VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NÁVRH SYSTÉMOVÉHO ŘÍZENÍ INTELIGENTNÍHO DOMU A JEHO ZABEZPEČENÍ

DESIGN OF SMART HOME CONTROL SYSTEM AND SECURITY MANAGEMENT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Kateřina Valentová

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Kateřina Valentová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh systémového řízení inteligentního domu a jeho zabezpečení

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout systém řízení inteligentního domu s důrazem kladeným na management bezpečnosti.

Základní literární prameny:

ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací. Praha: Český normalizační institut, 2014.

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

POČINKOVÁ, M. a D. ČUPROVÁ. Úsporný dům. 2. aktualiz. vyd. Brno: ERA, 2008. 182 s. ISBN 97880-7366-131-1.

POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978--7251-250-8.

VALEŠ, M. Inteligentní dům. 1. vyd. Brno: ERA, 2006. 123 s. ISBN 80-736-6062-8.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato diplomová práce se věnuje návrhu systémového řízení inteligentního domu, s důrazem kladeným na celkové zabezpečení systému z hlediska informační, síťové i fyzické bezpečnosti. Návrh je vytvořen a základě požadavků majitele domu a s ohledem na jeho potřeby. V práci je dále sestavena analýza možných rizik včetně bezpečnostních opatření k jednotlivým hrozbám. Součástí práce není celkový návrh kabelážního systému, práce se věnuje zejména otázkám související se zabezpečením celého inteligentního systému.

Klíčová slova

inteligentní elektroinstalace, inteligentní dům, management bezpečnosti, analýza rizik, bezpečnost informací

Abstract

This master's thesis is focused on design of smart home control system with focus on security of system in terms of information, network and physical security. Design is based on the requirements of the house owner and his needs. In thesis is assembled risk analysis with security measures to the individual threats. Complete design of cable system is not a part of this work, thesis is particularly focused on questions about security of the entire intelligent system.

Key words

smart wiring, intelligent house, security management, risk analysis, information security

Bibliografická citace

VALENTOVÁ, Kateřina. Návrh systémového řízení inteligentního domu a jeho zabezpečení [online]. Brno, 2019 [cit. 2019-05-11]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119711. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 10. května 2019 .....

podpis autora

Poděkování

Chtěla bych poděkovat zejména vedoucímu mé diplomové práce, panu Ing. Petru Sedlákovi za cenné rady a odborné vedení nejen při práci na této diplomové práci, ale v průběhu celého mého studia a současně i mým rodičům za podporu, kterou mi prokazovali během celého studia.

OBSAH

1 ÚVOD

Díky stále rychlejšímu vývoji technologií máme možnosti, jak stále více zjednodušovat každodenní život. V posledních letech se čím dál tím více objevují na trhu běžné věci, které jsou najednou schopny připojit se na internet a nechat se ovládat na dálku bez nutnosti fyzické přítomnosti člověka. Takového zařízení jsou čím dál tím více rozšířené a s tím souvisí i pokles jejich ceny, takže se stávají více a více dostupné pro většinu obyvatelstva. Díky inteligentním elektroinstalacím je nyní možné lépe zabezpečit a na dálku ovládat vlastní dům nebo byt, což přináší mnoho výhod. Jedna z hlavních předností takovýchto inteligentních domácností je bezesporu úspora energie, větší komfort každodenního života a samozřejmě i vyšší zabezpečení a možnost nepřetržitého monitorování celého objektu.

V současné době se v české republice objevuje již velké množství firem, které poskytují řešení pro řízení inteligentních domácností na míru. Jejich systémy se liší nejen cenou nebo funkcemi, které takovýto systém umí, ale zejména použitou technologií. Proto, pokud se člověk rozhodně pro inteligentně řízenou domácnost, je vhodné, aby celý systém byl řešen pomocí jednoho výrobce, a to zejména z důvodu, aby nedocházelo k případným komunikačním problémům, které mohou nastat při nekompatibilitě jednotlivých zařízení dodaných různými výrobci.

Díky masovému rozšíření inteligentních zařízení se bohužel otevírá i velký prostor pro potencionální útoky na tyto zařízení. Zařízení bývají většinou nezabezpečená (případně pouze chráněna továrním heslem, které je vždy stejné) a uživatelé si neuvědomují riziko možného zneužití útočníkem. V současnosti již nejsou vyhledávaným cílem pouze velké organizace, ale stále více se terčem útoků stávají domácí uživatelé, kteří si mnohdy ani neuvědomují, jak citlivé jejich data jsou. Proto je nutné situaci řešit a pokusit se inteligentní zařízení před útočníky co nejlépe ochránit.

2 CÍL PRÁCE A VYMEZENÍ POJMŮ

Cílem této práce je vypracovat návrh na zavedení vhodného systému pro řízení inteligentní domácnosti pro novostavbu rodinného domu s důrazem kladeným na bezpečnost celého systému. Díky systému bude možné ovládat nejdůležitější funkce domu jako např. vytápění nebo osvětlení a to pohodlně, přes mobilní zařízení a samozřejmě i na dálku, bez nutnosti fyzické přítomnosti v domě. V práci bude představeno několik dostupných řešení, jejich porovnání a výběr nejvhodnějšího z nich. Současně bude v práci řešena bezpečností otázka zvoleného systému a jeho celkové zabezpečení.

2.1 Přínosy inteligentní domácnosti

K hlavním výhodám inteligentně řízené elektroinstalace v domácnosti patří přednastavené scénáře, díky nimž je možné přednastavit akce, které se odehrávají, když obyvatelé nejsou doma a z toho plynoucí i úspora energií – topení se zapíná až před příchodem osob a není nutné, aby se topilo celý den, nebo se během dne automaticky zatáhnout žaluzie, aby se vnitřek domu zbytečně nezahříval a nebylo nutné prostory ochlazovat klimatizací. Další z výhod je například zabezpečení a vzdálené monitorování celého objektu proti vniknutí, protipožárních systémů, regulace teploty či řízení osvětlení.

2.2 IoT a využití v každodenním životě

IoT (Internet of Things) nebo v překladu také Internet věcí, je skupina samostatných zařízení připojených na internet. Jedná se o zařízení, jakou jsou například domácí spotřebiče (lednička, pračka, televize, …) nebo osobní automobily. Tyto zařízení se připojí k internetu a žijí si svým životem (generují a následně odesílají velké množství dat, o kterých mnohokrát nemáme přehled ani nevíme, jak je s nimi dále naloženo). Na jednu stranu tyto zařízení člověku zpříjemňují běžný život (možnost ovládání hlasem, ovládání zařízení na dálku pomocí internetu), na stranu druhou nesmíme zapomínat na možné bezpečnostní hrozby, které při používání takovýchto zařízení vznikají.

Mezi výhody, které nám IoT přináší patří možnost propojení takovýchto zařízení do jedné sítě a její vzdálená správa a ovládání. V současné době si člověk mnohokrát ani neuvědomuje, kolik inteligentních věcí během dne použije anebo naopak, kolikrát je pro nás nepředstavitelné (nebo přinejmenším velmi nepohodlné a nepříjemné), že bychom se bez těchto zařízení měli obejít.

3 TEORETICKÁ VÝCHODISKA PRÁCE

Tato kapitola diplomové práce je věnována vysvětlení pojmů týkajících se problematiky inteligentní elektroinstalace. Ukazuje nejen její výhody a nevýhody, ale také druhy instalací, které se v dnešní době používají. Dále je popsáno možné přenosové prostředí včetně konkrétních topologií zapojení a představeny jednotlivé prvky inteligentního systému. Následně jsou uvedeny a popsány vybrané možnosti realizace inteligentního systému, představení řešení jednotlivých výrobců a v neposlední řadě i představení a popsání základních používaných modulů inteligentních systémů. Konec kapitoly je věnován vysvětlení pojmů tykajících se bezpečnosti, a to jak informační, síťové tak i fyzické, včetně přiblížení pojmů jako je analýza a řízení rizik včetně jejich postupů.

3.1 Klasická vs. inteligentní elektroinstalace

Nejprve si přiblížíme pojmy klasická a inteligentní elektroinstalace a poté budou popsány hlavní rozdíly mezi nimi.

3.1.1 Klasická elektroinstalace

Jedná se o standartní způsob, používaný ve většině domácností. Klasický způsob elektroinstalace propojuje osvětlení, topení, případně i pevné domácí spotřebiče. Celý systém rozvodů nepřenáší žádné informace, dokáže pouze sepnout obvod a tím koncovému zařízení dát stav zapnuto anebo vypnuto. Jakékoliv změny v této elektroinstalaci jsou velmi nákladné a vyžadují stavební úpravy (1).

3.1.2 Inteligentní elektroinstalace

Hlavním cílem inteligentní elektroinstalace je vytvoření komplexního automatizovaného systému, který je schopný řídit vytápění, osvětlení, spínání ventilace, zatahování či vytažení předokenních žaluzií a mnoha dalších funkcí v celém objektu. Důležitým parametrem při rozhodování o inteligentní instalaci je požadavek pohodlnosti a

jednoduchosti ovládání celého systému a samozřejmě při správném nastavení i úspora energie a zvýšení bezpečnosti. Při návrhu a výběru konkrétního řešení by měl být kladen důraz na vyváženost mezi funkčností a komfortním ovládáním – uživateli nebude pravděpodobně vyhovovat systém, který sice zvládne ovládat každý spotřebič v domě, ale uživatelské prostředí bude tak nepřehledné a složité na ovládání, že výsledný pocit při užívání bude spíše negativní (1).

3.1.3 Výhody a nevýhody

U klasické elektroinstalace je výhodou jednoduchá instalace a současně i finanční nenáročnost. Navíc si v dnešní době můžeme pro realizaci zvolit z nepřeberného množství firem a živnostníků, kteří jsou schopni instalaci provést bez větších problémů.

Jako nevýhodu bychom mohli uvést zejména náročnost při změnách v elektroinstalaci. Je nutné počítat i se stavebními úpravami a pokud se jedná o složitější instalace nastává problém s nepřehledností (mnoho kabelů) (1).

Pokud se bavíme o inteligentní elektroinstalaci hlavní výhody jsou například vyšší komfort při používání – ovládání celého domu jednoduše a rychle přes aplikaci v mobilní zařízení. Další z výhod je automatizace celého systému a přednastavení scénářů – dle nastavení je například automaticky hlídána teplota, v případě že v místnosti klesne pod nastavenou teplotu, automaticky se zapne topení. S těmito funkcemi jde ruku v ruce i další z výhod, a to je úspora energie (1).

Největší nevýhodou inteligentní elektroinstalace je její pořizovací cena, která je mnohem vyšší než v případě elektroinstalace klasické. Další z nevýhod může být relativně malý počet firem poskytující instalaci a nákladnější materiál, který musí být při realizaci použit (1).

3.2 Kritéria pro klasifikaci

Pro dělení inteligentních elektroinstalačních systémů můžeme použít tyto tři základní kategorie: otevřenost systému, centralizovanost systému a komplexnost celého systému.

3.2.1 Otevřenost systému

Podle závislosti konkrétního systému na výrobci můžeme systémy rozdělit do dvou kategorií na uzavřené a otevřené systém.

Uzavřené systémy, pro které je charakteristická specifická komunikace prvků a fungování systému, které není kompatibilní řešením od jiných výrobců. Takovéto systémy jsou vhodnější zejména pro menší realizace jako jsou domy a byty, případně menší budovy a nejsou vhodnou volbou pro realizaci rozsáhlých projektů (2).

Jedná se například o systémy Loxon, iNELS, Somfy nebo ABB free@home.

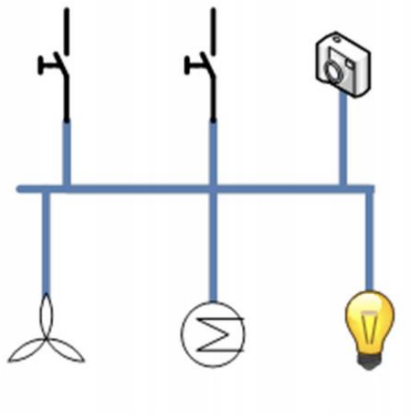
Otevřené systémy jsou založeny na otevřeném standardu a specifikacích – znamená to, že jakákoliv firma může vyrábět produkty, které pro komunikaci využívají tento standard (prvky od různých výrobců jsou kompatibilní a mohou se použít v rámci instalace jednoho systému). Aby produkt dostal certifikaci, je nutné, aby měl registraci a byla otestována jeho kompatibilita v testovacím centru. Díky mnoha výrobcům jsou na trhu dostupné různé zařízení, která se liší nejen designem a funkcemi ale zejména i cenou. Otevřené systémy jsou vhodné pro rozsáhlé realizace jako mohou být hotely, školy a podobně (2).

Jedná se například o standard KNX.

3.2.2 Centralizovanost

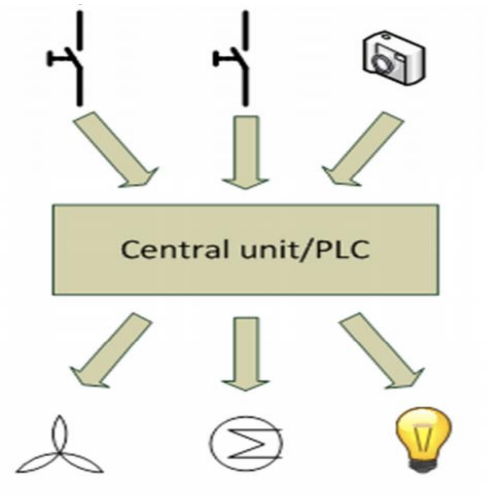
Systémy inteligentní elektroinstalace lze třídit i dle centralizovanosti, a to na decentralizované anebo centralizované.

Decentralizovaný systém je takový, ve kterém není žádná centrální řídící jednotka, která by spojovala jednotlivé prvky a starala se o jejich řízení. Řízení probíhá přímo u inteligentních senzorů, které mají integrovanou řídící jednotu. Hlavní výhodou decentralizovaného systému je, že při výpadku některého zařízení nedojde k funkčnímu ovlivnění ostatních. Jednotlivé zařízení na sobě totiž nejsou nijak závislá. Bohužel cena takového systému je několikanásobně vyšší oproti centralizovanému. Jedná se například o systém standardu KNX (mezinárodní norma ISO/EIC 14543, evropská norma EN 50090) (2).



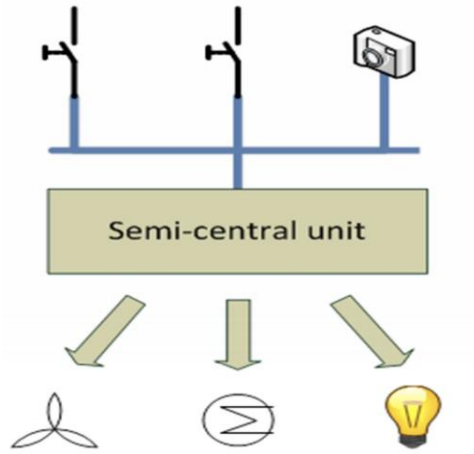
Obrázek č. 1: Decentralizovaný systém (Zdroj: 2)

Centralizovaný systém je systém, který je řízen jednou řídící jednotkou, nebo v některých případech i několika, které mají za úkol ovládat všechna připojená zařízení. Každé zařízení v takovémto systému musí být tedy přímo připojeno k řídící jednotce. Výhodou centralizovaných systémů je nižší pořizovací cena oproti decentralizovaným (odpadají vysoké náklady na inteligentní senzory s integrovanou řídící jednotkou). Nevýhodou při použití tohoto řešení je případ výpadku řídící jednotky – v tomto momentě se celý systém stává nefunkčním. Centralizované systémy jsou například Loxone a iNELS (2).



Obrázek č. 2: Centralizovaný systém (Zdroj: 2)

Polocentrální systém je systém, u kterého jedna část je centralizovaná a druhá decentralizovaná. V takovémto systému jsou vstupy připojeny nezávisle a výstupy jsou ovládány pomocí polocentrální řídící jednotky (případně více jednotek) (2).



Obrázek č. 3: Polocentrální systém (Zdroj: 2)

3.2.3 Komplexnost

Komplexnost systému znamená, zda je systém určen pro ovládání celé domácnosti (komplexní systém) anebo je určen jen pro jednu specifickou oblast, například řízení osvětlení (2).

3.3 Přenosové prostředí

V sítích obecně existují tři základní přenosové prostředí, kterými jsou metalické kabely, optické kabely a vzduch. V metalických kabelech jsou data přenášeny pomocí elektrického proudu, u optických kabelů hovoříme o přenosu pomocí světelných impulsů a u bezdrátového přenosu jsou data přenášena pomocí elektromagnetického vlnění (3).

3.3.1 Metalické kabely

Metalický kabel se skládá ze 4 párových kabelů. Metalické vodiče jsou chráněny nevodivým pláštěm a všechny 4 páry jsou spojeny pláštěm do jednoho kabelu. Podle konstrukce můžeme kabely rozdělit na nestíněné a stíněné (3).

- Unshielded Twisted Pair – UTP – párový kabel nestíněný, levnější varianta oproti ostatním kabelům, díky chybějícímu stínění není vhodný pro prostředí kde se může vyskytovat rušení,
- Foil Shielded Twisted Pair – FTP – párový kabel stíněný fólií, vysoká účinnost stínění,
- Shielded Twisted Pair – STP – párový kabel stíněný opletením, nižší účinnost stínění,
- Individually Shielded Twisted Pair – ISTP – párový kabel s individuálním stíněním jednotlivých párů – páry stíněny fólií, celkově stíněno opletením (3).

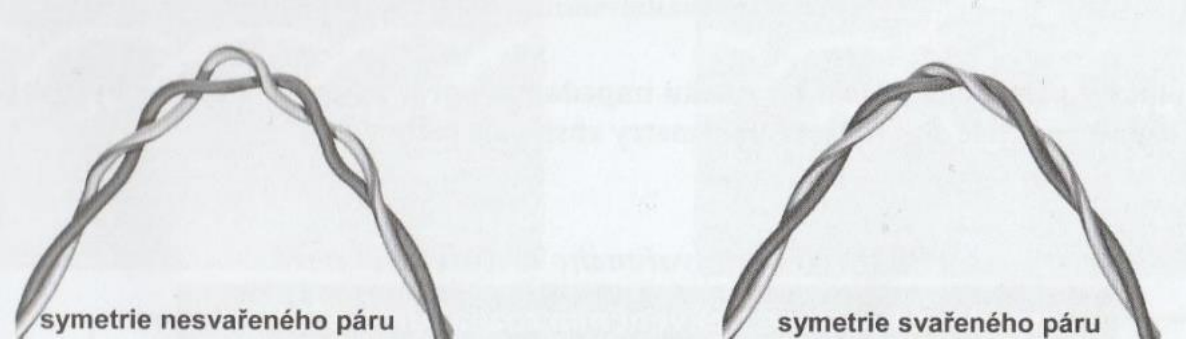
V prostředí, kde se může vyskytovat elektromagnetické rušení, je vhodné použití stíněných kabelů, aby nedocházelo k rušení přenášeného signálu a přeslechům. Pro správnou funkci stínění je nezbytné, aby veškeré použité prvky v kabelážním systému byly taktéž stíněné, při instalaci byl brán ohled na maximální poloměr ohybu kabelu a stíněná kabeláž musí být vždy uzemněna v datovém rozvaděči (3).

Další parametr, dle kterého můžeme kabely dělit je dle konstrukce párů vodičů.

Existují kabely s nesvařeným párem, u kterých jsou vodiče v páru pouze zakroucené. U těchto kabelů není možné zaručit konstantní symetrii párů, což může mít vliv na stabilitu

impedance. Ve výsledku to má za následek odrazy signálu, šumy a přeslechy které negativně ovlivňují přenášená data (3).

U kabelů se svařeným párem je dosaženo lepší podélné symetrie a přenosové parametry tak nejsou tolik ovlivněny. Velkou předností kabelů se svařenými páry je zachování veškerých parametrů i při ohybu či zkroucení kabelu (3).



Obrázek č. 4: Symetrie svařeného a nesvařeného vodiče (Zdroj: 3)

3.3.2 Optické kabely

Uvnitř optického kabelu je uloženo skleněné vlákno (někdy může být i platové, či kombinace skla a plastu), kterým se přenáší informace pomocí světelného paprsku. Základem je jádro a neoddělitelný plášť, který funguje jako odrazová vrstva. Data jsou přenášena na základě různého indexu lomu světla. Optické vlákno má dále vždy primární vrstvu, která zamezuje vlhkosti a chemickým vlivům. Vzhledem k tomu, že tato vrstva nefunguje jako mechanická ochrana vlákna, proto bývá dále ještě těsná sekundární ochrana, která je tvořena plastovou bužírkou anebo volná sekundární ochrana, které je tvořena gelem v ochranné trubičce (3).

Největší výhoda optických vláken je velká přenosová rychlost i na obrovské vzdálenosti a také odpadají problémy s rušením a přeslechy, které jsou u metalické kabeláže (3).

U optických vláken rozlišujeme dva přenosové režimy.

- Single Mode – SM – jedno vidový, index lomu je skokový, je nutné použít vlnovou délku světla 1310 - 1550nm (někdy se používají i jiné vlnové délky jako např. 1490nm nebo 1590nm, popřípadě jejich mix). Světelný paprsek se šíří v ose jádra a k odrazům dochází pouze v ohybu kabelu (3).
- Multi Mode – MM – mnoha vidový, tyto vlákna mohou mít buďto skokový index lomu anebo gradientní, při kterém se paprsky nejen odrážení ale dochází k plynulé změně a jsou tak ohýbány. Pro tyto vlákna se obvykle používá vlnová délka světla 850 - 1300nm (3).

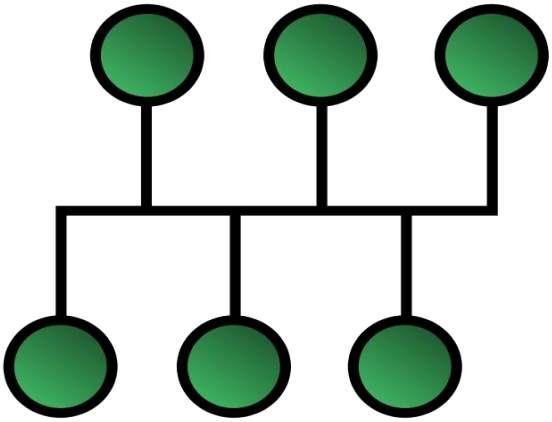
3.4 Topologie sítě

Topologie je způsob uspořádání jednotlivých prvků v síti – jak jsou jednotlivé prvky propojeny.

Topologie může být fyzická nebo logická. U fyzické topologie se jedná o skutečné uspořádání a zapojení prvků, u logické topologie se jedná o způsob propojení jednotlivých prvků. Logická topologie může být tedy odlišná od fyzického vedení kabeláže. Základní topologie jsou lineární, kruhová a hvězda. V běžné praxi se velmi často vyskytují kombinace těchto topologií (5).

3.4.1 Lineární/sběrnicová

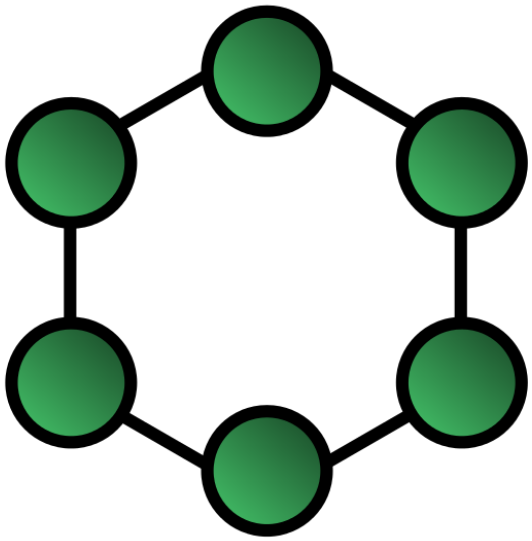
Jedná se o nejstarší, ale také nejjednodušší způsob propojení jednotlivých prvků – všechny jsou propojeny sériově, pomocí jednoho hlavního kabelu. Pokud dojde k poruše jednoho zařízení, znamená to automaticky výpadek celé sítě (5).



Obrázek č. 5: Sběrnicová topologie (Zdroj: 4)

3.4.2 Kruhová

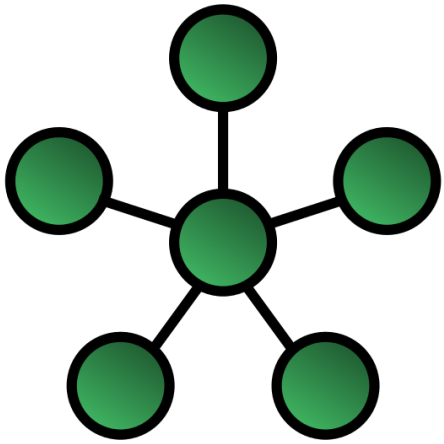
Kruhová topologie – zařízení jsou lineárně zapojena do kruhu. Není zde žádný centrální prvek a při výpadku jednoho prvku není nijak ovlivněna funkčnost zbytku sítě (5).



Obrázek č. 6: Kruhová topologie (Zdroj: 4)

3.4.3 Hvězda

U této topologie jsou všechny zařízení připojena do jednoho centrálního uzlu. Pokud dojde k poruše jednoho zařízení, nemá to žádný vliv na zbytek sítě. Pouze pokud by došlo k poruše v centrálním uzlu, znamenalo by to výpadek celého systému (5).



Obrázek č. 7: Topologie hvězda (Zdroj: 4)

3.5 Prvky inteligentního systému

Každý inteligentní systém je na základě požadavků investora složen z různých prvků. Mezi základní prvky, které systémy obsahují patří následující.

3.5.1 Centrální jednotka

Hlavní (centrální) řídící jednotka je základem centrálních nebo polocentrálních systémů. Jedná se o prvek, který řídí činnost ostatních prvků v systému a komunikuje s nimi. Po úspěšné instalaci systému je možné centrální jednotku připojit, ovládat i programovat přes lokální síť (LAN) (5).

3.5.2 Aktory

Jedná se o zařízení, provádějící naprogramované úkony. Spínají či regulují jednotlivé okruhy jako jsou například topení, osvětlení, rolety atd. Jednotlivé zařízení jsou schopny mezi sebou komunikovat a existují i zařízení fungující jak jako aktor tak i jako senzor a je díky nim možné ovládat více funkcí. Rozlišujeme binární, které detekují dvě hodnoty (někdy nazývané také jako pulsní) a analogové (6).

3.5.3 Senzory

Senzor je v podstatě snímač, který posílá informace do centrální jednotky a na základně vyhodnocení přijatých informací dává centrální jednotka další pokyny jiným částem systému. Mezi nejpoužívanější senzory patří: detektory pohybu, požádání detektory, teplotní senzory, senzory vlhkosti, venkovní senzor pro měření síly větru a další (7).

Detektory pohybu

Jsou to senzory, které rozpoznají jakýkoliv pohyb ve snímané oblasti. Detektory můžeme dělit na pasivní a aktivní (8).

Pasivní detektory jsou ty, které mají pouze přijímač, a jejich funkce je pouze zaznamenání změn (akustického/elektromagnetického vlnění) které jsou vyvolány pohybem tělesa ve sledované oblasti (8).

Aktivní detektory mají na rozdíl od pasivních nejen přijímač, ale i vysílač. Vytvoří si tak vlastní akustické/elektromagnetické pole které přenesou do střežené oblasti a reagují na změny v tomto jimi vytvořeném poli (8).

- Passive Infrared Senzor – pasivní infračervený senzor slouží k zaznamenávání změn v infračerveném pásmu elektromagnetického vlnění. Jedná se o snímač, který zaznamená teplotní změny, které následně vyhodnotí a pokud je zaznamenán pohyb – detekce funguje při zaznamenání teploty odlišné od okolního prostředí. U těchto senzorů mohou nastat falešné poplachy v případě např. při proudění vzduchu z

klimatizace, prudkých teplotních změn vyvolaných např. zapnutím topení, pohybu zvířat apod. (9).

- Active Infrared Senzor – aktivní infračervený senzor funguje na stejném principu jako pasivní senzory, liší se tím, že do sledované oblasti vysílá signál, který následně přijme zpět a vyhodnotí ho. Pokud je signál mezi přijímačem a vysílačem narušen, spustí se poplach (9).

- Ultra Sonic Senzor – aktivní ultrazvukové senzory pracují tak, že vysílají konstantní signál, který je pro člověka neslyšitelný. Signál se odráží zpět a jsou vyhodnoceny změny jeho amplitudy, frekvence a fáze. Poplach je spuštěn při zjištění změny v odraženém signálu (9).

- Microwave Senzor – mikrovlnné senzory fungují na obdobném principu jako ultrazvukové, jen využívají elektromagnetické vlnění. Jedná se o vysokofrekvenční signál v pásmu 9 až 11 GHz. Senzor vyhodnocuje změny a funguje na principu změny délky elektromagnetických vln, které jsou vyvolány pohybem zdroje a narušitele (9).

Kombinované senzory jsou určeny pro snížení nežádoucích vlastností výše popsaných senzorů. Je zde zkombinována technologie a prostor je pozorován dvěma částmi senzoru. Pokud nedojde k současnému zaznamenání narušení oběma částmi, poplach se nespustí – takže nedojde k falešnému poplachu (9).

Detektory destrukce skleněných ploch

Mezi nejčastější řešení patří poplachové fólie a skla, foliové polepy nebo pasivní detektory. Tyto detektory mohou být umístěny na povrchu (na rámu), kde je číslo viditelné, nebo zapuštěné přímo v rámu okna (v tomto případě je nutné instalace již při výstavbě – kabel musí být protažen rámem) (10).

Poplachové fólie a skla aktivují poplach, pokud dojde k přerušení vodivého kontaktu, který je umístěn po celé ploše skleněné výplně, která má být chráněna (10).

Foliové polepy fungují obdobně jako poplachové fólie, jen s rozdílem, že vodivým prvkem je hliníková vodivá fólie, která se umisťuje po obvodu chráněné skleněné výplně (10).

Pasivní detektory rozbití skla jsou nalepeny na sklo. Umisťují se do dolní části plochy a při pokusu o rozbití (či přímém rozbití) dochází k rozpohybování tabule a vím i generování střídavého napětí – tento stav je vyhodnocen jako narušení a je spuštěn poplach (10).

Požární detektory

Tyto detektory odhalí a upozorní na výskyt kouře, a tak může být včas odhalen začínající požár. Nejčastěji se používají tyto druhy:

- Tepelné – které vyhodnocují teplotu anebo její změnu během času. Může nastat situace, že při průvanu nebude teplo z ohně zaznamenáno a poplach tak nebude spuštěn. Z tohoto důvodu se doporučuje použití kombinovaných detektorů (jak tepelného, tak i kouřového), u kterých postačuje, že neshodu zaznamenal jeden ze senzorů (11).
- Optické – tyto detektory mají komůrku, která je prosvětlována diodou jejíž svit je snímán na protější straně senzorem a v případě narušení signálu spustí poplach. Tento typ detektorů není odolný proti prachu a detektory nejsou schopny zachytit malé částice, které vznikají například z rychle hořících ohňů (tyto ohně generují pouze maličké kouřové částice) (11).
- Ionizační detektory – mají komoru, ve které nepatrné množství radioaktivního materiálu ionizuje vzduch. Touto komorou prochází také elektrický proud mezi dvěma elektrodami – při vniknutí kouře do prostoru komory dochází ke zpomalení pohybu iontů. To má za následek přerušení elektrického proudu a dochází ke spuštění poplachu (11).

Senzory vlhkosti

Tyto senzory využívají změnu vlastností materiálů na absorpci vody z vodní páry a mezi nejčastěji používané patří odporové nebo kapacitní (12).

Odporové senzory využívají vodivost a změny posuzují na základě změn elektrického odporu. Tyto senzory jsou přesné a stabilní (12).

Kapacitní senzory fungují principiálně jako kondenzátory. Tyto senzory jsou relativně velmi málo závislé na teplotě a mají dobrou dobu odezvy (12).

Teplotní senzory

Fungují na principu fyzikálního převodu a dělíme je na:

- Odporové – senzory, které jsou nejčastěji používané a fungují na principu změn odporu kovu při změně teploty,
- Odporové polovodičové – taktéž využívající změny odporu při změně teploty,
- Termoelektrické – tyto senzory nepotřebují vnější napájení a pracují při pokojových teplotách, využívají principu převodu tepelné energie na elektrickou (12).

Další senzory mohou být například: optické, krystalové, akustické, magnetické, chemické, kapacitní atd. (12).

Senzory měření rychlosti větru

Mezi nejrozšířenější používané přístroje pro měření větru jsou mechanické anemometry. Jejich součástí je část, kterou vítr svojí silou otáčí či vychyluje z klidové polohy. Dle typu je dělíme na miskové, lopatkové anebo s výkyvnou deskou (13).

Snímací zařízení

Inteligentní zařízení obsahuje paměť (včetně přístupových údajů) díky které může rozhodovat o přístupu zcela samostatně a nezávisle. Řídící jednotka v tomto případě zasílá pouze aktualizované přístupové údaje a ukládá data o provedených transakcích (9).

Neinteligentní zařízení slouží pouze k předávání zadaného kódu řídící jednotce, která vyhodnocuje a rozhoduje o přístupu (9).

Polointeligentní zařízení předává řídící jednotce informaci s žádostí o rozhodnutí povolení přístupu a čeká na vyhodnocení (9).

3.5.4 Napájení

Zdroj napájení plní funkci přívodu elektrické energie ke všem prvkům. Bez dostatečného napájení prvků nebude systém stabilně fungovat a je proto nezbytné na to při návrhu systému nezapomínat a počítat i s rezervou (5).

3.6 Systém inteligentní elektronické instalace KNX

KNX je otevřený světový standard, který byl vyvinut přímo pro účely automatizace budov. Díky němu je možné jednotné ovládání regulace všech technologií v bodově jako je například topení, chlazení, větrání či osvětlení. Mezi největší výhody patří otevřenost – existuje mnoho výrobců, kteří nabízí zařízení fungující dle tohoto standardu. Uživateli tak vzniká obrovské množství volby nejen dle designu ale i funkčnosti a na rozdíl od ostatních firem zabývající se inteligentními systémy je možné kombinovat zařízení několika výrobců – pokud jsou zařízení certifikována, je zaručena vzájemná kompatibilita. Další z výhod je decentralizovaná struktura – neexistuje centrální jednotka a není tak možné, aby došlo k výpadku celého systému (14).

Obrázek č. 8 Logo standardu KNX (Zdroj: 14)

3.6.1 KNX secure

Z důvodu stále více kladené pozornosti na zabezpečení systémů byl vytvořen produkt KNX Secure – jedná se o zařízení, které klade důraz ne zvýšenou ochranu přenášených dat. Tento produkt nabízí dva způsoby ochrany – IP secure chrání IP komunikaci a Data secure chrání komunikaci přenášenou médii od přístroje k přístroji. Tyto dva způsoby lze samozřejmě i zkombinovat pro dosažení ještě vyšší bezpečnosti. Tyto přístroje jsou zacíleny na ověřování a šifrování komunikace ale lze je pohodlně začlenit do již existující instalace – není nutné žádných velkých zásahů a změn (14).

3.7 Dostupné systémy pro řešení inteligentní elektroinstalace

V dnešní době je na trhu k dispozici již relativně velký výběr výrobců inteligentních systémů pro řízení domácnosti. Při rozhodování a volbě nejvhodnějšího je nutné vždy vycházet z konkrétních požadavků daných investorem a najít řešení, které jim bude nejvíce vyhovovat. Pro účely této práce byly vybrány pouze některé systémy, které již na první pohled splňují funkčně (a současně i finančně) požadavky na instalaci v rodinném domě. Zvolili jsme centralizované systémy s řídící jednotkou, kterou je programovatelný logický automat (Programmable Logic Controller – PLC).

3.7.1 iNELS

Systém může být postaven na sběrnicovém (klasická instalace do zdí) či bezdrátové řešení, které je vhodné, pro již hotové budovy, ve kterých takto nejsou nutné stavební úpravy. K centrální jednotce pro sběrnicovou elektroinstalaci je možné připojit 2x32 jednotek a další jednotky je možné připojit pomocí rozšíření. Modul je určen k instalaci na DIN lištu. Systém je možné ovládat přes dotykový panel či smart zařízení (mobil, tablet, televize) (15).

Obrázek č. 9: Hlavní řídící jednotka systému iNELS (Zdroj: 15)

3.7.2 LOXONE

Řídící jednotkou systému LOXONE může být Miniserver (drátový) anebo Miniserver Go (bezdrátové řešení). Obě varianty jsou funkčně velmi podobné, bezdrátová má výhodu při instalaci do hotového interiéru – není potřeba zasahovat do zdí. Pro projekt novostavby použijeme klasické řešení Miniserveru, který by byl umístěn na DIN lištu. Tento Miniserver by tedy komunikoval se všemi vstupními i výstupními prvky. Dokáže pojmout 8 spínaných výstupů (např. žaluzie, světla), 8 digitálních vstupů (tlačítka, dveřní a okenní kontakty), 4 analogové vstupy (snímače teploty, vlhkosti), 4 analogové výstupy a je možné jej rozšířit až o 30 dalších rozšiřujících jednotek. Systém je možné ovládat pomocí bezplatné aplikace Loxone App a pro konfiguraci systému je dostupný bezplatný software Loxone Config (16).

Obrázek č. 10: Řídící jednotka Loxone Miniserver (Zdroj: 16)

3.7.3 Somfy

Řídící jednotkou od Somfy systém TaHoma®. Jedná se o bezdrátové řešení, které zvládne propojit veškeré ovládané jednotky. Systém je možné ovládat pomocí mobilní aplikace nebo dálkovým ovladačem na základě bezdrátové technologie io-homecontrol®. Výhodou systému TaHoma® je kompatibilita s mnoha výrobci jako např. Honeywell, Philips, Velux a mnoho dalších. Systém je možné postupně rozšiřovat předáváním nových modulů (17).

Obrázek č. 11: Hlavní bezdrátová jednotka Somy (Zdroj: 17)

3.7.4 ABB free@home

Systém společnosti ABB, který se ovládá skrze systémový modul, ke kterému je možné bezdrátově připojit počítač nebo mobilní telefon. Hlavní důraz je kladen na jednoduchost ovládání. Pro konfiguraci je využit vlastní software umístěný přímo v systémovém modulu – není potřeba instalovat další nástroje, kdykoliv se dá nastavení uložit anebo obnovit. Společnost uvádí dvě varianty řešení instalace – centralizovanou a decentralizovanou. Při bližším prozkoumání ale dojdeme k zjištění, že se jedná o dvě různé decentralizované varianty. U obou variant je možné do systému připojit až 64 zařízení (18).

Obrázek č. 12: Systémový modul ABB free@home (Zdroj: 19)

3.7.5 Porovnání vybraných systémů

Mezi hlavní kritéria pro porovnání vybraných systémů byly vybrány možné funkce systému, možnost ovládání a také provedení. Při výběru byl také brán zřetel na možnosti přizpůsobení systému a zejména na uživatelskou přívětivost (intuitivní ovládání, aplikace pro různé platformy mobilních zařízení).

Při porovnávání systémů jsme se řídili dle požadavků investora na funkčnost a podporované funkce. Požadované funkce byly vybrány na základě konzultace s investorem. Detailní porovnání požadovaných funkcí systémů je v následující tabulce.

Na základě srovnání lze říct, že nejlépe vyhovují požadavkům investora systémy Loxone a iNELS, které splňují veškeré požadované funkce.

Tabulka č. 1: Porovnání vybraných systémů (Zdroj: vlastní zpracování)

Funkce	Systém			
	iNELS	Loxone	Somfy	ABB
Provedení				
bezdrátové provedení	✓	✓	✓	×
drátové provedení	✓	✓	×	✓
možnost integrace zařízení systému KNX	✓	✓	×	×
Ovládání				
webové rozhraní	✓	✓	✓	✓
aplikace pro zařízení na platformě Android	✓	✓	✓	✓
aplikace pro iPhone	✓	✓	✓	✓
aplikace pro iPad	✓	✓	✓	✓
Vytápění				
individuální regulace teploty v každé místnosti	✓	✓	✓	✓
propojení vytápění a chlazení	✓	✓	✓	✓
propojení s okny a žaluziemi	✓	✓	✓	✓
sledování spotřeby	✓	✓	×	×
Větrání				
větrání pomocí rekuperace	✓	✓	×	✓
regulace větrání dle teploty a kvality vzduchu	✓	✓	×	×
Stínění				
automatické zatažení/vytažení dle slunečního záření	✓	✓	✓	✓
automatické zatažení/vytažení po západu/východu slunce	✓	✓	✓	✓
Osvětlení				
stmívání	✓	✓	✓	✓
individuální nastavení pro každou místnost	✓	✓	✓	✓
nastavení scén	✓	✓	✓	✓
automatické zapnutí/vypnutí světla	✓	✓	✓	✓
automatické zapnutí/vypnutí světla při příchodu/odchodu	✓	✓	✓	✓
centrální ovládání světel	✓	✓	✓	✓
Energie				
měření spotřeby energie	✓	✓	×	×
inteligentní regulace vytápění a stínění	✓	✓	✓	✓
měření spotřeby jednotlivých spotřebičů	✓	✓	×	×
Zabezpečení				
vzdálený přístup a správa	✓	✓	✓	×
SMS upozornění	✓	✓	✓	×
individuální nastavení alarmu	✓	✓	✓	×
možnost propojení s kamerovým systémem	✓	✓	✓	✓
domácí video interkom	✓	✓	✓	✓
Senzory				
detektor kouře	✓	✓	✓	×
záplavový senzor	✓	✓	✓	×
vnitřní senzor teploty	✓	✓	✓	✓
senzor kvality vzduchu	✓	✓	×	×
senzor vlhkosti vzduchu	✓	✓	×	✓

3.8 Bezpečnost informací

Pojem bezpečnost informací se zabývá nejen ochranou informací ale i jejich dostupností. Bezpečnost informací zahrnuje zásady bezpečné práce s různými druhy informací. Nezabývá se tedy pouze informacemi v digitální formě, ale i ostatními typy - např. informacemi v papírové podobě). Součástí je i způsob zpracování dat a jejich uložení, správa a postupy pro likvidaci dat. Jedná se tedy o ochranu aktiv, ať jsou v jakékoliv podobě. Bezpečnost informací v IS/ICT má za cíl zajistit ochranu aktiv informačního systému (20).

3.9 Fyzická bezpečnost

Při zajišťování bezpečnosti je nutné dbát na zajištění prostředí a fyzického přístupu. Zařízení, pracující s citlivými informacemi by měli být umístěny v zabezpečeném prostředí, kam mají přístup pouze oprávněné a důvěryhodné osoby. Rozsah zabezpečeného prostoru je vymezen tzv. Bezpečnostních perimetrem. Při přístupu neoprávněných osob by mohlo dojít k narušení bezpečnosti a případnému poškození důvěryhodnosti informací (20).

Do fyzické bezpečnosti také spadá zabezpečení jednotlivých prvků infrastruktury s cílem předejít ztrátě, poškození či krádeži. U veškerých zařízení musí být dodržena ochrana proti bezpečnostním hrozbám (20).

Prvním krokem k zajištění bezpečnosti informací je tedy zajištění fyzické bezpečnosti nejen samotných prvků, ale i celého prostředí. Efektivní není chránit pouze prostředí nebo jednotlivé prvky, ale komplexní ochrana tvořená kombinací obou možností (20).

3.9.1 Bezpečnost prostředí

Bezpečnostní perimetr – jedná se o jasně definovanou a vymezenou oblast, která by měla být zabezpečena a monitorována,

Fyzická kontrola při vstupu – identifikace osob při vstupu do prostoru, který je zabezpečen, kontrola oprávnění těchto osob pro vstup,

Zabezpečení prostorů – vymezené prostory by měly být zabezpečeny a monitorovány, aby se eliminovala možnost neoprávněného přístupu (20).

3.9.2 Zabezpečení zařízení

Umístění zařízení zpracovávajících citlivé informace by mělo být vždy v zabezpečeném prostoru, který je vytyčeném bezpečnostním perimetrem (20).

Související zařízení, které mají za úkol zajistit ochranu před výpadkem napájení – nepřetržitá dodávka elektrické energie i při výpadku dodávek z elektrické sítě může být zajištěna například pomocí záložního zdroje UPS (20).

Bezpečnost kabelážního systému (rozvodů a kabelových tras) by měla být zajištěna nejen po stránce fyzického přístupu ke kabeláži ale také proti poškození a případnému vzájemnému elektromagnetickému rušení (20).

Oprava a servis včetně pravidelné údržby by měla být zajištěna oprávněnou osobou (osobami) a v případě podezřelého chování či výskytu neočekávané chyby musí být pořízený záznamy a tyto informace podrobeny analýze (20).

3.10 Bezpečnost sítě

Zabezpečení sítě je nutné pro ochranu zpracovávaných informací. V nesprávně zabezpečené síti by mohlo dojít k zachycení citlivých informací třetí stranou anebo k úmyslné změně či poškození důležitých informací. Zabezpečení sítě má za cíl ochránit vnitřní síť před hackerskými útoky, trojskými koni, červy apod. (20).

Pro zabezpečení sítě se nejčastěji používá antivirový program, firewall, detekční systémy, které jsou schopny rozpoznat narušení sítě a detekovat hrozbu ještě před jejím průnikem do sítě anebo VPN (20).

3.11 PDCA model

Jedná se o model postupného zlepšování kvality služeb, výrobků a procesů. Jedná se o opakování cyklu stále dokola, čímž je dosaženo neustálého zlepšování a vylepšování.

Tento cyklus je složen ze 4 činností: Plan (plánuj), Do (dělej), Check (kontroluj) a Act (jednej) (20).

V prvním kroku jde o naplánování vhodných změn či vylepšení stávajícího stavu, následuje provedení (implementace) těchto změn, kontrola výsledků a jejích srovnání s původním plánem, a nakonec fáze úprav původního plánu (20).

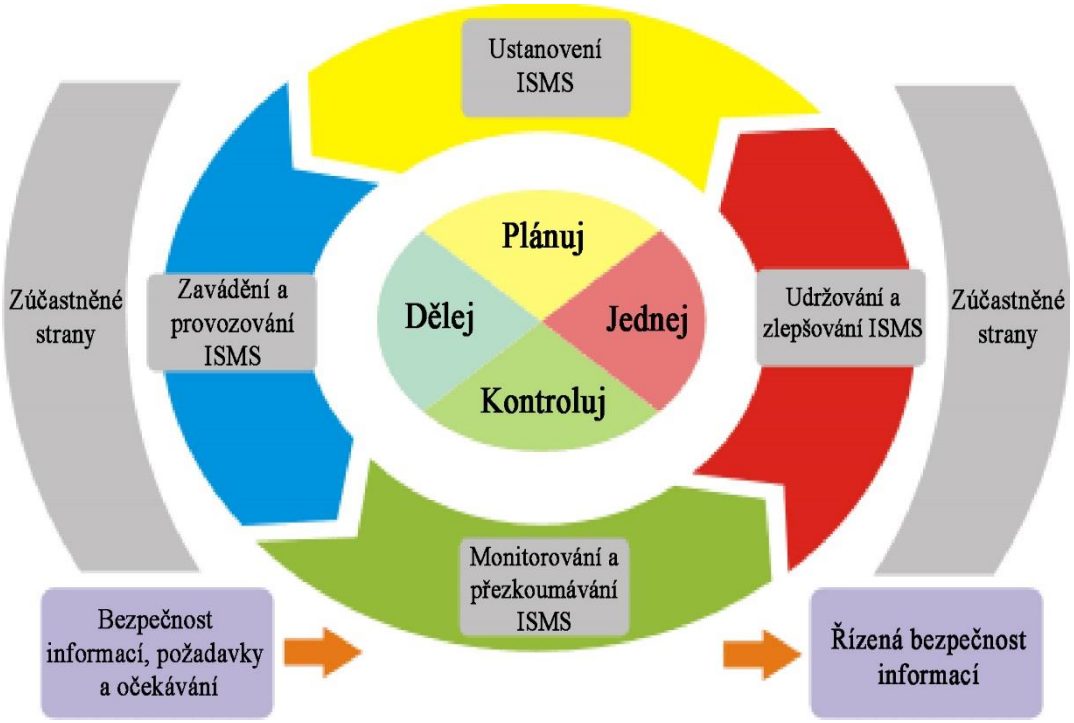
Velmi důležitou částí tohoto modelu je kompletní dokumentace každé etapy. Díky kompletní dokumentaci je možné sledovat průběh změn i výsledky jednotlivých kroků (20).

Obrázek č. 13: Model PDCA (Zdroj: 21)

3.12 Systém řízení bezpečnosti informací

Součástí systému řízení organizace by měl být Systém řízení bezpečnosti informací, tzv. ISMS (Information Security Management System). Cílem tohoto systému je ustanovení, zavádění a provoz, monitorování a přezkoumávání včetně údržby a zlepšování bezpečnosti informací v organizaci. Tento systém je založen na modelu PDCA a má taktéž čtyři fáze: ustanovení ISMS, zavádění a provozování, monitorování a přezkoumávání a následné udržování a zlepšování celého ISMS (20).

Celý životní cyklus modelu PDCA aplikovaného v ISMS je zobrazen na následujícím obrázku.



Obrázek č. 14: Životní cyklus modelu PDCA v ISMS (Zdroj: 20)

3.13 Normy zabývající se informační bezpečností

Oblast informační bezpečnosti pokrývají normy řady ISO/IEC 27000. Níže jsou popsány vybrané normy, věnující se bezpečnosti informační a síťové bezpečnosti, které souvisí s obsahem této práce.

ČSN ISO/IEC 27000

Jedná se o definici pojmů a ujasnění terminologie pro související normy z této řady.

První vydání této normy bylo v roce 2009, nyní prozatím poslední aktualizace je z roku 2018 (22).

ČSN ISO/IEC 27001

Tato norma poskytuje doporučení ohledně aplikace opatření v rámci procesu ustavení, provozu, údržby a zlepšování systému řízení bezpečnosti informace v organizaci, a to v souladu se systémy řízení kvality anebo bezpečnosti prostředí (ISMS). Norma zavadá model PDCA jako součást systému řízení bezpečnosti informací a také pokrývá kontinuální zajištění procesu zlepšování řízení bezpečnosti informací (25).

ČSN ISO/IEC 27005

Obsahuje doporučení pro řízení rizik bezpečnosti informací s ohledem na požadavky ISMS. V této normě jsou definovány činnosti řízení rizik jako jsou:

stanovení kontextu – vymezení základních podmínek pro řízení bezpečnosti informací, definování rozsahu, hranic a stanovení organizační struktury pro řízení rizik v organizaci, hodnocení rizik – identifikace a kvantifikace rizik, kvalitativní popis rizik a jejich prioritizace v souladu s kritérii a cíli hodnocení rizik, zvládání rizik – výběr vhodných protiopatření pro eliminaci, podstoupení anebo přesunutí rizika, definice plánu zvládání rizik, akceptace rizik – učinění rozhodnutí včetně zaznamenání rozhodnutí o akceptaci rizika i s odpovědností za toto rozhodnutí, seznámení s riziky – výměna či sdílení informací o rizicích, monitorování a přezkoumávání rizik – přezkoumání a monitorování rizik i jejich faktorů (26).

ČSN ISO/IEC 27033

Soubor norem obsahující doporučení pro implementaci protiopatřeních vztahujících se k bezpečnosti sítí (27).

3.14 Bezpečnostní událost

Bezpečnostní událost je situace, kdy v informačním systému či počítačové síti může dojít k selhání některého z opatřeních, což může mít následně vliv na informační bezpečnost. Každá bezpečnostní událost musí být důkladně vyhodnocena a klasifikována dle závažnosti a až po důkladném posouzení se rozhodně, zda se jedná o bezpečnostní incident nebo ne (20).

3.15 Bezpečnostní incident

Bezpečnostní incident je jedna nebo více bezpečnostních událostí, které nesou vysoké riziko narušení bezpečnosti nebo ohrožují hlavní či podpůrné procesy. Velmi důležité je správně identifikovat bezpečnostní incident a zvládnout jej odlišit od bezpečností události (20).

3.16 Bezpečnostní hrozby

Bezpečnostní incident, který může mít za následek poškození aktiva se nazývá bezpečnostní hrozba. Hrozby můžeme dělit dle původu po tří skupin:

- přírodní a živelné pohromy, mezi které můžeme zařadit zemětřesení, požáry či povodně,
- technické či technologické hrozby jako jsou poruchy počítačů či jiných technologických komponent v rámci IS/ICT,
- lidské hrozby, ať již úmyslné či neúmyslné poškození, vymazání souborů, čí situací zaviněných nedbalostí (20).

Mezi nejčasnější hrozby můžeme zařadit například:

Výpadek dodávky energií – v situaci, kdy dojde k přerušení dodávek elektrické energie může dojít k několika problémům, např.: k porušení integrity dat, selhání procesu zálohování, nefunkční klimatizace, která může mít za následek přehřátí a následné selhání hardwarových komponent apod.

Škodlivý software – pokud je systém infikován škodlivým softwarem může dojít k narušení autentizace i bezpečnosti informací,

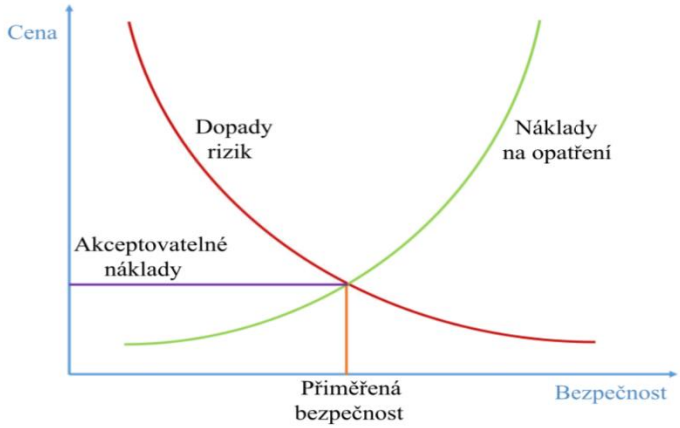
Selhání síťových prvků – při technické poruše v síti může nastat situace, kdy budou uchovávané či zpracovávané informace nedostupné či ztracené. Selhání může nastat z mnoha důvodů, například při nedostatečné údržbě zařízeních či umístěním prvků v nevhodném prostředí a vystavení tak nežádoucím vlivům (velké teplotní výkyvy, vlhkost nebo prach, …).

Pro eliminaci rizik slouží opatření proti hrozbám, které mají za cíl ochránit či alespoň zmírnit dopad bezpečnostních hrozeb. Opatření můžeme zařadit do jedné z kategorií: preventivní opatření, detekce, reakce anebo podpůrná opatření (20).

3.17 Úroveň bezpečnosti

Přiměřená bezpečnost je výsledkem posouzení velikosti dopadu rizika a velikosti vynaložených nákladů na opatření (20).

Určení přiměřené úrovně bezpečnosti vystihuje následující obrázek.



Graf č. 1: Graf pro určení přiměřené úrovně bezpečnosti (Zdroj: 20)

3.18 Analýza rizik

Rizika, související s konkrétním informačním systémem jsou zachycena v analýze rizik. Díky této analýze je možné identifikovaná rizika eliminovat a snížit je na přijatelnou úroveň. Existují také rizika, jejichž eliminace není možná, nebo je finančně příliš nákladná a nezbývá, než je přijmout a podstoupit (20).

Podle pravděpodobnosti výskytu dělíme rizika na:

- nahodilá
- nepravděpodobná
- pravděpodobná
- velmi pravděpodobná
- trvalá

Dále dle míry rizika rozdělujeme rizika do následujících kategorií:

- bezvýznamné riziko
- akceptovatelné riziko
- mírné riziko
- nežádoucí riziko
- nepřijatelné riziko

Bezvýznamná rizika, nebo též taky zanedbatelná jsou taková, která nevyžadují žádné zvláštní opatření a je sice nutné na tyto rizika upozornit, protože možnost tohoto rizika existuje, ale není nutné zavádět opatření – riziko přijmeme (20).

Akceptovatelná rizika – pokusíme se snížit riziko použitím technických opatřeních, pokud se nepodaří riziko takto snížit je potřebné zavedení vhodných a přiměřených opatření (20).

Mírná rizika, nebo též taky významná, jsou taková rizika, u kterých je potřeba realizovat bezpečnostní opatření pro snížení rizika (20).

Nežádoucí rizika jsou takové, u kterých je nezbytné neprodleně uskutečnit bezpečnostní opatření a snížit tak riziko na přijatelnou úroveň (20).

Nepřijatelné riziko je tak kritické riziko, u kterého je nutné provést nezbytná opatření, provést znovu vyhodnocení rizik a přijmout potřebná opatření (20).

Pro správnou analýzu rizik je důležité, vhodně si nastavit hranice, kterých prvků se bude analýza týkat a kterých již ne. Není totiž nutné analyzovat veškeré prvky, které pro konkrétní řešení nejsou důležité anebo se analýzy přímo netýkají (20).

3.18.1 Aktiva

Správně identifikovat aktiva je základní podmínkou pro úspěšnou analýzu. Aktivum je cokoliv, co má nějakou cenu. Aktiva můžeme dělit na hmotná a nehmotná (20).

Hmotná aktiva jsou prvky sítě – počítače, aktivní prvky, kabeláž apod.,

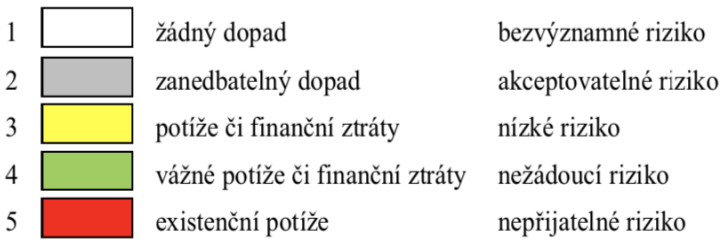
Nehmotná aktiva mohou být důležitá data, procesní postupy, software, který společnost využívá apod. (20).

Ohodnocení aktiv se provádí s použitím specializovaného programu, ale je možné použít i MS Excel. Pro ohodnocení aktiv je důležité sestavit kritéria pro ohodnocení a jejich stupnici, kde si vyjádříme, v jakých jednotkách budeme aktiva hodnotit (peněžní, kvantitativní, případně i kombinace obojího).

Pro správné ohodnocení aktiv je vhodné konzultovat hodnocením s vedením firmy, poněvadž hodnocení některých aktiv může být subjektivní – jedná se především o aktiva, která mají pro svého vlastníka vysokou hodnotu.

Pro zachování přehlednosti je vhodné hodnocení jednotlivých skupin i barevně odlišit.

Hodnotu aktiva zjistíme pomocí součtového algoritmu, který je pro vypočítání hodnoty aktiva jedním z nejpoužívanějších způsobů. Výpočet je jednoduchý, jedná se o součet hodnot dostupnosti, integrity a důvěrnosti a následným vydělením tohoto součtu číslem 3 (20).



Obrázek č. 15: Ohodnocení aktiv včetně barevného odlišení jednotlivých stupňů (Zdroj: 20)

3.19 Řízení rizik

Řízení rizik je složeno z několika fází, které na sebe vzájemně navazují a tvoří ucelený cyklus. Jedná se o identifikaci rizik, kvantifikaci a zvládnutí vybraných rizik. Pro zvládání rizik se nejčastěji používá metoda snižování rizika (20).

Prvním krokem je fáze, ve které je popsán proces řízení rizik – nebo také fáze stanovení kontextu. Určí se zde role a odpovědnost, kritéria a způsob kterým budou rizika hodnocena. V rámci tohoto kroku je také volba metodiky pro zvládání rizik (20).

Následuje analýza rizik, jejíž součástí je identifikování a ohodnocení aktiv, jejich zranitelnosti a stanovení míry rizika (20).

Poté, ve fázi vyhodnocení rizika, je stanovena priorita každého rizika jsou zvoleny vhodná opatření vedoucí ke snížení těchto rizik. Tato fáze hraje v procesu řízení rizik velmi důležitou roli (20).

Poslední z fází je rozhodování o vhodném způsobu zvládání rizik. Pokud hovoříme o možnostech zvládání rizik je na výběr z možnosti jejich retence, redukce, transferu, pojištění anebo vyhnutí se rizikům (20).

Každá fáze končí rozhodnutím, jaký způsob řešení bude zvolen. Pokud se jedná o nepřijatelné riziko, může dojít k vynucení zastavení procesu a zvolení opatření na snížení tohoto rizika. Ohledně zbytkových rizik, u kterých není možné zvolit opatření na jejich snížení je potřeba vypracování krizových plánů, aby bylo zdokumentováno, jak v případě nutnosti postupovat (20).

Obrázek č. 16: Cyklus fází řízení rizik (Zdroj: 20)

4 ANALÝZA SOUČASNÉHO STAVU

V této části se diplomová práce věnuje představení objektu, pro který je návrh sestaven a také požadavkům investora na celý systém. Dále je také uvedeno a představeno konkrétní řešení, které bylo na základě požadavků na vybráno a popsány hlavní funkce které budou použity.

4.1 Představení objektu

Jedná se o novostavbu rodinného domu, umístěnou na jihu města Brna v klidné městské části Brno – Přízřenice. Jedná se o jednogenerační rodinný dům, který bude mít dvě podlaží o celkové rozloze obytné plochy přibližně 220 m^2. V přízemí je umístěna vstupní hala, WC, kuchyně propojená s obývacím pokojem a garáž pro dva osobní automobily.

V prvním patře domu je hala, hlavní ložnice propojená s šatnou, technická místnost s kotlem, koupelna, dětský pokoj a pokoj pro hosty.

4.2 Stavebně technické řešení

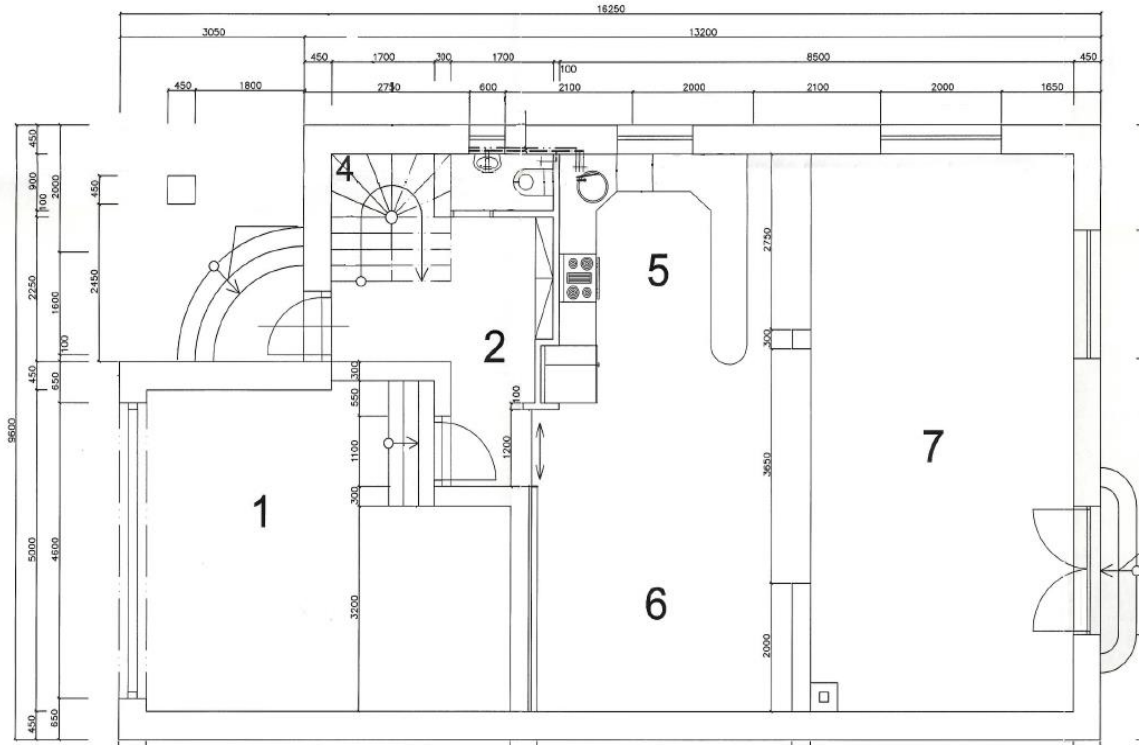
Obvodové a nosné zdi domu budou realizovány z klasických cihel, příčky mezi jednotlivými místnostmi jsou tvořeny z tvárnic Ytong. Celý dům bude zateplen skelnou vatou, aby byl co nejlépe izolován a nedocházelo k únikům tepla. V celém objektu (mimo garáže) bude instalováno podlahové topení.

4.3 Popis jednotlivých místností

Jednotlivé místnosti v domě, označené v půdorysu čísly, budou sloužit k následujícím účelům. Celý dům bude vytápěn pomocí podlahového vytápění (mimo garáže, která vytápěna nebude vůbec).

4.3.1 Místnosti – přízemí

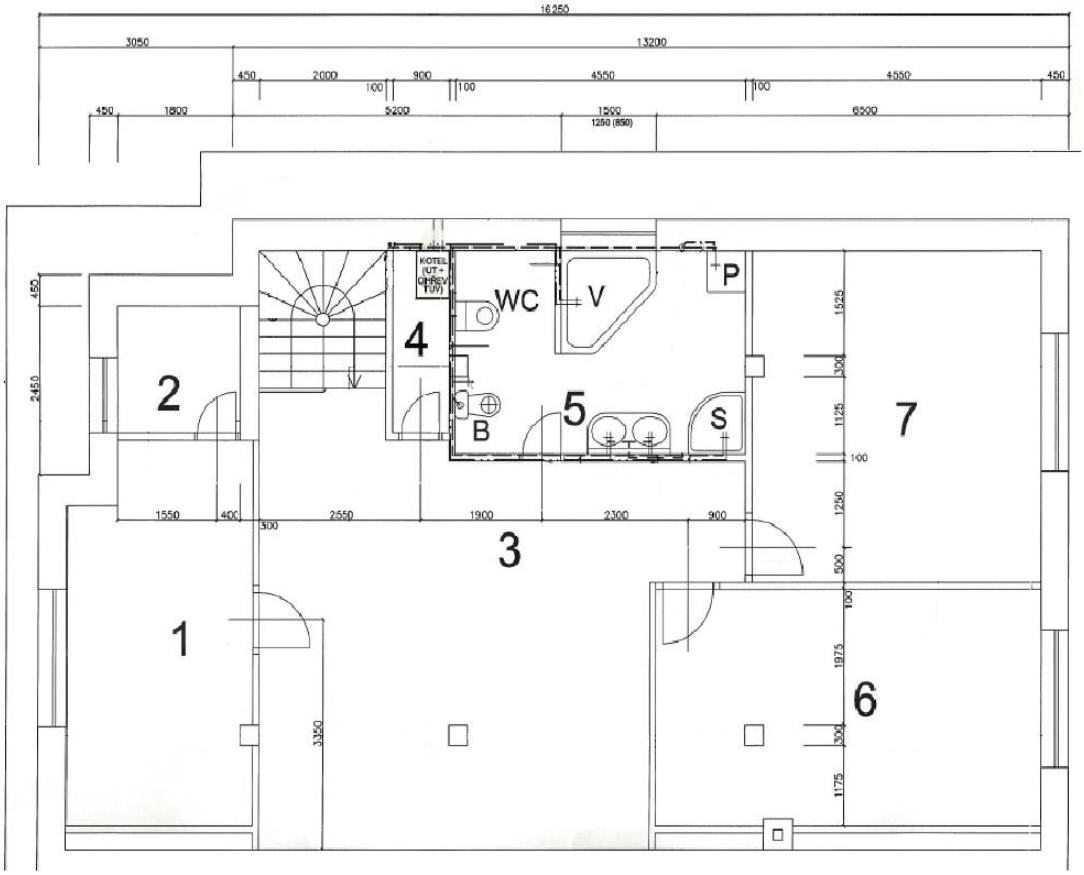
Garáž, v půdoryse označena číslem 1, má rozlohu 28 m^2 a primárně bude sloužit pro parkování aut a zahradního nářadí a v zadním rohu bude umístěn rozvaděč. Vstupní hala se schodištěm je v půdorysu označena číslem 2 a má rozlohu 9,8 m^2. Z této haly vedou dveře na WC (rozloha 1,5 m^2), dveře do garáže a vchod do kuchyně s jídelním koutem propojeným s obývacím pokojem. Kuchyně má rozlohu 16,9 m^2 (v půdorysu číslo 5), jídelní kout s rozlohou 20,6 m^2 (číslo 6) a obývací pokoj o celkové rozloze 47 m^2(v půdoryse označeno číslem 7).



Obrázek č. 17: Půdorys přízemí (Zdroj: projektová dokumentace investora)

4.3.2 Místnosti - 1. patro

Po vystoupáním schodištěm do 1. patra se ocitneme v hale o rozloze 40,3 m^2 (označena číslem 3). Místnost označená číslem 1 je ložnice s rozlohou 15,8 m^2, z ní vedou dveře do šatny (číslo 2), která má rozlohu 3,6 m^2. Další místnost v 1. patře je označena číslem 4 a jedná se o technickou místnost s kotlem s výměrou 2,4 m^2. Číslem 5 je označena koupelna o celkové výměře 13,4 m^2. Dětský pokoj je označen číslem 7 a má rozlohu 21,8 m^2. Poslední místnost v prvním patře je pokoj pro hosty označený číslem 6 o rozloze 20,9 m^2.



Obrázek č. 18: Půdorys 1. patro (Zdroj: projektová dokumentace investora)

4.4 Požadavky investora

Investor požaduje zejména jednotný systém pro ovládání celého domu a jeho komfortní ovládání. Důraz má být kladen na zabezpečení celého objektu a také na snížení nákladů na provoz domu (úspora spotřeby energie).

Dále jsou požadovány: automaticky ovládané žaluzie z důvodu uchování teploty uvnitř (zejména v létě využití stínění pro zachování chladu), regulace vytápění, regulace osvětlení a včetně možnosti stmívání světel v místnostech číslo 6 a 7 (jídelní kout a obývací pokoj) a elektronický zabezpečovací systém, který bude aktivován při odchodu a deaktivován při příchodu. Na každém patře má být umístěn jeden detektor kouře, u myčky nádobí a pračky i senzor zatopení. Přístup do domu bude zajištěn díky elektrickému zámku vstupních dveří, případně přes garáž.

Současně je požadováno ovládání celého systému skrze aplikaci na chytrém zařízení (telefony, tablety) a umožnění monitorování zabezpečovacího systému na dálku.

Mezi další požadavky patří pokrytí WiFi signálem obou pater, datová zásuvka v obývacím pokoji a datová zásuvka umístěná v 1. patře v hale pro připojení stolního počítače a tiskárny.

V neposlední řadě je požadován kvalitní a nadčasový kabelážní systém. Celková cena celého systému by se měla pohybovat do 350 000 Kč.

4.5 Výběr konkrétního systému a jeho představení

V současné době je na trhu mnoho výrobců a je nutné pečlivě zvážit výběr nejvhodnějšího řešení pro konkrétní realizaci. Nejvhodnější řešení již byly představena v kapitole 3.7 této práce. Z těchto systémů byl po pečlivém zvážení a konzultaci s investorem vybrán systém Loxone, který se jeví jako nejvhodnější volba pro tento projekt.

4.6 Popis použitých funkcí

4.6.1 Vytápění a větrání

Uvnitř objektu budou v jednotlivých místnostech umístěna teplotní čidla. Inteligentní regulace vytápění zajistí, že bude dům vytápěn v přednastavených intervalech. Vzhledem ke zvolenému způsobu vytápění domu (podlahové vytápění) není možné regulovat teplotu přímo v každé místnosti pomocí fyzického ovladače, nicméně centrální ovládání umožňuje nastavení a regulaci teploty pro každý vytápěný okruh (okruhy rozděleny stejně jako jednotlivé místnosti) zvlášť přímo z centrálního ovladače případně v aplikaci pro chytré zařízení.

Otevření oken bude monitorováno a bude tak kontrolováno, aby nedošlo k situaci, kdy při odchodu z domu zůstanou některé okna otevřené a tím nebude zajištěna možnost regulace teploty (prostor by mohl být ochlazován či případně ohříván venkovním vzduchem a klimatizace či topení by se zbytečně neustále snažilo o dosažení optimální teploty).

4.6.2 Stínění venkovními žaluziemi

Princip automatického zatahování a vytahování předokenních venkovních žaluzií má za cíl udržet požadovanou teplotu uvnitř domu a snížit tak energetickou náročnost stavby. Nastavení bude přizpůsobeno potřebám obyvatelů domu a přes mobilní aplikaci bude možné kdykoliv toto nastavení upravit.

Po setmění budou venkovní žaluzie ve spodním patře (kuchyně a obývací pokoj mimo dveří na terasu) a současně i v prvním patře v ložnici, šatně, dětském pokoji a pokoji pro hosty automaticky zataženy. V přízemí je to zejména z důvodu zajištění soukromí, v pokojích určených ke spánku je důvodem zajištění klidného prostředí a tmy pro klidný a nerušený spánek. Ráno je možné nastavit konkrétní čas automatického vytažení jednotlivých žaluzií, případně provádět vytahování ručně pomocí tlačítka či aplikace.

Přes den, pokud se teplota uvnitř domu vyšplhá na předem stanovenou maximální teplotu, dojde k automatickému zatažení venkovních žaluzií. Je to z důvodu udržení optimální vnitřní teploty. Například v létě dochází k přehřátí pokojů sluncem a je nutné místnosti ochladit klimatizací, což vede k výším nákladům na energie. Naopak v zimě je vhodné, aby slunce pokoje vyhřívalo co nejvíce a mohly se tak ušetřit náklady spojené s vytápěním, proto žaluzie zůstanou celý den vytažené.

Celkové ovládání jednotlivých žaluzií bude možné pomocí tlačítek, které budou umístěny vždy v jednotlivých místnostech a samozřejmě je všechny žaluzie možné ovládat i přes mobilní aplikaci na chytrém zařízení.

4.6.3 Osvětlení prostor

Osvětlení každé místnosti bude řešeno pomocí světelných led zdrojů, které mají možnost regulace intenzity osvětlení. V systému bude možné přednastavit různé světelné scény, nebo ovládat a regulovat osvětlení přímo. Nastavení světelných scén je možné přes ovládací aplikaci.

4.6.4 Zabezpečení

Přístup do domu bude realizován pomocí čtečky iButton, ke které obyvatel domu přiloží svůj čip a na základě nastaveného oprávnění bude vpuštěn do domu. Díky tomu, že každý uživatel bude mít svůj el. klíč (iButton), je možné i přednastavit jednotlivé scény pro různé uživatele (např.: majitel domu se vrací z práce vždy až pozdě v noci – při odemčení dveří se automaticky rozsvítí světlo ve vstupní hale). Uživatel bude vpuštěn po úspěšné autentizaci a současně dochází k vypnutí pohybových senzorů, aby při vstupu nedošlo ke spuštění poplachu.

Pokud by došlo k neoprávněnému vniknutí do domu bude spuštěn poplach a odeslány informační SMS na přednastavené mobilní zařízení. Systém je možné připojit i na bezpečnostní agenturu, která při zaznamenání poplachu vyjede k objektu (při tomto řešení

je potřeba počítat s vyššími finančními náklady, zejména z důvodu možných falešných poplachů, které se dají eliminovat, ale nejde zaručit, že k nim nikdy nedojde – ať už z důvodu chyby na straně uživatele, nebo systému).

Vstupní dveře budou připojeny na systém Loxone, díky němuž bude možné i vzdálené odblokování zámku skrze mobilní aplikaci (výhoda např. v situaci, kdy si některý ze členů domácnosti zapomene svůj čip, případně při příchodu návštěvy není nutné jít a fyzicky dveře otevřít).

5 VLASTNÍ NÁVRH ŘEŠENÍ

V této kapitole se diplomová práce zabývá nejen samotným fyzickým návrhem inteligentního systému, ale je zde kladen důraz na celkovou bezpečnost tohoto řešení. Pro zabezpečení systému je nutné nejprve identifikovat možná slabá místa, určit, jaké by byly dopady při vzniku bezpečnostního incidentu a zvážit možnosti opatření, jak potencionální hrozby eliminovat.

5.1 Aktiva a rizika

Pro úspěšné ohodnocení aktiv a rizik je nejprve nutné, provést jejich identifikaci. Prvním krokem tedy bude identifikace aktivit a určení jejich hodnoty (ohodnocení dle integrity, dostupnosti a důvěrnosti). Dále provedeme identifikace možných hrozeb a také možný způsob jejich ošetření.

5.1.1 Identifikace aktiv

Aktiva v domácnosti můžeme rozdělit do následujících skupin:

- hardware – jedná se aktiva (zařízení) inteligentního systému řízení domácnosti, při jejichž narušení může dojít k nefunkčnosti systému. Patří sem ovládací zařízení systému, komunikační kanály a samozřejmě i koncové zařízení, kterými je systém ovládán jako jsou mobilní telefony, tablety, PC atd.
- software – softwarem se rozumí zejména Loxone Config. přes který se provádí veškerá konfigurace a při jehož narušení by mohly být změněny základní informace - např. práva přístupu, čímž by byla narušena bezpečnost systému
- citlivé informace – elektronická či tištěná forma – jedná se o informace, jako jsou například hesla, osobní údaje o majiteli a veškeré citlivé informace
- dostupnost – do této kategorie spadá dostupnost služeb, dat a vzdáleného přístupu do celého systému

5.1.2 Ohodnocení aktiv

Ohodnocení aktiv probíhalo za spolupráce investora, aby bylo zajištěno přesné určení významnosti jednotlivých prvků a ohodnocení bylo tak co nejvíce přesné. Vzhledem k tomu, že investor je současně majitelem domu, bude v něm bydlet a systém využívat, je snaha o maximální přizpůsobení systému jeho požadavkům. Výsledná hodnota aktiv se vypočítá na základě součtu podle součtového algoritmu, který byl již popsán dříve.

Tabulka č. 2: Ohodnocení aktiv (Zdroj: vlastní zpracování)

Skupina	Aktivum	Důvěrnost	Integrita	Dostupnost	Hodnota aktiva
Informace	Citlivé data uživatelů	4	3	3	3
	Citlivé data systému	5	4	5	5
Software	Nastavení systému	3	3	3	3
	Mobilní zažízení s aplikací Loxone	3	3	4	3
Hardware	Stolní počítač v domácnosti	4	3	3	3
	Notebooky obyvatel domu	4	3	3	3
	Čidla a senzory systému	3	3	4	3
	UPS	2	2	3	2
	Aktivní prvky	2	2	3	2
	Kabeláž systému	2	2	3	2
Dostupnost	Dostupnost dat	5	4	5	5
	Vzdálený přístup	5	4	4	4
	Dostupnost služeb systému	5	4	5	5

Dle hodnot z tabulky ohodnocení aktiv je možné jednotlivá aktiva shrnout do skupin a seřadit je podle jejich celkové hodnoty. Díky tomu získáme jasný přehled, která aktiva jsou nejvíce ohrožena a kterým je potřeba věnovat největší pozornost.

Tabulka č. 3: Seskupení aktiv (Zdroj: vlastní zpracování)

Aktivum	Hodnota aktiva
Citlivé data systému	5
Dostupnost dat	5
Dostupnost služeb systému	5
Vzdálený přístup	4
Citlivé data uživatelů	3
Nastavení systému	3
Mobilní zažízení s aplikací Loxone	3
Stolní počítač v domácnosti	3
Notebooky obyvatel domu	3
Čidla a senzory systému	3
UPS	2
Aktivní prvky	2
Kabeláž systému	2

5.1.3 Identifikace hrozeb

Pro určená aktiva jsou identifikovány a ohodnoceny hrozby související s těmito aktivy. U každé hrozby je také uveden zdroj jejího vzniku.

Pravděpodobnost výskytu, jak již bylo dříve zmíněno, dělíme do následujících skupin: nahodilé (1), nepravděpodobné (2), pravděpodobné (3), velmi pravděpodobné (4) a trvalé (5). Dále u hrozeb rozlišujeme příčinu jejich vzniku, a to buď na náhodu anebo úmysl.

Tabulka č. 4: Identifikace hrozeb (Zdroj: vlastní zpracování)

Hrozba	Pravděpod. vzniku	Příčina rizika
Živelné pohromy		
požár	nahodilá	náhoda/úmysl
povodeň	nahodilá	náhoda
úder bleskem	nahodilá	náhoda
Základní zdroje		
výpadek dodávky el.energie	pravděpodobné	náhoda/úmysl
výpadek datového připojení	pravděpodobné	náhoda/úmysl
Technické poruchy		
porucha PC	pravděpodobné	náhoda
porucha zařízení systému (pohon rolet, ovládání světel,...)	nepravděpodobné	náhoda/úmysl
porucha řídící jednotky - Miniserveru	nepravděpodobné	náhoda/úmysl
porucha aktivních prvků	nepravděpodobné	náhoda/úmysl
porucha senzorů inteligentního systému	nepravděpodobné	náhoda/úmysl
porucha čtečky iButton	nepravděpodobné	náhoda/úmysl
Ohrožení informací		
odcizení PC	nepravděpodobné	úmysl
odcizení notebooku, tabletu a jiného mobilního zařízení	pravděpodobné	úmysl
ztráta dat	nepravděpodobné	náhoda/úmysl
ztráta přihlašovacích údajů	nepravděpodobné	náhoda/úmysl
odcizení přihlašovacích údajů	nepravděpodobné	úmysl
napadení systému - hackerský útok	nahodilá	úmysl
napadení systému - škodlivý software	nahodilá	úmysl
Fyzické poškození		
porucha na síťové infrastruktuře	pravděpodobné	náhoda/úmysl
neoprávněné vniknutí do domu	nepravděpodobné	úmysl

5.1.4 Matice zranitelnosti

V matici zranitelnosti jsou uvedeny hodnoty pro zranitelnost mezi aktivem a možnou hrozbou. Hodnotu zranitelnosti jsme získali stejný postupem, jakým bylo provedeno ohodnocení aktiv.

Tabulka č. 5: Matice zranitelnosti (Zdroj: vlastní zpracování)

Zranitelnost	Pravděpodobnost výskytu	Citlivé data uživatelů	Citlivé data systému	Nastavení systému	Mobilní zařízení s aplikací Loxone	Stolní počítač v domácnosti	Notebooky obyvatel domu	Čidla a senzory systému	UPS	Aktivní prvky	Kabeláž systému	Dostupnost dat	Vzdálený přístup	Dostupnost služeb systému
Hodnota aktiva		3	5	3	3	3	3	3	2	2	2	5	4	5
Požár	1	3	2	3	3	4	4	4	4	3	3	3	4	4
Povodeň	1	3	2	3	3	4	4	4	4	3	3	3	4	4
Úder bleskem	1	3	2	3	3	4	4	4	4	3	3	3	4	4
Výpadek dodávky el.energie	3					3		1					4	4
Výpadek datového připojení	3					3		1					4	3
Porucha PC	3	3				3							1	
Porucha zařízení systému (pohon rolet, ovládání světel,...)	2							3						
Porucha řídící jednotky - Miniserveru	2		3	3				3					4	4
Porucha aktivních prvků	2							3					4	
Porucha senzorů inteligentního systému	2							3						3
Porucha čtečky iButton	2							3						4
Odcizení PC	2	3										4		
Odcizení notebooku, tabletu a jiného mobilního zařízení	3	3			4							3		
Ztráta dat	2	3	3	4								4		3
Ztráta přihlašovacích údajů	2	3	3	4	3	2	1			1		3	3	
Odcizení přihlašovacích údajů	2	4	4	3	3	3	3			2		4	3	
Napadení systému - hackerský útok	1	5	4	3	2	3	1	4		4		3	3	
Napadení systému - škodlivý software	1	5	4	3	2	3	1	4		4		3	3	
Porucha na síťové infrastruktuře	3					2	1			2	3	3	4	3
Neoprávněné vniknutí do domu	2					2	2			2	3			

5.1.5 Matice rizik

Pro vypočítání míry rizika jsme zvolili metodu se třemi parametry, ve které násobíme zranitelnost rizika s hodnotou aktiva a pravděpodobností výskytu. Díky tomuto výpočtu zjistíme hodnotu míry rizika – výsledné hodnoty jsou zaznačeny v tabulce níže. Pro lepší přehlednost jsou opět jednotlivé stupně barevně zvýrazněny dle následující škály.

	0-10	bezvýznamná míra rizika
	11-20	akceptovatelná míra rizika
	21-30	nízká míra rizika
	31-60	nežádoucí míra rizika
	61 a více	nepřijatelná míra rizika

Obrázek č. 19: Ohodnocení míry rizika (Zdroj: 20)

Tabulka č. 6: Matice míry rizika (Zdroj: vlastní zpracování)

Míra rizika	Pravděpodobnost výskytu	Citlivé data uživatelů	Citlivé data systému	Nastavení systému	Mobilní zařízení s aplikací Loxone	Stolní počítač v domácnosti	Notebooky obyvatel domu	Čidla a senzory systému	UPS	Aktivní prvky	Kabeláž systému	Dostupnost dat	Vzdálený přístup	Dostupnost služeb systému
Hodnota aktiva		3	5	3	3	3	3	3	2	2	2	5	4	5
Požár	1	9	10	9	9	12	12	12	8	6	6	15	16	20
Povodeň	1	9	10	9	9	12	12	12	8	6	6	15	16	20
Úder bleskem	1	9	10	9	9	12	12	12	8	6	6	15	16	20
Výpadek dodávky el.energie	3					27		9					48	60
Výpadek datového připojení	3					27		9					48	45
Porucha PC	3	27				27							12	
Porucha zařízení systému (pohon rolet, ovládání světel,...)	2							18						
Porucha řídící jednotky - Miniserveru	2		30	18				18					32	40
Porucha aktivních prvků	2							18					32	
Porucha senzorů inteligentního systému	2							18						30
Porucha čtečky iButton	2							18						40
Odcizení PC	2	18										40		
Odcizení notebooku, tabletu a jiného mobilního zařízení	3	27			36							45		
Ztráta dat	2	18	30	24								40		30
Ztráta přihlašovacích údajů	2	18	30	24	18	12	6			4	0	30	24	
Odcizení přihlašovacích údajů	2	24	40	18	18	18	18			8	0	40	24	
Napadení systému - hackerský útok	1	15	20	9	6	9	3	12		8	0	15	12	
Napadení systému - škodlivý software	1	15	20	9	6	9	3	12		8	0	15	12	
Porucha na síťové infrastruktuře	3					18	9			12	18	45	48	45
Neoprávněné vniknutí do domu	2					12	12			8	12			

5.1.6 Analýza síťové bezpečnosti

V objektu budou data uložena buďto na šifrovaném disku anebo na osobních počítačích či noteboocích. Mezi daty se budou nacházet i citlivé osobní informace, jako jsou fotografie, emailové komunikace, údaje pro přístup k internetovému bankovnictví a podobné citlivé informace, se kterými v každodenním životě běžně pracujeme.

Primární určení síťového připojení v domě je zajištění připojení k internetu a samozřejmě také využití pro ovládání systému Loxone. V domě bude tedy jedna privátní síť.

Zařízení – Miniserver, PC, tiskárna a WiFi přístupový bod budou připojena do privátní sítě konektorem RJ45.

Přístup ke správě a nastavení sítě (včetně nastavení Miniserveru) bude vytvořen pro jednoho uživatele, ostatní uživatelé mohou síť využívat, ale ne měnit nastavení. Všechna

zařízení pro osobní použití – PC, notebooky, tablety a chytré telefony budou chráněny pomocí antivirového programu.

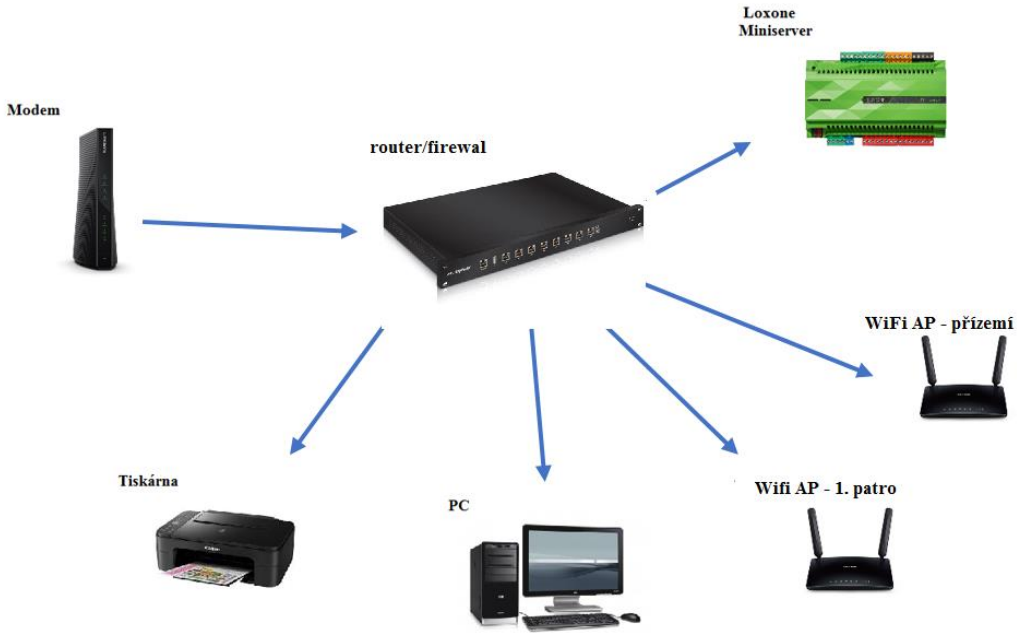
Připojit nové zařízení do privátní sítě lze jednoduše – z prostor domu, rozvaděče či přes zabezpečenou Wifi. Poté se lze připojit k Miniserveru díky aplikaci v chytrém zařízení, nebo přes webové rozhraní. Pokud bychom se chtěli připojit k Miniserveru z jiné sítě, možné to je skrze připojení přes VPN do naší privátní sítě.

Pro úspěšné připojení k Miniserveru je vždy vyžadováno také ověření uživatele pomocí uživatelského jména a hesla.

Prvky inteligentního systému jsou propojeny buďto pomocí kabelových rozvodů vedených ve stěnách anebo pomocí bezdrátového řešení Loxone Air.

Loxone Air komunikaci šifruje dle aktuální bezpečnostní normy – protokolu IPSec. Navíc každý nainstalovaný systém má svůj vlastní unikátní klíč, díky čemuž je vyloučen zásah další strany.

Rozsah pokrytí pomocí této bezdrátové sítě je díky technologii Mesh větší a stabilnější – každé připojené zařízení současně rozšiřuje dosah signálu.



Obrázek č. 20: Schéma sítě (Zdroj: vlastní zpracování)

Fyzická bezpečnost domu je zajištěna bezpečnostními vstupními dveřmi certifikovanými 4. bezpečnostní třídou (pro vchodové dveře se doporučuje minimálně třída 3. a vyšší).

Pokud by došlo k výpadku elektrické energie, systém Loxone bude nouzově napájen ze záložního zdroje a zašle informaci o přerušení dodávky na nastavené mobilní číslo.

5.1.7 Vyhodnocení analýzy

Na základě výsledku analýzy jsme zjistili, že k nejvíce ohroženým aktivům patří zejména dostupnost celého systému a dat, citlivá data, která jsou v systému uložena a možnost vzdáleného přístupu k systému. Nejzásadnější je tedy riziko spojené s dostupností celého systému.

Mezi největší hrozby můžeme zahrnout poruchu na síťové infrastruktuře (neúmyslné porušení vodičů), nedostupnost datového připojení od poskytovatele, výpadek dodávek elektrické energie a poruchu či odcizení některého ze zařízeních používaných ke správě a ovládání systému (PC, notebook, chytrá zařízení) včetně citlivých dat, které tyto zařízení mohou obsahovat.

5.2 Návrh bezpečnostních opatření

Dle výsledků analýzy rizik jsem navrhla následující bezpečnostní opatření. Tyto opatření mají sloužit ke snížení pravděpodobnosti vzniku některé hrozby a současně i velikosti jejich dopadu. Hrozby působící na celý systém můžeme rozdělit do tří základních kategorií, a to na hrozby informační bezpečnosti, hrozby síťové bezpečnosti a hrozby související s fyzickou bezpečností objektu.

5.2.1 Informační bezpečnost

Do kategorie informační bezpečnosti spadají následující hrozby:

Napadení systému útočníkem / škodlivým softwarem

Opatření: Nejdůležitější je bezesporu správné nastavení všech síťových prvků a VPN pro vzdálený přístup. Jedna ze základních podmínek je nastavení silného hesla a použití zabezpečení typu WPA2. Pro zajištění maximální ochrany navrhujeme použití bezpečnostní brány firewall, pro řízení a monitoring síťového provozu.

Zařízení Miniserver má navíc svůj vlastní firewall, který v případě zahlcení dotazy provede automatický restart. Konfigurační nastavení ani data nejsou v takovémto případě nijak ohrožena, pouze v případě opakovaného kontinuálního zahlcování dotazy vzniká riziko častých restartů, které budou mít negativní vliv na dostupnost systému.

Zařízení Loxone Air využívající bezdrátovou komunikaci komunikují vždy šifrovaně a každá instalace má vždy svůj unikátní šifrovací klíč.

Ztráta dat

Opatření: Proti ztrátě dat, ať už elektronických či v tištěné podobě, se lze bránit pouze jejich dostatečným zabezpečením. To znamená tištěná data uchovávat na bezpečném místě (a nejlépe fyzicky uzamčené), elektronická data šifrovat a zamezit k nim tak neoprávněné osobě přímý přístup. Také je vhodné elektronická data pravidelně zálohovat na externí disk, a i tyto zálohy šifrovat.

Odcizení přihlašovacích údajů

Opatření: Veškerá hesla by měla být dostatečně silná a žádné heslo nesmí být použito vícekrát (každý účet musí mít své unikátní heslo). Hesla by se neměla nikam zapisovat, v ideálním případě by měl každý člen znát pouze své heslo a pamatovat si ho bez jakéhokoliv uložení. Pokud by došlo k pokusu o útok hrubou silou (tedy odhadováním hesla zkoušením různých možností), po několika nesprávných zadáních přístup zablokovat.

Zvýšení bezpečnosti můžeme také dosáhnout zavedením více faktorového ověřování.

5.2.2 Síťová bezpečnost

Do kategorie síťové bezpečnosti spadají tyto následující hrozby:

Porucha síťové infrastruktury

Opatření: Proti této poruše není možné provést vhodné opatření. Jedna z možností, jak tuto hrozbu snížit, je např. zavedením redundantních tras, což by ale v případě projektu tohoto rozsahu přineslo nepřiměřené náklady, a proto není vhodné toto opatření použít.

Porucha iButton čtečky

Opatření: Použití elektromechanického zámku u vstupních dveří. Jedná se o variantu zámku, který je možné otevřít (z venkovní strany) pomocí čtečky elektronických čipů (iButton) nebo pomocí klasického klíče. Zámek je také možné otevřít pomocí mobilní aplikace, ale v případě nefunkčnosti celého systému je stále k dispozici záložní možnost, a to klasický bezpečnostní klíč.

Porucha některého ze senzorů inteligentního systému

Opatření: Nelze se nijak bránit, proti poruše některého ze senzorů. V případě, že takováto situace nastane, obdrží majitel alespoň informační zprávu o poruše.

Porucha aktivních prvků

Opatření: Zde není možné zajistit adekvátní opatření, a tudíž není možné se proti neočekávané poruše předem ochránit. Aktivní prvek je umístěn v uzamčeném rozvaděči, díky kterému je zajištěna ochrana proti úmyslnému poškození. Náhodné poruše ale není možné předejít (náklady na takovéto opatření by byly neúměrně vysoké, proto ho nenavrhujeme).

Porucha řídící jednotky – Miniserveru

Opatření: Proti náhodné poruše Miniserveru není možné zajistit potřebné opatření. Díky elektromechanickému zámku bude možné se do domu dostat, ale veškeré funkce systému budou mimo provoz. V domě tedy v případě poruchy bude vyřazeno z provozu osvětlení, zabezpečení (pohybová čidla, čtečka iButton, detektor kouře), stínění i vytápění. Pro případy neočekávané poruchy je vhodné uchovávat vždy aktuální zálohu nastavení systému, aby bylo možné při výměně Miniserveru za nový okamžité spuštění systému a obnovení původní konfigurace.

V Brně se nachází několik partnerů firmy Loxone, u kterých je možné nový Miniserver ihned získat.

Porucha některého ze zařízení systému (pohony, ovládání světel)

Opatření: Proti této hrozbě se nelze zajistit adekvátní opatření. V případě poruchy je nutné obstarat výměnu vadné součástky – v Brně se nachází několik servisních partnerů firmy Loxone, kteří výměnu provedou.

Porucha osobního počítače

Opatření: Proti poruše počítače se nelze adekvátně bránit. Důležité data je vhodné pravidelně zálohovat na šifrovaný disk, jak již bylo popsáno.

Výpadek elektrické energie

Opatření: Pro zajištění funkcí systému je vhodné připojení záložního zdroje – UPS. Díky tomuto záložnímu zdroji bude možné systém používat i v případě výpadku elektrické energie. Pro zajištění správné funkce, je nezbytná pravidelná kontrola správné funkčnosti UPS (alespoň 2x do roka).

Výpadek datového připojení

Opatření: Proti výpadku datového připojení od poskytovatele není možné najít adekvátní ochranu (Jako možnost se nabízí zřízení redundantního datového přívodu, což by znamenalo ale nepřiměřené náklady). Navíc při nedostupnosti datového připojení sice

nebude možné systém ovládat pomocí vzdáleného přístupu, ale veškerá ostatní funkcionalita systému bude zachována.

5.2.3 Fyzická bezpečnost

Kategorie fyzické bezpečnosti a s tím i související bezpečnost prostředí zahrnuje tyto hrozby:

Neoprávněné vniknutí do domu

Opatření: Použití vstupních dveří splňující standard bezpečnostní kategorie 4, která poskytuje nevyšší možnou ochranu používanou pro soukromé objekty. Současně použít i elektromechanický zámek stejné bezpečnostní úrovně. Dále je možné chránit se proti následným škodám na majetku při pokusu o neoprávněné vniknutí pomocí pojištěním.

Odcizení osobního počítače, notebooku, tabletu apod.

Opatření: Snížit dopady při odcizení předmětů z domu je možné sjednáním pojištění domácnosti. Toto pojištění může také krýt případné poškození na majetku, vzniklé pokusem o vloupání či samotným vloupáním. Veškeré citlivé údaje uložené v těchto zařízeních by měly být šifrované, a pravidelně zálohované na externí disk, abychom o ně v případě okradení nepřišli.

Požár, povodeň, úder blesku

Opatření: Vznik požáru uvnitř domu bude zaznamenám detektorem kouře, který předá informaci Miniserveru a ten ihned zašle upozornění majiteli domu. V domě by se na každém patře měl nacházet malý hasicí přístroj, aby v případě vzniku požáru jej bylo možné uhasit. Opět platí, že důležitá data by měly být zálohovány na externím disku, který je uchováván na jiném místě.

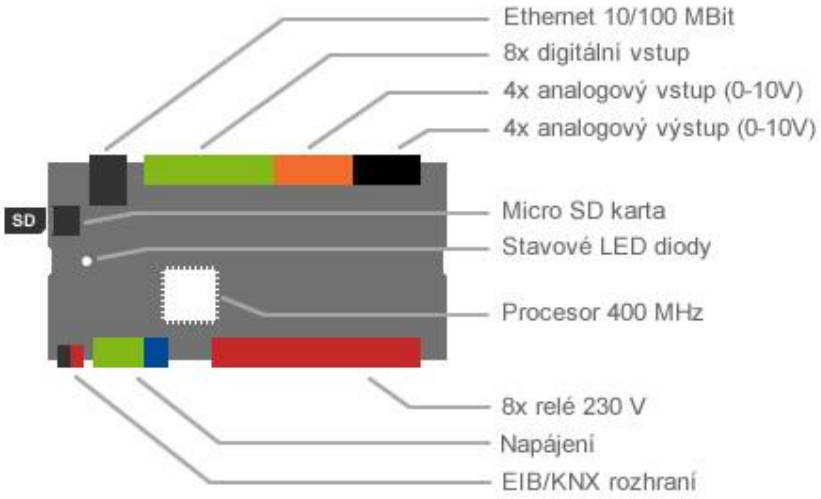
Obecně proti živelným pohromám není možné provést opatření proti vzniku, ale je možné se pojistit, a tím následně vzniklé škody snížit.

5.3 Výběr hardwaru (čidla a zařízení)

Realizace inteligentního systému pomocí systému Loxone bude sestavena z následujících prvků.

5.3.1 Centrální jednotka

Centrální řídící jednotka je nejdůležitější částí celého systému. Ovládá osvětlení, stínění, vytápění i regulaci jednotlivých místností, zabezpečení a ostatní části inteligentní elektroinstalace. Centrální jednotka – Loxone Miniserver obsahuje 4 digitální vstupy a výstupy, 4 analogové vstupy a výstupy a konektor pro připojení EIB/KNX sběrnice. Některé senzory a zařízení je tedy možné připojit přímo k centrální jednotce a není nutné použít pro ně další aktory (16).

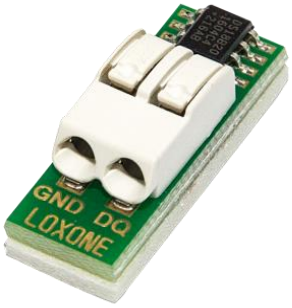


Obrázek č. 21: Loxone Miniserver (Zdroj: 16)

5.3.2 Senzory a zařízení

Teplotní senzor 1-Wire – DS18B20Z+

Tento teplotní senzor je určený k vnitřnímu použití. Díky kompaktnímu rozměru je možné jej umístit do krytu tlačítka. Napájení je zajištěno z datové linky.



Obrázek č. 22: Teplotní senzor Loxone (Zdroj: 23)

Senzor úniku vody Loxone Air

Tento senzor bude umístěn pouze v kritických místech, kde by mohlo dojít k úniku vody jako je například pod dřezem (kde bude současně do odpadu sveden i vývod myčky nádobí) nebo v koupelně, kde je odpad od pračky a vany. Princip senzoru je hlášení poplachu v momentu kontaktu čidel senzoru, umístěných na spodní části ploše čidla, s vodou. Senzor je napájen pomocí baterie, která dle výrobce vydrží déle než 2 roky (23).

Obrázek č. 23: Senzor úniku vody (Zdroj: 23)

Okenní a dveřní kontakt Air

Senzor sloužící k rozpoznání, zda je okno otevřené nebo ne. Tento senzor bude umístěný na každém okně. Senzor funguje bezdrátově, pomocí technologie Loxone Air, nejsou tedy potřebné žádné instalační úpravy. Funkce senzoru spočívá v kontaktu magnetu, který je umístěn na pohyblivém křídle okna a zařízení, které je připevněné na rám okna – v momentě kdy zařízení ztratí magnetický kontakt detekuje tím, že okno je otevřené. Senzor je napájen pomocí baterie, která dle výrobce vydrží déle než 2 roky (24).

Obrázek č. 24: Okenní a dveřní kontakt (Zdroj: 24)

Pohybový senzor

Detektor pohybu, který patří k jedné z nejdůležitějších součástí systému inteligentní domácnosti. Díky tomuto senzoru pro zaznamenávání pohybu lze zajistit nejen bezpečnost prostoru, ale například i rozsvícení osvětlení při vstupu do místnosti. Pokud je senzor instalován na strop, snímá prostor o průměru 8 metrů. Vzhledem k novostavbě, bude použita verze tree – tedy pro napojení na kabeláž vedenou ve zdi. Je možné zvolit z varianty v bílé nebo antracitové barvě.

Obrázek č. 25: Pohybový senzor (Zdroj: 23)

Čtečka elektronického klíče

Díky technologii 1-Wire lze pro přístup do objektu použít čtečku elektronického čipu (iButton). V Miniserveru jsou uloženy informace, které čipy mají přístup do objektu (a případně i jaká scéna se má aktivovat). Díky softwaru Loxone Config lze nakonfigurovat práva pro jednotlivé čipy (23).

Obrázek č. 26: Čtečka elektronického klíče (Zdroj: 23)

Detektor kouře

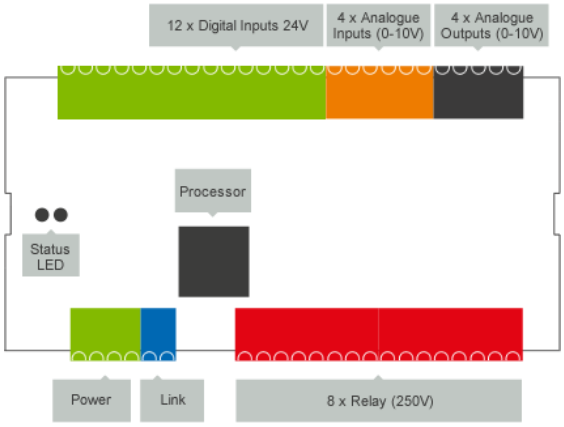
Detektor kouře, který v případě poplachu vydává jak akustický, tak optický signál a přes Miniserver je informace o poplachu předána do aplikace na chytrém zařízení a dle nastavení případně i uskutečněn hovor na předem stanovené číslo (23).

Obrázek č. 27: Detektor kouře (Zdroj: 23)

5.3.3 Aktory

Loxone Extension

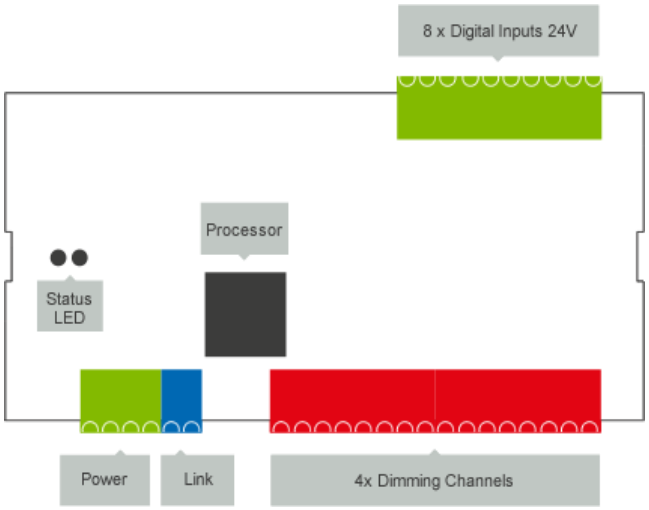
Jednotka pro rozšíření Miniserveru o další vstupy a výstupy (digitální i analogové). Extension obsahuje 12 digitálních vstupů a 8 digitálních výstupů, 4 analogové vstupy a 4 analogové výstupy (24).



Obrázek č. 28: Loxone Extension (Zdroj: 24)

Loxone Dimmer Extension

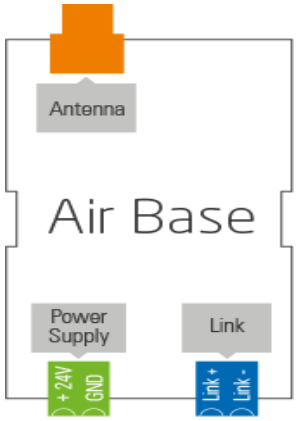
Tato jednotka nabízí 4 smývatelné kanály pro běžné osvětlení a 8 digitálních vstupů pro připojení tlačítek (24).



Obrázek č. 29: Loxone Dimer Extension (Zdroj: 24)

Loxone Air Base Extension

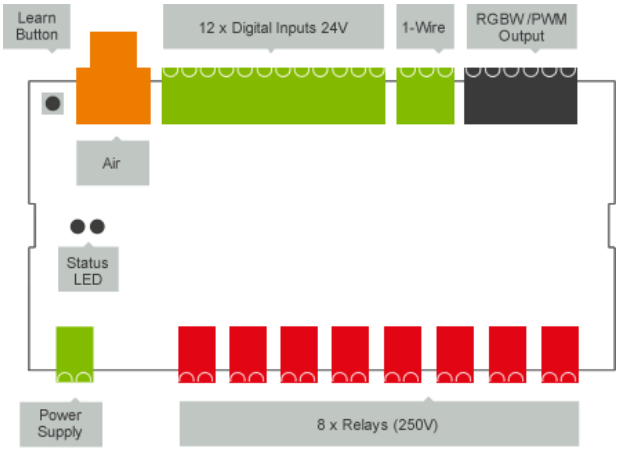
Jednotka umožňující připojení až 128 bezdrátových zařízení – připojené zařízení mohou komunikovat i navzájem mezi sebou (24).



Obrázek č. 30: Loxone Air Base Extension (Zdroj: 24)

Loxone Multi Extension Air

Rozšiřující jednotka, obsahuje 12 digitálních vstupů a 8 digitálních výstupů. Součástí jednotky je i integrované 1-Wire rozhraní, sloužící pro připojení teplotních senzorů, čtečky iButtonu, senzoru úniku vody atd. K Miniserveru je jednotka připojena pomocí Air Base Extension (24).



Obrázek č. 31: Loxone Multi Extension Air (Zdroj: 24)

5.3.4 Napájení

Celý systém bude napájen pomocí dostatečného množství napájecích zdrojů. Pro zajištění bezproblémového provozu bude použit záložní zdroj UPS, který v případě výpadku elektrické sítě zajistí bezproblémový chod kritických částí systému (např.: přístup do objektu pomocí iButton).

5.3.5 Kabeláž

Veškeré senzory a zařízení inteligentního systému budou připojeny do rozvaděče. Při realizaci budou použity dva druhy kabelů, a to datový kabel ISTP Cat. 7 a kabely CYKY 1,5mm.

Datové kabely jsou použity pro připojení zařízení a senzorů, které jsou napájeny napětím 24V, CYKY kabely budou použity pro připojení osvětlení a pohonu žaluzií a garážových vrat.

Veškerá kabeláž bude vedena ve zdech, kde budou kabely uloženy v elektroinstalačních trubkách.

5.3.6 Ovládání systému

Inteligentní systém bude ovládán skrze mobilní aplikace v chytrých zařízeních, webové rozhraní přístupné z počítače anebo pomocí tlačítek umístěných v jednotlivých místnostech domu.

5.4 Rozmístění čidel a senzorů

V následující kapitole bude orientačně popsáno rozmístění čidel a senzorů. Návrh rozmístění je součástí přílohy této práce.

Přízemí

U vstupních dveří se po levé straně čtečka iButton, která po přiložení čipu odblokuje elektromechanický zámek umístěný ve dveřích. Po vstupu do domu se po pravé straně na stěně nachází vypínač pro ovládání světla ve vstupní chodbě a ovládací panel zabezpečení, sloužící pro manuální vypnutí alarmu (pro případ, kdy by došlo k otevření pomocí bezpečnostního klíče a systém tak neidentifikoval uživatele oprávněného ke vstupu je možné alarm vypnout zadáním bezpečnostního PINu). Na stropě ve vstupní chodbě je umístěno světlo a pohybové čidlo.

Při průchodu dále je po levé straně vedle schodiště místnost s WC – při vstupu na pravé straně je umístěn vypínač osvětlení, na stropě je umístěno světlo.

Po pravé straně se dostaneme do uličky, která končí dveřmi do garáže po pravé straně a vstupem do kuchyně a obývacího pokoje, který je po levé straně.

Při vstupu do garáže je po levé straně umístěn vypínač na světlo a ovládání pohonu garážových vrat. Na stropě v garáži je umístěn pohybový senzor, osvětlení a v přední části pohon garážových vrat. V zadním rohu je umístěn centrální rozvaděč.

Při vstupu do kuchyně se nachází po levé straně 3 vypínače na světla (světlo v kuchyni, v jídelním koutě a v průchodu do obývacího pokoje.), teplotní senzor a dvoj vypínač na centrální ovládání žaluzií v přízemí. Po levé straně u stropu se nachází klimatizační jednotka. Uprostřed prostoru kuchyně a jídelního koutu je umístěn detektor kouře. Jedno stropní světlo je umístěno v kuchyni, jedno v jídelním koutě (toto světlo je opatřeno stmívačem pro regulaci intenzity osvětlení) a jedno v průchodu mezi kuchyní a obývacím pokojem. U okna v kuchyni je po pravé straně umístěn vypínač pro ovládání žaluzií. V kuchyni se také nachází umístění ovládacího panelu inteligentního systému (tablet), které je možné libovolně přemísťovat a na stanovené místo vrátit pouze pro dobití baterie.

Osvětlení obývacího pokoje zajišťují 3 stropní svítidla u kterých je možné regulovat intenzitu. Ovládání těchto světel je umístěno v průchodu z kuchyně na stěně po pravé straně společně s teplotním senzorem. V obývacím pokoji se nachází klimatizační jednotka (na stěně mezi balkónovými dveřmi a oknem) a každé okno (i balkonové dveře) jsou opatřeny vypínačem pro individuální ovládání žaluzií po své pravé straně.

Mimo těchto prvků jsou ještě v každém okně nainstalovány okenní kontakty, které detekují otevřená okna a v rohu kuchyně, kde se nachází odpad dřezu a myčky je umístěn senzor zaplavení.

Na venkovní fasádě domu je mezi vstupními dveřmi a garážovými vraty umístěna poplašná siréna.

1. patro

Po vystoupání schodiště ze vstupní chodby v přízemí se ocitneme v hale v 1. patře. U schodiště po pravé straně je umístěn vypínač na světlo a teplotní senzor. Po levé straně je u stropu umístěna klimatizační jednotka. V hale jsou umístěny 2 stropní světla, senzor pohybu a celkem 3 síťové porty. Místnost označená v půdoryse č.1 je hlavní ložnice – po vstupu jsou po pravé straně umístěny vypínač na světlo, tlačítko pro ovládání žaluzií a teplotní senzor. Stropní světlo je umístěno na středu místnosti.

Průchodem ložnice se dostaneme do místnosti označené č.2, tedy šatny, kde jsou vypínače pro světlo a ovládání žaluzií umístěny po levé straně hned u vstupu do místnosti. Stropní světlo je umístěno opět přibližně na středu místnosti.

Z haly vedou dveře do technické místnosti (č.4), koupelny (č.5), dětského pokoje (č.7) a pokoje pro hosty (č.6).

V technické místnosti je umístěn elektrický kotel, centrální ovládání podlahového vytápění, světlo a vypínač pro ovládání světla.

V koupelně je umístěno pouze stropní světlo a jeho vypínač společně s teplotním senzorem.

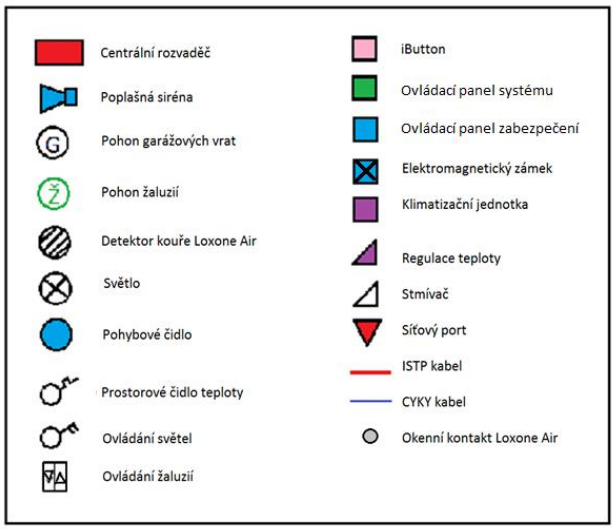
V pokoji pro hosty jsou při vstupu po levé straně umístěny vypínač světla společně s teplotním senzorem a ovládáním žaluzií. Uprostřed pokoje je umístěno stropní světlo.

V dětském pokoji je rozmístěn stejné – po levé straně při vstupu jsou vypínače pro ovládání světla a žaluzií a světlo je umístěno na stropě ve středu místnosti.

Všechny okna v 1. patře jsou opatřena okenními kontakty pro detekci otevřeného okna.

5.5 Použité značení

Pro zaznamenání jednotlivých prvků systému a rozlišení použitých vodičů byly použity tyto symboly:



Obrázek č. 32: Značení použité v návrhu (Zdroj: vlastní zpracování)

5.6 Rozsah návrhu inteligentního systému

Návrh je zaměřen na prvky, které jsou součástí inteligentního systému ovládání domácnosti. Tyto prvky byly zvoleny tak, aby poskytli zabezpečení domu a jeho komfortní ovládání společně se zkvalitněním každodenního života.

Po navrhnutí prvků, ze kterých bude systém složen a jejich orientačního umístění, byla provedena identifikace hrozeb a analýza rizik, které mohou na systém působit.

Práce se zabývá zejména tedy zabezpečení toho navrženého systému pro inteligentní řízení domácnosti, a to nejen z pohledu dat, celé sítě, jednotlivých prvků této sítě ale také z pohledu fyzického zabezpečení objektu. Součástí práce je návrh opatření, díky kterým lze snížit pravděpodobnost vzniku jednotlivých hrozeb.

Součástí práce není konkrétní zapojení jednotlivých prvků a jejich konfigurace.

Práce má za cíl poskytnou ucelený pohled na problematiku inteligentního řízení domácnosti, a to jak z pohledu potřebných prvků takového systému, tak z pohledu zabezpečení těchto prvků, potažmo celého systému, včetně orientačních nákladů spojených s pořízením celého řešení zabezpečeného řešení pro řízení inteligentní domácnosti.

5.7 Požadavky na stavební připravenost

Mezi datovými kabely a silovými musí být dodržena vzdálenost daná dle normy ČSN 50174-2. Tato norma udává pravidla pro přípravu a instalaci kabelových rozvodů uvnitř budov. Norma řeší vnější vlivy kabeláže a zabývá se možnými vhodnými opatřeními. Také obsahuje doporučení a požadavky pro jednotlivé zhotovitele i pro jednotlivé součásti kabelážního systému.

Datový rozvaděč bude částečně zapuštěn do nosné zdi musí být řádně uzemněn.

Protože datové i silové kabely budou vedeny ve zdech a stropech, je nutná příprava instalačních trubek, ve kterých pak budou moct být kabely rozvedeny k potřebným prvkům.

Jednotlivá tlačítka i senzory budou mít přístrojovou krabici, nainstalovanou pod omítkou, sloužící k uložení kabelu včetně případné rezervy.

5.8 Ekonomické zhodnocení projektu

Do cenové kalkulace jsou zahrnuty náklady na pořízení veškerých prvků pro ovládání systému Loxone, včetně instalačních materiálů. Součástí cenové kalkulace nejsou pouze náklady na instalační trubky a jejich umístění do zdí a stropů.

Celková cena všech prvků tohoto projektu je 222 000 Kč s DPH. V této částce nejsou zahnuty náklady na montáž, instalaci a zprovoznění systému ani související náklady potřebné pro stavební úpravy. Předběžnou cenu těchto prací lze odhadnout na 70 000Kč s DPH. Finální cena tedy bude blížit k 300 000Kč s DPH.

Cenová kalkulace je přiložena v příloze.

6 ZÁVĚR

Cílem této práce bylo navrhnout řešení systému inteligentní domácnosti za účelem zabezpečení daného objektu. Celá práce včetně návrhu systému byla vytvořena na základě požadavků investora, bezpečnostních norem a s ohledem na jednotlivá rizika působící na systém.

Investor se rozhodl pro vytvoření chytré domácnosti z důvodu zkvalitnění každodenního života a zajištění komfortu a bezpečnosti. V návrhu inteligentní elektroinstalace byl tedy kladen důraz na maximální komfort pro ovládání, a toho je dosaženo především díky propojení všech dílčích částí v jeden ucelený a snadno spravovatelný celek.

Jedna z částí této práce je zaměřena na vytvoření návrhu konkrétního řešení systému, který je složen z rozvržení jednotlivých prvků tak, aby byla zajištěna optimální funkce systému. Toho je dosaženo i díky výběru vhodných systémových prvků, které vyhovují požadavkům investora a poskytují nejlepší možnou úroveň celého systému.

Dále se práce věnuje zabezpečení již navrženého systému, a s tím souvisejících částí jako je analýza objektu, identifikace hrozeb a analýza rizik, které mohou na systém působit.

Následně jsou navržena konkrétních opatření, jak pravděpodobnost vzniku hrozeb snížit

Vzhledem k tomu, že byl navržen systém splňující všechny požadavky investora, včetně stanoveného rozpočtu, cíl práce byl splněn a věřím, že systém bude svým majitelům zjednodušovat každodenní život dlouhé roky.

SEZNAM POUŽITÝCH ZDROJŮ

(1) BURDKOVÁ, M. a P. VESELÝ. Inteligentní budovy [online]. [cit. 2019-03-04]. Dostupné z: http://www.jilova.cz/Projekty/projekty-rozvoj-inteligentniBudovyStudium1.pdf.

(2) NÝVLT, O. Buses, Protocols and Systems for Home and Building Automation [online]. 2009-2011 [cit. 2019-01-04]. Dostupné z: http://www.tecnolab.ws/pdf/Buses,%20Protocols%20and%20Sytems%20for%20Home%20and%20Building%20Automation.pdf.

(3) JORDÁN, V. a V. ONDRÁK. Infrastruktura kabelážních systémů I: Univerzální kabelážní systémy. Brno: Akademické nakladatelství CERM,s.r.o., 2013. ISBN 978-80-214-4839-1.

(4) Topologie sítí. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2019, 6.4.2019 [cit. 2019-05-10]. Dostupné z: https://cs.wikipedia.org/wiki/Topologie_s%C3%ADt%C3%AD#/media/File:NetworkTopologies.png.

(5) BAUDYŠ, A. INELS jako řídící systém domovní elektroinstalace. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 74 s. Vedoucí bakalářské práce Ing. Branislav Bátora.

(6) NOVÁK, P. Průmyslové řídící systémy. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, Fakulta strojní, 2013. ISBN 978-80-248-3032-2.

(7) KŘÍSTEL, J. Zabezpečovací zařízení s GSM modulem. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2012. 40 s., 15 s. příloh. Semestrální práce. Vedoucí práce Ing. Jan Prokopec, Ph.D..

(8) ČERNÝ, J. Návrh zabezpečovacího systému areálu společnosti. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2014. 91 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

(9) LUKÁŠ, L. a kolektiv. Bezpečnostní technologie, systémy a management I. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.

(10) PAVLÍNEK, R. Bezkontaktní detektory rozbití skla. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2012. 73 s. Bakalářská práce. Vedoucí práce doc. Ing Luděk Lukáš, CSc..

(11) KAŠPAR, P. Přednáška 11-14: Protipožární senzory, senzory plynů, detektory pohybu a další senzory pro zabezpečení [online]. © 2008-2015 [cit. 2019-03-04]. Dostupné z: http://measure.fel.cvut.cz/system/files/files/cs/vyuka/predmety/A5M38MEB/A5M38EMBP11_13SECURITY.pdf.

(12) DVOŘÁK, J. Domácí meteorologická stanice. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 40 s. Diplomová práce. Vedoucí práce Ing. Zbyněk Fedra, Ph.D..

(13) ŘEZNÍČEK, O. Zařízení pro kalibraci snímačů malých rychlostí proudění. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011. 31 s., 1 příloha. Vedoucí práce doc. Ing. Josef Štětina, Ph.D..

(14) How to became a KNX Member. KNX [online]. 2015[cit. 2019-03-02]. Dostupné z: http://www.knx.org/fileadmin/downloads/08%20%20KNX%20Flyers/How%20To%20Become%20A%20KNX%20Member/How_TO_Become_A_KNX_Member_English.pdf.

(15) Bezdrátová elektroinstalace: Bezdrátové řešení bytů a domů [online]. © 2019 [cit. 2019-04-03]. Dostupné z: https://www.elkoep.cz/media/files/download/item/files-193/l1_sec_Bezdratova_elektroinstalace_CZ_2019_view.pdf.

(16) Srdce Loxone Chytrého domu: Miniserver. Loxone [online]. © 2016 [cit. 2019-02-04]. Dostupné z: http://www.loxone.com/cscz/produkty/miniserver/miniserver.html.

(17) Inteligentní domácnost [online]. [cit. 2019-04-03]. Dostupné z: https://www.somfy.cz/produkty/automatizace-domacnosti/inteligentni-domacnost.

(18) ABB-free@home® Inteligentní elektroinstalace: Domovní automatizace snazší než kdykoliv předtím. ABB [online]. ABB s. r. o. Elektro-Praga, 3/2016 [cit. 2019-03-28]. Dostupné z: https://nizke-napeti.cz.abb.com/files/document/5873/files/12854-ABB-Pruvodce-moderni-elektroinstalaci-2017-150dpi.pdf.

(19) *Inteligentní instalace ABB-free@home®* [online]. ABB©, 2019 [cit. 2019-05-10]. Dostupné z: https://nizke-napeti.cz.abb.com/inteligentni-instalace-abb-freehome.

(20) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(21) Model PDCA. *VectorStock* [online]. [cit. 2019-05-10]. Dostupné z: https://www.vectorstock.com/royalty-free-vector/plan-do-check-act-pdca-cycle-vector-8728634.

(22) ČSN EN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

(23) *Příslušenství pro inteligentní domy* [online]. Loxone [cit. 2019-05-10]. Dostupné z: https://shop.loxone.com/cscz/prislusenstvi.html.

(24) *Extensions: jednoduché rozšíření pro Miniserver* [online]. Loxone [cit. 2019-05-10]. Dostupné z: https://shop.loxone.com/cscz/extensions.html.

(25) ČSN EN ISO/IEC 27001: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(26) ČSN EN ISO/IEC 27005: Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Česká agentura pro standardizaci, 2019.

(27) ČSN EN ISO/IEC 27033: Informační technologie – Bezpečnostní techniky – Bezpečnost sítě. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016.

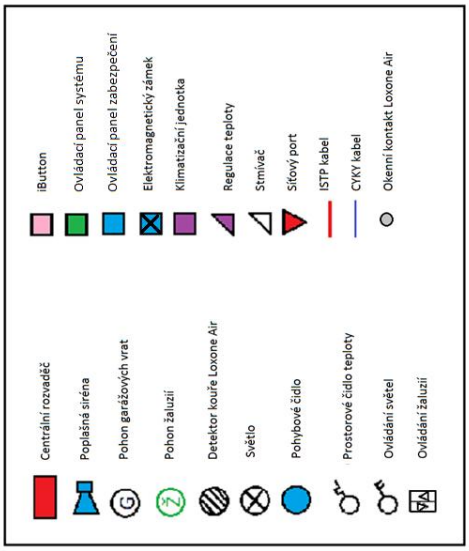
SEZNAM POUŽITÝCH OBRÁZKŮ

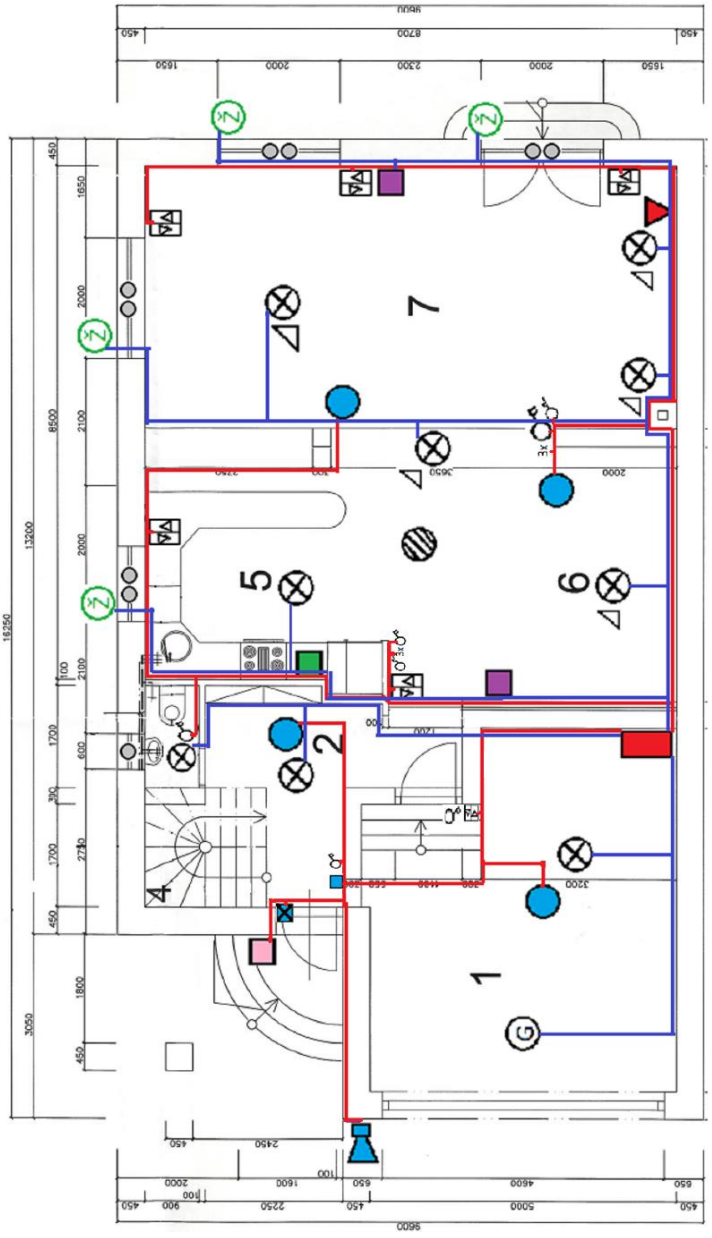
SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ

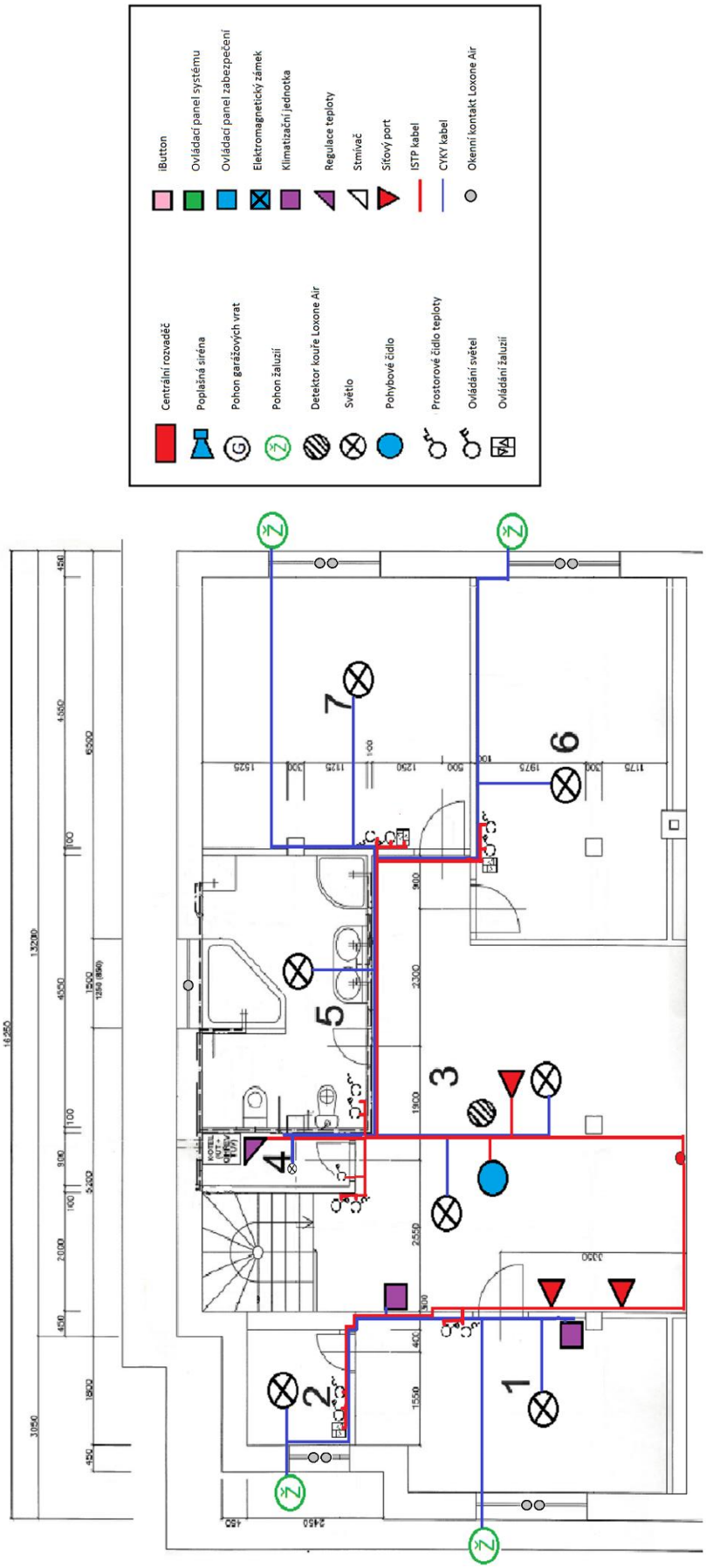
SEZNAM PŘÍLOH

Příloha č. 1: Návrh systému přízemí





Příloha č. 2: Návrh systému 1. patro



Příloha č. 3: Matice – Míra rizika

Míra rizika	Pravděpodobnost výskytu	Citlivé data uživatelů	Citlivé data systému	Nastavení systému	Mobilní zařízení s aplikací Loxone	Stolní počítač v domácnosti	Notebooky obyvatel domu	Čidla a senzory systému	UPS	Aktivní prvky	Kabeláž systému	Dostupnost dat	Vzdálený přístup	Dostupnost služeb systému
Hodnota aktiva		3	5	3	3	3	3	3	2	2	2	5	4	5
Požár	1	9	10	9	9	12	12	12	8	6	6	15	16	20
Povodeň	1	9	10	9	9	12	12	12	8	6	6	15	16	20
Úder bleskem	1	9	10	9	9	12	12	12	8	6	6	15	16	20
Výpadek dodávky el.energie	3					27		9					48	60
Výpadek datového připojení	3					27		9					48	45
Porucha PC	3	27				27							12	
Porucha zařízení systému (pohon rolet, ovládání světel,...)	2							18						
Porucha řídící jednotky - Miniserveru	2		30	18				18					32	40
Porucha aktivních prvků	2							18					32	
Porucha senzorů inteligentního systému	2							18						30
Porucha čtečky iButton	2							18						40
Odcizení PC	2	18										40		
Odcizení notebooku, tabletu a jiného mobilního zařízení	3	27			36							45		
Ztráta dat	2	18	30	24								40		30
Ztráta přihlašovacích údajů	2	18	30	24	18	12	6			4	0	30	24	
Odcizení přihlašovacích údajů	2	24	40	18	18	18	18			8	0	40	24	
Napadení systému - hackerský útok	1	15	20	9	6	9	3	12		8	0	15	12	
Napadení systému - škodlivý software	1	15	20	9	6	9	3	12		8	0	15	12	
Porucha na síťové infrastruktuře	3					18	9			12	18	45	48	45
Neoprávněné vniknutí do domu	2					12	12			8	12			

Příloha č. 4: Cenová kalkulace použitých prvků

Označení	Popis	ks	cena v Kč s DPH/kus	cena v Kč s DPH celkem
100001	Miniserver	1	13671	13671
100002	Extension	3	10936	32808
100029	Dimmer Extension	1	12358	12358
100114	Air Base Extension	1	2777	2777
100116	Multi extension Air	1	13124	13124
200109	Teplotní senzor 1-Wire 5ks	2	1388	2776
100211	Záplavový senzor Air	2	1917	3834
motion-sensor	Pohybový senzor	5	2645	13225
door-window-contact-air	Okenní a dveřní kontakt Air	18	1917	34506
200191	Čtěčka iButton	1	305	305
200064	Elektronický klíč	5	108	540
valve-actuator	Hlavice regulace topení	8	2314	18512
100142	Detektor kouře Air	2	2711	5422
nfc-code-touch	Ovládací panel zabezpečení	1	8375	8 375
SZLD92	El. zámek FAB Bera	1	7805	7805
3558E-A00651 01	Kryt vypínače jednoduchý	10	49	490
3558E-A00652 01	Kryt vypínače dělený	3	61	183
3558E-A00662 01	Kryt ovladače žaluzií	9	66	594
3558-A01340	strojek vypínače	13	117	1521
3559-A89345	strojek ovladače žaluzií	9	192	1728
200001	napájecí zdroj	3	1858	5574
200129	ISTP kabel 250m	3	6218	18654
CYKY-O 3x1,5	CYKY kabel 3x1,5 1m	600	12	7200
CYKY-J 5x1,5 (C)	CYKY kabel 4x1,5 1m	700	21	14700
RMA-18-A68-CAX-A1	Datový rozvaděč Triton	1	6999,0	6 999
instalační materiál - svorky, svorkovnice			3000	3000
Ubiquiti EdgeRouter ER-8		1	7 990	7 990
Ubiquiti UniFi AP		2	1 699	3398
ESET licence na 1 rok pro 3 zařízení WIN/Mac a 3 zařízení iOS/Android		1	1590	1590
UPS - záložní zdroj Fortron Nano 800		1	1349	1349
Cena celkem:			103883	221644