Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Rozbor moderních trendů zabezpečovacích systémů směrem k systémům IoT

Bakalářská práce

Autor: **Jiří Dalík**

Vedoucí práce: Ing. Zdeněk Votruba, Ph.D.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jiří Dalík

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Rozbor moderních trendů zabezpečovacích systémů směrem k systémům IoT

Název anglicky

Analysis of modern trends in security systems towards IoT systems

---

Cíle práce

Cílem práce je posoudit současný stav zabezpečovacích systémů, především jejich aktuální limity ve vztahu k technickému vývoji a navrhnout konceptuálně nové řešení zaměřené na distribuované zabezpečovací systému zaměřené na cloudové řešení a využívající IoT komunikaci.

Metodika

1. analýza základních trendů současných systémů PZTS
2. komparace vybraných parametrů typických systémů
3. explanace systémů PZTS vůči technologiím IoT
4. syntéza optimální konstrukce
5. analýza ve vztahu k ČSN EN 50131 a navazujícím
6. abdukce navržených parametrů
7. konstrukce modelu a jeho ověření
8. diskuse, potvrzení/vyvrácení hypotézy
9. komparace ceny a užitné hodnoty

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

PZTS, cloud, bezpečnost, IoT

Doporučené zdroje informací

CASTLEDINE, Earle; EFTOS, Myles; WHEELER, Max. *Vytváříme mobilní web a aplikace pro chytré telefony a tablety.* Brno: Computer Press, 2013. ISBN 978-80-251-3763-5.

HILPISCH, Yves J. *Python for algorithmic trading : from idea to cloud deployment.* Boston: O'Reilly Media, 2021. ISBN 978-1492053354.

KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* Blatná: Blatenská tiskárna, 2006. ISBN 80-902938-2-4.

MURUGESAN, San; BOJANOVA, Irena; IEEE COMPUTER SOCIETY. *Encyclopedia of cloud computing.* Chichester: IEEE Press, 2016. ISBN 978-1-118-82197-8.

UHLÁŘ, Jan; POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY. KATEDRA TECHNICKÝCH PROSTŘEDKŮ BEZPEČNOSTNÍCH SLUŽEB. *Technická ochrana objektů. II. díl, Elektrické zabezpečovací systémy II.* Praha: Vydavatelství PA ČR, 2005. ISBN 80-7251-189-0.

Předběžný termín obhajoby

2023/2024 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 15. 2. 2022

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 2. 2022

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 26. 03. 2024

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci na téma:

Rozbor moderních trendů zabezpečovacích systémů směrem k systémům IoT

vypracoval samostatně a citoval jsem všechny informační zdroje, které jsem v práci použil a které jsem rovněž uvedl/a na konci práce v seznamu použitých informačních zdrojů.

Jsem si vědom, že na moji bakalářskou/diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Svým podpisem rovněž prohlašuji, že elektronická verze práce je totožná s verzí tištěnou a že s údaji uvedenými v práci bylo nakládáno v souvislosti s GDPR.

V ……. dne ……

…….
(podpis autora práce)

PODĚKOVÁNÍ

Tímto bych chtěl poděkovat Ing Zdeňku Votrubovi Ph.D. za vstřícné vedení mé práce, bezproblémovou komunikaci a výborné vedení po celou dobu práce. Dále bych chtěl poděkovat své rodině a svým přátelům, kteří pro mě byli největší oporou a podporovali mě skrz těžké momenty, které jsem prožil v průběhu zpracování této práce.

Rozbor moderních trendů zabezpečovacích systémů směrem k systémům IoT

Abstrakt

Touto prací je proveden základní rozbor poplašných zabezpečovacích a tísňových systémů, které jsou dnes často využívány. Zároveň po této části je proveden jednoduchý rozbor technologie Internetu věcí a s tím spojenými tématy jakou je například Cloud. Po rozboru v teoretické části je vysvětlena spojitost těchto technologií a základních norem, pod které zmíněné obory spadají. Nakonec je nahlédnuto do prvků a myšlenek, které se dají označit jako trendy v těchto spojitostech. Praktická část je tvořena návrhem, popisem systému a následném sestrojení. U každé části tohoto zapojení je proveden rozbor prvků a následně je jsou dva prvky vybrány a otestovány pro ověření jejich vlastností. Následně je sepsán popis provedeného měření a jejich výsledků, které jsou zobrazeny v přiložených tabulkách nebo zpracovány jiným způsobem, pokud to situace vyžadovala, pro lepší zobrazení. V konečné fázi praktické části je zhodnocena kvalita systému a zároveň je brána v potaz cenová hodnota, která byla nutná pro sestrojení jednotlivých části systému.

Klíčová slova: poplachový a zabezpečovací systém, iot, cloud, gateway, trendy

Analysis of modern trends in security systems towards IoT systems

Abstract

This thesis provides a basic analysis of alarm security and emergency systems, which are often used today. At the same time, after this part, a simple analysis of Internet of Things technology and related topics such as the Cloud is carried out. After the analysis in the theoretical part, the connection between these technologies and the basic standards under which these fields fall is explained. Finally, elements and ideas that can be identified as trends in these connections are examined. The practical part consists of the design, description of the system and subsequent construction. For each part of this connection, an analysis of the elements is performed and then two elements are selected and tested to verify their properties. Subsequently, a description of the measurements performed, and their results is written, which are displayed in the attached tables or processed in another way, if the situation required it, for a better display. In the final phase of the practical part, the quality of the system is evaluated and at the same time the price value that was necessary for the construction of the individual parts of the system is considered.

Key words: intruder and hold-up alarm system, iot, cloud, gateway, trends

Obsah

1 Úvod 1

2 Cíl práce 2

3 Metodika práce 3

4 Teoretická východiska 4

4.1 Rozbor zabezpečovacích systémů 4

4.2 Poplachové zabezpečovací a tísňové systémy 4

4.2.1 Podle způsobu zapojení čidel 5

4.2.2 Podle typu rozvodu 5

4.2.3 Podle stupně zabezpečení 6

4.2.4 Podle podsystému 7

4.3 Internet věcí 7

4.3.1 Aplikace a nasazení 8

4.3.2 Druhy systémů 9

4.4 Cloud 11

4.4.1 Veřejný 12

4.4.2 Privátní 12

4.4.3 Hybridní 12

4.4.4 Distribuční modely 13

4.5 Trendy zabezpečovacích systémů 13

4.6 Legislativa 14

4.6.1 ČSN EN 50 131 15

4.6.2 ČSN EN 50 398-1 16

5 Praktická část 17

5.1 Pojednání o projektu 17

5.2 Návrhy projektů 18

5.3 Rozbor použitých prvků u projektu 1 20

5.3.1 Terminál K3F 20

5.3.2 Elektromagnetický zámek O&C MEX100 21

5.3.3 Gateway STAR smart modul G3 22

5.4 Realizace projektu 1 23

5.5 Uživatelské rozhraní projektu 1 23

5.6 Testování spolehlivosti projektu 1 24

5.7 Rozbor použitých prvků u projektu 2 25

5.7.1 SONOFF SNZB-03 Zigbee chytrý pohybový PIR senzor 25

5.7.2 SONOFF Zigbee Bridge-P 27

5.8 Realizace projektu 2 27

5.9 Uživatelské rozhraní projektu 2 28

5.10 Ověření detekčních vlastností senzoru 29
5.11 Finanční náročnost jednotlivých projektů 30
5.12 Výsledné hodnocení systému 31

6 Závěr 33

7 Seznam použité literatury 35

8 Seznam obrázků 39

9 Seznam tabulek 40

10 Seznam použitých zkratek a termínů 41

1 Úvod

Zabezpečovací systémy jsou v dnešní době velice známým pojmem, pod kterým si široká veřejnost představí hlavně kamerové systémy nebo alarmy, ale vznik zabezpečovacích systému jako takových je starý téměř tak jako je majetek. Ačkoliv první zabezpečení majetku bychom si mohli představit jako velmi primitivní systém s lanem, které po přerušení shodí na potenciálního zloděje kámen či zavře dveře, kterými vetřelec přišel, tak princip je stejný. Zabezpečovací systémy musí zajistit detekci narušitele potažmo i ochranu majetku a zároveň v dnešní době být jejich ochranné prostředky úměrné prostoru či majetku, který chrání. Vývoj těchto technologií se neustále posouvá kupředu a pravděpodobně se budou technologie těchto systému posouvat stejným tempem jako útoky narušitelů na objekt či majetek v objektu. Velký průlom pro zabezpečovací systémy přišel v Česku až po průmyslové revoluci, kdy vzniká soukromý bezpečnostní sektor.

Tím se můžeme přesunout do dnešní doby, kde je možné si nechat nainstalovat zabezpečení téměř na jakýkoliv objekt. Každý systém se může velice lišit na základě objektu, který je tímto systémem chráněn. V některých případech to může být z důvodů legislativy a v jiných případech spíše technologií, která se nehodí pro danou situaci. To rozvíjí různé typy systémů, které mohou být přímo určeny pro objekt nebo obecné systémy, které mohou být zaznamenány často například u firem nebo domácnostech.

Použití nových technologií je v dnešní době velice žádaným procesem a zabezpečovací technologie nejsou odlišné. Právě proto se pomalu rozšiřuje i využití IoT systémů, které nahrazují přesun dat z fyzického vedení na signál. Využití IoT si lze povšimnout každým rokem častěji a je možné ho nacházet ve stále širším počtu oborů od chytrých domácností přes strojírenskou výrobu až po zabezpečovací systémy. Avšak jako s každou novější technologií zde přichází problematika v praxi, to bude rozebráno v této bakalářské práci.

2 Cíl práce

Cílem této práce je poukázat na spojitosti mezi poplachovými zabezpečovacími a tísňovými systémy a internetem věcí. Tyto společné charakteristiky, které jsou vzájemně kompatibilní pro oba systémy, následně sjednocujeme do praktického projektu, který poukazuje na očekávaně rozšiřovanou budoucnost oborů zabývajícími se zabezpečením. Dále v této práci je vedena úvaha nad budoucností zabezpečovacích technologií, které budou částí internetu věcí.

3 Metodika práce

Práce je rozdělena do několika částí, kde bude veden rozbor jednotlivých technologií, které se týkají zabezpečovacích systémů, hlavně z důvodu. Následně bude nutné podobným způsobem zpracovat Internet věcí, kde budou rozvedeny jednotlivé prvky, který spadají do tohoto okruhu technologií. Pro správnost informací bude nutné použít různé zdroje zaměřující se na danou problematiku a zároveň zakomponovat různé názory a trendy, které v těchto technologiích kolují.

V praktické části této práce bude nutné navrhnout systém, který lze využít pro základní zabezpečení domácnosti a tento systém sestrojit dle požadavků zákazníka. Zároveň je snaha o to poukázat na finanční rozdílnost jednotlivých prvků systému a zakomponovat proces výběru a následné konstrukce do této sekce. Konečným výstupem tohoto projektu bude zkouška spolehlivosti, která je spojena s bezpečím, které systém nabízí.

4 Teoretická východiska

4.1 Rozbor zabezpečovacích systémů

Zabezpečovací systémy je oblast technologií, které fungují jako nástroj pro ochranu objektu a osob, které by se v době útoku v chráněném objektu nacházely. Důležitým bodem je také rozdělení těchto systémů, protože mechanické zábranné systémy fungují jako fyzická bariéra mezi narušitelem a majetkem, ke kterému se útočník pokouší dostat. Avšak Poplachové zabezpečovací a tísňové systémy (dříve známé pod názvem Elektronické zabezpečovací systémy) fungují v principu jako hlásící a zjišťovací prvky při narušení prostoru, ve kterém se objekt nachází. (1)

Dělí se na:

- Mechanické zábranné systémy (MZS)
- Poplachové zabezpečovací a tísňové systémy (PZTS)

4.2 Poplachové zabezpečovací a tísňové systémy

Jak je zmíněno v kapitole 4.1, tak PZTS plní funkci pro ohlášení nebezpečí a tím pádem nezajišťuji zamezení útočníka ve vniknutí do objektu jako MZS, ale nehledě na to jsou jedním z nejrozšířenějšího typu zabezpečení právě kvůli jednoduché funkci a možnosti zavolat příslušné složky pro ochranu majetku nebo objektů. Pro zjednodušení je možné pohlížet na prvky PZTS dle několika hledisek. (1)

Dělí se:

- Podle způsobu zapojení čidel
  - Smyčkové
  - Sběrnicové
  - Smíšené
- Podle typu rozvodu
  - Drátové
  - Bezdrátové
- Podle stupně zabezpečení
- Podle podsystému

4.2.1 Podle způsobu zapojení čidel

V každém systému, kde se nachází jedno a více čidel je nutné se rozhodnout, jakým způsobem budou čidla propojena, protože jednotlivé metody těchto zapojení mají své výhody a nevýhody. Zároveň je nutno přistupovat k těmto metodám, jako specifickým možnostem, kterými lze řešit danou problematiku obvodu.

Smyčkové zapojení je jedním ze základních zapojení. Funkce zahrnuje dva stavy, kde v klidovém režimu je čidlo spojeno s ústřednou a tím je detekován minimální odpor ve spojení. V momentě, kdy je čidlo otevřeno, tak tím dochází k přerušení spojení a je detekován zvýšený odpor, tím ústředna vyhlašuje poplachový stav. Výhoda tohoto spojen je, že aktivně brání proti sabotáži, protože pokud by došlo k rozpojení v jakémkoliv místě mezi čidle a ústřednou, tak bude tento úkon ústředna detekovat. Zároveň je možné zapojit více než jedno čidlo a v ten moment je detekován poměr odporů jednotlivých čidel. Toto zapojení lze nalézt v menších objektech jako jsou například rodinné domky, byty a kanceláře. (1)

Sběrnicové zapojení je určeno svou stavbou pro větší objekty, kde je odhadováno desítky různých čidel. Každé čidlo má svojí vlastní adresu, podle které jsou rozděleny a komunikují po datové sběrnici s ústřednou. Velký rozdíl oproti smyčkovému zapojení je možnost adresace a zároveň připojování snímačů, které se mohou nacházet v celé délce obvodu, ale s tímto systémem dochází ke komplikacím ztráty napětí a v některých situacích vyšším proudovým odběrem. Velikost těchto komplikací je možné snížit druhem topologie. (1)

Smíšené zapojení funguje na principu dvou hlavních prvků, a to ústředny a koncentrátoru. Koncentrátor je zařízení, které propojuje dvě a více čidel a tvoří tím možnost připojit koncové prvky smyčkovým zapojením. Tento typ není tak rozšířený z důvodu problematiky, kterým je navrhnutí a programování jednotlivých svazků. (1)

4.2.2 Podle typu rozvodu

Další velice důležitým prvkem jakéhokoliv zabezpečovacího systému je výběr rozvodu, kterého využijeme, protože toto rozhodnutí určuje, zdali bude systém schopný vykonávat svou funkci, což je u PZTS ten nejdůležitější prvek. Zároveň s těmito parametry je nutno zvažovat, zdali je daný typ rozvodu vhodný pro řešenou aplikaci.

Drátové rozvody jsou i dnes nejrozšířenějším druhem propojovacích prvků mezi jednotlivými členy rozvodů. V principu se jedná o vedení tvořené měděnými dráty. Největšími výhodami tohoto typu rozvodu je spolehlivost a životnost, které jsou

dominantní mezi ostatními typy přenosů, ale zároveň je nejlepší tyto rozvody aplikovat při samotné výstavbě objektu, protože následné úpravy v hotových budovách mohou být složité a někdy i prakticky nemožné z důvodu jiných vedení. (1)

Bezdrátové rozvody se v dnešní době rozšiřují ve spoustě různých technických odvětvích, mezi které patří i zabezpečovací systémy. Tento typ funguje na principu přenosu dat pomocí signálu s vlnovou délkou mezi 433 MHz a 868 MHz. Největší výhodou tohoto typu přenosu je jednoduchá instalace, kterou je možné provést i u dokončeného projektu nebo ve funkčních prostorech. Čidla jsou v těchto systémech napájena bateriemi a je nutné je obnovovat při poklesu napětí, které je signalizováno ústřednou. Právě díky vlnové délce pásma lze počítat s velkým rozsahem signálu, který se může pohybovat řádově od stovek metrů při nižší frekvenci 433 MHz až po tisíce metrů, pokud budeme uvažovat s vyšší frekvencí dosahující 868 MHz. Bohužel největší nevýhodou tohoto systému je snížení rozsahu kvalitního signálu při použití systému v budovách, kde signál prochází několika vrstvami. V těchto případech je možné odhadnout účinný rozsah na desítky metrů. Dalším nebezpečím je úmyslné narušení přenosového pásma útočníkem, kde systém reaguje velice zpomaleně oproti již zmíněnému drátovému rozvodu, kde reakce je ve většině případů okamžitá. (1)

4.2.3 Podle stupně zabezpečení

Pokud jde o zabezpečení, tak je velice důležité mít jistotu, že prvky, které jsou použity při návrhu a konstrukci systému, jsou vysoce spolehlivé a zároveň mají funkce, které jsou potřebné pro daný projekt. Veškeré prvky musí odpovídat určeným stupňům zabezpečení, které jsou rozdělený dle normy ČSN EN 50 131 ed.2. Na prvky dle normy lze nahlížet z několika hledisek. (1) (2)

Dělí se na:

- Přístupové úrovně
- Provozování
- Vyhodnocování
- Detekce
- Napájení
- Zabezpečení při sabotáži
- Monitorování
- Propojení
- Záznam událostí

Dále norma určuje samotné třídy zabezpečení, které je možné vidět v tabulce 1.

Tabulka 1: Stupně zabezpečení

Stupeň	Míra rizika	Předpokládaný typ narušitele
1.	Nízké	Narušitel má malé znalosti PZTS a omezený sortiment snadno dostupných nástrojů
2.	Nízké až střední	Narušitel má určité znalosti o PZTS a omezený sortiment základních přenosových nástrojů
3.	Střední až vysoké	Narušitel je obeznámen s PZTS a úplný sortiment základních přenosových přístrojů a elektrických zařízení
4.	Vysoké	Narušitel je schopen, nebo má možnost zpracovat podrobný plán vniknutí a kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků PZTS

Zdroj: ČSN EN 50 131 ed. 2, 2007

4.2.4 Podle podsystému

Pokud bude brán systém zabezpečení jako jeden, tak dochází k několika problémům, mezi kterými je například ovládání, protože pokud bude systém, který funguje ve dvou různých budovách chráněného objektu, tak časový harmonogram systému je v obou budovách stejný, ale pokud uživatel vyžaduje pro obě budovy například jiný čas spouštění systému, tak je nutno vytvořit takzvané podsystémy, které mohou být obsluhovány a nastaveny odděleně. Ve většině domácností lze nalézt systémy, které jsou rozčleněny na 2 podsystémy, avšak některé ústředny, které jsou uřečeny pro komerční sektor s rozsáhlým systémem mohou být členěny až ve stovkách podsystémů. (1)

4.3 Internet věcí

IoT - Internet of Things (Internet věcí) je systém vzájemně propojených výpočetních zařízení, mechanických a digitálních strojů, objektů, zvířat i lidí, které jsou vybaveny unikátními identifikátory (UID) a schopností přenášet data přes síť bez nutnosti interakce člověk - člověk nebo člověk – počítač. „Věc“ v IoT může být člověk s implantátem monitoru srdce, hospodářské zvíře s transpondérem biočipu, automobily vestavěnými senzory, které upozorní řidiče na možný problém (např. nedostatek paliva,

nízký tlak v pneumatikách, nutnost údržby) nebo jakýkoli jiný přírodní nebo umělý objekt, kterému lze přiřadit adresu internetového protokolu (IP) a je schopen přenášet data přes síť. Organizace v různých průmyslových odvětvích stále více využívají IoT k efektivnějšímu fungování a lepšímu porozumění zákazníkům, aby mohli poskytovat vylepšené služby zákazníkům a měli možnost lépe rozhodovat a navyšovat hodnotu podnikání. (3)

IoT se skládá z inteligentních zařízení s podporou webu, která používají vestavěné systémy, jako jsou procesory, senzory a komunikační hardware, ke shromažďování, odesílání a chování na základě získaných dat. Tyto zařízení sdílejí data ze senzorů, která shromažďují a analyzují. Připojením k bráně IoT nebo jinému hraničnímu zařízení, se data odesílají do cloudu. Zde dochází k jejich zpracování a následně tato zařízení mohou komunikovat s jinými připojenými „chytrými" zařízeními, která „jednají" na základě informací, které od sebe navzájem získají. Inteligentní zařízení provádí většinu činnosti bez lidského zásahu. Lidé mohou zařízení např. nastavit nebo jim dát určitý pokyn, případně i k získaným datům přistupovat. Protokoly připojení, sítě a komunikace používané těmito zařízeními do značné míry závisí na konkrétních nasazených aplikacích IoT. Internet věcí může také využívat umělou inteligenci a strojové učení, které pomáhá usnadnit procesy sběru dat. (4)

4.3.1 Aplikace a nasazení

Existuje mnoho aplikací IoT, od spotřebitelského a podnikového až po výrobní a průmyslový. Aplikace IoT pokrývají řadu odvětví, např. automobilové, telekomunikační nebo energetické. Asi nejznámějším způsobem nasazení je spotřebitelský segment, kdy prostřednictvím počítače nebo smartphone lze ovládat na dálku tzv. chytrou domácnost, která je vybavena chytrými termostaty nebo jinými senzory (kouře, zaplavení) a chytrými spotřebiči, připojenými ventily pro topení, světly a zásuvkami a dalšími zařízeními.

Zařízení se senzory a softwarem mohou shromažďovat a analyzovat uživatelská data a na jejich základě odesílat zprávy o uživatelích dalším technologiím s cílem usnadnit život jiným uživatelům. Například smartphony uživatelů se senzorem určování polohy a se spuštěnou navigací odesílají data o průjezdu dané trasy a dalším uživatelům, kteří si tuto trasu zvolili, jejich smartphone se stejnou navigací poskytne na základě vyhodnocení dat buď stejnou, nebo jinou optimalizovanou trasu. I ve zdravotnictví nabízí IoT mnoho výhod, včetně možnosti podrobněji sledovat pacienty

pomocí analýzy generovaných dat. Nemocnice často používají systémy IoT k dokončení úkolů, jako je řízení zásob léčiv nebo pro lékařské přístroje. Inteligentní budovy mohou například snížit náklady na energii pomocí senzorů, které detekují, kolik obyvatel je v místnosti. Teplota se může automaticky přizpůsobit např. zapnutím klimatizace, pokud senzory detekují, že konferenční místnost je plná, nebo snížením teploty, pokud všichni opustili kanceláře. V zemědělství mohou inteligentní zemědělské systémy založené na IoT pomocí připojených senzorů monitorovat světlo, teplotu a vlhkost půdy na polích s plodinami a automatizovat zavlažovací systémy. V inteligentním městě mohou senzory s nasazením IoT, jako pouliční 4 osvětlení a inteligentní měřiče, pomoci regulovat dopravu, šetřit energii, monitorovat a řešit problémy životního prostředí a zlepšit hygienu. (4)

4.3.2 Druhy systémů

IoT je založen především na konektivitě, ale protože IoT je široká a mnohostranná oblast, určitě není možné použít jedno univerzální komunikační řešení. Právě proto existuje spousta různých prostředí pro přenos dat.

LPWAN je nízkopříkonová a širokopásmová síť založená na poskytování komunikace s dlouhým dosahem pomocí malých a levných baterií s dlouhou životností. Technologie podporuje sítě IoT v rozsáhlých průmyslových a komerčních areálech. LPWAN mohou propojit všechny typy senzorů IoT. To umožňuje mnoho možností nasazení systémů od sledování aktiv, monitorování životního prostředí a správy budov až po detekci obsazenosti a monitorování spotřebního materiálu. LPWAN mohou odesílat pouze malé bloky dat nízkou rychlostí, a proto jsou vhodné pro nasazení systémů, které nevyžadují velkou šířku pásma a nejsou časově citlivé. (5)

Mobilní 5G sítě jsou spolehlivou širokopásmovou komunikací, které podporují různé hlasové hovory a aplikace pro streamování videa. Nevýhodou jsou vysoké provozní náklady a vysoká spotřeba energie připojených zařízení. Tento druh připojení není vhodný pro většinu systémů, jejichž zařízení jsou napájené bateriemi, ale lze je nalézt např. u automobilů.

Zatímco mobilní sítě nejsou vhodné pro většinu aplikací IoT se senzory napájenými bateriemi, naopak jsou vhodné pro propojené automobily, správu vozového parku nebo dopravu a logistiku. Infotainment ve vozidle, navigace, pokročilé asistenční systémy řidiče nebo sledovací služby vozového parku se mohou spolehnout na všudypřítomnou mobilní konektivitu s vysokou šířkou pásma.

Mobilní síť 5G s podporou vysokorychlostní mobility a nízkou latencí je vhodná pro autonomní vozidla a rozšířenou realitu. Předpokládá se, že 5G umožní video dohled v reálném čase pro veřejnou bezpečnost, přenášení lékařských dat v reálném čase pro sledování zdraví pacientů a časově citlivých průmyslových automatizačních aplikací. (5)

Zigbee je bezdrátový standard s krátkým dosahem a nízkou spotřebou energie, běžně používaný v topologicky širokých sítích, kdy zařízení přenášejí data přes více uzlů. Ve srovnání s LPWAN má Zigbee vyšší přenosovou rychlost, zároveň ale nižší energetickou náročnost, a to díky konfiguraci sítě. (5)

Vzhledem ke krátkému dosahu do 100 m je Zigbee a jemu podobné protokoly (např. Z-Wave, Thread apod.) vhodné pro IoT aplikace středního dosahu s rozložením uzlů jednotlivých zařízení v malých vzdálenostech. Zigbee je tedy vhodné pro domácí IoT jako je chytré osvětlení, zabezpečení a řízení spotřeby energie

Bluetooth je jednou z nejrozšířenějších pro bezdrátový přenos dat na krátkou vzdálenost. Ačkoliv první zmínky o Bluetooth byly v roce 1994 od firmy Ericsson. První verze byla vydána pro širokou veřejnost v roce 1999. O rok později následovala první zařízení a postupně další aktualizace systému.

Přenos dat pomocí technologie Bluetooth je za pomocí radiových vln a tím pádem k jakémukoliv úspěšnému propojení je za potřebí menší vzdálenost a nejlépe i volný prostor mezi zařízeními. Bluetooth několika hlavními verzemi, ale nejaktuálnější verze je 5.0. Tato verze je velice nenáročná na spotřebu energie, a pokud zvětšíme vzdálenost mezi zařízeními, která jsou propojena a chceme mezi nimi přenášet data, tak se jejich přenos zmenší. Zároveň oproti předešlým verzím můžeme přenášet zprávy až o velikosti 255 bajtů, což je pokrok od předešlých verzí, kdy maximální hodnota zprávy mohla dosahovat okolo 30 bajtů. To vše je možné díky tomu, že pracuje na bezlicenčním pásmu 2,4 GHz, což je stejné jako využívá technologie Wi-Fi a využívá metodu FHSS, což je metoda při přenosu dat, kdy data přeskakují mezi frekvencemi s minimálním rozestupem. Klasické Bluetooth bylo původně určené pro výměnu dat point-to-point nebo point-to-multipoint (až sedm podřízených uzlů) mezi zařízeními. Technologie Bluetooth Low-Energy (BLE) je optimalizovaná na spotřebu energie a určená pro malé IoT aplikace. Zařízení s podporou BLE se většinou používají ve spojení se zařízeními, jako smartphony, které slouží jako rozbočovač pro přenos dat do cloudu. Dnes je BLE integrována např. do tzv. nositelných zařízení jako fitness náramků a „chytrých“ hodinek nebo do zdravotnických nositelných zařízení (např.

glukometry). Dále to mohou být i zařízení chytré domácnosti (dveřní zámky), kde jsou data přenášena a vizualizována na smartphonech. (5)

Wi-Fi je technologie s vysokou propustností dat pro firemní a domácí prostředí. Při využití v IoT má však omezení v pokrytí a vysoké spotřebě energie a není tedy vhodná pro IoT s bateriovými senzory. Je možné ji využít pro zařízení, které jsou připojené k rozvodu elektřiny jako domácí spotřebiče nebo bezpečnostní kamery. Nejnovější generace Wi-Fi 7 umožňuje ještě výrazně větší šířku pásma sítě (až 320 MHz) a prostupnost dat (až 46 G/s) a na uživatele v dnes přetíženém prostředí. Veškeré tyto hodnoty udává standard **802.11be**. Při využití Wi-Fi 7 i ve veřejném sektoru by bylo možné tuto technologii převratně využít i v automobilech pro infotainment a diagnostiku. (5)

Radio Frequency Identification (RFID) využívá rádiové vlny k přenosu malého množství dat z RFID tagu do čtečky ve velmi krátké vzdálenosti. Tato technologie usnadňuje např. správu maloobchodu 6 a logistiku. Propojením čárových kódů produktů jako RFID tagů a systému je možné sledovat zásoby a aktiva v reálném čase a plánovat a optimalizovat zásobování nebo výrobu. RFID a jeho propojení se systémy IoT je tedy především využíváno v maloobchodním sektoru, kde se využívají nové aplikace jako Scan&Go (zákazník před vložením zboží do košíku naskenuje čárový pomocí čtečky nebo smartphone a před opuštěním prodejny celý nákup zaplatí, aniž by jej musel znovu na pokladně vyndat na pás), chytré regály, samoobslužné pokladny nebo chytré inventury. (5)

4.4 Cloud

Cloud je na internetu už delší dobu známým pojmem a většina uživatelů vnímá možnost využívat tento typ úložiště jako standardní možnost. Princip je velice jednoduchý a nabízí uživatelům široké možnosti, protože pokud uživatel potřebuje například zálohovat složky, data či jakékoliv jiné soubory a nemá fyzické úložiště na které by mohl nahrát obsah, který se snaží uchovat, tak může využít právě cloud, pokud využívá určitou službu nebo prostředí. Zároveň je možné, aby několik zařízení klidně i cizích uživatelů mohlo sdílet jedno cloudové úložiště a tím i sdílet veškeré soubory nahrané v této pomyslné databázi. Při všech těchto funkcích ani jedno fyzické zařízení není využito jako server, ale je danému uživateli propůjčen část servu, který vlastní daná společnost.

4.4.1 Veřejný

Tento druh cloudu je jedním z nerozšířenějších typů tohoto úložiště dnešní doby. V principu je úložiště spravováno firmou, která se specializuje na poskytování této služby a zákazníci využívají toto úložiště buď zadarmo nebo za poplatek, který je stanoven firmou, která zprostředkovává tuto službu. Název tohoto druhu cloudového úložiště je odvozen od architektury, kdy jeden hardware je pronajímán více uživatelům. Největší výhodou tohoto druhu je velice nízká cena právě díky spoluvlastnictví hardwaru několika různými uživateli, což snižuje celkovou cenu, která by na jednoho uživatele mohla být až příliš vysoká. (6) (7)

4.4.2 Privátní

Typ privátního cloudu je přímým opakem veřejného. Tím pádem jak hardware, tak software je vlastněn jedním uživatelem a veškeré procesy probíhají na dedikované síti. S tímto typem je možné se setkat buď u samotných cloudových poskytovatelů, kteří musí dodržet již zmíněné podmínky dedikovaného serveru za zvýšenou cenu nebo tento server, který je využíván pro ukládání uživatelských dat, je přímo v datacentru zákazníka.

Hlavní myšlenka, která stojí za vznikem privátních cloudů je bezpečnost a kontrola, protože pokud veškeré procesy, kterými uživatelská data prochází, se dějí na síti, kde je pouze jeden uživatel, tak je snížené riziko případného úspěšného útoku na server. Avšak tento princip má také velkou nevýhodu v podobě ceny a ztrátě flexibility. (6) (7)

4.4.3 Hybridní

Jak název napovídá, tak hybridní cloud kombinuje výhody privátního a veřejného cloudu, kdy uživateli jsou zpřístupněna dvě úložiště, kde jedno funguje na principu privátního zabezpečení a jsou na něm ukládána data, která jsou kritická nebo citlivá. Následně je zde veřejná část, kde je možné také ukládat méně důležitá data, ale ve většině případů je tato druhá část využívána jako dodatečná výpočetní síla, což znamená, že při výjimečném vytížení, kdy uživatelská privátní část není schopna zpracovat veškeré procesy, tak je dynamicky vytvořen další výpočetní zdroj na veřejném cloudu. Díky tomuto rozpoložení je tento typ úložiště na veliké úrovni zabezpečení, ale také velmi flexibilní v krajních případech. (7)

4.4.4 Distribuční modely

Pojem distribuční modely je označení pro rozdělení podle typu služby, která je poskytovatelem cloudu nabízena. Může se jednat o samotný software, hardware anebo kombinace těchto dvou typů. Základními modely, se kterými je možné se nejčastěji setkat při vyhledávání těchto služeb jsou:

- Infrastruktura jako služba (IaaS)
- Platforma jako služba (PaaS)
- Software jako služba (SaaS)

(8)

4.5 Trendy zabezpečovacích systémů

Technologie jako takové se neustále vyvíjí a zabezpečovací systémy nejsou žádnou výjimkou a spíše naopak se zlepšují rychleji než některá jiná odvětví. Velký skok, který byl v posledních několika letech zaznamenán v zabezpečovacích systémech, je komunikace jednotlivých prvků systému pomocí IoT. Tento krok otevírá možnost pro jednoduchou instalaci fyzických prvků, zlepšení propojené ochrany objektů, ale například i použití umělé inteligence, která by mohla fungovat jako hlasový asistent při horším obrazu kamerového systému nebo pro digitalizaci fyzického prostoru, který by mohl být vložen jako virtuální lokalita, kterou může technik otevřít v aplikaci při jakékoliv příležitosti a kdekoliv, kde se zrovna nachází, dokud je připojen na funkční síť, díky které má přístup k systému.

Jednou z nejvíce ambiciózních inovací v použití IoT jsou takzvaná chytrá města (Smart Cities), která integrují informační, komunikační a digitální technologie do každodenního fungování měst. Například mezi taková města náleží Amsterdam, kde je pouliční osvětlení regulováno dle vytíženosti ulic chodci a touto regulací snižuje energetickou náročnost. U zabezpečovacích prvků můžeme nalézt město v Kalifornii Santa Cruz, které integrovalo technologie monitoringu, kde je pomocí prvků smart city analyzována historie trestné činnosti v jednotlivých částech města a na základě těchto informací poté město posiluje hlídky v oblastech, kde je očekávána vyšší trestná činnost. Stejně tak, jako zmíněná města se i Praha rozvíjí k integraci technologií pro zvýšení úspornosti a celkového zlepšení fungování města o což se například v minulosti již snažila budováním chytrých košů nebo laviček, ale tyto projekty nebyly natolik úspěšné a nápad se nerozšířil. Avšak se zlepšujícími se technologiemi a záměru světové politiky o úspornější provoz měst je očekávatelné, že toto odvětví IoT se bude každým rokem více rozvíjet hlavně pro regulaci, ale také například zabezpečení. (9) (10)

Pro přesnou ukázku výrobků, které mohou být řazeny jako inteligentní zařízení a tím pádem komunikují s ostatními přístroji se kterými jsou propojeny, lze vybrat například pohybové čidlo na bázi PIR od značky Tesla. Tento výrobek může být propojen se světelným obvodem, ale také s ostatními technologiemi jako jsou asistenti pro chytrou domácnost. S těmi komunikuje pomocí Zigbee, ale musí být instalována centrální jednotka. (11)

Další typ výrobku, který je v dnešní době velice rozšířený, jsou automatické pohony pro otevírání brány. Tyto technologie jsou rozšířené kvůli jednoduché instalaci a nízké ceně. Funkce je zařízena používáním aplikace na mobilu, avšak lepší modely mohou mít propojení s automobilem a tím se eliminuje jakákoliv lidská interakce. (12)

4.6 Legislativa

Tím, že se jedná o zabezpečovací systémy, je důležitým bodem jakéhokoliv systému, který zahrnuje zabezpečovací prvky s integrovanými zařízeními využívající principu IoT, sledovat a řídit se předpisy, které stanovují normy, pod které spadají jednotlivá zařízení, která budou použita. Normy, které je nutno sledovat, pokud pracovník aplikuje jakékoliv zařízení, které je určeno pro zabezpečovací nebo poplašné účely, jsou normy ve svazku ČSN EN 50 131 ed.2, který zahrnuje veškeré PZTS a také norma ČSN EN 50 398-1, pod kterou náleží kombinované a integrované poplachové systémy. (2)

4.6.1 ČSN EN 50 131

Tato evropská norma specifikuje požadavky na jednotlivé prvky bezpečnostních systémů, jako jsou například detektory, signalizace a komunikace. Hlavní myšlenka stojící za vznikem této normy je standardizace a poskytnutí směrnic pro instalaci, údržbu a provoz zabezpečovacího systému se zaměřením na minimalizaci rizika pro uživatele a zároveň maximalizaci ochrany objektu. Tento svazek norem lze rozdělit na jednotlivé normy jako jsou například:

- **ČSN EN 50 131-1 ed. 2** Poplachové zabezpečovací systémy a tísňové systémy – Část 1: Systémové požadavky
- **ČSN EN 50 131-2-2 ed. 2** Poplachové zabezpečovací systémy a tísňové systémy – Část 2-2: Detektory narušení – Pasivní infračervené detektory
- **ČSN EN 50 131-2-10 ed. 2** Poplachové zabezpečovací systémy a tísňové systémy – Část 2-10: Detektory narušení – Detektory stavu otevření (magnetické kontakty)

Existuje samozřejmě mnoho dalších, ale tyto normy jsou důležité ke smyslu této práce. Norma se také skládá z několika segmentů, které se zaměřují na přesnou problematiku. Mezi tyto části normy se řadí:

Úvod této normy rozebírá několik jednotlivých aspektů, které jsou důležité pro správné pochopení normy a její aplikaci do reálných podmínek. Hlavní aspekty zahrnují například definice a klíčové pojmy, které zahrnují prvky jako je například bezpečnostní systém, detektor pohybu monitorovací středisko a mnohé další názvy se kterými je pravděpodobné se setkat při práci se zabezpečovacími systémy.

Dále nalezneme v této části obecné principy, které zahrnují zásady na provedení a vlastnosti instalovaných systémů. Mezi těmito zásadami je možné nalézt například kroky pro ochranu osobních údajů a bezpečnosti dat nebo spolehlivost příslušných systémů. Kromě toho první segment zahrnuje rozsah normy, což specifikuje identifikaci typů objektů, aplikace, pro které je norma určena a v neposlední řadě vyloučení konkrétních technologií a aplikací, které nejsou touto normou pokryty. Avšak tato norma neobsahuje požadavky na návrh, projekci, instalaci, provoz a údržbu. Tyto parametry doplňuje norma ČSN CLC/TS 50 131-7.

Oblasti použití pojednávají o typech objektů, ve kterých je možná instalace, jako jsou například domácnosti, komerční budovy, průmyslové objekty, veřejné budovy a specifické aplikace. Každé prostředí, do kterého chce uživatel instalovat zabezpečovací systém je nutno přiřadit do správné kategorie, s tím mohou napomoci

třídy zabezpečení, které jsou zobrazeny v předešlé kapitole pojednávající o rozdělení PZTS podle stupně zabezpečení (viz Tabulka 1).

Systémové požadavky jsou jednou z nejdůležitějších částí normy, a to právě kvůli tomu, že se norma zaměřuje na požadavky jednotlivých bezpečnostních prvků a stanovuje standardy, kterými je nutno se řídit pro korektní následování normy. Je možné rozdělit tento segment do několika různých bodů jako je například: detekce, signalizace, uzávěry, komunikace a napájení.

U detekce norma popisuje požadavky na jednotlivé typy detektorů, jako jsou například senzory pohybu, u kterých norma stanovuje požadavky na citlivost a spolehlivost pro detekci pohybu v závislosti s umístěním ve kterém je daný detektor nainstalován. Dalšími důležitými senzory z hlediska této práce jsou detektory otevření, jako jsou například magnetické kontakty na dveřích. U těchto se norma zaměřuje na spolehlivou detekci při otevírání, zavírání a manipulaci s chráněným objektem.

Velice důležitá část z hlediska této práce je segment ČSN EN 50 131-5-3 ed. 2, která stanovuje požadavky pro zařízení v PZTS, která využívají bezdrátové propojení, avšak zahrnuje pouze spoje, které využívají pro způsob přenosu dat radiokomunikaci a jsou zároveň instalovány ve střežených prostorech a zároveň nepokrývá rádiové komunikace na dlouhé vzdálenosti. Tím, že v této normě nejsou zahrnuta zařízení, která jsou používána pro systémy, které využívají technologií integrovaných komunikačních spojů, tak je nutné nalézt normu, která udává pravidla a požadavky pro tuto část poplašných a zabezpečovacích prvků. (2)

4.6.2 ČSN EN 50 398-1

Tato evropská norma se zaměřuje na kombinované a integrované poplachové systémy, jak bylo zmíněno v úvodní části této kapitoly. Norma definuje požadavky a postupy pro základní zkoušky specifických aspektů funkčnosti a integrity, které jsou úzce spojeny se sloučením, ke kterému dochází mezi zařízeními nebo systémy a aplikacemi. (24)

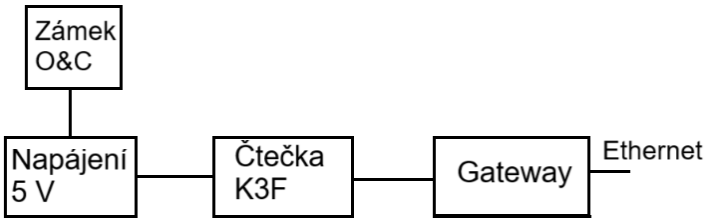
Norma se převážně zaměřuje na detekci ohně a kouře, avšak pro tuto práci je nejdůležitější část, která pojednává o odolnosti proti rušení z vnějších zdrojů, mezi které lze zařadit elektromagnetické rušení, vibrace a další podobné faktory, které mají velký dopad na spolehlivost a výkon. (24)

5 Praktická část

5.1 Pojednání o projektu

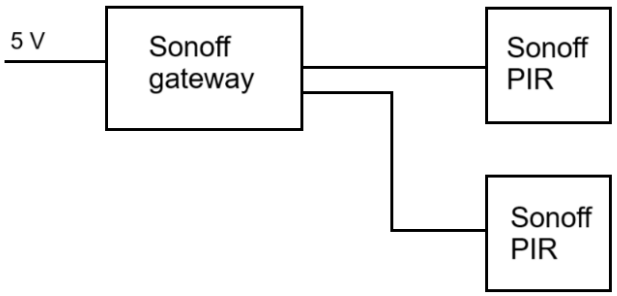
Praktická část se zaměřuje na problematiku poplachových a zabezpečovacích systémů, které mají zakomponované prvky, jež jsou schopny komunikace mezi sebou i bez lidského zásahu. Zároveň při prvním návrhu projektu pro praktickou část bylo v plánu, že do něj budou zakomponovány dva různé pohledy na podobnou problematiku, a to hlavně ze stránky cenové náročnosti a znalostech, které jsou potřebné k navržení, instalaci a ovládání systému. Proto byly navrženy 2 systémy, které fungují jako zabezpečovací prvky s využitím IoT.

Prvním z těchto projektů je systém inteligentního terminálu, přes který lze ovládat magnetický kontakt nainstalovaný na vchodových dveřích a pro účel této práce bude tato část nazývána jako Projekt 1. Zapojení mezi prvky je viditelné v podobě blokového schématu viz Obrázek č. 1.



Obrázek 1 Blokové schéma Projektu 1 (vlastní)

Druhý segment praktické části je systém, který tvoří dva pohybové PIR senzory, které jsou propojeny s gateway, přes kterou je možné sledovat detekci těchto senzorů a zároveň s nimi dále pracovat pro zvýšení účinnosti nebo propojování s dalšími prvky. Po celou praktickou část bude tento systém označován jako Projekt 2. Pro ilustraci je možné vidět blokové schéma na Obrázku č. 2.

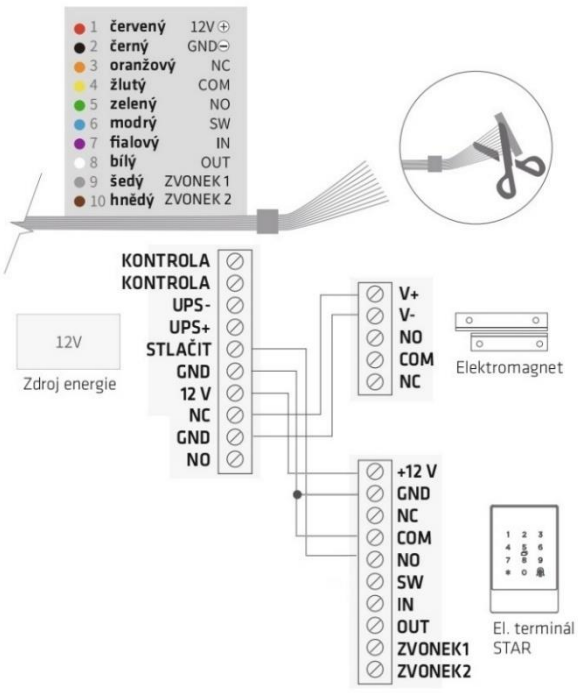


Obrázek 2 Blokové schéma Projekt 2 (vlastní)

5.2 Návrhy projektů

Z počátku bylo v plánu vytvořit jednotný systém, kde by veškeré senzory a ostatní prvky dokázaly mezi sebou komunikovat, aniž by je musel kdokoliv ovládat po instalaci, avšak pro účel projektů nebylo možné nalézt produkty, které by nastiňovaly finanční rozdíl, a tak byl tento systém rozdělen na dva různé.

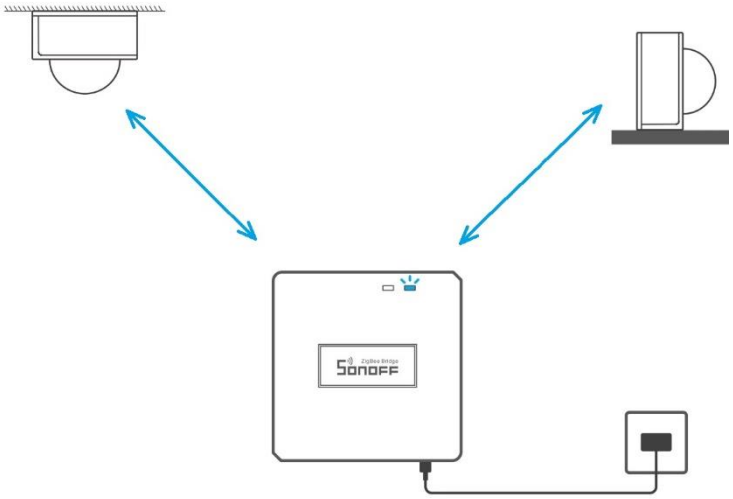
Projekt 1 byl navržen s vyššími finančními prostředky, které dovolovaly pořídit novější typ technologie od známějších a prokazatelně spolehlivých značek, které mají vysoký ohlas v tomto okruhu jak mezi techniky, tak uživateli. Smyslem tohoto projektu bylo navrhnout jednoduchý systém s přístupovým terminálem, který bude mít několik možností ovládání a bude mít vysokou spolehlivost. Právě proto byl vybrán Elektronický terminál STAR – K3F, který má jednoduché zapojení a velkou rozmanitost funkcí. Tento terminál komunikuje s Elektromagnetickým zámkem O&C MEX100 přes zdroj, který má funkci pro vstup impulsů a terminál do něj zasílá informace, kdy má zdroj napájet elektromagnet, zároveň tento zdroj napájí terminál 12 V stejnosměrného napětí. Terminál komunikuje s mobilním telefonem uživatele přes gateway STAR Smart. Zapojení lze vidět na Obrázku č. 3. (13)



Obrázek 3 Zapojení obvodu terminálu (upraveno) (13)

Na Obrázku č. 3 je také možné si všimnout barevného značení jednotlivých spojů. To zajišťuje spolehlivé rozpoznání jednotlivých propojení mezi prvky a tím zvyšuje i jistotu správného zapojení i bez podrobné znalosti celého napájecího obvodu. Toto zapojení je součástí uživatelského návodu, který lze nalézt zdarma na stránkách produktu nebo dorazí v balení se zásilkou.

Projekt 2 byl navržen s myšlenkou, že budou tyto dva systémy odděleny a bylo rozhodnuto při plánování obvodu zaměřit se na méně známé značky, které jsou oblíbené převážně velice nízkou pořizovací cenou, ale zároveň představují nejistotu u jejich spolehlivosti a funkčnosti. Pro tento účel byla zvolena značka SONOFF. Tento výrobce se zaměřuje převážně na širokou škálu elektronických produktů, které mají funkce sahající od chytré domácnosti až po chytré zabezpečení. Při vyhledávání senzorů byl zvolen typ SONOFF SNZB-03, který zaujmul drobnou konstrukcí a dobrými parametry při tomto cenovém ohodnocení. Dále bylo potřeba pořídit prvek, který bude propojovat senzory s mobilním telefonem, aby mohla být data ukládána v aplikaci. To bylo vyřešeno pořízením SONOFF ZB Bridge-P, což je prvek, který komunikuje s jednotlivými zařízeními, která jsou na něj připojená (viz Obrázek č. 4) a v tomto systému funguje jako most s mobilní aplikací, kde může uživatel ovládat nastavení jednotlivých prvků, které jsou spárovány s mobilním zařízení.



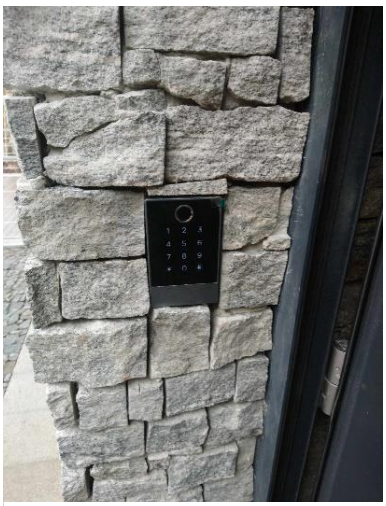
Obrázek 4 Komunikace mezi PIR senzory a Gateway (upraveno) (14) (15)

5.3 Rozbor použitých prvků u projektu 1

Za správným fungováním jakéhokoliv obvodu jsou vždy vědomosti a informace technika, které má o daném systému. K chybám může dojít například špatnou instalací prvku nebo rušivými vlivy, se kterými nebylo počítáno. Právě proto v této kapitole budou jednotlivé prvky tohoto projektu sepsány a bude vysvětlen jejich princip.

5.3.1 Terminál K3F

Jako první a zároveň nejdůležitější část tohoto obvodu, je Elektronický terminál K3F od společnosti STAR. Jako většina terminálů je i tento tvořen integrovanou dotykovou klávesnicí, jak je možné vidět na Obrázku č. 5.



Obrázek 5 Terminál K3F (vlastní)

Princip používání tohoto terminálu je jednoduchý, protože stačí zadat předem nastavený kód a tím uživatel dveře otevře. Dalšími způsoby, kterými je možné aktivovat terminál, aby otevřel elektromagnetický spínač je například otisk prstu, e-klíč a čipy na principu technologie RFID. (13)

Co se týče technických parametrů, tak výrobce udává následující:

- **Model:** K3F
- **Rozměry:** 80 mm x 125 mm x 15,5 mm
- **Materiál:** Tvrzený skleněný panel, hliníkový rám
- **Komunikace:** Bluetooth 4.1
- **Podporovaný systém:** Android 4.3/IOS7.0
- **Pohotovostní proud:** ~ 5 mA
- **Provozní napětí:** ~ 1 A
- **Zdroj napětí:** 12 V DC
- **Doba pro odemknutí v sek.:** 1.5 s
- **Kapacita čipů/PIN kódů:** max 2000/500
- **Kapacita otisků prstů:** max 100
- **IP krytí:** IP 67

(13)

Zároveň výrobce varuje proti maximálním teplotám pro správnou funkci, které sahají od -25 °C až po 65 °C. Dalším parametrem, který bude zmíněn je ten, že terminál automaticky ukládá historii vstupů, pokud je tak nastaven v uživatelské aplikaci, což je v některých použitích potřeba například ve scénáři, kdy je toto zařízení použito pro firmu čítající 800 zaměstnanců, což je i standardně maximální hodnota zařízení, čipů a další přístupových prvků, kterou udává výrobce. (13)

Průběh funkce systému je možné vyčíst ze Obrázku č. 3, kde je na terminál přivedeno stejnosměrné napětí v hodnotě 12 V společně se zemnícím vodičem na vstup a z výstupu je poté veden vodič zpět do zdroje a tímto je ovládáno napájení elektromagnetického zámku. (13)

5.3.2 Elektromagnetický zámek O&C MEX100

Další vysoce důležitý prvek tohoto systému je samotný zámek, který zabezpečuje dveře, na kterých je nainstalovaný. Elektromagnety fungují na jednoduchém principu, kdy cívkou, která je v jedné straně zámku, prochází proud a tím, že cívka má jádro, které je tvořeno měkkou ocelí, tak vytváří magnetické pole, jehož intenzita je přímo úměrná velikosti procházejícího proudu a počtu závitů cívky. Toto magnetické pole následně přitáhne druhou část zámku, která je tvořena nejlépe feromagnetickým kovem jako je například železo, nikl, kobalt a slitiny s obsahem železa. Obě části elektromagnetického kontaktu jsou viditelné na Obrázku č. 6. (16)

Obrázek 6 Ilustrační fotografie elektromagnetického zámku O&C MEX100 (17)

5.3.3 Gateway STAR smart modul G3

Třetí velice důležitý prvek tohoto systému je gateway, která zajišťuje komunikaci mezi zařízeními pomocí internetu. V principu každá gateway může být použita jako propojovací článek mezi dvěma různými sítěmi LAN, takže lze tento proces popsat, že pokud je uživatel v neznámé síti LAN a nutně se potřebuje spojit se zařízením v jiné LAN síti, ke které má přístup, tak mu to gateway umožňuje.

V tomto případě, slouží toto zařízení pro komunikaci mezi terminálem a aplikací, kterou může mít uživatel na svém osobní zařízení jako je například mobil nebo PC. Následně je možné ovládat terminál po celém světě bez ohledu na lokalitu a vzdálenosti, pokud se uživatel dokáže připojit na síť WAN. Pro zvýšení spolehlivosti a jednoduchost byl modul G3, který je možné vidět na Obrázku č. 7, zapojen přes Ethernet, tímto krokem lze vyřešit některé problémy, které by mohly nastat, pokud by se systém nacházel v oblasti se špatným Wi-Fi signálem. (18)

Obrázek 7 Ilustrační fotografie Gateway STAR modulu G3 (18)

Dále výrobce udává základní technické parametry:

- **Model:** G3
- **Rozměry:** 70 mm x 70 mm x 26 mm
- **Rozhraní pro síť:** Ethernet
- **Rozhraní pro napájení:** Ethernet

(18)

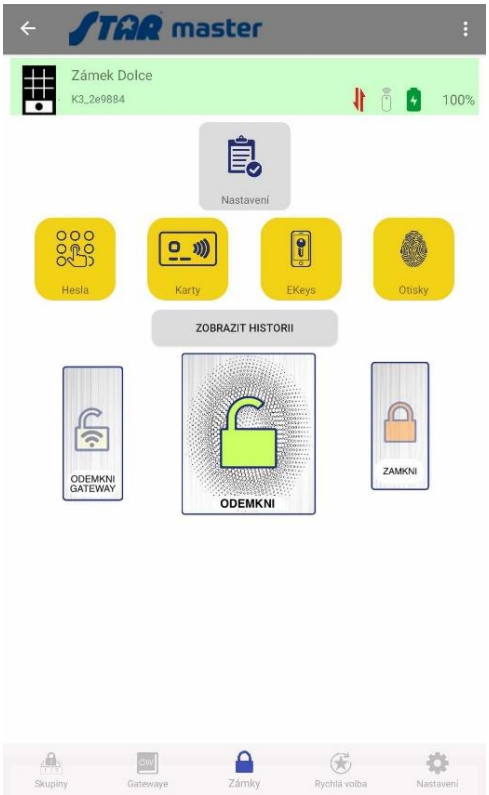
5.4 Realizace projektu 1

Základním bodem realizace, bylo převážně zapojení jednotlivých zařízení. V první řadě byl terminál připevněn k podložce, která je založena ve zdi u vchodu. Následně byly zapojeny jednotlivé spoje s tím, že přívod byl zapojen jako poslední. Dále při konstrukci byla přesunuta pozornost k elektromagnetickému zámku, který byl nainstalován na vchodové dveře a připojen na napájení 12 V stejnosměrného napětí. Celý tento proces zabral nejvíce času z celé instalace, odhadem přibližně 45 minut, což bylo zaviněno opakovanými kontrolami zapojení.

Jakmile byl celý systém fyzicky propojen, tak začala instalace gateway, která byla zapojena do hlavní elektrické sítě přes napájecí zdroj, který zajišťuje napájení stejnosměrným napětí o velikosti 5 V a proudem 500 mA. Po kontrole, že gateway je řádně zapojena, byla propojena s mobilním zařízením pomocí předem stažené aplikace STAR master. Po tomto kroku byl na gateway připojen terminál K3F, který byl nastaven dle požadavků uživatele. Při nastavení aplikace byl postup řízen návodem od výrobce, který je volně dostupný na stránkách výrobku.

5.5 Uživatelské rozhraní projektu 1

Systémy od značky STAR je možné ovládat přes jejich aplikaci STAR master viz Obrázek č. 8 Tato aplikace dovoluje technikovi, ale hlavně uživateli přizpůsobit systém dle jeho potřeb a zároveň získávat veškeré informace, které systém může zaznamenávat. Velkou výhodou je správa jednotlivých prvků, které jsou připojeny na gateway a zároveň řízení další případných uživatelů. Největší výhoda, dle mého názoru je možnost zamykat a odemykat vchodové dveře, i když je uživatel vzdálený mimo oblast, kde se systém nachází. Rozhodně je to další znatelný krok vývoje k integraci zabezpečovacích technologií a Internetu věcí.



Obrázek 8 Design aplikace STAR master (vlastní)

5.6 Testování spolehlivosti projektu 1

Systém byl otestován z důvodu ověření spolehlivosti. Jak bylo zmíněno v předešlé kapitole 5.5, tak je možné dálkově ovládat zámek za pomoci aplikace, což sebou nese samozřejmě určité domněnky, zdali systém bude za každé okolnosti fungovat tak, jak má a nedojde tím pádem k otevření nebo zavření dveří bez uživatelova vědomí. Tato myšlenka byla testována procesem, kdy bylo opakovaně v aplikaci stisknuto tlačítko pro zamknutí a odemknutí dveří, aby bylo ověřeno, zdali budou mít nějakou chybovost. Jak je možné vidět v prvním sloupci Tabulky č. 2, tak zámek byl ve 100% spolehlivý.

V tomto bodě byl průběh měření upraven ke snížení kvality signálu, na které bylo mobilní zařízení připojeno, protože snížené množství přenesených dat by mělo mít účinky na fungování systému. Tohoto umělého snižování kvality připojení bylo docíleno zvyšováním vzdálenosti mezi mobilním zřízením a routeru na kterém byl telefon celou dobu pokusu připojen. Jak je možné vidět, tak při první a druhém zhoršení signálu nedošlo ke změně, avšak u třetího poklesu je viditelné, že úspěšnost klesla o 2 %, což bylo v tomto momentu lehce znepokojivé. Větší skok nastal, když bylo připojeno zařízení na tento systém s velice špatným přenosem, protože tehdy se spolehlivost, při které byl zámek schopen poslouchat ovládání z aplikace, se snížila na 8 %. U konečné úrovně byl přenos téměř nulový a tím došlo k ohromnému skoku, kdy spolehlivost byla rovna 6 %. Lze očekávat, že statistika by byla mnohem přesnější, čím více pokusů by bylo vykonáno, avšak z důvodu časového omezení k přístupu objektu, byla tato statistika zpracována v tomto počtu pokusů.

Tabulka 2: Závislost spolehlivosti na síle signálu

Grafické znázornění síly signálu					
Síla signálu (dBm)	> -50	-50 až -60	-60 až -70	-70 až -80	< -85
Počet pokusů / Počet úspěšných	100 / 100	100 / 100	100 / 98	100 / 92	100 / 6
Spolehlivost (%)	100	100	98	92	6

Zdroj: vlastní šetření, 2024; GoGlides.dev, 2023 (20)

Toto měření mělo za účel zjistit, jak vysokou spolehlivost lze očekávat od tohoto systému, pokud je uživatel připojen na Wi-Fi, která má špatné přenosové vlastnosti například z důvodu rušení. Výsledkem je, že v krajních případech je lepší použít mobilní data nebo se připojit na Wi-Fi s lepšími přenosovými vlastnostmi.

5.7 Rozbor použitých prvků u projektu 2

Stejně jako u Projektu 1, tak i Projekt 2 by nemusel fungovat dle určených parametrů, pokud by byly jakékoliv prvky použity ve špatném smyslu, než v jakém byly navrženy a vyrobeny. K prvkům v tomto projektu patří celkem 2, a to pohybové PIR senzory od značky SONOFF a zároveň gateway od stejnojmenné značky k propojení všech okolních zařízení, která se nachází v tomto daném systému a jsou kompatibilní s typem komunikace Zigbee.

5.7.1 SONOFF SNZB-03 Zigbee chytrý pohybový PIR senzor

Tento obvod byl zamýšlen jako levná, ale spolehlivá alternativa, která bude fungovat se dvěma pohybovými senzory, se kterými je možné manipulovat v případě potřeby, aniž by bylo nutné je, jakkoliv odpojovat. Právě proto byly vybrány PIR senzor od značky SONOFF viz Obrázek č. 9, které byly cenově velice nízké oproti konkurenci a zároveň zajišťují velice jednoduchou uživatelskou instalaci, kterou je schopen provést samotný zákazník se základními znalostmi chytrých technologií. Avšak bez znalosti samotného čidla by mohl zákazník nevědomky umístit senzor do špatné oblasti, ve které by čidlo nefungovalo, jak bylo zamýšleno.

Obrázek 9 PIR senzor SNZB-03 (vlastní)

Princip PIR čidel je postaven na bázi infračerveného záření, které dokáže detekovat pohyb za pomoci změn, které probíhají v měřeném prostředí. Důležitý bod, který je nutno zmínit, je vlastnost čidla být pasivním, což znamená, že čidlo nevysílá signál jako některé ostatní typy, ale pouze přijímá tepelné záření z objektů v perimetru, kde se čidlo nachází. S tímto je důležité zmínit, že čidlo v našem senzoru přijímá jako signál pohybu jakéhokoliv změnu tepelného záření, které se bude nacházet v aktivním poli daného čidla, Právě z tohoto důvodu musí uživatel přemýšlet nad místem, do kterého tento senzor bude instalovat, protože s dostatečným slunečním svitem by senzor nemusel detekovat jakýkoliv pohyb. (19)

Poslední důležitou vlastností tohoto senzoru je schopnost být propojeno s mobilní aplikací uživatele, kde je možné vytvořit virtuální prostředí a spojit například další prvky systému bez fyzického zapojení. To zajišťuje Zigbee, na jehož principu je založen tento systém. Všechny potřebné informace udává výrobce v návodu k instalaci, kde se nachází i technické parametry:

- **Model:** SNZB-03
- **Model napájecí baterie:** CR2450 (3 V)
- **Komunikace:** ZigBee (IEEE 802. 15. 4)
- **Pracovní teplota:** -10 °C až 40 °C
- **Pracovní vlhkost:** 10 až 90 % RH (nekondenzující)
- **Rozměry:** 40 mm x 35 mm x 28 mm

(14)

5.7.2 SONOFF Zigbee Bridge-P

Stejně jako u Projektu 1 je nutné vytvořit prostředí, ve kterém mohou jednotlivé prvky systému společně komunikovat a pomocí kterého jsme schopni ovlivňovat funkce a propojení jednotlivých prvků v systému. Pro tuto funkci je připojeno zařízení SONOFF Zigbee Bridge-P, které zajišťuje propojení mezi jednotlivými prvky obvodu. Princip tohoto zařízení je totožný s již zmíněným výrobkem v kapitole 5.3.3, ale na první pohled je viditelný značný rozdíl viz Obrázek č. 10.

Obrázek 10 SONOFF Zigbee Bridge-P (vlastní)

Dále výrobce udává technické parametry pro správnou funkci tohoto zařízení a jeho technické vlastnosti:

- **Model:** ZBBridge
- **Vstupní napětí a proud:** 5 V a 1 A DC
- **Verze ZigBee:** Zigbee 3.0
- **Wi-Fi:** IEEE 802. 11 b/n/n 2.4 GHz
- **Operační systémy:** Android & iOS
- **Pracovní teplota:** -10 °C až 40 °C
- **Rozměry:** 62 mm x 62 mm x 20 mm

(15)

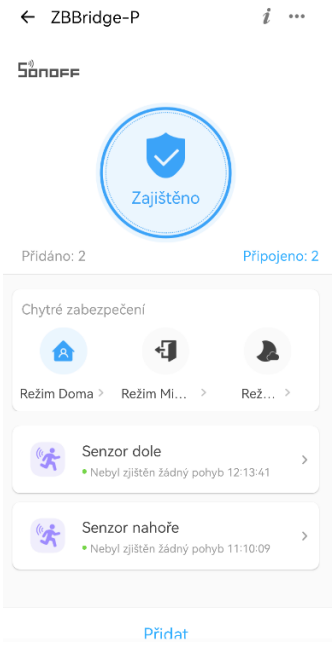
5.8 Realizace projektu 2

Instalace Projektu 2 byla oproti předešlému projektu znatelně jednodušší, a to právě díky bezdrátovému připojení jednotlivých prvků. Jako první zařízení, které bylo uvedeno do provozu byla gateway, která byla zapojena přes zdroj napětí do hlavní elektrické sítě. Tento zdroj napětí upravoval napájecí hodnoty na 5 V stejnosměrného napětí a 1 A stejnosměrného proudu. Následně byla po této aktivaci otevřena aplikace v mobilním zařízení, kde bylo zařízení vyhledáno za pomocí Bluetooth. Po krátkém spárování bylo zařízení připraveno k propojení se zbytkem systému.

Senzory byly aktivovány následováním uživatelského katalogu, kde byl v krátkých krocích popsán proces, které by měl uživatel následovat. Po tomto spuštění obou senzorů byly spárovány v aplikaci s gateway, aby mohl zákazník získávat veškeré záznamy o jejich funkcích. Po tomto dokončení tohoto kroku byl obvod otestován v jeho funkci a správnosti propojení s aplikací.

5.9 Uživatelské rozhraní projektu 2

Jak již bylo zmíněno, tak i v tomto projektu uživatel propojuje svůj mobilní telefon přes aplikaci eWeLink (viz Obrázek č. 11) s ostatními zařízeními a tímto spojem komunikují jednotlivé prvky mezi sebou. Zároveň je možné vytvářet takzvané scény, kde můžeme propojit jednotlivá zařízení, aby byly prvky spojeny a mohli jsme tím vytvářet sekvence pro osobní potřeby. Příkladem může být propojení jednoho pohybového senzoru na světelný obvod a spojení druhého senzoru, který je propojen s alarmem. Tato funkce je jedna z nejflexibilnějších, protože ve virtuální aplikaci je možné měnit smysl některých již nainstalovaných prvků bez propojování fyzických spojů. V aplikaci lze také zobrazit historii aktivací jednotlivých senzorů, jak je možné vidět na Obrázku č. 12.



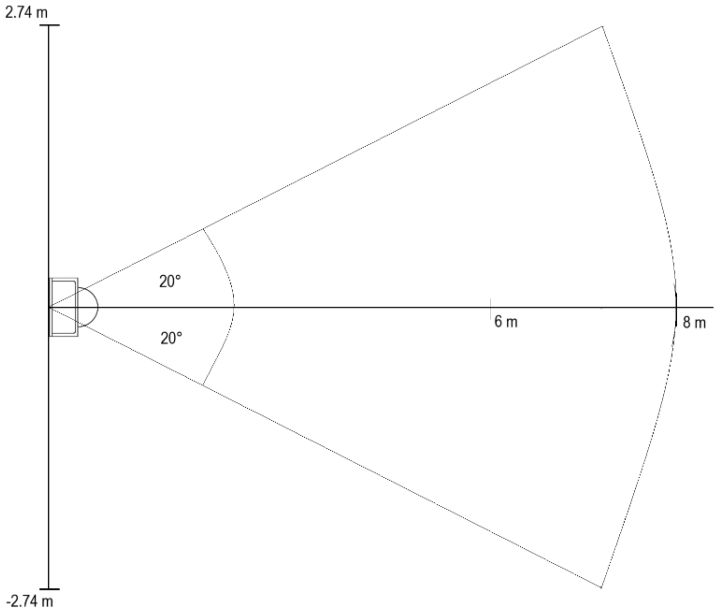
Obrázek 11 Aplikace eWeLink (vlastní)

Obrázek 12 Záznam historie aktivací (vlastní)

5.10 Ověření detekčních vlastností senzoru

Pro kontrolu použitých senzorů bylo nutno ověřit spolehlivost měření a maximální detekční vzdálenost podle té, kterou udává výrobce. Tato zkouška byla provedena v prostředí bez přímého světelného záření a spočívá v tom, že je senzor postaven na platformu, kde může detektor využít svůj maximální detekční potenciál. V tomto případě bylo prostředí připraveno dle parametrů od výrobce a maximální vzdálenost byla nastavena na 6 m. Poté byla zkouška provedena opakovaným přiblížením k danému senzoru objektem, který je detektor schopen zaznamenat. Tento objekt se přibližoval ze tří různých směrů, které byly před tímto pokusem určeny. Pro základní vyhodnocení byly použity směry pod úhly 70°, 90° a 110°, což je v maximálním rozmezí, které udává výrobce.

Při počátku testu byl senzor aktivovaný i přes to, že testovací subjekt byl v prostoru za maximálním dosahem senzoru. Tato aktivace trvala, než byl objekt přesunut do vzdálenosti 9 m. Až v tomto momentu byl senzor deaktivován a nezaznamenával jakýkoliv pohyb. V tento moment započal objekt pohyb k senzoru. Ten se však přes očekávání aktivoval již na hranici 8 m, a to při opakovaném zkoušení. Měření pokračovalo ve stejném duchu u všech směrů. Měření bylo zopakováno pod každým úhlem padesátkrát, ale i přesto byla účinnost aktivace 100 %.



Obrázek 13 Grafické znázornění provedeného měřené (vlastní)

Podobné měření bylo provedeno i ve vertikálním směru, kde byla měřená vzdálenost detekce, ale také maximální úhel. Následně po ukončení měření byla data zpracována a bylo sestaveno grafické znázornění viz Obrázek č. 13, které nastiňuje přibližný perimetr detekce, ve kterém je senzor schopný zaznamenat pohyb.

Je možné si povšimnout rozdílu, který je mezi hodnotou danou výrobcem a hodnotou naměřenou. Tím, že horizontální perimetr je srovnatelný s vertikálním, tak lze zobrazit toto měření v jednom zobrazení viz Obrázek č. 13. I přes umístění senzoru do prostoru, kde nebylo přímé světelné záření, mohlo docházet ke zkreslení měřených hodnot. Avšak bylo i přesto překvapivé, že senzor dokázal detekovat pohyb na vyšší vzdálenost, než která je udána výrobcem.

5.11 Finanční náročnost jednotlivých projektů

Důležitým parametrem, podle kterého byly vybrány jednotlivé prvky daných projektů je pořizovací cena. Jak bylo již zmíněno v úvodním segmentu praktické části, tak oba projekty se zásadně rozdělují cenovou hladinou, ve které byly navrženy.

Oba projekty lze tedy rozdělit jednoduše dle výši potřebných finančních prostředků. Projekt 1 dosáhl cenové hodnoty bez přidané práce, ceny zdroje energie a ceny použitých vodičů, kterými byli některé prvky obvodu propojeny, na přibližných 8000 Kč. Projekt 2 byl navržen pro nízkou cenovou kategorii a díky tomu se jeho hodnota vyšplhala na pouhých 1030 Kč, což je znatelný rozdíl mezi projekty. Ceny jednotlivých prvků lze nalézt v Tabulce č. 3.

Tabulka 3 Finanční náročnost jednotlivých prvků a celková hodnota

Projekt 1			Projekt 2	
Zařízení	Cena (Kč)		Zařízení	Cena (Kč)
Stěnová čtečka STAR Smart	3 497		Sonoff SNZB-03 ZigBee Motion Sensor	279
Elektromagnetický zámek O&C MEX100	2 491		Sonoff ZB Bridge-P	649
Modul Gateway STAR Smart	1 997			
Celková hodnota	7 985		Celková hodnota	928

Zdroj: Klicovecentrum.cz, 2024 (18) (19) (21); Alza.cz, 2024 (23) (24)

Avšak každý z těchto dvou projektů je rozdílný jak cenově, tak i funkcí, kterou splňují a z tohoto důvodu nelze mezi těmito cenami hledat prokazatelnou spojitost. Na druhou stranu je toto ukázka, že lze vytvořit různé prvky zabezpečení v různých cenových rovinách, ale při faktu toho, že pokud budou jednotlivé prvky vybrány špatně, tak společně nemusí komunikovat, což bohužel eliminuje prvek propojenosti celého zabezpečovacího obvodu.

5.12 Výsledné hodnocení systému

Jak bylo několikrát zmíněno, tak oba systémy je nutné hodnotit odděleně právě z důvodu jejich různých funkcí a zároveň, jak již bylo několikrát v této práci zmíněno, jejich odlišných finančních nároků. Avšak lze provést základní rozbor, ve kterém lze pojednávat o jednotlivých vlastnostech, které mohou být převážně pro uživatele důležité. Nejdříve bude vyhodnocen Projekt 1

Projekt 1 byl specifický převážně díky požadavkům uživatele, kterému byl systém nainstalován do jeho domácnosti. Tím, že z prvopočátku bylo jisté, že systém bude integrovaný s prvky IoT, bylo jasné odvození systémových vlastností na kvalitě poskytnutého přenosového prostředí, do kterého byly prvky instalovány. Tou nejdůležitější vlastností byla spolehlivost, bez které by systém nemohl být řazen jako zabezpečovací. Přesvědčení o kvalitě zařízeních, která byla instalována vzrostlo díky měření, jehož výsledky je možné nalézt v Tabulce č. 2, kde je přesněji popsán proces zhoršování spolehlivosti. Ta se zhoršila až v momentu, kdy bylo mobilní zařízení prakticky odpojeno od internetu, takže lze prohlásit systém jako vysoce spolehlivý, ačkoliv s vyšší cenovou náročností.

Projekt 2 je typ systému, který je téměř pravým opakem projektu 1. I přesto, že systém má zabezpečovací prvky, tak jsou tyto senzory na úplně jiném principu než zmíněný elektromagnetický spínač. Hlavním bodem tohoto projektu byla myšlenka navrhnout systém, který by dokázal fungovat, jako poplachový, a to za co nejpřijatelnější cenu. Díky správnému výběru detekční prvky systému překonaly očekávání s jejich maximální naměřenou detekční vzdáleností, která přesahovala udanou hodnotu od výrobce. Společně s nízkou cenou, jednoduchou instalací a prostředky v aplikaci, se kterými je možné vytvořit systémy s jedinečnými funkcemi dle každého majitele, tak je zde systém, který definitivně nalezne skupinu uživatelů, kteří budou aktivně odebírat tyto výrobky.

Ve shrnutí by bylo dobré ujasnit, že díky podobným systémům, které byli zpracovány v této praktické části, bude propojení PZTS a IoT nevyhnutelné například pro oblasti jako jsou domácnosti nebo malé podniky. Ale pokud by bylo v blízké době nutno navrhnou systémy podobného principu, tak lze vybrat prvky, které budou vzájemně kompatibilní a tímto krokem je možné sestavit zabezpečovací systém, který bude řízen jednotně.

6 Závěr

Zadáním práce bylo prozkoumat a popsat základní typy trendů v zabezpečovacích technologií se zaměřením na technologie s prvky IoT. Následně bylo dáno, že bude sestrojen obvod, který bude na tomto principu fungovat. Tento obvod po sestrojení a následné kontrole funkčnosti byl zkoušen různými typy testovacích procesů.

První část se zaměřuje na rozbor zabezpečovacích technologií, které se rozdělují dle různých parametrů a popis jednotlivých typů na které jsou tyto technologie rozděleny. Dále se v této části pojednává o technologii IoT, která je principiálně popsána a je proveden krátký rozbor o různých možnostech, které tato technologie dovoluje. Zároveň jsou zde rozebrány typy komunikací, kterých lze využívat, pokud se v praxi setkáme s možností vybírat druh této komunikace. Každý tento typ má své specifické vlastnosti, díky kterým je lze rozdělit pro případná použití v praxi. Posledním bodem první části je rozbor o technologii cloud a jeho druhy. V kapitole je Cloud popsán a je nastíněna jeho funkce jak pro běžné uživatele, tak i poskytovatele v části pojednávající o distribučních modelech.

Dalším prvkem je kapitola o trendech, které se mohou řadit jako zabezpečovací prvky s využitím IoT. Zde je krátkým textem obecně sepsána myšlenka autora o těchto technologiích a je zde zmíněno několik typů výrobků, které jsou podkladem pro domněnku, že se tato technologie bude v blízké době více rozvíjet, a to do takových mezí, kdy budou téměř všechna zařízení schopna komunikovat mezi sebou.

Před tímto krokem je však nutno zmínit i normy, pod které podléhají tyto technologie a je nutno dbát na jejich dodržování při instalaci. Avšak nynější znění těchto norem neumožňují plnohodnotnou implementaci technologií IoT hlavně pro zabezpečovací prvky, které podléhají normě ČSN EN 50 131 ed. 2 a bude nutné provést v budoucnosti úpravu.

V druhé části jsou navrženy dva projekty, které jsou následně uvedeny do aktivního stavu a je provedena zkouška spolehlivostí, které mohou definovat kvalitu pořízených prvků a jejich rozdílnou cenu. Také je v této části proveden rozbor jednotlivých prvků a jejich obecných principů, pro lepší pochopení celkového obvodu. Následně je u těchto systémů provedena zkouška spolehlivosti a vyhodnocení kvality těchto systému v závislosti na ceně.

Nakonec je nutné udělat rozbor, jednotlivých řešení, která byla vytvořena v praktické části. Jedním aspektem řádného rozboru je pohlédnout na uživatelskou skupinu, pro kterou jsou dané systémy určeny. Projekt 1 je velice spolehlivým typem zabezpečovacího systému, který je definitivně určen pro středně velké firmy, kde může zaměstnavatel nastavit čtečku dle vlastních potřeb a všichni pracovníci díky tomuto zařízení budou mít přístup do areálu. Zároveň je možné si představit tento typ zapojení u bytových domů a v objektech, které zaznamenávají vysokou aktivitu pohybu od uživatelů. V neposlední řadě je možné použít tento obvod pro větší domácnosti, kde zákazníkovi nezáleží ve velké míře na ceně, ale hlavně na různých přístupových funkcích a zabezpečení objektu. Tento systém by mohl být také v průběhu času vylepšován dalšími kompatibilními zařízeními, které lze propojit s gateway. Tato zařízení mohou být poté propojena mezi sebou a může tím být vytvořen rozsáhlejší systém než ten, který je vypracován v praktické části.

Projekt 2 je z prvního pohledu stavěn převážně na domácí použití, kde si například uživatel chce sestavit inteligentní systém pro ovládání světel nebo právě systém poplachový do kterého by samozřejmě muselo být přidáno více zařízení. Díky široké kompatibilitě různých zařízení s aplikací eWeLink je možné velice volně vylepšovat daný systém a tím tvořit různé principy jednotlivých segmentů obvodu, jako může být například zmíněné ovládání světel při aktivaci s jedním senzorem a zároveň spuštěním alarmu s druhým senzorem. Možnosti takovýchto flexibilních systémů jsou omezeny jen technickými parametry použitých zařízení a kreativitou uživatelů.

7 Seznam použité literatury

(1) Ing. Zdeněk Votruba, Ph.D. *Terminologie a funkce prvků EZS Mobilis in Mobili* [online]. Slideserver.com 2014. [cit. 2023-12-17]. Dostupné z: https://www.slideserve.com/biana/terminologie-a-funkce-prvk-ezs-mobilis-in-mobili

(2) ČSN EN 50 131-1. *Poplachové systémy: Část 1: Systémové požadavky. Vyd. 2.* Praha: Úřad pro technickou normalizaci, 2007.

(3) Alexander S. Gillis. *What is IoT (Internet of Things) and How Does it Work?* [online]. TechTarget.com 2023. [cit. 2024-1-28]. Dostupné z: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

(4) *Aeris Intelligent IoT Network* [online]. Aeris.com 2024 [cit. 2024-1-28]. Dostupné z: https://www.aeris.com/resources/aeris-intelligent-iot-network/

(5) *6 Leading Types of IoT Wireless Technologies* [online]. Behrtech.com 2018. [cit. 2024-1-28]. Dostupné z: https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/

(6) *Co jsou veřejné, privátní a hybridní cloudy?* [online]. Azure.microsoft.com 2024. [cit. 2024-2-4]. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#deployment-options

(7) *Cloud* [online]. Managementmania.com 2019. [cit. 2024-2-5]. Dostupné z: https://managementmania.com/cs/cloud-computing

(8) Holistic CIS, Industry Articles. *The three service models of Cloud Computing* [online]. Openintl.com 2019. [cit. 2024-2-15]. Dostupné z: https://www.openintl.com/the-three-service-models-of-cloud-computing/

(9) *Fenomén jménem Smart Cities* [online]. Svetuspesnych.cz. [cit. 2024-2-23]. Dostupné z: https://svetuspesnych.cz/fenomen-jmenem-smart-cities/?fbclid=IwAR3mUwJA8GQOJNCPC1K4I2-28CFd4lzPMRSiU4WJIuHYcQwh8VDGtJVrsUE_aem_Ac85v7jMkSQ2ZD4Tq2Pt8m23mDYcN8f_mCv9vP06EKzIDvn23-XWWnTNEAQqaS-Su749j2SVCquB0KQ1lYddMXkV

(10) *Inovace pro lepší život v Praze* [online]. Smartprague.eu 2023. [cit. 2024-2-23]. Dostupné z: https://www.smartprague.eu/?fbclid=IwAR1WoieFJTNj78dzuIIT6qURLnMK9KGmM7m1YMx9D7K6F_7t4A31M7z5JB8_aem_Ac8o3ZNe1ry-hi1GF3NuD0pv1EFd4ZZwRNjGp7JJAderPxy4zCzn-9jfeNHKzDlAyugfcJU_ozDhlsZ_fGkQLKMV

(11) *Tesla Smart Sensor Motion* [online]. Alza.cz 2024. [cit. 2024-2-25]. Dostupné z: https://m.alza.cz/EN/tesla-smart-sensor-motion-d6730996.htm?gclid=CjwKCAjw5ImwBhBtEiwAFHDZx6XObjajlm5ri9NVEsYZLG-2kqihat6Cdr_xYAbmQrIXJSfu6x-xhBoCtNkQAvD_BwE&kampan=adwsma_smart_pla_all_obecna-css_smart-home-detektory_m_1003796___Tslpt2115_605137456065_~140962427914~&fbclid=IwAR1WoieFJTNj78dzuIIT6qURLnMK9KGmM7m1YMx9D7K6F_7t4A31M7z5JB8_aem_Ac8o3ZNe1ry-hi1GF3NuD0pv1EFd4ZZwRNjGp7JJAderPxy4zCzn-9jfeNHKzDlAyugfcJU_ozDhlsZ_fGkQLKMV

(12) *Chytrý WiFi Otevírač Garážových Vrat* [online]. Chytré vypínače 2023. [cit. 2024-2-26]. Dostupné z: https://www.chytrevypinace.cz/Chytry-WiFi-Otevirac-Garazovych-Vrat-d61.htm?fbclid=IwAR1WoieFJTNj78dzuIIT6qURLnMK9KGmM7m1YMx9D7K6F_7t4A31M7z5JB8_aem_Ac8o3ZNe1ry-hi1GF3NuD0pv1EFd4ZZwRNjGp7JJAderPxy4zCzn-9jfeNHKzDlAyugfcJU_ozDhlsZ_fGkQLKMV

(13) *Čtečka STAR Smart K3 a K3F – návod* [online]. Klíčové centrum 2024. [cit. 2024-3-15]. Dostupné z: https://www.hbgroup.cz/images/stranky/navody/Elektronick%C3%A9%20p%C5%99%C3%ADstupov%C3%A9%20syst%C3%A9my/Manua%CC%81l_K3-K3F.pdf

(14) SONOFF. *SNZB-03 User Manual* [online]. Sonoff tech products 2021. [cit. 2024-3-20]. Dostupné z: https://sonoff.tech/wp-content/uploads/2021/03/%E8%AF%B4%E6%98%8E%E4%B9%A6-SNZB-03-V1.0-20210305.pdf

(15) SONOFF.*ZB Bridge User Manual* [online]. Sonoff tech products 2021. [cit. 2024-3-20]. Dostupné z: https://sonoff.tech/wp-content/uploads/2021/03/%E8%AF%B4%E6%98%8E%E4%B9%A6-ZBBridge-V1.1-20210305.pdf

(16) *Dveřní elektromagnetické zámky* [online]. ASSA ABLOY. [cit. 2024-3-21]. Dostupné z: https://www.assaabloy.com/cz/cs/solutions/products/elektromechanicke-produkty/elektromagnety

(17) Openers&Closers. *Elektromagnetický zámek O&C MEX* [online]. Klíčové centrum.2024. [cit. 2024-3-21]. Dostupné z: https://www.klicovecentrum.cz/produkt/elektromagneticky-zamek-oc-mex/?fbclid=IwAR1uI6Ol0jSAx_fsiC4owqDPZpXzgTskpiqu3XXqXHN64DQt9RMIz61bysA_aem_AWqtnf8PjOKDdYnapyw_V90XPxWkRri2vonFCCDyMffaw0z7ayX97chMXg8IWqzKGOEnDjTKyy7LV4oZ2gKY8ncq

(18) *Modul gateway STAR Smart* [online]. Klíčové centrum 2024. [cit. 2024-03-21]. Dostupné z: https://www.klicovecentrum.cz/produkt/modul-gateway-pro-star-smart/?fbclid=IwAR1WoieFJTNj78dzuIIT6qURLnMK9KGmM7m1YMx9D7K6F_7t4A31M7z5JB8_aem_Ac8o3ZNe1ry-hi1GF3NuD0pv1EFd4ZZwRNjGp7JJAderPxy4zCzn-9jfeNHKzDlAyugfcJU_ozDhlsZ_fGkQLKMV

(19) *Mikrovlnné vs PIR pohybové senzory: Jaký je rozdíl?* [online]. AZ-LED.cz 2023 [cit. 2024-3-21]. Dostupné z: https://www.az-led.cz/a/mikrovlnne-vs-pir-pohybove-senzory-jaky-je-rozdil

(20) Roshan Thapa. *How to determine Wi-Fi signal strength on Windows 10* [online]. GoGlides.dev 2023 [cit. 2024-3-21]. Dostupné z: https://www.goglides.dev/roshan_thapa/how-to-determine-wi-fi-signal-strength-on-windows-10-4101

(21) *Stěnová čtečka STAR Smart* [online]. Klíčové centrum 2024. [cit. 2024-3-21]. Dostupné z: https://www.klicovecentrum.cz/produkt/stenova-ctecka-star-smart/?fbclid=IwAR2to8I_dI-HPpduLLBAqxrvou63U6vmKKVxt4S1R9mbE95HDXRxXozm-OI_aem_AWoVUmtEcHMxtHN46JbGHu9mbilyr7tPYMLylvt7I4UyHEqGkFdRuP2QbeAbpqDXaX3MbSn7f1HtxIswAfEOtLXD

(22) *Sonoff SNZB-03 ZihBee Motion Sensor* [online]. Alza.cz 2024. [cit. 2024-3-21]. Dostupné z: https://m.alza.cz/EN/sonoff-snzb-03-zigbee-motion-sensor-d6370982.htm?gclid=CjwKCAjw5ImwBhBtEiwAFHDZxx3ejUN-aCa52vg8H1bbQdr8cIJO9QCPZLizqVNwGIvHzYGG90771xoCZLMQAvD_BwE&kampan=adwsma_smart_bee_pro_obecna_smart-smart-home-sonoff-snzb03-zigbee-motion-sensor-snf21a050&ppcbee-adtext-variant=rsa_pro_seg1-short&fbclid=IwAR3SP-MWTmT7F4FI5uQ2nit9YqBYn_4cjRiTjmSSSOCfeIHKr0jwlVaXY-0_aem_AWp9UrtWcxMhyhSiM2c6NDqTay9T2srhk9BAdbQNzvW9hzdV10zWzvvkwUvFdZ04l8C8zUFLOxdfXrzPmgcnF7nR

(23) Sonoff ZB Bridge-P [online]. Alza.cz 2024. [cit. 2024-3-21]. Dostupné z: https://m.alza.cz/EN/sonoff-zb-bridge-p-d7471236.htm?gclid=CjwKCAjw5ImwBhBtEiwAFHDZx5aMqeS92WUx7lalWC1gZeXw6CuUOqZXQYkQObQLVeJ9iHhKz-bF1RoCoA0QAvD_BwE&kampan=adwsma_smart_bee_pro_obecna_smart-smart-home-sonoff-zb-bridgep-snfa041&ppcbee-adtext-variant=rsa_pro_seg1&fbclid=IwAR2gpgSCWLhPhGyWIXHYhZ_3_-ge17GQMPhckdDiyGQsrYoUb0wy783HIaE_aem_AWo6qz67lKAAKaFye6avAJuNCuRv7u2O5h7yyKC7sjumL3RyZA_irbokpwymz7NsKXQOTMu3TiKot3vE5coOiDjI

(24) ČSN EN 50 398-1. *Poplachové systémy – Kombinované a integrované poplachové systémy – Část 1: Obecné požadavky*. Praha: Úřad pro technickou normalizaci, 2018.

8 Seznam obrázků

Obrázek 1 Blokové schéma Projektu 1 17
Obrázek 2 Blokové schéma Projektu 2 17
Obrázek 3 Zapojení obvodu terminálu 18
Obrázek 4 Komunikace mezi PIR senzory a Gateway 19
Obrázek 5 Terminál K3F 20
Obrázek 6 Ilustrační fotografie elektromagnetického zámku O&C MEX100 21
Obrázek 7 Ilustrační fotografie Gatewa\y STAR modulu G3 22
Obrázek 8 Design aplikace STAR master 23
Obrázek 9 PIR senzor SNZB-03 25
Obrázek 10 SONOFF Zigbee Bridge-P 27
Obrázek 11 Aplikace eWeLink 28
Obrázek 12 Záznam historie aktivací 28
Obrázek 13 Grafické znázornění provedeného měřené 29

9 Seznam tabulek

Tabulka 1 ___ Stupně zabezpečení.....7
Tabulka 2 ___ Závislost spolehlivosti na síle signálu 24
Tabulka 3 ___ Finanční náročnost jednotlivých prvků a celková hodnota.....30

10 Seznam použitých zkratek a termínů

IoT ..... Internet of Things (Internet Věcí)

PZTS ..... Poplachové Zabezpečovací a Tísňové Systémy

UID ..... User identifier (Identifikátor uživatele)

Wi-Fi ..... Wireless Fidelity

PIR ..... Passive Infra Red

LAN ..... Local Area Network (lokální síť/místní síť)

dBm ..... Jednotka reprezentující měřitelnou sílu signálu

Ethernet ..... Název souhrnu technologií pro počítačové sítě