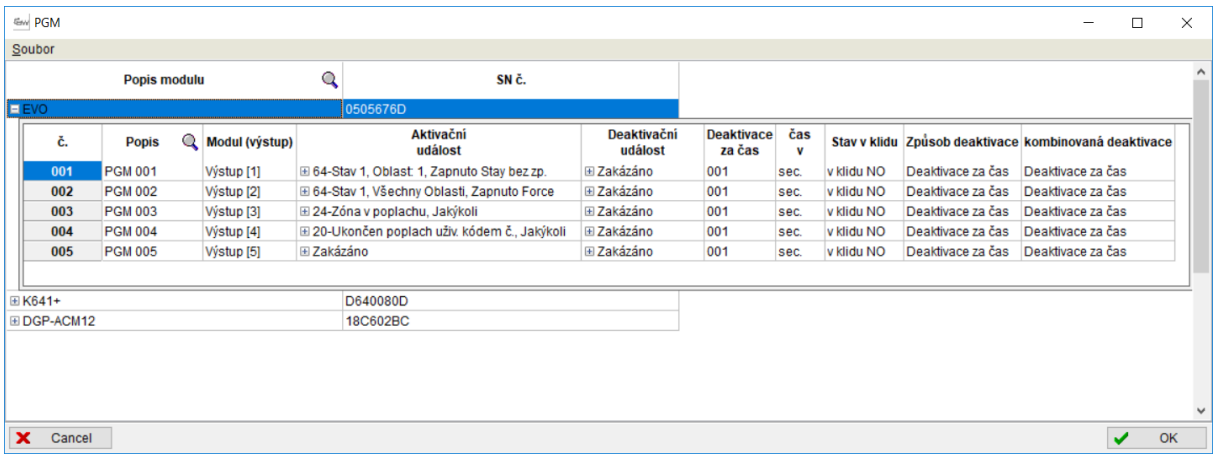
*Obr. 35 Nastavené uživatelské kódy v software Babyware*

Na zónové vstupy 1 a 2 jsou zapojena keyswitch tlačítka. Sepnutím tlačítka keyswitch 1 dojde k zastřežení STAY bez zpoždění, opětovným sepnutím je zastřežení vypnuto. Stiskem keyswitch 2 je zapnuto zastřežení FORCE. Jejich nastavení je zobrazeno na Obr. 36 na následující straně. Jsou připojeny první dva zónové vstupy.




*Obr. 36 Nastavené keyswitch v software Babyware*

Na výstupy PGM s napěťovými výstupy je připojen releový modul se čtyřmi relé. Nastavené PGM výstupy jsou zobrazeny na Obr. 37. Na sběrnici ústředny je zapojený modul přístup ACM 12 se čtečkou karet EM CR1. Program v Babyware je přiložený v Příloze 6.




*Obr. 37 Nastavené PGM výstupy v software Babyware*

**Popis binárních vstupů a výstupů zabezpečovací ústředny**

PGM výstupy

Výstup 1 – Sepnutí při zastřežení systému do režimu STAY bez zpoždění.

Výstup 2 – Sepnutí při zastřežení systému do režimu FORCE.

Výstup 3 – Sepnut při poplachu jakékoli zóny.

Výstup 4 – Sepnuto při zrušení poplachu zadání uživatelského kódu na klávesnici.

Keyswitch

Zónový vstup 1 – Zapnutí/vypnutí zastřežení STAY bez zpoždění.

Zónový vstup 2 – Zapnutí zastřežení FORCE.

**Seznam použitých komponent PZTS**

Zabezpečovací ústředna EVO192

Modul přístupu ACM 12

Čtečka karet EC EM1

Magnetické kontakty 3G-SM-60

Magnetický kontakt TAP-10

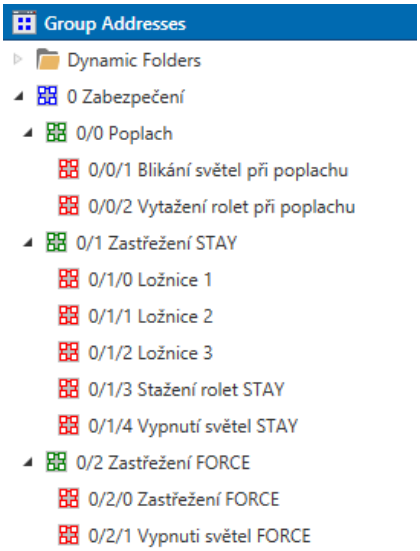
PIR detektor DG65

PIR detektor DG75

Modul interface 307USB

### 9.1.4 Popis SH systému

Projekt KNX instalace pro tuto realizaci jsem vytvořil v programu ETS 5. Číslo oblasti 4 vychází z toho, že jsem projekt vytvářel na stanovišti s číslem 4. Toto číslo je neměnné. Struktura skupinových adres je vytvořena tak, aby všechny funkce spojené s implementací PZTS ve SH byly v jedné hlavní skupinové adrese. Přehled skupinových adres je vyobrazen na Obr. 38. Vytvořený program v ETS 5 je přiložen v příloze 7.




*Obr. 38 Skupinové adresy*

**Popis binárních vstupů a výstupů SH KNX**

Modul binárních vstupů

Vstup 1 – Vypnutí světel při zastřežení STAY bez zpoždění.

Vstup 2 – Stažení rolet při zastřežení STAY bez zpoždění.

Vstup 3 – Vypnutí světel při zastřežení FORCE.

Vstup 4 – Rozblikání světel při poplachu.

Vstup 5 – Vytažení rolet při poplachu.

Vstup 6 – Vypnutí blikání světel při zrušení poplachu

Akční člen MTN646991

Výstup 1 – Zapnutí a vypnutí zastřežení STAY bez zpoždění.

Výstup 2 – Zapnutí zastřežení FORCE.

**Seznam použitých komponent SH KNX**

Seznam použitých komponent je uveden na Obr. 39.

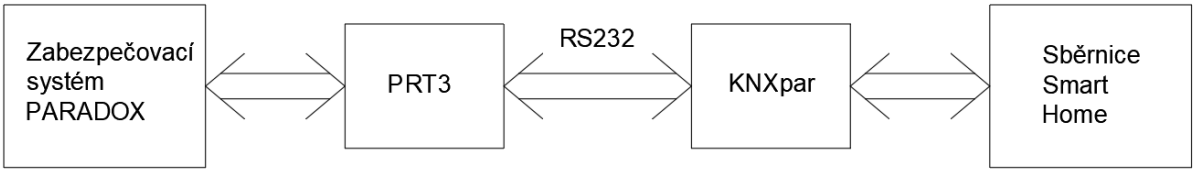
| | | |
|---|---|---|
| 1 | MTN6171xx | Push-button 1-gang plus |
| 3 | MTN6172xx | Push-button 2-gang plus |
| 1 | MTN644592 | Binary input REG-K/ 8x10 |
| 1 | MTN646991 | Control unit 0-10 V REG-K/3f with manual mode |
| 1 | MTN647595 | Switch actuator REG-K/4x230/16 |
| 1 | MTN649908 | Blind/Switch actuator REG-K/8x/16x/10 manual mode |
| 2 | MTN680204 | Coupler REG-K |

*Obr. 39 Seznam komponent SH KNX vyexportovaný z ETS 5*

# 10 Propojení sběrnic PTZS a SH KNX

Sběrnice zabezpečovacích ústředen firmy Paradox a sběrnice KNX jsou odlišné. Z tohoto důvodu je nutné sběrnice propojit zařízením, které dokáže převést informace z jedné sběrnice na druhou a obráceně.

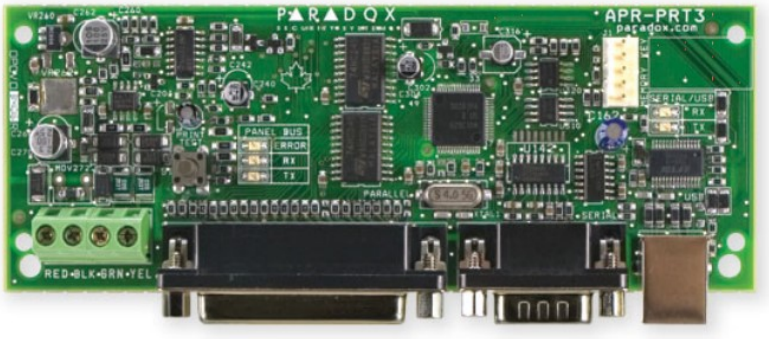
Pro tuto funkci lze využít integrační modul firmy Paradox PRT3. Pro propojení tohoto modulu a sběrnice KNX slouží modul KNXpar, který byl vyvinut přímo za tímto účelem. Použitím těchto dvou modulů vznikne obousměrná komunikace mezi systémy.




*Obr. 40 Blokové schéma komunikace mezi sběrnicemi Paradox a KNX*

**Integrační modul PRT3**

Datovým výstupem jsou zde univerzální znaky a příkazy ASCII/E-BUS. Skrze modul je možné načítat jednotlivé stavy ústředny a také její ovládání. Funkce modulu umožňuje připojení ústředen DIGIPLEX EVO do jiných systémů, které jsou v budově využívány.




*Obr. 41 Modul PRT3 [36]*

**Modul KNXpar**

Tento modul převádí telegramy vysílané na sběrnici KNX na znaky ASCII. Tyto znaky je možní

Propojení mezi moduly PRT3 a KNXpar je realizováno sériovou linkou RS232.

Toto spojení však umožňuje přenos jen některých informací. Jsou přenášeny informace o stavu podsystémů a stav spojení mezi ústřednou a sběrnicí KNX. Z instalace KNX lze vyčíst povely k zapnutí zastřežení.

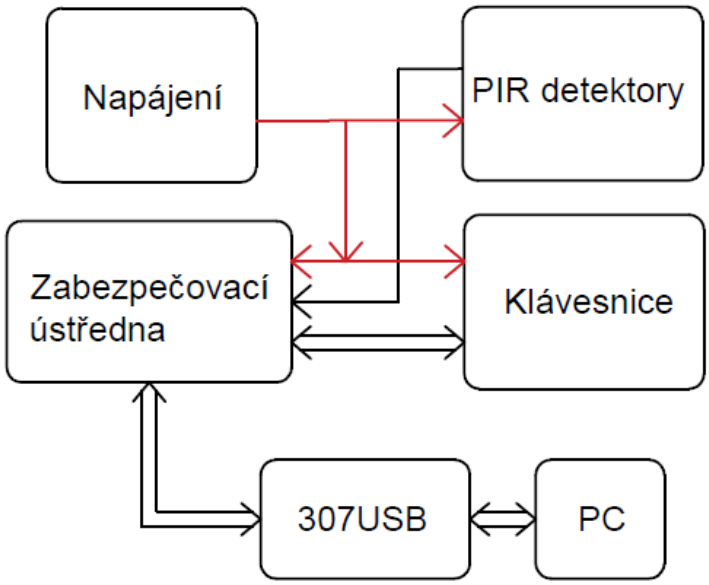
# 11 Realizace laboratorních úloh

V rámci této práce jsem vytvořil pět laboratorních úloh, které slouží jako podklady k výuce zabezpečovacích systémů. Každá z těchto úloh obsahuje technickou specifikaci použitých komponentů, včetně popisu funkce detektorů v dané úloze. Dále je zde popsáno a schematicky znázorněno zapojení jednotlivých komponent. Přesný postup pro oživení a nastavení systému prostřednictvím klávesnice a PC s instalačním software Babyware. Na závěr každá úloha obsahuje postup pro odzkoušení nastaveného systému a také postup pro simulaci napadení zabezpečovacího systému a popis reakce systému na daný druh napadení. Jednotlivé úlohy jsou umístěny v kufřících.

## 11.1 Laboratorní úloha 1 – Pohybové detektory

Tato laboratorní úloha se zabývá použitím pohybových detektorů v PZTS. Je zde použita drátová ústředna SP5500. Blokové schéma zapojení je zobrazeno na Obr. 42.

Kompletní laboratorní úloha je k nahlédnutí v Příloha 1.




*Obr. 42 Blokové schéma zapojení laboratorní úlohy s PIR detektory*

**Seznam použitých komponent:**

Zabezpečovací ústředna SPECTRA SP5500

Infrapasivní PIR detektor DG75

Infrapasivní PIR detektor DG65

Analogový PIR detektor 476

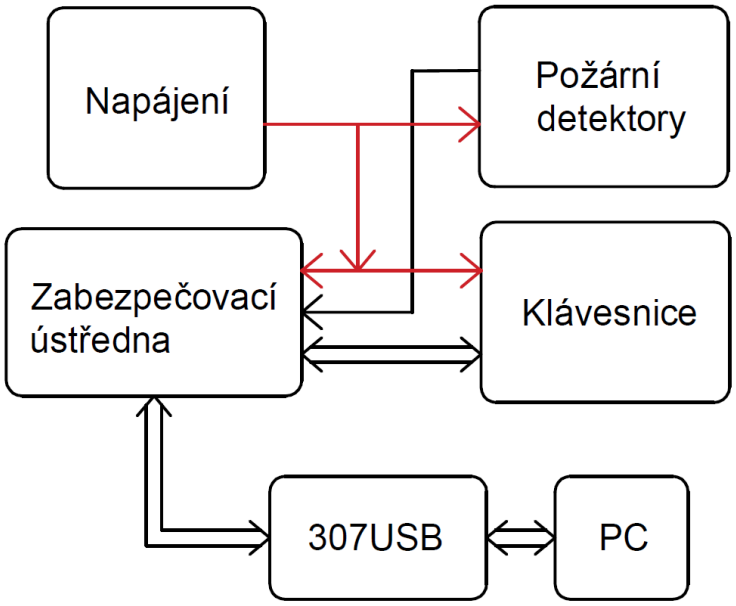
Klávesnice K32LCD+

Modul interface 307USB

## 11.2 Laboratorní úloha č. 2 – požární detektory

V této laboratorní úloze jsou použity požární detektory. Konkrétně jsou použity čtyři detektory, přičemž každý má jiný způsob vyhodnocování požáru. Jeden z detektorů je určen pro detekci cigaretového kouře.

Kompletní laboratorní úloha je k nahlédnutí v Příloha 2.




*Obr. 43 Blokové schéma zapojení laboratorní úlohy s požárními detektory*

**Seznam použitých komponent**

Zabezpečovací ústředna řady SPECTRA SP5500

Klávesnice K32LCD+

Teplotní a termodiferenciální FDR-16-HR

Opticko kouřový FDR-26-S

Opticko kouřový s termistorem FDR-36-SHR

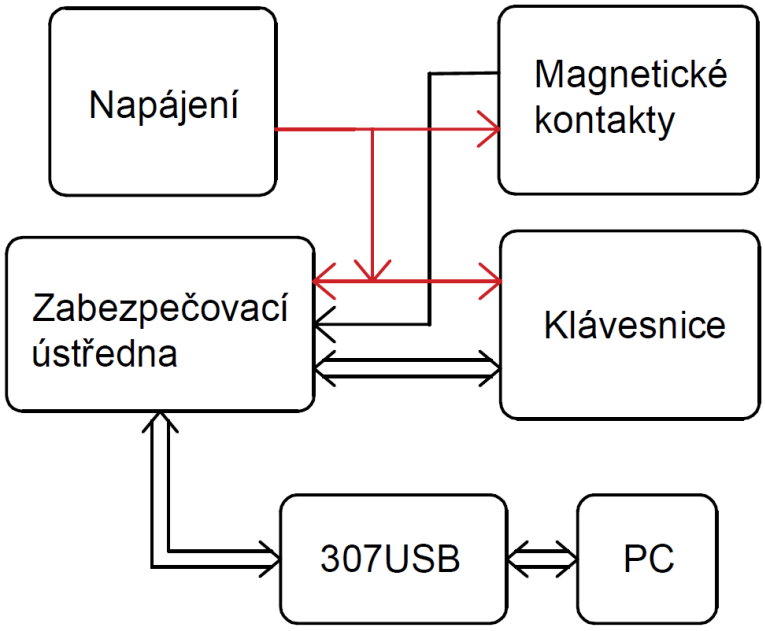
Opticko-kouřový detektor CDR-727

Modul interface 307USB

## 11.3 Laboratorní úloha č. 3 – magnetické kontakty

V této laboratorní úloze jsou použity celkem čtyři různé magnetické kontakty.

Kompletní laboratorní úloha je k nahlédnutí v Příloha 3.




*Obr. 44 Blokové schéma zapojení laboratorní úlohy s magnetickými kontakty*

**Seznam použitých komponent**

Zabezpečovací ústředna řady SPECTRA SP5500

Klávesnice K32LCD+

Povrchový mg. kontakt 3G-SM-60

Povrchový mg. kontakt SM-50-T

Povrchový mg. kontakt FM-102

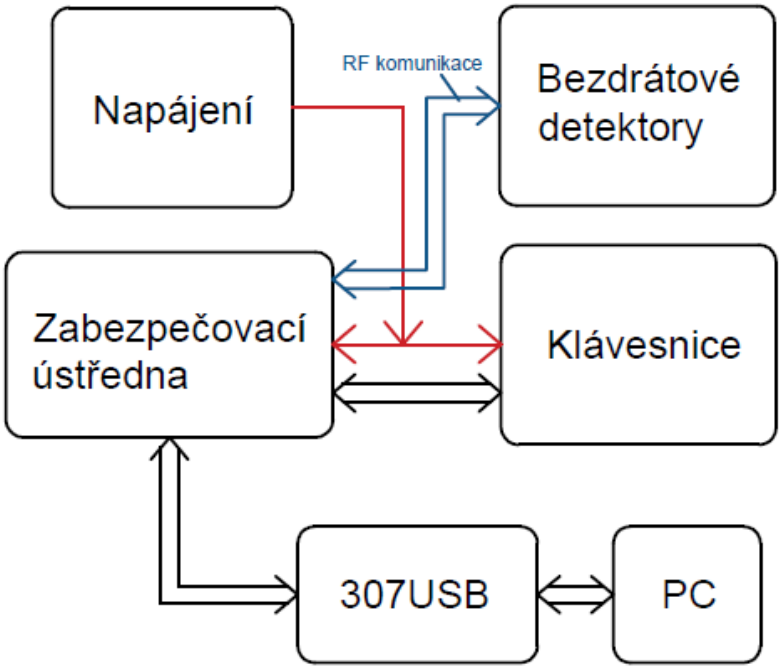
Zápustný mg. kontakt TAP-10

Modul interface 307USB

## 11.4 Laboratorní úloha č. 4 – bezdrátové detektory

V laboratorní úloze č. 4 se nacházejí bezdrátové detektory. Přesněji jeden PIR detektor a magnetický kontakt.

Kompletní laboratorní úloha je k nahlédnutí v Příloha 4.




*Obr. 45 Blokové schéma zapojení laboratorní úlohy s bezdrátovými detektory*

**Seznam použitých komponent a pomůcek**

Zabezpečovací ústředna řady MAGELLAN MG5000

Klávesnice K32LCD+

Bezdrátový PIR detektor PDM2P

Bezdrátové magnetické kontakty DCT10 v2.2

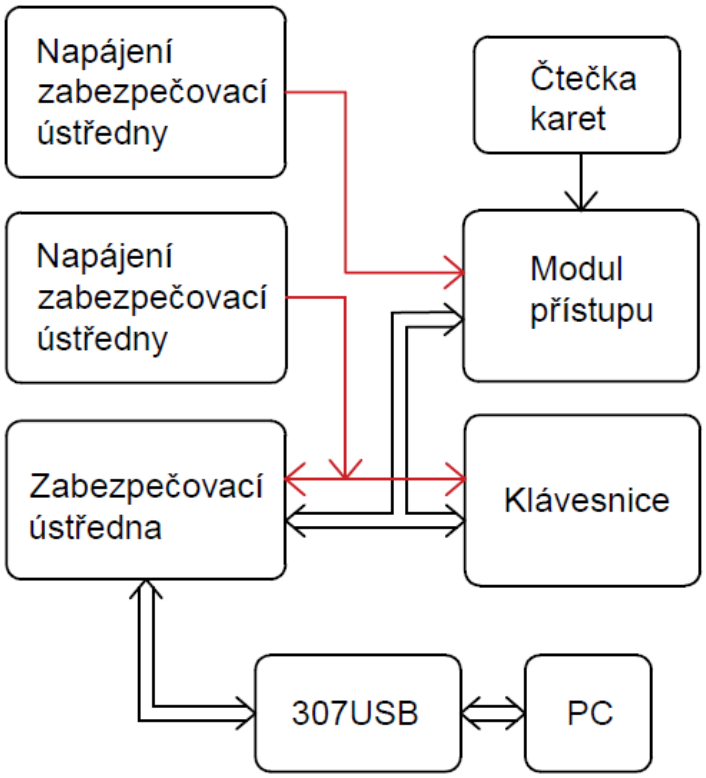
Klíčenka REM2

Kabel RS232

Modul interface 307USB

## 11.5 Laboratorní úloha č. 5 – přístupové body

Kompletní laboratorní úloha je k nahlédnutí v Příloha 5.




*Obr. 46 Blokové schéma zapojení laboratorní úlohy přístupových bodů*

**Seznam použitých komponent:**

Zabezpečovací ústředna EVO 192

Klávesnice K641+

Modul přístupu ACM 12

Čtečka karet EM CR1

Modul interface 307USB

# 12 Závěr

V první kapitole je vytvořena rešerše, kterou jsem vytvořil z dvaceti odborných článků, které byly vydány v posledních čtyřech letech. Z jejího obsahu vyplívá, že v dnešní době jsou vyvíjeny a testovány systémy, které v sobě přímo kombinují zabezpečovací systémy a systémy SH. Dalším trendem je úspora energií a šetrnost k životnímu prostředí při používání těchto systémů. Při vývoji těchto systémů se nezapomíná ani na péči o seniory a lidi s vážným onemocněním.

V následující kapitole je vytvořen stručný popis PZTS. Celý tento systém je zde rozdělen na základní části, které jsou popsány včetně popisu jejich funkce. V navazující kapitole jsou popsány způsoby zapojení jednotlivých komponent, včetně schématických zapojení. Také jsou zde vysvětleny základní pojmy, které se k systémům PZTS vztahují.

V kapitole číslo pět je uveden rozbor systémů SH spadajících pod asociaci KNX. Je zde popsána topologie tohoto systému a média, která lze v rámci tohoto systému využít k přenosu informace.

Šestá a sedmá kapitola se věnuje legislativě systémů PZTS a SH KNX. Jsou zde popsány základní normy vztažené k těmto systémům.

Praktická část této práce začíná sednou kapitolou. Nejprve jsou zde zhodnoceny možné způsoby implementace PZTS ve SH. Prvním popsaným způsobem je propojení sběrnic obou systémů. Dalším způsobem je propojení systémů přes jejich binární vstupy a výstupy.

V deváté kapitole je popsána praktická realizace implementace PZTS ve SH prostřednictvím binárních vstupů a výstupů. Je zde uveden detailní popis funkce a propojení výsledného systémů, který vznikl spojením PZTS Paradox a SH KNX.

Poslední kapitola je věnována stručnému popisu pěti laboratorních úloh, které byly vytvořeny v rámci této práce. Je zde pouze uveden stručný popis jednotlivých úloh, blokové schéma zapojení dané úlohy a seznam použitých komponent. Je zbytečné zde tyto úlohy více rozvádět, jelikož jsou v tištěné formě přiloženy jako příloha.

# 13 Zdroje


[1] AHMED, I., A. P. SALEEL, B. BEHESHTI, Z. A. KHAN, et al. *Security in the Internet of Things (IoT)*. Edtion ed. New York: Ieee, 2017. 84-90 p. ISBN 978-1-5386-3330-4.

[2] MANIMUTHU, A. AND R. RAMESH Privacy and data security for grid-connected home area network using Internet of Things. Iet Networks, Nov 2018, 7(6), 445-452.

[3] GUO, Z. M., N. KARIMIAN, M. M. TEHRANIPOOR, D. FORTE, et al. Hardware Security Meets Biometrics for the Age of IoT. In *2016 Ieee International Symposium on Circuits and Systems.* New York: Ieee, 2016, p. 1318-1321.

[4] RADOVAN, M. AND B. GOLUB *Trends in IoT Security*. edited by P. BILJANOVIC, M. KORICIC, K. SKALA, T.G. GRBAC, M. CICINSAIN, V. SRUK, S. RIBARIC, S. GROS, B. VRDOLJAK, M. MAUHER, E. TIJAN AND F. HORMOT. Edtion ed. New York: Ieee, 2017. 1302-1308 p. ISBN 978-953-233-092-2.

[5] S. ur Rehman and V. Gruhn, "An approach to secure smart homes in cyber-physical systems/Internet-of-Things," *2018 Fifth International Conference on Software Defined Systems (SDS)*, Barcelona, 2018, pp. 126-129. doi: 10.1109/SDS.2018.8370433

[6] JOSHITTA, R. S. M., L. AROCKIAM AND IEEE *Device Authentication Mechanism for IoT Enabled Healthcare System*. Edtion ed. New York: Ieee, 2017. ISBN 978-1-5090-3378-2.

[7] BUJNOWSKA-FEDAK, M. M. AND U. GRATA-BORKOWSKA Use of telemedicine-based care for the aging and elderly: promises and pitfalls. Smart Homecare Technology and Telehealth, 2015, 3, 91-105.

[8] ALI, N., A. K. ALBANNA, M. ABU ARQOUB, G. ISSA, et al. *Clicker: Converting Modern Homes to Smart Modern Homes through the Use of IoT*. edited by G.F. ISSA, A. ALMAQOUSI, N. ELKHALILI AND M. ABUARQOUB. Edtion ed. New York: Ieee, 2017. ISBN 978-1-5386-1986-5.

[9] BIN SHAHIN, F., P. TAWHEED, M. F. HAQUE, M. R. HASAN, et al. Smart Home Solutions with Sun Tracking Solar Panel. In *2017 4th International Conference on Advances in Electrical Engineering.* New York: Ieee, 2017, p. 766-769.

[10] KHAN, M., B. N. SILVA AND K. J. HAN Internet of Things Based Energy Aware Smart Home Control System. Ieee Access, 2016, 4, 7556-7566.

[11] ASLAN, E. S., O. F. OZDEMIR, A. HACIOGLU, G. INCE, et al. *Smart Pass Automation System*. Edtion ed. New York: Ieee, 2016. 225-228 p. ISBN 978-1-5090-1679-2.

[12] ALIM, M. A., M. M. BAIG, S. MEHBOOB AND I. NASEEM. Method for secure electronic voting system: Face recognition based approach. In X. JIANG, M. ARAI AND G. CHEN eds. *Second International Workshop on Pattern Recognition.* Bellingham: Spie-Int Soc Optical Engineering, 2017, vol. 10443.

[13] CHEGGOU, R., E. H. KHOUMERI AND K. FERHAH. Energy-Saving Through Smart Home Concept. In M. HATTI ed. *Artificial Intelligence in Renewable Energetic Systems: Smart Sustainable Energy Systems.* Dordrecht: Springer, 2018, vol. 35, p. 50-58.

[14] BODYANSKIY, Y., O. VYNOKUROVA, G. SETLAK, D. PELESHKO, et al. Adaptive multivariate hybrid neuro-fuzzy system and its on-board fast learning. Neurocomputing, Mar 2017, 230, 409-416.

[15] LEE, C. T., T. C. SHEN AND W. D. LEE A Novel Optical Morse Code-Based Electronic Lock Using the Ambient Light Sensor and Fuzzy Controller. Applied Sciences-Basel, Feb 2017, 7(2), 16.

[16] KUSTIJA, J., K. S. N. ADILLAWATI AND D. FAUZIAH Smart Home System to Support Bandung Smart City Programme. Pertanika Journal of Science and Technology, Nov 2017, 25, 77-88.

[17] LODHA, R., S. GUPTA, H. JAIN AND H. NARULA. Bluetooth Smart based

Attendance Management System. In H. VASUDEVAN, A.R. JOSHI AND N.M. SHEKOKAR eds. *International Conference on Advanced Computing Technologies and Applications.* Amsterdam: Elsevier Science Bv, 2015, vol. 45, p. 524-527.

[18] RANGKUTI, H. A., J. W. SIMATUPANG AND IEEE *Security Lock with DTMF Polyphonic Tone Sensor*. Edtion ed. New York: Ieee, 2015. 119-122 p. ISBN 978-1-4673-7408-8.

[19] ALDROUBI, S., W. ADI AND IEEE *Towards Clone-Resistant Building Structures*. Edtion ed. New York: Ieee, 2016. ISBN 978-1-4673-8743-9.

[20] DEBABHUTI, N., S. DAS, S. DUTTA, A. SARKAR, et al. Advanced Bi-directional Home Appliance Communicator with Security System. In J.K. MANDAL, S.C. SATAPATHY, M.K. SANYAL, P.P. SARKAR AND A. MUKHOPADHYAY eds. *Information Systems Design and Intelligent Applications, Vol 1.* Berlin: Springer-Verlag Berlin, 2015, vol. 339, p. 145-156.

[21] *Princip fungování EZS* [online]. [cit. 2019-04-03]. Dostupné z: http://www.ladinn.cz/ostatni/technika/princip-EZS.html

[22] *Jihočeská univerzita vČeských BudějovicíchPřírodovědecká fakultaZabezpečení objektů prvky I&HAS*. České Budějovice, 2013. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích.

[23] KNX cable. *Fs cables* [online]. [cit. 2019-01-02]. Dostupné z: https://www.fscables.com/products/knx-cable.html

[24] KNX Základy [online]. s. 1-20 [cit. 2018-12-28]. Dostupné z: https://www.knx.org/media/docs/downloads/Marketing/Flyers/KNX-Basics/KNXBasics_cz.pdf

[25] ČSN EN 50131-1 ed.2 (334591). Poplachové systémy - poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky. Praha. Český normalizační institut, 2007, 40 s.

[26] ČSN CLT/TS 50131-7 (334591). Poplachové systémy - poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace. Praha. Český normalizační institut, 2011.

[27] *Magnetické kontakty* [online]. 2008 [cit. 2019-02-11]. Dostupné z: http://www.htv-hodina.cz/soubory/magneticke-kontakty-man-b.pdf

[28] HOŠEK, Zdeněk Hošek. *Autonomní hlásiče kouře* [online]. 13.8.2008 [cit. 2019-04-10]. Dostupné z: https://www.tzb-info.cz/elektricka-pozarni-signalizace/5011-autonomni-hlasice-koure

[29] *Variant.cz* [online]. [cit. 2019-02-25]. Dostupné z: https://www.variant.cz/zbozi/0702-178-evo192-panel

[30] *Variant.cz - webové stránky společnosti Variant* [online]. [cit. 2019-02-25]. Dostupné z: https://www.variant.cz/zbozi/1408-012-k641

[31] *Variant.cz - webové stránky společnosti Variant* [online]. [cit. 2019-02-25]. Dostupné z: https://www.variant.cz/zbozi/0701-007-dg75

[32] *Variant.cz* [online]. [cit. 2019-02-25]. Dostupné z: https://www.variant.cz/zbozi/1608-016-nv75mw

[33] *Variant.cz* [online]. [cit. 2019-02-25]. Dostupné z: https://www.variant.cz/zbozi/0701-064-3g-sm-60-bila

[34] *Variant.cz* [online]. [cit. 2019-02-25]. Dostupné z: https://www.variant.cz/zbozi/0701-028-fdr-26-s

[35] *Stasanet.cz* [online]. [cit. 2019-03-15]. Dostupné z: https://www.stasanet.cz/out/media/MG,%20SP%20-%20IM.pdf

[36] *Variant.cz* [online]. [cit. 2019-04-15]. Dostupné z: https://www.variant.cz/zbozi/0702-211-prt3

# 14 Přílohy

Příloha 1: Laboratorní úloha č. 1 – pohybové detektory

Příloha 2: Laboratorní úloha č. 2 – požární detektory

Příloha 3: Laboratorní úloha č. 3 – magnetické kontakty

Příloha 4: Laboratorní úloha č. 4 – bezdrátové detektory

Příloha 5: Laboratorní úloha č. 5 – přístupové body

Příloha 6: Program BabyWare

Příloha 7: Program ETS 5

Příloha 8: Vyexportovaný program z ETS 5