



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

ODBOR INŽENÝRSTVÍ RIZIK

DEPARTMENT OF RISK ENGINEERING

ANALÝZA RIZIK TECHNOLOGIÍ CHYTRÝCH DOMÁCNOSTÍ V RÁMCI KONCEPTU INTERNET OF THINGS

RISK ANALYSIS OF SMART HOME TECHNOLOGIES WITHIN THE INTERNET OF THINGS CONCEPT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Patrik Brych

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Michal Urbánek

BRNO 2021

Zadání diplomové práce

Student:	Bc. Patrik Brych
Studijní program:	Řízení rizik technických a ekonomických systémů
Studijní obor:	Řízení rizik ekonomických systémů
Vedoucí práce:	Ing. Michal Urbánek
Akademický rok:	2020/21
Ústav:	Odbor inženýrství rizik

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Analýza rizik technologií chytrých domácností v rámci konceptu Internet of Things

Stručná charakteristika problematiky úkolu:

Moderní technologie a zařízení, které jsou vzájemně propojeny jsou využívány stále ve větší míře. Způsobem propojení spadají do oblasti internetu věcí (IoT), která je součástí průmyslové revoluce 4.0. Tyto technologie jsou využívány pro automatizaci chytrých domácností a jejich vzdálené bezdrátové ovládání. Využíváním těchto technologií může docházet k finančním úsporám díky funkčnosti zavedených prvků. Součástí práce bude provedení částečného finančního plánu modelového domu. Pro správnou implementaci chytrých technologií do domácnosti a jejich bezpečné využívání bude provedena riziková analýza.

Cíle diplomové práce:

Cílem diplomové práce je analyzovat a ohodnotit rizika spojená se zapojováním a využíváním technologií, používaných pro propojení chytrých domácností, které jsou součástí oblasti internetu věcí.

Seznam doporučené literatury:

VAN HOOFF, Joost, George DEMIRIS a Eveline J.M WOUTERS. Handbook of Smart Homes, Health Care and Well-Being. Cham: Springer International Publishing, 2017. DOI: 10.1007/978-3-319-01-83-5. ISBN 9783319015828.

HUA, Goh Bee. Smart cities as a solution for reducing urban waste and pollution. Hershey: Information Science Reference, An Imprint of IGI Global. ISBN 978-1-5225-0302-6.

MACAULAY, Tyson. RIoT Control: Understanding and Managing Risks and the Internet of Things. 2016. ISBN 9780124199903.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně, dne

L. S.

Ing. Jana Victoria Martincová, Ph.D.
vedoucí odboru

prof. Ing. Karel Pospíšil, Ph.D., LL.M.
ředitel

Abstrakt

Tato diplomová práce se zabývá moderními technologiemi, které bývají využity pro vybavení chytrých domácností. Analýza současného stavu je věnována konceptu Internet věcí, do kterého technologie chytrých domácností lze zařadit. Výzkumná část je zaměřena na analýzu rizik spojených se zavedením a využíváním chytrých technologií. Analyzována jsou finanční, technická a bezpečnostní rizika pomocí adekvátních výzkumných metod. Finanční rizika byla analyzována pomocí finančního plánu modelového domu. Technická, pod která byla zahrnuta i procesní rizika, a bezpečnostní rizika byla analyzována pomocí metod síťové analýzy a metod rizikové analýzy. Pro analýzu procesních rizik byla využita metoda síťového grafu a metoda hodnocení a kontroly projektů (PERT). Analýza technických a bezpečnostních rizik byla zpracována pomocí metody analýzy způsobů a důsledků poruch (FMEA) a analýzy stromu poruchových stavů (FTA).

Abstract

This diploma thesis deals with modern technologies that are used as smart home equipment. The analysis of the current state is devoted to the concept of the Internet of Things, into which smart home technologies can be included. The research part is focused on the analysis of risks that are associated with the implementation and use of smart technologies. Financial, technical and security risks are analyzed using adequate research methods. Financial risks were analyzed using the financial plan of the model house. Technical, which also included process risks, and security risks were analyzed using network analysis methods and risk analysis methods. The network graph method and the project evaluation and control method (PERT) were used for the analysis of process risks. The analysis of technical and safety risks was performed using the Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) methods.

Klíčová slova

Internet věcí, chytré technologie, chytrá domácnost, rizika chytré domácnosti, modelový dům

Keywords

Internet of Things, Smart Technologies, Smart Home, Risks of Smart Home, Model House

Bibliografická citace

BRYCH, Patrik. *Analýza rizik technologií chytrých domácností v rámci konceptu Internet of Things* [online]. Brno, 2021 [cit. 2021-06-11]. Dostupné z: <https://www.vutbr.cz/studenti/zav-prace/detail/128383>. Diplomová práce. Vysoké učení technické v Brně, Ústav soudního inženýrství, Odbor inženýrství rizik. Vedoucí práce Michal Urbánek.

Prohlášení

Prohlašuji, že svou diplomovou práci na téma „Analýza rizik technologií chytrých domácností v rámci konceptu Internet of Things“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně

.....

Podpis autora

Poděkování

Na tomto místě bych chtěl poděkovat vedoucímu mé diplomové práce, Ing. Michalovi Urbánkovi, za cenné rady a odborná doporučení, která mi poskytl během psaní diplomové práce. Dále bych chtěl ocenit jeho pochopení, trpělivost, ochotu a rychlé jednání během naší spolupráce.

Poděkovat bych také chtěl expertům dvou společností, které se zabývají energetickou náročností budov a chytrými domácnostmi, za jejich odborné konzultace.

OBSAH

OBSAH	13
1 ÚVOD.....	15
2 SOUČASNÝ STAV	17
2.1 Internet věcí	17
2.1.1 Složení IoT sítí.....	19
2.1.2 Oblasti využití IoT technologií.....	22
2.2 Chytré domácnosti.....	23
2.2.1 Komunikační technologie.....	25
2.2.2 Programovatelný hardware chytrých domácností.....	28
2.2.3 Správa chytrých domácností.....	30
2.2.4 Koncová zařízení a technologie chytrých domácností.....	34
2.2.5 Automatizace chytrých domácností.....	36
2.2.6 Hospodaření se zdroji.....	37
2.2.7 Bezpečnost chytrých domácností.....	37
3 FORMULACE PROBLÉMŮ A STANOVENÍ CÍLŮ ŘEŠENÍ.....	38
3.1 Problémy.....	38
3.2 Výzkumné otázky.....	39
3.3 Stanovení cílů řešení.....	39
4 POUŽITÉ METODY A JEJICH ZDŮVODNĚNÍ	41
4.1 Modelový dům.....	41
4.1.1 Finanční plán modelového domu.....	41
4.2 Síťová analýza procesu zapojení chytré domácnosti	42
4.2.1 Síťový graf a časová analýza projektu	42
4.3 Riziková analýza	43
4.3.1 Metoda FMEA.....	43
4.3.2 Metoda FTA.....	45
5 VLASTNÍ ŘEŠENÍ.....	46
5.1 Finanční plán modelové domácnosti.....	46
5.1.1 Modelový dům	46
5.1.2 Finanční plán vybavení.....	47
5.1.3 Finanční plán elektrické spotřeby modelového domu.....	47
5.2 Analýza procesních, technických a bezpečnostních rizik.....	50
5.2.1 Analýza procesních rizik.....	50

5.2.2	<i>Analýza technických a bezpečnostních rizik</i>	51
6	DISKUZE / ANALÝZA VÝSLEDKŮ ŘEŠENÍ	56
7	ZÁVĚR	58
	SEZNAM POUŽITÝCH ZDROJŮ	60
	SEZNAM TABULEK	68
	SEZNAM GRAFŮ	68
	SEZNAM OBRÁZKŮ	68
	SEZNAM ZKRATEK	69
	SEZNAM PŘÍLOH	70

1 ÚVOD

Tato diplomová práce se zabývá technologiemi chytrých domácností, které jsou součástí konceptu Internet věcí (IoT – Internet of Things). Koncept IoT je součástí čtvrté fáze průmyslové revoluce Průmysl 4.0 (Industry 4.0). Čtvrtá průmyslová revoluce slibuje různé změny nejen v průmyslu, ale také ve společnosti. Postupná digitalizace a vytváření sítí tak mění nejen oblast průmyslu, ale také prostředí a náš život. Chytré technologie mohou propojovat reálný svět se světem digitálním. Aplikace chytrých technologií umožňuje změnit úroveň elektronického vybavení v různých oblastech života. Budoucnost mají systémy, které využívají funkční, bezemisní, úsporná a udržitelná řešení. Trendy jsou například v budování chytrých měst, propojování a posilování sítí, jako je například internetová síť 5G, v budování inteligentních dopravních systémů a infrastruktury, rozvoji společnosti, využití umělé inteligence a strojového učení. Tyto tendence lze sledovat i na menších celcích, než jsou města a těmi jsou inteligentní budovy nebo přímo chytré domácnosti, které umožňují automatizovat zařízení v domácnosti, mohou být ovládány na dálku, mohou přinášet úspory v energetické spotřebě, mají zabudované kontrolní a bezpečnostní systémy a inteligentní senzory, poskytují data a analýzy využití svým uživatelům a zabezpečují komfort bydlení. Tyto technologie přináší zvýšení úrovně bydlení, ale mohou být spojeny s určitými riziky. Cílem diplomové práce je popsat současný stav problematiky a analyzovat možná rizika.

Současný stav problematiky je popsán v úvodní teoretické části. Nejdříve je popsán koncept Internetu věcí, složení a architektura IoT sítí. Dále jsou představeny oblasti využití IoT technologií a následuje kapitola o chytrých domácnostech, která tento pojem definuje a uvádí statistická data o jejich počtu. Kapitola o chytrých domácnostech je dále zaměřena na představení využívaných komunikačních technologií, využitelný programovatelný hardware, využitelné technologie pro jejich správu a koncová zařízení. V rámci této kapitoly je popsána automatizace, hospodaření se zdroji a bezpečnost chytrých domácností.

V kapitole s názvem formulace problémů a stanovení cílů řešení jsou blíže specifikovány možné problémy, které souvisejí s vybavením domácností chytrými technologiemi. Tyto problémy jsou blíže určeny a jsou vytvořeny výzkumné otázky. Cílem práce je na tyto otázky najít pomocí výzkumných metod odpovědi. Cíle řešení jsou stanoveny na základě očekávaných odpovědí na výzkumné otázky a je definováno, čeho by v nich mělo být dosaženo.

V následující kapitole je zpracován metodologický koncept řešení problematiky. Jednotlivé metody jsou představeny a popsány. Nejdříve je specifikován modelový dům a dále postup metodického řešení. Jako první bylo potřeba popsat finanční plán, dále metody síťové a rizikové analýzy.

Pátá kapitola je zaměřena na prezentaci vlastních výsledků získaných z využitých metod. Nejdříve jsou prezentovány výsledky finančního plánu modelového domu, následně jsou představeny výsledky síťové analýzy a závěr kapitoly tvoří popis výsledků vybraných metod rizikové analýzy. Výsledky jsou v této kapitole prezentovány s odkazy na kompletní metody, obsahující všechna data a informace, nacházející se v přílohách. Výsledky jednotlivých analýz jsou diskutovány v šesté kapitole. Diskuze je zaměřena na možné proměnné vstupní hodnoty, varianty provedení a využitelnost výsledků pro praxi. Součástí šesté kapitoly je i kritické zamyšlení se nad řešenou problematikou.

2 SOUČASNÝ STAV

Technologie chytrých domácností spadají do konceptu IoT, který je součástí Průmyslu 4.0. Průmysl 4.0 se skládá z více složek. Za hlavní složky se považují kyberfyzikální systémy (CPS – Cyber Physical Systems), neboli systémy fyzických entit, které jsou řízeny počítačovými algoritmy a jsou schopny samovolně rozhodovat a řídit. Další složkou je Internet služeb (IoS – Internet of Services), který nabízí služby fungující uvnitř a napříč různými organizacemi. IoS zahrnuje i inteligentní dopravní systémy, tedy informační a komunikační technologie pro zajištění optimální dopravy a přepravy na stávající infrastrukturu, pro snížení energetické náročnosti, zvýšení bezpečnosti a efektivnosti přepravy. Další složkou je digitální ekonomika, která představuje nový způsob alokace zdrojů pomocí informačních technologií, klasickým projevem vzniku digitální ekonomiky je vytvoření virtuálních obchodů neboli e-shopů. Za další z hlavních složek se považuje Internet věcí (IoT – Internet of Things) [1].

2.1 INTERNET VĚCÍ

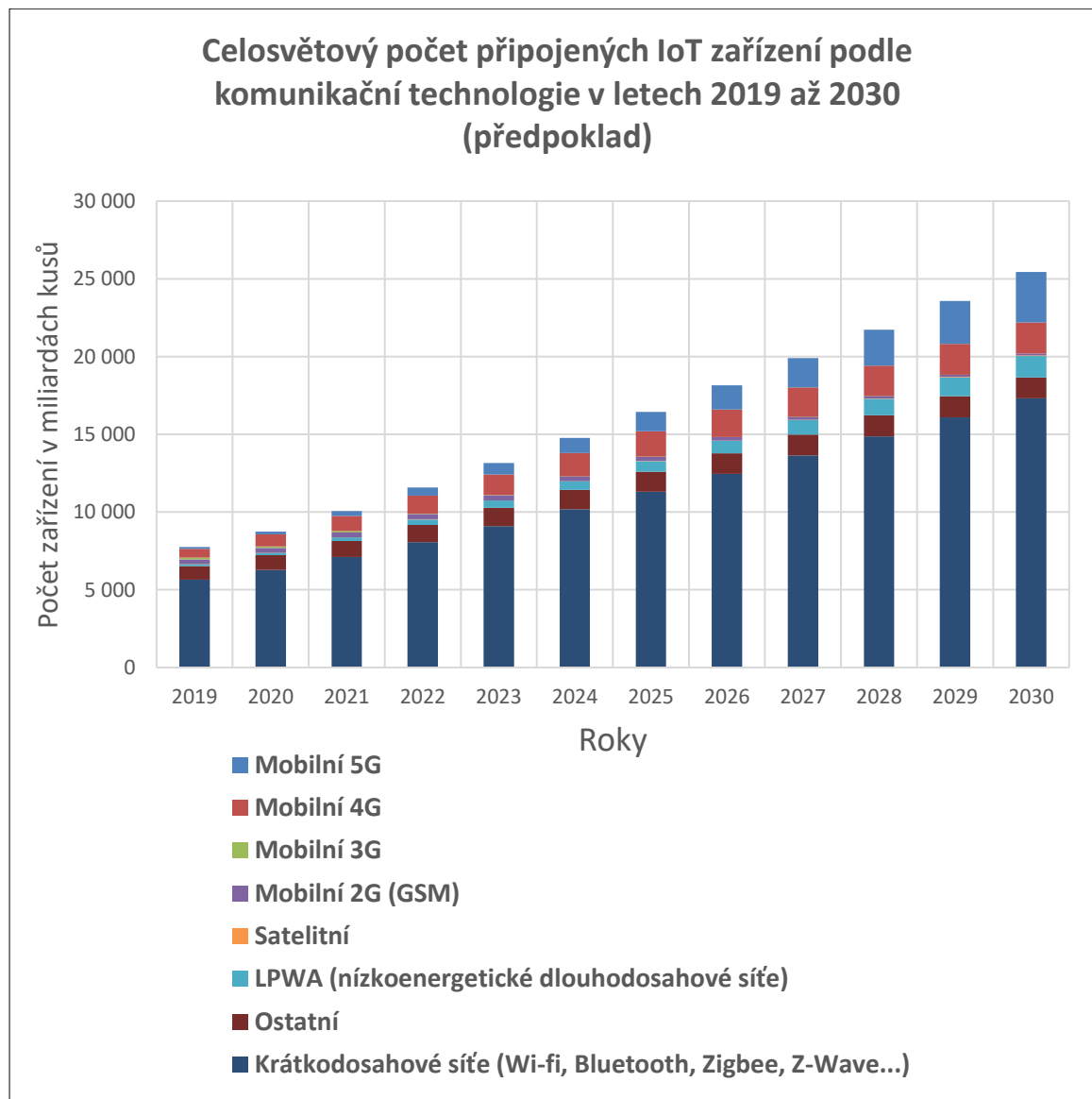
Internet věcí je celosvětová síť nebo infrastruktura, která je propojena protokoly pro komunikaci a jednotlivé fyzické či virtuální věci a zařízení v ní získávají vlastní identitu s vlastnostmi. Ty mohou komunikovat mezi sebou nebo například s inteligentními rozhraními a jsou tím zapojeny do informační sítě [2].

Internet věcí může být definován jako množina chytrých věcí nebo objektů, jako jsou mobilní telefony, osobní počítače a notebooky, vybavení domácnosti a další, které jsou zařazeny jedinečným adresovacím schématem a jsou připojeny k internetu pomocí jednotného rámce, kterým může být například cloudové výpočetní prostředí (Cloud Computing) [3].

IoT může být chápáno i jako síť, skládající se z různých připojených zařízení, která využívají senzory, komunikaci, třídění a zpracování informací a jsou propojeny pomocí bezdrátového připojení. Za nejdůležitější pro propojení je považována komunikace přes rádiové vlny a bezdrátové senzory [2].

Internet věcí zahrnuje jednotlivé přístroje, které komunikují a sdílí data s centralizovanými zařízeními a často se rozhodují a vykonávají akce či změny v nich samotných, bez zásahu člověka. Jedná se o velké množství zařízení, která komunikují mezi sebou, vyměňují si data a na jejich základě následně provádí změny na daných zařízeních v reálném světě. Tyto postupy provádí za účelem zlepšení služeb, které poskytují, hlavně zvyšují efektivitu a přidanou hodnotu z dané služby či funkce zařízení [4].

Následující graf č. 1 zobrazuje celosvětový počet připojených IoT zařízení v letech 2019 až 2030. Součástí grafu je i rozdělení IoT zařízení dle využívané komunikační technologie. Jednotlivé komunikační technologie jsou vypsány v legendě grafu. Datum vydání je rok 2020, data pro následující roky jsou předpokladem založeným na stávajících datech [5].



Graf č. 1 – Celosvětový počet připojených IoT zařízení podle komunikační technologie v letech 2019 až 2030 (předpoklad) [5] (upraveno autorem)

Graf č. 1 zobrazuje počet připojených IoT zařízení na celém světě. Celkový počet připojených IoT zařízení v roce 2020 byl zhruba 8,7 miliard kusů. V grafu je zobrazena prognóza těchto dat až do roku 2030, kdy je předpokládán počet připojených IoT zařízení na světě necelých 25,5 miliard kusů [5].

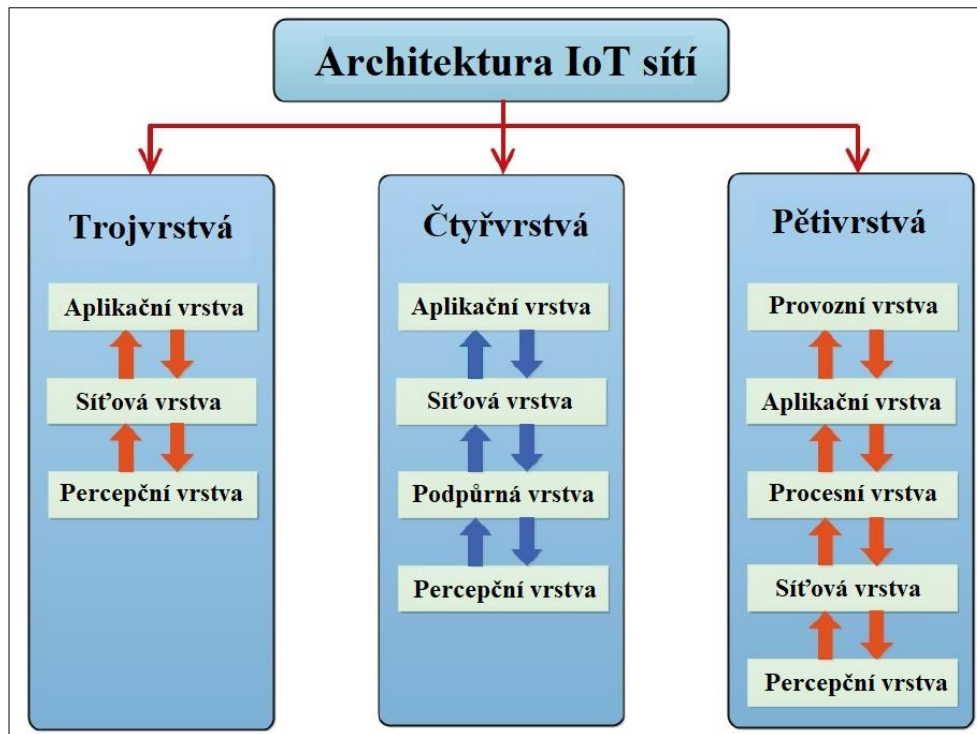
2.1.1 Složení IoT sítí

Následující kapitola se zabývá složením IoT sítí. Struktura těchto sítí může být popsána pomocí vrstvené architektury, která zachycuje rozdělení prvků sítě do několika úrovní podle jejich funkce. IoT zařízení v sobě obsahují senzory, pomocí kterých komunikují. Bezdrátová síť senzorů popisuje typy umístění a zapojení jednotlivých prvků sítě.

Vrstvená architektura IoT sítí

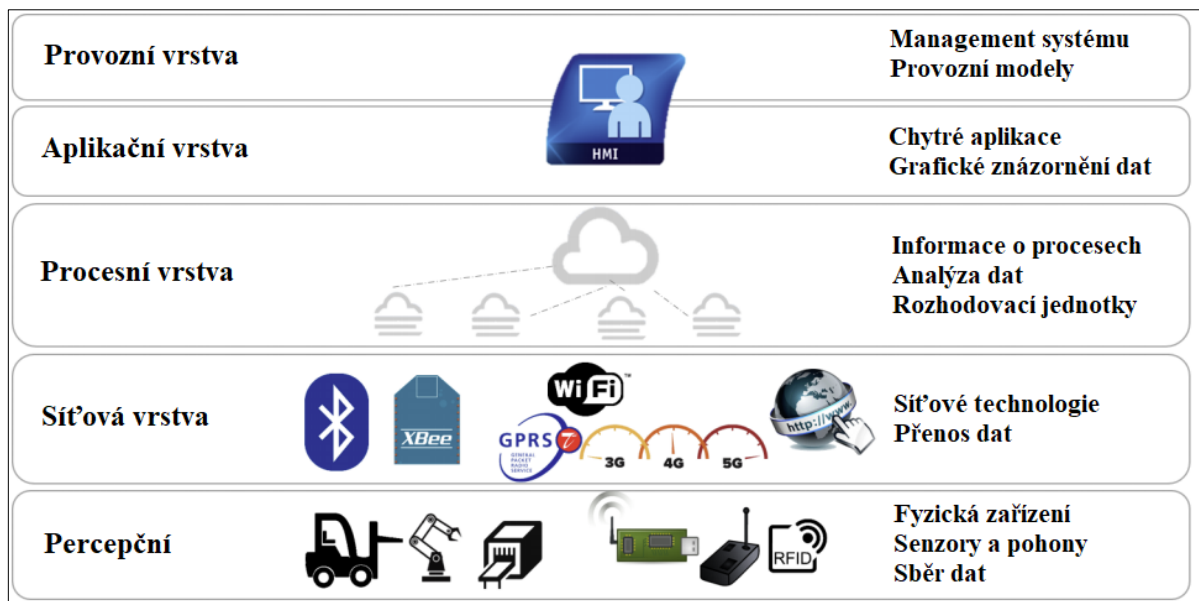
Architektura IoT sítí má několik vrstev, ze začátku vývoje IoT sítí byly tři vrstvy, postupně byly přidávány další vrstvy, v současné době je nejvíce využívána architektura s pěti vrstvami. Každá vrstva představuje úroveň určitého typu zařízení a dochází ke komunikaci zařízení v jednotlivých úrovních. Nové vrstvy vznikaly s vývojem IoT, nárůstem možností a typů zařízení a také z důvodu bezpečnosti využívání IoT sítí. Trojvrstvá architektura zahrnuje úrovně, které se nazývají: percepční vrstva (vnímací), síťová vrstva a aplikační vrstva. Percepční vrstva zahrnuje koncová zařízení, která vnímají jejich aktuální stav, stav okolí a další data. Tato data jsou přenášena pomocí síťové vrstvy nebo také přenosové vrstvy do třetí úrovně a tou je vrstva aplikační, která data sbírá a vyhodnocuje, nabízí uživatelům možnost kontroly atd. S vývojem IoT byla přidána čtvrtá úroveň, která se nazývala jako podpůrná vrstva a měla zabezpečit tok dat z percepční vrstvy do sítě a ověřit jejich pravost, například pomocí autentizace hesel a kódů. Následně byly vytvořeny další dvě vrstvy, které nahradily podpůrnou vrstvu a to zpracovávací (procesní) vrstva a provozní (business) vrstva. Síťová vrstva je v obr. 1 vrstvou přenosovou (transportační), která obstarává transport dat mezi vrstvami. Procesní vrstva zpracovává data a vybírá z nich podstatná, která jsou následně odesílána. Provozní vrstva zahrnuje aplikace pro správu a funguje jako správce celé sítě [6].

Přehled mezi jednotlivými architekturami IoT sítí lze vidět na obrázku č. 1, který se nachází na další straně. Na obrázku č. 2 jsou jednotlivým vrstvám přiřazeny koncová zařízení a je popsána funkce jednotlivých vrstev.



Obrázek č. 1 – Vrstvená architektura IoT sítí [6] (upraveno autorem)

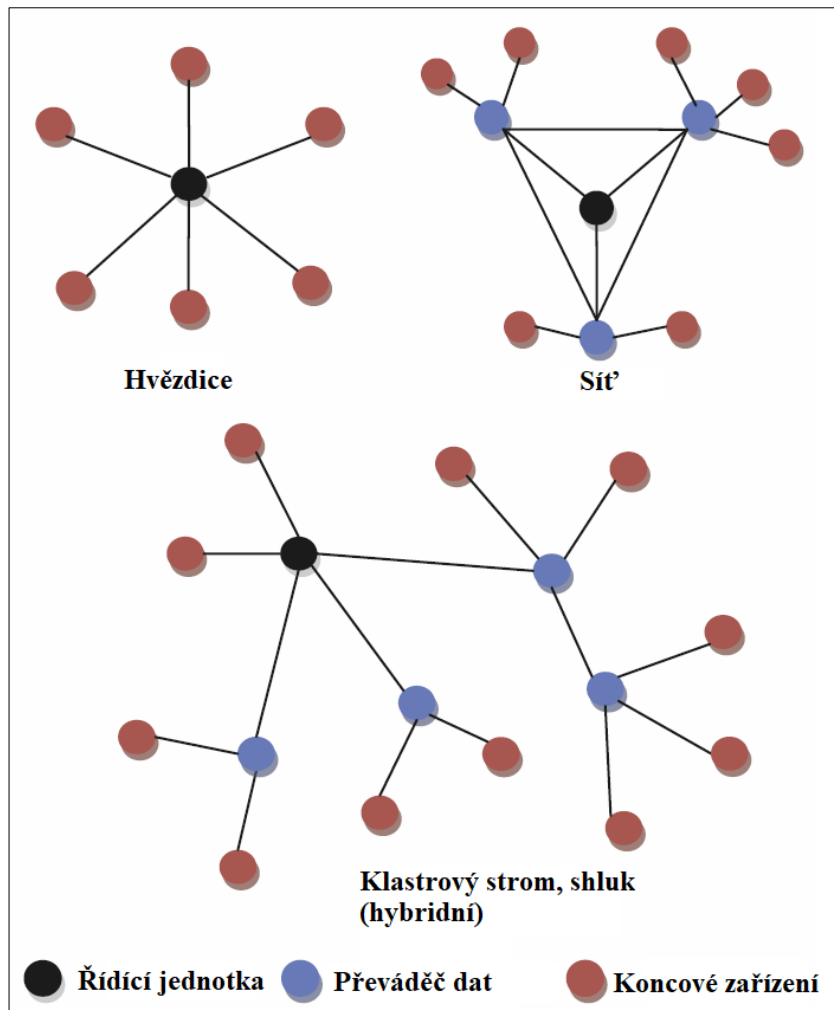
V pětivrstvé architektuře obsahuje každá vrstva určitý typ technologií (viz obrázek č. 2). Percepční vrstva obsahuje koncová zařízení, která mohou představovat senzory, kamery, stroje, zařízení a další. Síťová nebo transportační vrstva obsahuje technologie pro přenos dat, jedná se především o komunikační protokoly. Procesní vrstva nebo také middleware vrstva zahrnuje cloudové služby pro uložení, třídění a výběr dat. Přednastavením určitých schémat, může procesní vrstva vydat informace či příkaz zpět do percepční vrstvy. Vybraná a analyzovaná data dále putují do aplikační vrstvy, která je také využije pro ovládání systému, například koncových zařízení. Provozní vrstva slouží pro správu celé sítě, na základě sesbíraných dat, může správce této sítě strategicky rozhodovat a ovládat jednotlivé prvky sítě, pro dosažení požadovaných výsledků [7].



Obrázek č. 2 – Pětivrstvá architektura IoT sítě s koncovými zařízeními a funkcemi vrstev [7] (upraveno autorem)

Bezdrátová síť senzorů

Bezdrátová síť senzorů (WSN – Wireless Sensor Network) představuje síť nebo infrastrukturu zapojení zařízení, senzorů, datových převaděčů a řídicích jednotek. Topologií zapojení těchto zařízení je velké množství, ale nejpoužívanějšími jsou tři druhy zapojení (viz obrázek č. 3). Prvním druhem je hvězdicové (star) zapojení, které představuje zapojení od jednoho bodu k dalšímu. Koncová zařízení jsou napojena přímo na řídicí jednotku. Výhodou je, že zařízení či senzory v tomto typu zapojení potřebují pouze základní levné přijímače a vysílače signálu. Nevýhodou je velká energetická náročnost na dané senzory a zařízení, pokud jsou bateriově napájeny, tak je to pro větší síť problémem při provozu. V klastrovém zapojení (cluster tree) se jednotlivé uzly považují za převaděče a přenáší a řídí data v celé síti. Každý uzel se tak chová jako řídicí jednotka u hvězdicového zapojení. Problémem tohoto zapojení je, že pokud jeden převaděč (uzel) selže, pak následně nefungují ani jednotlivá zařízení v daném stromu. Nejpoužívanějším typem zapojení je typu síť (mesh). V tomto zapojení jsou jednotlivé uzly komunikovat s dalšími uzly. Což znamená, že koncové zařízení nebo senzor může komunikovat s řídicí jednotkou i pomocí jiných uzlů, než je mu přidělen. Výhodou je, že v tomto případě je energetická náročnost na jednotlivé uzly výrazně snížena [8].



Obrázek č. 3 - Topologie zapojení WSN [8] (upraveno autorem)

2.1.2 Oblasti využití IoT technologií

IoT technologie jsou využívány ve stále více odvětvích. IoT zařízení jsou nyní využívána například ve zdravotnictví a v průmyslu, ale s jejich rostoucím počtem je očekáváno rozšíření i do dalších odvětví. Oblasti využití IoT zařízení jsou tedy ve zdravotnictví, v průmyslu, v logistice a přepravě, ve výstavbě a vybavení měst a domů, v zabezpečení objektů, v zemědělství a dalších. V oblasti zdravotnictví jsou využívány zdravotnické přístroje, ale také například zařízení pro pozorování pacientů. Součástí průmyslové aplikace jsou chytré továrny, které využívají propojení strojů, monitorování spotřeby, dodavatelských řetězců a další. V logistice a přepravě je využíváno například optimalizace tras, komunikačních zařízení, monitorování provozu a dalších. V zabezpečení objektů jsou využívány například kamerové systémy nebo senzory pro úniky nebezpečných látek. Propojením více zařízení vzniká síť, které je možno využít i ve městech. Vznikají chytrá města, ve kterých jsou zařízení propojena a jsou využívána v každodenním životě. Jedná se o propojení celého města a jeho ovládání probíhá přes vzniklou síť a

město tak může být automatizováno. Jedná se například o propojení infrastruktury, kontroly ovzduší, management zdrojů, management odpadů a mnoho dalšího. S tím souvisí i uplatnění IoT zařízení do jednotlivých domácností. Vytvořením sítě IoT zařízení v domácnosti, která umožňuje jejich ovládání, monitorování, možnou automatizaci a další, vzniká chytrá domácnost [9].

2.2 CHYTRÉ DOMÁCNOSTI

Chytrá domácnost (SH – Smart Home) je budova, která obsahuje síť vybraných elektrických zařízení a služeb a umožňuje jejich dálkové ovládání, sledování jejich stavu, vzájemnou komunikaci, sběr a vyhodnocování dat. Chytrá domácnost je inteligentní budova, určená pro bydlení. Nedílnou součástí je tedy síť zařízení, ve které komunikují, schopnost zařízení být ovládána a kontrolována na dálku, přítomnost senzorů, které sbírají data a chytré systémy, například pro stínění či vytápění, které jsou schopny reagovat na aktuální změny dat ze senzorů či na pokyn uživatele [10].

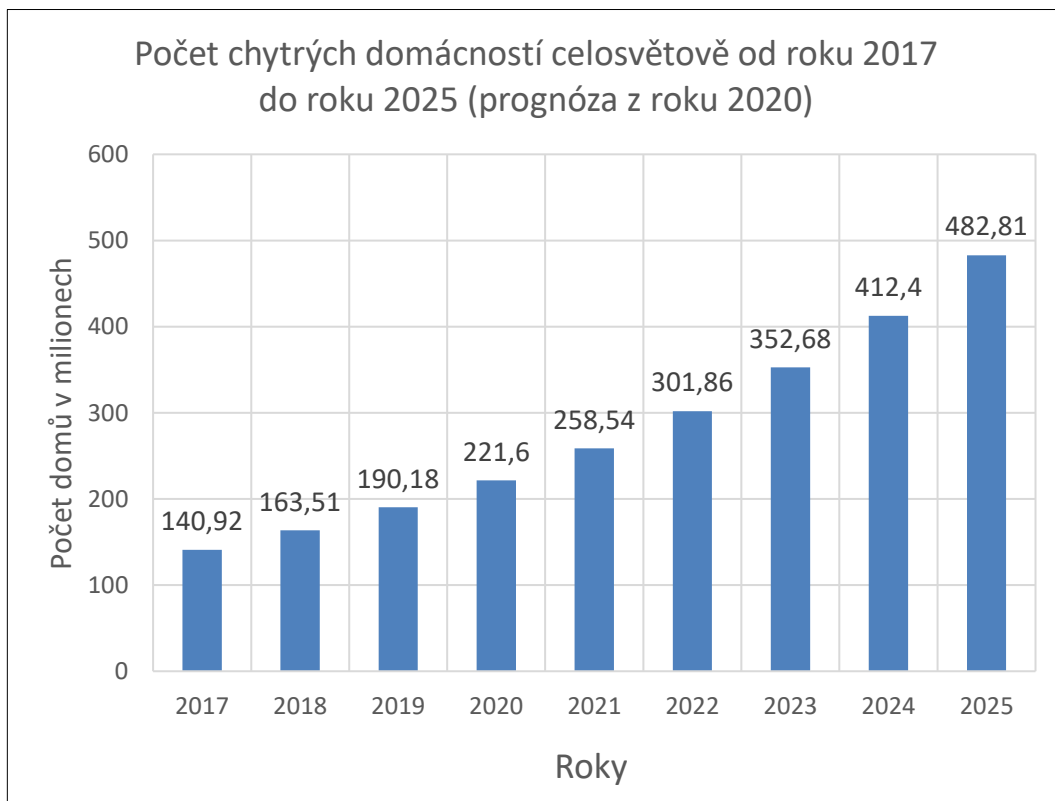
Chytrá domácnost může být chápána i jako inteligentní dům, který obsahuje senzory, akční členy, řídicí jednotky a síť. Primárním cílem inteligentní domácnosti je zvýšit úroveň automatizace zařízení v domácnosti, usnadnit hospodaření se zdroji a snížit odpadovou a emisní náročnost domácnosti. Automatizaci domácnosti lze zlepšit vylepšenou komunikační sítí, která obvykle využívá elektroinstalace kroucené dvoulinky, radiofrekvenčních signálů nebo optických vláken propojených do sítě, založené na standardu sběrnice nebo komunikačního protokolu. Hospodaření se zdroji může být zlepšeno pomocí výběru efektivních zařízení, ale také v poskytnutí informací ze zařízení uživatelům, pro lepší zacházení se zdroji a zařízeními [11].

Na obrázku č. 4 lze vidět schéma zapojení chytré domácnosti. Jsou zde zaznačena koncová zařízení, která jdou vzdáleně ovládat, odesílají data, monitorují situaci a plní další funkce. Senzory pro sběr dat jsou zaznačeny šedými symboly, to mohou být například pohybové, požární, teplotní a další senzory. Jednotlivá koncová zařízení jsou označena zelenými symboly. Mezi koncová zařízení patří například osvětlení, žaluzie, garážová vrata, zábavní spotřebiče a další. V bílém kruhu se nachází zařízení pro ovládání koncových zařízení, tedy například řídicí jednotka, mobilní telefon, nástěnný panel pro ovládání a dálkový ovladač [12].



Obrázek č. 4 – Příkladové schéma vybavení chytré domácnosti [12]

Celkový počet chytrých domácností je v současné době zhruba 220 milionů. Na základě statistických dat byla vytvořena prognóza, která předpokládá, že počet chytrých domácností naroste do roku 2025 dvojnásobně, až na počet okolo 482 milionů budov chytrých domácností (viz graf č. 2) [13].



Graf č. 2 – Celosvětový počet chytrých domácností v letech 2017 až 2025 [13] (upraveno autorem)

V grafu č. 2 lze vidět nárůst počtu chytrých domácností od roku 2017 do roku 2020 ze 140 milionů na 221 milionů domů. Graf dále zobrazuje prognózu nárůstu počtu chytrých domácností do roku 2025, kdy by měl počet tohoto typu domů celosvětově přesáhnout 482 milionů [13].

S příchodem různých komunikačních technologií, jako jsou například IoT protokoly Bluetooth a Wi-fi, došlo napříč různými zařízeními k zvýšení autonomie a integrace do systémů. IoT zařízení mají svou aplikaci v různých oblastech, jako jsou například chytrá města, chytré domácnosti, chytrá koncová zařízení, automatizovaná doprava a další. To znamená, že představují klíčový faktor pro hospodářský růst a zlepšování kvality života lidí (QoL – Quality of Life). Tyto technologie, zavedené například do inteligentní budovy, přinášejí vzdálené a jednodušší ovládání koncových zařízení, informace o spotřebě a aktuálním stavu zařízení. Dále mohou poskytovat péči pro nemocné pacienty či starší osoby a další funkce, které zvyšují kvalitu života lidí [14].

2.2.1 Komunikační technologie

V oblasti IoT je využíváno velkého množství komunikačních technologií. V následující kapitole je popsán výběr nejpoužívanějších komunikačních protokolů. Pro komunikaci v sítích chytrých domácností se používá především komunikačních technologií s krátkým dosahem.

Wi-fi

Wi-fi (wireless fidelity) je bezdrátová technologie, běžně používaná v domácnostech pro připojení k internetu. Vychází ze standardu sítí IEEE 802.11. (Institute of Electrical and Electronics Engineers). Součástí technologie jsou funkce jako: MIMO (Multiple – Input, Multiple – output), která zajišťuje možnost připojení a komunikaci více zařízení najednou, OFDM (Orthogonal Frequency – Division Multiplexing), která umožňuje sdílení Wi-fi kanálů pro lepší efektivitu a odezvu v objektech s vyšší hustotou sítí nebo také funkce TWT (Target Wake Time), která umožňuje zapnutí a vypnutí zařízení v určenou dobu, což může přispívat k šetření energie u bateriově napájených zařízení. V současné době je na trhu již sedmá verze vysílačů wifi sítí [15].

Ethernet

Jedná se o drátové spojení lokální sítě pomocí internetového připojení. Vychází ze standardu IEEE 802.3. Jedná se o jeden posledních způsobů internetového kabelového propojení. Výhodou ethernetu je například jednoduchost zapojení, stabilita připojení a vysoké přenosové rychlosti [16].

Bluetooth

Technologie Bluetooth je bezdrátová technologie, která vytváří síť pro propojení zařízení na malé vzdálenosti. V současné době je pátá generace Bluetooth, která spolu se čtvrtou verzí má výhody oproti předchozím verzím, především ve vyšší přenosové rychlosti dat, větší rozsah sítě, a především menší energetickou náročnost. Zkratka BLE (Bluetooth Low Energy) označuje novou generaci Bluetooth s nízkou spotřebou energie, a proto se Bluetooth řadí mezi využívané komunikační technologie v oblasti IoT. Technologie BLE umožňuje komunikovat se zařízeními, která jsou v pohotovostním režimu (StandBy), uvést je do chodu na krátké časové intervaly a šetřit tak baterii bezdrátových zařízení [17].

Zigbee

Další variantou k propojení sítě IoT zařízení je komunikační protokol Zigbee. Protokol Zigbee je založen na standardu sítě IEEE 802.15.4. Zigbee představuje bezdrátovou síť, kterou je možno nakonfigurovat i do typu zapojení sítě (mesh) a zařízení v této síti tak mohou komunikovat mezi sebou a nemusí vždy využívat nadřazený uzel. Nevýhodou Zigbee je menší datová propustnost, oproti předchozím technologiím, avšak je vhodná pro ovládání zařízení chytré domácnosti, která jsou na baterie, protože přenos dat je zde energeticky nenáročný. Technologie je vhodná pro zařízení, která vyžadují pouze jednoduché stavové příkazy, nebo přenáší informace o stavu zařízení, například o teplotě a vlhkosti [18].

Z-Wave

Z-Wave technologie vytváří síť pro zařízení IoT, které se do této sítě napojují a v ní komunikují pomocí rádiových frekvencí, které jsou nižší než například u Wi-fi zařízení. Zařízení jsou v síti zapojena pomocí typu sítě (mesh), takže jednotlivá koncová zařízení mohou vzájemně komunikovat a předávat si informace, pokud se například některé nenachází v dosahu řídicí jednotky [19].

RFID

RFID (Radio Frequency Identification) je technologie pro identifikaci jednotlivých zařízení pomocí rádiových vln. Technologie byla původně vyvinuta pro identifikaci zboží, ale dá se využít i pro identifikaci bezdrátových zařízení. RFID systémy se skládají z přijímače signálu neboli čtečky, která přijímá signály od zařízení, kterým je přiděleno označení tzv. TAG. Zařízení TAG jsou identifikována čtečkou pomocí signálu. Zařízení mohou být identifikována v různých frekvenčních pásmech, avšak nejvyužívanější jsou nízkofrekvenční pásma, která však mají nižší dosah [20].

NFC

NFC (Near Field Communication) je technologie s velmi krátkým dosahem, která umožňuje přenos dat mezi zařízeními, která přiložíme k sobě, nebo přiblížíme na pár centimetrů. Technologie

využívá podobných principů jako RFID, avšak slouží i k přenosu dat, a ne pouze k identifikaci. Zařízení má tedy svůj tag, který může být přečten, přepsán, nebo změněn jiným zařízením. NFC technologie je využívána především v mobilních telefonech a pro bezkontaktní platby [21].

MQTT

Technologie MQTT (Message Queuing Telemetry Transport) je protokol, založený na odesílání zpráv. Jedná se o mechanismus, který využívá principu zveřejnění dat a odběr dat (publish/subscribe). Zařízení v této síti sbírají data a odesílají je ve formě zpráv. Pro komunikaci využívá nízkofrekvenční vlny a je poměrně jednoduchý k instalaci [22].

PLC

PLC (Power Line Communication) technologie využívá pro komunikaci elektrickou síť, využívá tedy kabely elektroinstalace. I když se nejedná o bezdrátové propojení sítě, tak je tento systém využíván pro propojení chytrých domácností. Pro komunikaci využívá napájecí kabely k daným zařízením, ale může využít i telekomunikačních, koaxiálních a dalších kabelových vedení. Jeho výhodou je, že nevyužívá rádiových frekvencí, které by se mohly rušit a představuje poměrně levnou variantu řešení chytré domácnosti. Tento systém ale nepodporuje bezdrátová zařízení, jako jsou senzory a hůře se implementuje do již postavené a vybavené budovy [23].

Cloudové prostředí

Cloudové výpočetní prostředí (Cloud Computing), poskytuje služby a programy, které jsou lokalizovány na externích datových serverech a uživatelé se k nim mohou vzdáleně připojit. Cloud poskytuje uložení dat, služby a aplikace podle druhu cloudu, které jsou díky tomu dostupné přes internet, energetickou úsporou, díky vzdálenému připojení a možnosti obsluhovat více uživatelů z jednoho serveru a poskytuje uživatelům data a výsledky [24].

2.2.2 Programovatelný hardware chytrých domácností

Následující kapitola je zaměřena na dostupný programovatelný hardware, který může sloužit jako řídicí jednotka chytré domácnosti. Výhodou využití tohoto hardwaru je širší kompatibilita s různými typy výrobků a komunikačních protokolů, než mají například již před programované zařízení pro správu chytrých domácností.

Arduino

Arduino je hardwarové zařízení, které je programovatelné a považuje se za mikrokontroler. Typ Arduino UNO Wi-fi Rev2 lze vidět na obrázku č. 5. K zařízení se dá připojit další hardware pomocí portů a pinů. Do sítě může být zapojeno pomocí Wi-fi, Ethernetu a dalších protokolů a funguje na internetu, ale i na krátkodosahových sítích, proto je vhodné pro použití v projektech spojených s IoT. Jedná se o poměrně levné zařízení, které má velké možnosti programovatelnosti. Tento mikrokontroler má USB port a má vlastní programovací rozhraní. Arduino je vhodné pro učení se s IoT zařízeními, testování prototypů, ale i jako řešení ovládání chytré domácnosti [25].



Obrázek č. 5 – Arduino UNO Wi-fi Rev2 [26]

Raspberry PI

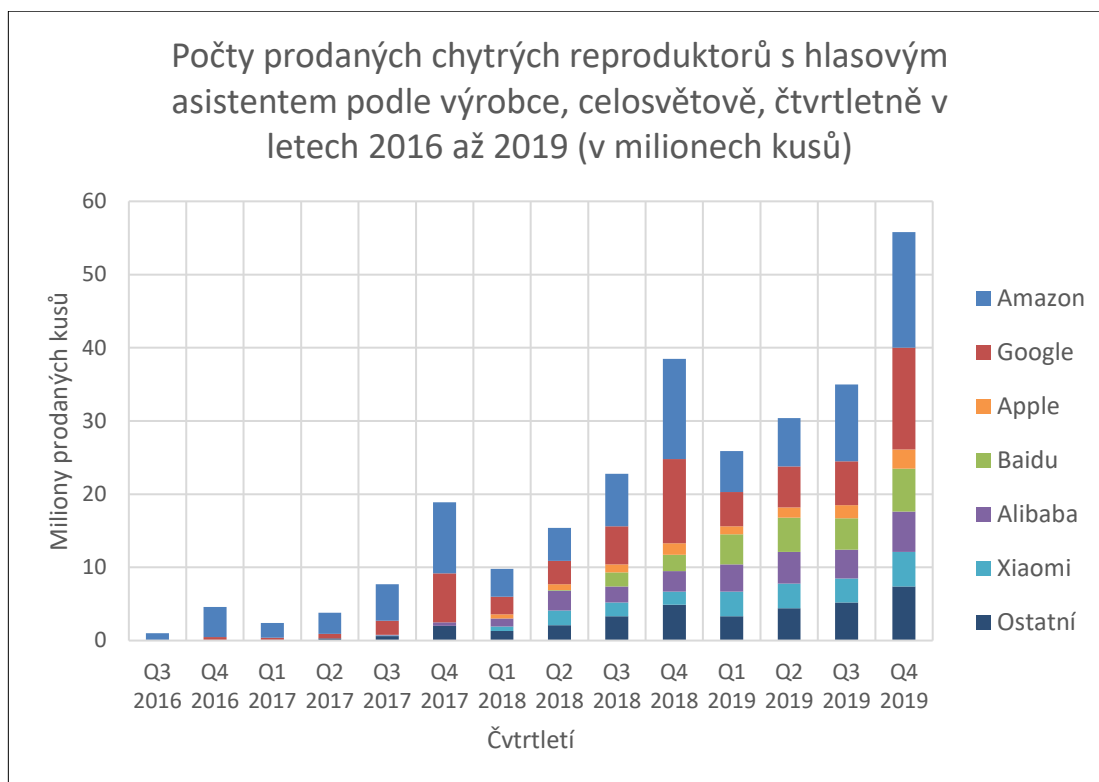
Raspberry PI je další programovatelné zařízení, které již obsahuje procesor a paměť RAM. Typ Raspberry Pi 4 Model B lze vidět na obrázku č. 6. Raspberry PI je považováno za mini počítač. Funguje na operačním systému Linux (Raspbian) a umožňuje komunikaci přes Wi-fi. Toto zařízení má i HDMI port pro připojení obrazu a zvuku, dále také USB a Ethernet porty. Přes toto zařízení se dá programovat další zařízení v programovacích jazycích Python, C, C++, Java a dalších. Spolu s Arduinem jsou cenově dostupná a dobře programovatelná zařízení [27].



Obrázek č. 6 – Raspberry Pi 4 Model B [28]

2.2.3 Správa chytrých domácností

Hotové řešení správy chytrých domácností se snaží nabídnout více výrobců. Obvykle nabízí řídicí jednotku ve formě chytrého reproduktoru s hlasovým asistentem. Uživatel tak může domácnost ovládat pomocí hlasu, ale i přes nabízené aplikace daných výrobců. Nevýhodou může být nekompatibilita s různými typy produktů od rozdílných výrobců. V následujícím grafu č. 3 jsou zachyceny počty prodaných chytrých reproduktorů s hlasovým asistentem, včetně rozlišení výrobců dle čtvrtletí v letech 2016 až 2019. Uživatel si však může správu chytré domácnosti vyřešit i vlastním způsobem, například pomocí některého ze zmíněných programovatelných zařízení.



Graf č. 3 - Počty prodaných chytrých reproduktorů s hlasovým asistentem podle výrobce, celosvětově, čtvrtletně v letech 2016 až 2019 (v milionech kusů) [29] (upraveno autorem)

V grafu č. 3 jsou zobrazeny čtvrtletní počty prodaných chytrých reproduktorů, celosvětově prodávaných od roku 2016 do roku 2019, umožňujících ovládnutí chytré domácnosti přes hlasového asistenta a příslušnou aplikaci dle výrobce. Nejprodávanějším je řešení společnosti Amazon s hlasovým asistentem Alexa a druhým nejprodávanějším je řešení společnosti Google. Na grafu lze vidět velký nárůst prodeje těchto zařízení a také nárůst konkurentů na trhu. Ve čtvrtém čtvrtletí roku 2019 přesáhl celkový počet prodaných chytrých reproduktorů 55 milionů kusů [29].

Google Home

Google Home je platforma pro správu chytrých domácností od společnosti Google. Jedno z provedení chytrého reproduktoru od společnosti Google lze vidět na obrázku č. 7. Google nabízí ovládání pomocí chytrého reproduktoru s hlasovým asistentem Google Assistant. Bezdrátové ovládání přes mobilní telefony funguje přes aplikaci Google Home. Výhodou může být široká škála podporovaných produktů a jejich hlasové ovládání přes hlasového asistenta. Nevýhodou, tak jako u většiny dalších zařízení používajících internetové připojení k ovládání je nutnost připojení. Pokud zařízení nejsou připojena, pak jsou jejich nastavení uložena a znovu jdou dálkově ovládat až po připojení [30].



Obrázek č. 7 – Chytrý reproduktor Google Home Mini [31]

Apple HomeKit

Apple HomeKit nabízí zařízení pro propojení a správu chytré domácnosti. Chytrý reproduktor společnosti Apple lze vidět na obrázku č. 8. Bezdrátový reproduktor s hlasovým asistentem Siri poskytuje možnost pro hlasové ovládání domácnosti. Ovládání koncových zařízení probíhá i přes mobilní aplikaci. Limitující pro toto řešení je kompatibilita pouze s výrobky od společnosti Apple a některými certifikovanými zařízeními jiných výrobců. Ovládání může probíhat pouze ze zařízení s operačním systémem iOS, především pomocí iPhone telefonů. Pro komunikaci v této síti je použita Wi-Fi. Databáze pro data ze zařízení poskytuje iCloud, tedy cloudová služba od společnosti Apple [32].



Obrázek č. 8 – Chytrý reproduktor Apple HomePod Mini [33]

Amazon Echo

Amazon Echo je řešení od společnost Amazon. Chytrý reproduktor od společnosti Amazon lze vidět na obrázku č. 9. Uživatel může ovládat chytrou domácnost pomocí chytrého reproduktoru s hlasovým asistentem Alexa. Hlasový asistent Alexa funguje s podporou Amazon cloudu a data jsou ukládána také zde. Připojení a komunikace probíhá přes internet, stejně jako u konkurentů. Dálkové ovládání funguje přes aplikaci Amazon Alexa. Amazon Echo je jedním z prvních chytrých reproduktorů a také jedním z nejprodávanějších hotových řešení pro správu chytrých domácností [34].



Obrázek č. 9 – Chytrý reproduktor Amazon Echo Dot 3. generace [35]

Alibaba Smart Living

Alibaba Smart Living je další platforma pro správu chytré domácnosti. Výhodou tohoto řešení je široká nabídka produktů z e-shopů společnosti Alibaba a finančně dostupné produkty. Nevýhodou může být kvalita jednotlivých zařízení, optimalizace, způsob servisu a dostupnost z na lokálním trhu [36].

IBM Watson

IBM Watson je platforma od společnosti IBM sloužící k připojení IoT zařízení do prostředí IBM Cloud a pro jejich správu. Pro komunikaci používá protokol MQTT. Uživatel může pomocí této platformy, nebo pomocí mobilní aplikace spravovat zařízení připojená v této síti. Pro vzdálený přístup k zařízením, změnu funkcí, kontrolu, analýzu dat a další funkce musí být zařízení připojena ke cloudu [32].

Baidu

Baidu je čínská společnost nabízející řešení pomocí zařízení Tiangong, představující platformu pro připojení IoT zařízení do sítě pomocí Baidu Cloud. Využívá se především v průmyslové výrobě, energetice, logistice a dalších odvětvích, jako platforma k správě a přístupu materiálu, vytváření pravidel a časovacích databází, strojovému učení a k integraci velkých dat a technologií umělé inteligence. Umělá inteligence pomáhá uživatelům a vývojářům k efektivnímu vytvoření sítě či aplikace [37].

2.2.4 Koncová zařízení a technologie chytrých domácností

Následující kapitola je zaměřena na koncová zařízení chytrých domácností. Jedná se o vybavení budovy, jako jsou například světla, uzavírací a stínící prvky, senzory pro měření teploty a vlhkosti, zabezpečovací a kamerové systémy, ale také zařízení pro zábavu, jako je například televize či audio. Tato zařízení jsou vybavena přijímači, vysíláči a senzory, přes které mohou být ovládána a předávají informace uživateli.

Osvětlení

Osvětlení je v chytrých domácnostech obvykle řešeno pomocí žárovek, které jsou vybaveny některou z komunikačních technologií, například mají Bluetooth nebo ZigBee modul. Osvětlení celého domu tak může být spojeno na centrální ovládání přes aplikaci či platformu pro správu. Osvětlení může být regulováno na základě několika faktorů. Prvním z nich je intenzita světla v určité místnosti, takže umělé osvětlení je zapnuto při určitém množství světla, které snímá senzor. Dalším je obsazenost místnosti, tedy zda se v místnosti někdo nachází. Případně co daná osoba v místnosti dělá. Na regulaci osvětlení může také mít vliv estetický vzhled místnosti. Světla tak mohou měnit barvu, být ztlumována, nebo nastavena na časovač [38].

Stínění

Pro regulaci množství denního světla v různých místnostech jsou na každém okně či prosklených dveřích instalovány stínící prvky s elektrickým pohonem. Jsou vybaveny komunikační technologií pro napojení jednotlivých žaluzií či rolet do správy chytré domácnosti. Stínící prvky slouží i jako izolační vrstva. Mohou krýt okna před negativními vlivy počasí a odrážet sluneční teplo ve vysokých teplotách. Žaluzie také mohou být napojeny na automatizovaný systém, který podle světelného senzoru ovládá žaluzie tak, aby v místnostech bylo co nejvíce světla. Uživatel si tak může vytvořit možné scénáře pro energetické úspory [39].

Teplota a vlhkost

Zařízení pro kontrolu teploty a vlhkosti jsou jednoduché senzory, které pomocí komunikačních protokolů předávají informace do řídicí jednotky či přes cloud do aplikace. Uživatel tak zná aktuální informace o budově a může měnit nastavení vytápění či klimatizace, pokud má dálkově ovládané uzávěry větracích oken či větráky, může regulovat i vlhkost. Regulace podmínek v místnosti může sloužit k zvýšení pohodlí, energetické úspore, ale i k zajištění zdravého prostředí pro uživatele [40].

Nastavení teploty v místnostech je prováděno pomocí termostatů, které ovládají topení a komunikují s řídicí jednotkou. Teplota může být automaticky regulována na přednastavené teploty v určitý čas. Topení v jednotlivých místnostech může být přednastaveno na zapnutí pouze pokud je

místnost obývána, pomocí pohybových senzorů. Termostaty se mohou řídit i pomocí informací z internetu či meteostanic a reagovat tak na aktuální situaci. Topení může být řízeno na základě scénářů uživatele, zvyků obyvatel domu či vzdálených pokynů, pro snížení energetické spotřeby a nastavením optimálních teplot pro danou chvíli [41].

Zabezpečovací systémy

Zabezpečovací systémy jsou složeny ze sítě pohybových senzorů, ovládacích obrazovek, řídicí jednotky a zvukového alarmu. Pokud je v uzamčeném režimu zachycen pohyb, vyšle senzor pohybu informaci do řídicí jednotky, která spustí alarm. V případě chytrého zabezpečovacího systému je řídicí jednotka vybavena komunikačním modulem pro umožnění dálkového ovládní a předání okamžité informace uživateli. Zabezpečovací systémy se dají napojit i na kamery s funkcí rozpoznání obličeje a umožnit tak odemčení zabezpečeného prostoru autorizované osobě. Do zabezpečovacího systému se dají přidat i elektrické zámky dveří, vrat a brán. Ty mohou být následně také vzdáleně ovládný [42].

Kamerové systémy jsou složeny z jednotlivých kamer, které mohou komunikovat bezdrátově či drátově, napojením do video rekordéru. Video rekordér může sloužit jako řídicí jednotka odesílající data na cloud nebo lokální server a poskytovat tak uživateli možnost sledovat kamery přes mobilní aplikaci, ovládat jejich pozice a nastavení, nebo nahrávat. Kamery mohou být vybaveny nočním viděním, pro případnou identifikaci pohybu za tmy. Kamery však mohou i spouštět poplach a sloužit tak jako pohybový senzor. Kamery mohou obsahovat funkci rozpoznání obličeje a fungovat tak zároveň jako zabezpečovací systém a systém pro otevírání zámků [43].

Zábava a spotřebiče

Uživatelé často využívají chytrých zařízení pro zábavu. Příkladem jsou mobilní telefony a počítače, přes které lze ovládat chytrá domácnost. Chytrými zařízeními pro zábavu v domácnosti jsou reproduktory, televize, tablety, konzole, projektory a další. Reproduktory, které jsou vybaveny hlasovým asistentem obvykle nabízí ovládní všech dalších kompatibilních zařízení v domácnosti. Uživatel tak může regulovat teplotu nebo světlo, měnit hudbu či film, nastavit upozornění nebo například vypnutí v určitou dobu a další. Tato zařízení mají tendenci navyšovat energetickou spotřebu domácnosti [44].

2.2.5 Automatizace chytrých domácností

Propojením všech zařízení v chytré domácnosti vzniká systém, který může být řízen nejen uživatelem, ale i pomocí implementace umělé inteligence (AI – Artificial Intelligence), která podle daných faktorů vyhodnocuje, co se má stát s určitými zařízeními. Umělá inteligence má několik hlavních funkcí, jimiž jsou: rozpoznávání aktivity, zvuku či obrazu, zpracování dat, rozhodování a predikce. Rozpoznávání aktivity slouží jako zabezpečení pohybovými senzory, na základě, kterých AI vyhodnotí neobvyklé činnosti a spustí alarm. Rozpoznávání zvuku funguje pro rozpoznání hlasu a řízení hlasem ovladatelných technologií. Rozpoznávání obrazu slouží pro rozpoznání obličeje a ověření biometrie, ale také například pro rozpoznání emocí. Funkce zpracování dat analyzuje data z různých vstupů, třídí je a hledá mezi nimi vztahy. Z hlediska funkce rozhodování může AI rozhodnout o opatřeních na danou situaci. Funkce tvorby predikcí je založena na sběru a vyhodnocení dat o rutinních zvycích uživatelů a na podle těchto dat mohou být generovány scénáře, vzory, předpovědi a trendy. Pomocí funkcí a nasbíraných dat může AI vybírat a automatizovat akce vhodné pro daný moment [45].

Existuje více možností pro úspěšné shromažďování, správu a analýzu velkého množství dat, která přichází z IoT zařízení. Některé z těchto možností zahrnují strojové učení (Machine Learning) a technologie velkých dat (Big Data). Technologie velkých dat umožňuje shromažďovat a analyzovat velké objemy informací ze senzorů, které mají být analyzovány a efektivně použity. Strojové učení je součástí umělé inteligence, která je odpovědná za algoritmy a statistické modely, které systémy používají k naplnění svých cílů. Příkladem takových algoritmů může být Java C4.5, který je součástí algoritmu strojového učení J48. Tyto algoritmy jsou klasifikační a jsou využívány pro generování rozhodovacích stromů. Dalšími algoritmy mohou být například náhodný les (Random Forest), náhodný strom (Random Tree) nebo také fuzzy množiny (Fuzzy Clustering). Strojové učení poskytuje alternativu k řešení problémů, založených na učení a identifikuje okolí a charakteristiky těchto problémů, z nichž se poučí a zvýší tak funkčnost systému. Strojové učení provádí akce na zařízeních, ke kterým využívá předem získané znalosti a posiluje tak své učení, které může probíhat s dozorem nebo bez dozoru uživatele [46].

2.2.6 Hospodaření se zdroji

IoT technologie poskytují velkou základnu pro snímání, sběr a vyhodnocení dat. Data jsou sbírána z jednotlivých senzorů a přístrojů a jsou dále vyhodnocována. Tato data uživateli poskytují informace o domácím prostředí, ale také data o energetické spotřebě. Data mohou být vyhodnocena různými způsoby, například formou zpráv, tabulek či grafů. Uživatel tak lépe zjistí svoje návyky a na nich závislou spotřebu energie. Díky těmto informacím a možnosti ovládat elektrická zařízení centralizovaně, může uživatel snížit náklady na provoz, především snížením elektrické spotřeby [47].

2.2.7 Bezpečnost chytrých domácností

Technologie chytrých domácností přináší určité benefity, jako je například vzdálená ovladatelnost jednotlivých zařízení, řízení energetické spotřeby, hospodaření se zdroji a další. Spolu se zavedením těchto technologií však vznikají i rizika pro bezpečnost uživatelů, jejich soukromí, bezpečnost systému a také pro možnou funkčnost zařízení. Sbíráni velkého množství dat, odhaluje citlivá osobní data a může odhalit vzorce chování obyvatel dané domácnosti. Rizika tak plynou z častých poruchových stavů zařízení, ze softwarových chyb, ze sběru dat, ale mohou také představovat bránu pro útoky na domácnost, kterých je několik typů. Prvním typem je útok na webové prostředí, které může být špatně zabezpečeno, nebo není použito dost silné heslo. Dalším typem útoku je tzv. sniffing attack, díky kterému útočník získá přehled nad přenášenými daty a získá tak neoprávněný přístup k systému chytré domácnosti. Třetím typem útoku je tzv. replay attack, díky kterému získá útočník zdrojový kód nebo typ příkazu odesílaný řídicí jednotkou a může pak tento příkaz sám zopakovat [48].

Útočníci mohou tento útok provést i díky chybám ve firmwaru zařízení, jejich zadních vrátkách (Hidden Backdoors) nebo opravných nástrojích (Debugging Tools), které jsou v zařízeních ponechány pro vývojáře. Čtvrtým typem útoku je zamezení přístupu uživatelů k systému a zařízením. Tento typ útoku bývá především proveden pomocí přehlcení vyrovnávací paměti (Buffer Overflow) řídicí jednotky, nebo také DDoS (Denial of Service) útokem, který je proveden za pomoci přehlcení některých zařízení opakovanými příkazy, následně dojde k prolomení zabezpečení například vlivem přehlcení a resetu zařízení. Častou obranou proti těmto typům útoků je vytvoření vlastní sítě s lokálním serverem a silným heslováním, případně se dá útoku předejít kontrolou firmwaru jednotlivých zařízení [49].

3 FORMULACE PROBLÉMŮ A STANOVENÍ CÍLŮ ŘEŠENÍ

Následující kapitola je zaměřena na formulaci problémů řešených v této diplomové práci. Nejdříve jsou určeny a popsány problémy, které jsou spojené s vybavováním domů chytrou domácností. Z formulovaných problémů vychází výzkumné otázky. Odpovědi na výzkumné otázky jsou zjišťovány pomocí metod představených v kapitole 4.

3.1 PROBLÉMY

Při zavádění chytrých technologií do domácností lze využít široké spektrum nejen samotných produktů, ale také možností jejich zapojení a provozu. Z analýzy současného stavu (viz kapitola 2) vyplývá, že se uživatel musí zorientovat v nabídce mnoha prodejců, jejichž výrobky mají různou kvalitu, cenově se liší a využívají rozdílné komunikační technologie. Při volbě chytrých technologií může dojít k problémům v různých aspektech celého procesu. Rovněž při procesu zapojování chytrých domácností mohou být některé činnosti kritické. K problémům může dojít například při plánování realizace vybavení domácnosti a koordinace různých činností.

Pro rozhodnutí zabudovat do domácnosti chytré technologie je určitě potřeba zvážit finanční náklady. Problémem může být vysoká pořizovací cena a relativně krátká životnost produktů. Cílem vybavení domácnosti chytrými technologiemi bývá zlepšení kvality života, ale také snížení ekonomické a energetické náročnosti provozu domu. Aby tohoto cíle bylo dosaženo, nesmí být počáteční investice vyšší než úspory vzniklé díky využívání těchto technologií.

Moderní chytré technologie mohou přinášet zlepšení kvality života a úspory, ale nesou s sebou určitá rizika. Rizika těchto technologií mohou být technická, tedy mohou nastat časté poruchové stavy daných zařízení. Dále mohou představovat rizika z pohledu zabezpečení domu, protože zařízení jsou závislá na elektřině a připojena přes komunikační technologii. Chytré technologie sbírají velké množství dat o prostředí, ale také o uživatelích a mohlo by tak vzniknout riziko úniku osobních dat.

3.2 VÝZKUMNÉ OTÁZKY

Finanční rizika

1. Jak vysoké finanční investice jsou potřeba na vybavení modelové chytré domácnosti ve srovnání s domácností bez chytrých technologií?

2. Za jakou dobu, při maximálním využití chytrých technologií, které přinášejí energetické úspory, jsou investice návratné?

Technická rizika

3. Které činnosti v procesu zavádění chytrých technologií do domácností jsou kritické z hlediska plánování?

4. U kterých prvků chytré domácnosti dochází nejvíce k častým poruchovým stavům?

Bezpečnostní rizika

5. Představují chytré technologie bezpečnostní rizika pro uživatele z hlediska zabezpečení objektu a bezpečí uživatelů samotných, například vnějšími vlivy, vlivem úniku osobních dat nebo technické poruchy?

3.3 STANOVENÍ CÍLŮ ŘEŠENÍ

Cílem řešení problémů spojených se zaváděním a využíváním chytrých technologií v domácnostech je zjistit jejich povahu a rozsah. Problémy jsou spojeny s riziky, která budou pomocí finančního plánu modelového domu a rizikové analýzy identifikována, ohodnocena a budou navržena opatření k jejich snížení. Po vytvoření modelového domu budou aplikovány vybrané metody řešení problémů.

Cílem řešení první výzkumné otázky je zjistit, jak vysoké náklady budou potřebné pro vybavení modelového domu chytrými zařízeními. Pro porovnání bude dům vybaven zařízeními bez chytrých technologií, následně budou pro vybavení vybrána chytrá zařízení s podobnou technickou specifikací. Rozdílem celkových nákladů za oba typy vybavení budou zjištěny potřebné investice do vybavení.

Cílem řešení druhé výzkumné otázky je zjistit, za jak dlouhou dobu pokryjí úspory, plynoucí ze zavedení chytrých technologií, rozdíl nákladů na vybavení. Výše ročních úspor bude stanovena na základě výpočtu energetické spotřeby modelového domu bez chytrých technologií a s chytrými technologiemi. Energetická spotřeba v domě se zavedenými chytrými technologiemi bude snížena o hodnotu uváděnou výrobcem zařízení, při jejich maximálně efektivním využití. Rozdíl cen energetické

spotřeby modelové domácnosti bude porovnán s rozdílem cen za oba druhy vybavení a jejich podílem bude stanoven počet let návratnosti investice do vybavení domácnosti chytrými technologiemi.

Cílem řešení třetí výzkumné otázky je zachytit proces zavádění chytrých technologií do domácnosti. Bude stanoven seznam činností a jejich délky trvání pro síťovou analýzu implementace chytrých zařízení. Pomocí této analýzy bude stanoven potřebný čas pro dokončení. Dále budou identifikovány činnosti, které leží na kritické cestě a projekt implementace chytrých zařízení do domácnosti bude zanesen do síťového grafu.

Cílem řešení čtvrté a páté výzkumné otázky je zjistit, u kterých zavedených prvků chytré domácnosti může docházet k častým poruchovým stavům a které prvky chytré domácnosti mohou představovat bezpečnostní rizika pro uživatele samotné. Řešením čtvrté a páté výzkumné otázky bude zpracování rizikové analýzy, pomocí které budou rizika identifikována a ohodnocena. Součástí řešení je i identifikace jednotlivých systémů a jejich prvků. Následně budou stanoveny chyby jednotlivých prvků, které budou kvalitativně ohodnoceny a graficky zpracovány.

4 POUŽITÉ METODY A JEJICH ZDŮVODNĚNÍ

Následující kapitola je zaměřena na teoretický popis použitých metod pro hledání odpovědi na stanovené výzkumné otázky. Pro lepší specifikaci zkoumané oblasti je nejdříve definována modelová budova. Následně je popsán postup vytvoření finančního plánu, který představuje kvantitativní metodu pro řešení definovaných problémů. Dále jsou popsány metody rizikové analýzy, které jsou zpracovány kvalitativně. Nejdříve metoda síťové analýzy projektu, síťový graf a časová analýza pomocí metody PERT (Program Evaluation and Review Technique), následně metoda nazývaná jako Analýza způsobů a důsledků poruch (FMEA – Failure Mode and Effect Analysis), na kterou navazuje Analýza stromu poruchových stavů (FTA – Fault Tree Analysis).

4.1 MODELOVÝ DŮM

Pro porovnání investic do technologií a úspor na spotřebě bude vytvořen částečný orientační finanční plán domu bez chytrých technologií a s chytrými technologiemi. Pro zpracování finančního plánu byly stanoveny okrajové podmínky (viz kapitola 5), podle kterých se postupovalo při výpočtu.

Nejdříve byly definovány prvky, které budou použity pro vybavení modelové chytré domácnosti, následně byly vybrány prvky bez chytrých technologií a nákupní hodnota vybavení byla srovnána. Prvky bez chytrých technologií byly vybírány ve co nejvíce srovnatelném provedení, aby došlo k co nejlepšímu porovnání. Široké spektrum výrobců a výrobků samotných však zamezuje přesnému srovnání dvou stejných zařízení, z nichž jedno je vybaveno chytrými technologiemi a druhé nikoliv. K takovému srovnání došlo u výrobků od výrobců, kteří poskytují stejný produkt v obou variantách.

4.1.1 Finanční plán modelového domu

Pro porovnání domácností s chytrými technologiemi a bez nich, byl vytvořen částečný finanční plán, který zahrnuje dříve zmiňované porovnání modelových domácností. Výrobci uvádí, že při používání chytrých technologií dochází k úsporám na energiích vlivem kratší doby používání daných zařízení, ale také například zkrácení doby potřebné pro vytápění a ohřev teplé vody. Pro vybraná zařízení byly stanoveny roční spotřeby elektrické energie (viz rovnice č. 1) a pro modelový dům byl vytvořen finanční plán spotřeby energií na vytápění, ohřev teplé vody, osvětlení a spotřebu dalších zařízení (viz přílohy č. 3, 4, 5, 6). Tyto hodnoty byly porovnány s investicemi do chytrých technologií a byla posouzena jejich návratnost. Výsledný počet let, za které je domácnost schopna pokrýt náklady na pořízení, při využití maximálních úspor, je podílem rozdílů spotřeby a ceny vybavení porovnávaných domácností (viz rovnice č. 2). Výpočet doby návratnosti pracuje s neměnnými podmínkami.

$$C = \frac{P * d * 365}{1000} \quad (1)$$

Kde:

C...Roční spotřeba zvoleného zařízení [kW]

P...Příkon zvoleného zařízení [W]

d...Denní doba provozu zvoleného zařízení [hodina]

$$T = \frac{I}{S} \quad (2)$$

Kde:

T...Prostá doba návratnosti investice [roky]

I...Investiční výdaje [Kč]

S...Roční úspory ve spotřebě [Kč]

4.2 SÍŤOVÁ ANALÝZA PROCESU ZAPOJENÍ CHYTRÉ DOMÁCNOSTI

Pro správnou implementaci chytrých technologií do domácnosti je provedena síťová analýza procesu zapojování, montáže a uvedení do provozu jednotlivých zařízení.

4.2.1 Síťový graf a časová analýza projektu

Pro identifikaci kritických činností v procesu instalace a implementace chytrých zařízení do domácnosti byl vytvořen soubor činností, které jsou součástí procesu vybavení domu chytrými zařízeními.

Při vytváření síťového grafu bylo postupováno od začátku ke konci. Pro stanovení počtu řádů a rozdělení činností do jednotlivých řádů síťového grafu byla sestavena hrano-hranová matice. Pro určení řádu uzlů bylo využito metody přeškrťování hran a postupným výpočtem v grafu byla stanovena kritická cesta projektu. Doby trvání činností jsou považovány za náhodné proměnné a využitý síťový graf je tedy stochastický. Pomocí metody PERT byla vytvořena časová analýza projektu. Projekt byl zachycen do hranově definovaného síťového grafu [50].

Časová analýza projektu metodou PERT začíná definováním posloupnosti jednotlivých činností a jejich trváním ve dnech. Je vytvořen vážený průměr hodnot optimistického (a) realistického (m) a

pesimistického (b) odhadu trvání pomocí rovnice č. 3. Následně jsou spočítány statistické ukazatele pro tyto hodnoty a těmi jsou rozptyl a směrodatná odchylka. Vzorec pro výpočet rozptylu hodnot je zachycen v rovnici č. 4, směrodatná odchylka je vypočtena jako odmocnina z rozptylu. Jsou stanoveny začátky a konce možné, začátky a konce přípustné. Rozdílem začátků přípustných a začátků možných nebo konců přípustných a konců možných je vypočtena časová rezerva jednotlivých činností, která představuje počet možných časových jednotek k práci. Přes činnosti s časovou rezervou rovnou nule, vede kritická cesta projektu [51].

$$t(ij) = \frac{a + 4m + b}{6} \quad (3)$$

Kde:

t(ij)...Doba trvání činnosti [hodina]

a...optimistický odhad doby trvání činnosti [hodina]

m...realistický odhad doby trvání činnosti [hodina]

b...pesimistický odhad doby trvání činnosti [hodina]

$$\sigma^2 = \frac{(b - a)^2}{36} \quad (4)$$

Kde:

σ^2 ...rozptyl hodnot dob trvání

a...optimistický odhad doby trvání činnosti

b...pesimistický odhad doby trvání činnosti

4.3 RIZIKOVÁ ANALÝZA

Pro identifikaci a ohodnocení rizik bude provedena riziková analýza. Součástí rizikové analýzy budou dvě metody. První metodou bude Analýza způsobů a důsledků poruch (FMEA – Failure Mode and Effect Analysis) a druhou bude Analýza stromu poruchových stavů (FTA – Fault Tree Analysis).

4.3.1 Metoda FMEA

Analýza způsobů a důsledků poruch, která může být nazývána i jako Analýzy selhání a jejich dopadů je metoda, která rozebírá způsoby selhání jednotlivých prvků a jejich důsledky. Umožňuje hledat

dopady a příčiny selhání jednotlivých zařízení. Slouží jako kontrola všech prvků systému a jeho provozu. Metoda FMEA slouží i jako nástroj pro identifikaci rizik zkoumaného systému a identifikuje možné chyby na úrovni jednotlivých komponentů. Hodnota rizika je stanovena na základě rizikového prioritního čísla, které je násobkem pravděpodobnosti výskytu, dopadu a pravděpodobnosti odhalení vad [52].

Metoda FMEA byla vybrána pro identifikaci a ohodnocení rizik zavedených technologií, které se řadí do určitých oblastí a dále se dělí na jednotlivé prvky. Metoda byla zpracována kvalitativně a rizika byla ohodnocena za spolupráce expertů zabývajících se problematikou technologií chytrých domácností. Hodnocení pravděpodobnosti výskytu, dopadu vady a pravděpodobnosti odhalení bylo vytvářeno na základě tabulky č. 1, ve které je určena stupnice hodnocení. Jednotlivá identifikovaná rizika byla rozdělena do intervalů, podle kterých bylo rozhodnuto o nutnosti vytvoření opatření pro snížení hodnoty daných rizik (viz tabulka č. 2).

Tabulka č. 1 - Stanovené stupnice hodnocení intervalů výskytu, dopadu a odhalení vady [vlastní]

Pravděpodobnost výskytu	Stupnice hodnocení	Dopad vady	Stupnice hodnocení	Pravděpodobnost odhalení	Stupnice hodnocení
Velmi nízká	<0;2>	Nepatrný	<0;2>	Velmi vysoká	<0;2>
Nízká	<2,1;4>	Přijatelný	<2,1;4>	Vysoká	<2,1;4>
Střední	<4,1;6>	Významný	<4,1;6>	Střední, za určitých podmínek	<4,1;6>
Vysoká	<6,1;8>	Velmi významný	<6,1;8>	Nízká	<6,1;8>
Velmi vysoká	<8,1;10>	Kritický	<8,1;10>	Velmi nízká	<8,1;10>

Rozdělení do intervalů rizikového prioritního čísla lze vidět v tabulce č. 2. Rozsah jednotlivých intervalů je stanoven na základě hodnot rizikových prioritních čísel, aby mohlo dojít k jejich snížení vlivem opatření.

Tabulka č. 2 - Stanovené intervaly rizikového prioritního čísla [vlastní]










Intervaly RPN	Hodnocení intervalů
<0;99>	Přijatelná hodnota rizika
<100;149>	Přijatelná hodnota, ale vyžaduje opatření
<150;299>	Kritická hodnota rizika, nutnost vytvoření opatření
<300;1000>	Nepřijatelná hodnota rizika

4.3.2 Metoda FTA

Metoda FTA je vytvářena na základě analýzy vzniku a příčin událostí, které mohou vést k vybrané vrcholové události. Metoda FTA se zaměřuje na vrcholovou událost a stanovuje příčiny vzniku této události. Poruchové stromy jsou zakreslovány graficky a zachycují poruchy jednotlivých prvků nebo lidských chyb, které mohou vést k vrcholové události, představující nehodu či havárii. Zpracování metody umožňuje zaměřit se na problémové oblasti systémů, vytvořit opatření pro zamezení příčin vzniku nehod či chyb [53].

Metoda FTA byla vypracovávána na základě metody FMEA. Na metodu Metoda FTA byla zpracována kvalitativně. Pro některé součásti systému nejsou výrobcem uváděny spolehlivosti či četnosti poruch. Pro grafické zpracování bylo využito symbolů, které jsou zobrazeny a popsány v tabulce č. 3.

Tabulka č. 3 – Použité grafické symboly pro metodu FTA [54] (upraveno autorem)

Doporučená značka	Alternativní značka	Název a popis
		Blok s názvem nebo popisem vrcholové události (TOP jevu).
		Blok s názvem nebo popisem události (jevu).
		Základní (primární) událost – událost, která se dále nedělí.
		Nerozvíjená událost – událost, která není dále rozvíjena (zpravidla proto, že se to nepovažuje za nutné)
		Událost analyzovaná jinde - událost dále rozvíjená v jiném stromu poruch.
		Hradlo OR (nebo) – událost nastane tehdy, když nastane kterákoliv vstupní událost, nebo jejich libovolná kombinace.
		Hradlo AND (a) – událost nastane pouze tehdy, když současně nastanou všechny vstupní události.

5 VLASTNÍ ŘEŠENÍ

Následující kapitola je zaměřena na prezentaci výsledků použitých metod. Metody byly využity pro hledání odpovědí na výzkumné otázky, které plynou z problematiky řešeného tématu (viz kapitola 3). Nejdříve budou prezentovány výsledky kvantitativní analýzy finančních rizik, která se týká finančního plánu modelové domácnosti, do které jsou zaváděny chytré technologie. Následují výsledky řešení kvalitativní analýzy procesních, technických a bezpečnostních rizik.

5.1 FINANČNÍ PLÁN MODELOVÉ DOMÁCNOSTI

Následující kapitola je zaměřena na srovnání finančního plánu modelového domu bez chytrých technologií a s chytrými technologiemi. Nejdříve jsou nastaveny okrajové podmínky modelového domu a vstupní hodnoty pro výpočet nákladů na spotřebu elektrické energie. Jednotlivé položky vybavení a jejich technické specifikace byly zjišťovány na základě zdrojů, uvedených u daných vybavení v přílohách č. 1 a č. 2. Výpočet nákladů na vytápění, ohřev teplé vody a spotřebu některých základních zařízení, byl zpracován na základě zdroje [55].

5.1.1 Modelový dům

Pro zpracování finančního plánu byly stanoveny okrajové podmínky modelové budovy bez vybavení chytrými zařízeními. Jedná se o rodinný jednopodlažní dům. Dům se nachází v České republice ve městě Brně. Vstupní veličiny pro výpočet jsou stanoveny následovně: venkovní výpočtová teplota (t_e): $-12\text{ }^\circ\text{C}$, základní délka otopného období (d): 232 dní. Hodnota tepelné ztráty domu je $7,5\text{ kW}$, což závisí na tepelných ztrátách celého objektu. Intenzita výměny vzduchu (n) je stanovena na $0,4\text{ h}^{-1}$. V objektu se nepoužívá řízená ventilace s rekuperací tepla. Počet dnů přípravy teplé vody (N) je stanoven na 365 dní v roce a je ohřívána energií na vytápění. Podlahová plocha domu je 180 m^2 , objem domu je 486 m^3 . V domě žije čtyřčlenná rodina, jedná se o dva dospělé s prací mimo domácnost a dvě děti. Pro výpočet ohřevu teplé vody je předpokládána denní spotřeba na obyvatele 50 L a teplá voda je ohřívána po dobu 365 dní [55].

Popsaný modelový dům lze vybavit standardními nebo chytrými technologiemi. V dalších podkapitolách budou porovnávány rozdíly finanční náročnosti na vybavení domu a jeho provoz. Vstupní hodnoty modelového domu bez chytrých technologií budou upraveny na základě dat stanovených výrobcí chytrých technologií. Snížené hodnoty vstupních údajů jsou přesněji popsány v kapitole 5.1.3 Finanční plán elektrické spotřeby modelového domu.

5.1.2 Finanční plán vybavení

Následující kapitola je zaměřena na srovnání zařízení pro vybavení běžné a chytré domácnosti. Jednotlivá zařízení byla zařazena do skupin a blíže technicky specifikována. Byl stanoven potřebný počet kusů a cena. Cena a další informace o zařízeních byly čerpány přímo od výrobců, kteří jsou uvedeni u jednotlivých výrobků v tabulce (příloha č. 1 a č. 2)

V příloze č. 1 se nachází rozpis a vybavení domácnosti zařízeními bez chytrých technologií. V příloze č. 2 je rozpis a nacenění vybavení domácnosti chytrými technologiemi s podobnou specifikací, včetně DPH. Zařízení jsou rozčleněna do následujících skupin: 1. Vytápění, ohřev teplé vody a chlazení; 2. Osvětlení; 3. Zabezpečení; 4. Stínící technika; 5. Elektroinstalace; 6. Síťové a řídicí jednotky.

Srovnáním pořizovacích nákladů obou typů vybavení ukazuje cenový rozdíl mezi nimi. Cena vybavení bez chytrých technologií byla vypočtena na 40 690 Kč. Cena vybavení s chytrými technologiemi byla vypočtena na 223 247. Celkový rozdíl nákladů na vybavení činí 182 557 Kč.

Tabulka č. 4 – Srovnání celkových nákladů na vybavení v Kč [vlastní]

Cena základního vybavení [Kč]	Cena chytrého vybavení [Kč]	Rozdíl ceny vybavení [Kč]
40690	223247	182557

5.1.3 Finanční plán elektrické spotřeby modelového domu

Pro výpočet nákladů na vytápění, ohřev teplé vody a další spotřeby bylo využito online kalkulačky na odborném portálu Technická zařízení budov (TZB – info) [55]. Celková spotřeba je dále stanovena na základě výsledků výpočtu vytápění, ohřevu TV, dalších spotřeb a spotřeby dodaných technologií nezahrnutých do prvotního výpočtu.

Pro vytápění a ohřev teplé vody je využíván teplovodní elektrokotel. Do výpočtu spotřeby energie byly zahrnuty i některé domácí spotřebiče pro vytvoření reálnějšího obrazu spotřeby modelového domu. Vybrány byly: elektrický sporák o příkonu 2 kW, elektrická trouba o příkonu 2 kW, rychlovarná konvice o příkonu 2 kW, mikrovlnná trouba o příkonu 600 W, kombinovaná chladnička s mrazničkou o příkonu 120 W, myčka nádobí o příkonu 650 W, pračka o příkonu 600 W, sušička prádla o příkonu 750 W, televize o příkonu 70 W, osobní počítač o příkonu 80 W, modem pro internet o příkonu

12 W a 15 W pro silnější modem v domácnosti se zavedenými chytrými zařízeními. U těchto jmenovaných zařízení byly do výpočtu zahrnuty i tepelné zisky, které vychází z jejich provozu. [55]

Pro výpočet spotřeby energie modelového domu, který je vybaven chytrými technologiemi byly stanoveny kratší časové úseky pro vytápění, ohřev teplé vody, svícení a dobu využití jednotlivých zařízení a spotřebičů na základě údajů uváděných výrobcí. Pro vytápění a ohřev teplé vody bylo počítáno se snížením dob, v rámci délky otopného období a počtu dnů přípravy teplé vody o 20 %, přesné hodnoty vstupních údajů jsou zapsány v příloze č. 3 a č. 5. Spotřeba v rámci osvětlení byla vlivem pohybových senzorů, intenzity denního světla a pomocí dálkového ovládání snížena o 3 hodiny na den u žárovek a o 1 hodinu na den u LED pásek. Spotřeba v rámci klimatizace byla snížena na základě využití venkovních žaluzií o polovinu doby denního využití klimatizace. Spotřeba některých domácích spotřebičů byla snížena průměrně o 5 % doby využití na den. Doba denního využití modemu pro internet byla zkrácena o 4 hodiny na den z důvodu nepoužívání internetové sítě v noci. K úsporám dochází především díky vypínání jednotlivých zařízení v jejich neprovozní době. Výhodou dálkového a centrálního ovládání je také vypnutí vytápění, ohřevu teplé vody a dalších spotřebičů v době, kdy se uživatelé nenachází delší dobu v domě, například při rodinných dovolených. Přesné údaje o spotřebě jednotlivých zařízení se nachází v příloze č. 4 a č. 6.

Do výpočtu celkových nákladů byly zahrnuty i výdaje na baterie. Cena baterií typu AA a AAA se pohybuje okolo 6 Kč za kus. Cena baterií typu CR123a se pohybuje okolo 56 Kč za kus a cena baterií typu LR20 se pohybuje okolo 50 Kč za kus (viz příloha č. 4 a č. 6). Ceny baterií byly stanoveny na základě průzkumu trhu autorem práce. Energetický odběr některých zařízení, jako jsou například sirény, je zanedbatelný. Tepelný zisk z dodaných zařízení není zahrnut do výpočtu, jelikož z některých zařízení neplyne anebo se jedná o zanedbatelné hodnoty.

Z následujících tabulek č. 5 a č. 6 lze vyčíst roční náklady na vytápění, ohřev teplé vody, provoz ostatních domácích spotřebičů obou typů domácností. Dalšími položkami jsou paušální platby za energii a investice a údržba topného systému, se kterými je při výpočtu nutné počítat. Tyto položky jsou zahrnuty do celkové částky za vybrané složky spotřeby a byly spočítány pomocí online kalkulačky [55]. K těmto nákladům byly připočteny roční náklady na spotřebu dodaných vybavení, která byla spočítána na základě jejich příkonu a denní doby využití.

Tabulka č. 5 – Roční energetické náklady domácnosti bez chytrých technologií [55] (upraveno autorem)

Roční náklady v Kč (včetně DPH)		
Vytápění	38112	Kč
Teplá voda	11107	Kč
Ostatní spotřebiče	19446	Kč
Paušální platby	5604	Kč
Investice a údržba	7900	Kč
Celková částka za vybrané složky spotřeby	82169	Kč
Spotřeba dodaného vybavení + baterie [Kč]	5264	Kč
Celková částka za rok	87433	Kč

Následující tabulka je zaměřena na výpočet složek spotřeby v modelové domácnosti vybavené chytrými technologiemi. Náklady na jednotlivé položky jsou nižší než u domácnosti bez chytrých technologií.

Tabulka č. 6 – Roční energetické náklady domácnosti s chytrými technologiemi [55] (upraveno autorem)

Roční náklady v Kč (včetně DPH)		
Vytápění	32374	Kč
Ohřev teplé vody	8886	Kč
Ostatní spotřebiče	13853	Kč
Paušální platby	5604	Kč
Investice a údržba	7900	Kč
Celková částka za vybrané složky spotřeby	68616	Kč
Spotřeba dodaného vybavení + baterie [Kč]	5314	Kč
Celková částka za rok	73930	Kč

Srovnáním ročních nákladů na spotřebu vyplývá, že náklady domácnosti bez chytrých technologií vycházejí na celkovou roční částku 87 433 Kč. Náklady domácnosti se zavedenými chytrými technologiemi jsou levnější a vycházejí na 73 930. Rozdíl nákladů na elektrickou spotřebu obou typů domácností vychází na 13 503 Kč.

Tabulka č. 7 – Srovnání nákladů na vybavení, energie a stanovení počtu let návratnosti [vlastní]

Cena ročních nákladů – původní [Kč]	Cena ročních nákladů – chytré [Kč]	Rozdíl nákladů na energie [Kč]	Rozdíl ceny vybavení [Kč]	Počet let návratnosti investice [roky]
87433	73930	13503	182557	13,5197364

Rozdíl pořizovacích nákladů na vybavení je 182 557 Kč. Pořizovací cena chytrých technologií je vyšší než technologií standardních. Avšak náklady na spotřebu domácnosti s chytrými technologiemi je nižší a to o 13 503 Kč za rok. Podílem rozdílu cen obou typů vybavení a rozdílu nákladů na energie je vypočtena prostá doba návratnosti investice. Doba, za kterou při neměnných podmínkách úspory ve spotřebě energie pokryjí počáteční investice do chytrého vybavení, je vypočtena na 13,5 roku (prostá doba návratnosti).

5.2 ANALÝZA PROCESNÍCH, TECHNICKÝCH A BEZPEČNOSTNÍCH RIZIK

Následující kapitola je zaměřena na analýzu a ohodnocení procesních, technických a bezpečnostních rizik chytrých domácností. Pro analýzu procesu implementace chytrých technologií do domácnosti byla provedena síťová analýza procesu zavádění chytrých technologií do domácnosti. Pro analýzu technických a bezpečnostních rizik zavedených technologií byly provedeny Metody FMEA a FTA.

5.2.1 Analýza procesních rizik

V rámci analýzy procesních rizik byla využita síťová analýza vytvořeného procesu. Vytvořením síťového grafu (příloha č. 9) byl proces graficky a časově zpracován. Do síťového grafu byla zaznačena kritická cesta procesu, která leží na činnostech, které mají celkovou časovou rezervu rovnu nule, to znamená, že u nich nejsou volné časové jednotky využitelné k práci. Činnosti byly rozčleněny a časově ohodnoceny v rámci metody PERT (Příloha č. 7 a č. 8).

Bylo využito hranově definovaného síťového grafu, ve kterém červená barva zvýrazňuje kritickou cestu projektu. Modrá barva je využita pro zvýraznění rozhodujících hodnot konců přípustných a zelená barva pro zvýraznění rozhodujících konců možných (Příloha č. 9). Vzniklé fiktivní činnosti byly zaneseny do tabulky metody PERT (Příloha č. 8).

Kritická cesta procesu vede přes činnosti s označením A, B, C, F, G, H, CH, J, K, L, M, O, P, Q, U, V, W, X. Celková doba trvání procesu zavedení chytrých technologií do domácnosti je 828 hodin. Což

představuje práci na celých 34 dní. Pokud by se jednalo o pracovní dny, s osmihodinovou směnou, pak by dokončení procesu trvalo 103,5 pracovních dní, což jsou 3 měsíce a dva týdny, včetně víkendů.

5.2.2 Analýza technických a bezpečnostních rizik

Analýza technických a bezpečnostních rizik byla zpracována aplikací metody FMEA a FTA. Pro aplikaci metody FMEA byly vytvořeny skupiny prvků podle jejich funkce nebo společného znaku. Jedná se o tyto skupiny prvků: 1. Vytápění a chlazení; 2. Osvětlení; 3. Stínění; 4. Elektroinstalace; 5. Zabezpečení; 6. Připojení; 7. Bezpečí uživatelů; 8. Bezpečnost budovy. Následně byly v rámci skupin rozčleněny jednotlivé prvky podle konkrétních zařízení. Potenciální chyby, jejich příčiny, důsledky, ohodnocení pravděpodobnosti výskytu, dopadu vady, pravděpodobnosti odhalení, vytvoření opatření a přehodnocení rizik bylo vypracováváno s týmem odborníků soukromé stavební firmy zabývající se zřizováním chytrých domácností.

Metoda FMEA

Chyby s nejvyšším rizikovým prioritním číslem ve skupině prvků vytápění a chlazení mají za důsledek omezení nebo znemožnění regulace teploty a ohřevu teplé vody. Chyby s nejvyšším rizikovým prioritním číslem ve skupině prvků osvětlení mají za důsledek ztrátu funkčnosti osvětlení. Chyby s nejvyšším rizikovým prioritním číslem ve skupině prvků stínění mají za důsledek ztrátu funkčnosti žaluzií a jejich poškození. Chyby s nejvyšším rizikovým prioritním číslem ve skupině prvků elektroinstalace mají za důsledek znemožnění dálkového ovládní spotřebičů. Důsledkem chyb s nejvyšším rizikovým prioritním číslem ze skupiny prvků zabezpečení je omezení zabezpečení budovy, ztráta záznamu kamer a ztráta funkčnosti zabezpečovací jednotky či elektronického zámku.

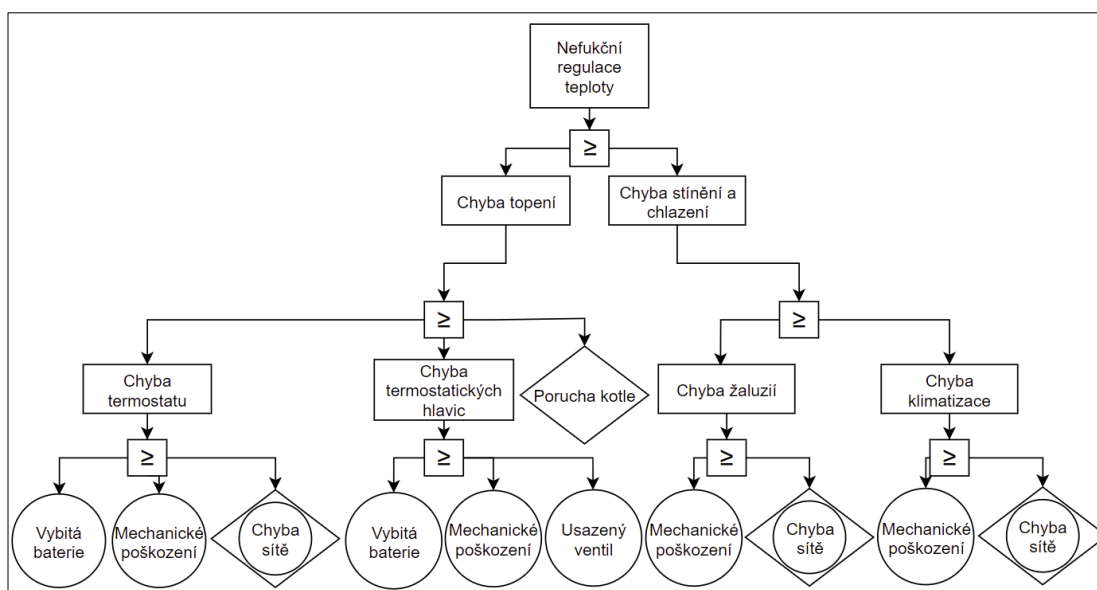
Ve skupině prvků připojení je důsledkem chyb s nejvyšším rizikovým prioritním číslem omezení funkčnosti internetové sítě, ztráta funkčnosti a dat z řídicí jednotky a ztráta kontroly nad zařízeními. Nejvyšší rizikové prioritní číslo s hodnotou 300, které se jako jediné pohybuje v intervalu pro nepřijatelnou hodnotu rizika, vykazuje ztráta zabezpečení budovy a sítě, plynoucí z neoprávněného přístupu k zařízením, a proto představuje riziko pro bezpečí uživatelů. Poslední skupinou prvků je bezpečnost budovy, kde chyby s nejvyšším rizikovým prioritním číslem mají důsledek v omezení a ztrátě zabezpečení budovy a sítě, umožnění neoprávněného přístupu do objektu a krádeže majetku. Suma rizikových prioritních čísel byla po zavedení opatření snížena zhruba 1,7krát. Kompletní metoda FMEA se nachází v příloze č. 10.

Metoda FTA

Na základě metody FMEA a rozdělení prvků do skupin byly vypracovány analýzy stromů poruchových stavů pro vybrané vrcholové události. Na základě těchto analýz vyplývají jednotlivé elementární prvky systému, které vedou k vrcholové události. Na základě těchto prvků je uživatel schopen lépe odhalit základní chyby vedoucí k chybám a poruchám systému chytré domácnosti.

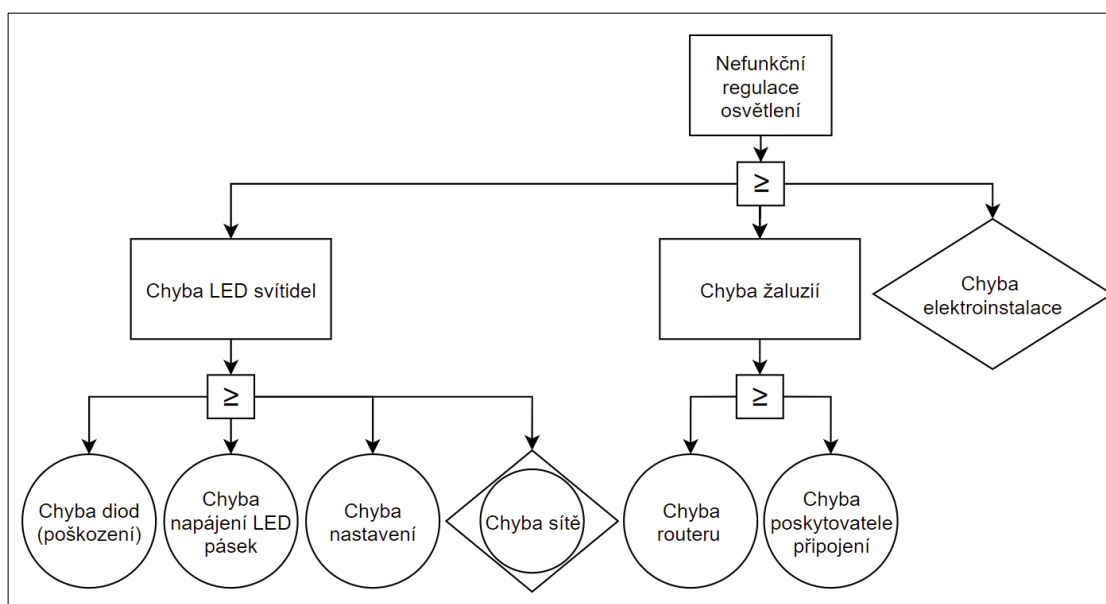
Jednotlivé FTA jsou zpracovány kvalitativně, protože některé údaje o spolehlivosti a četnosti chyb nejsou výrobcem zveřejněny. Spolehlivostní data bývají stanovovány výrobcem na základě reklamací, oprav anebo například testováním výrobků a tato data nebývají výrobcem zařízení zákazníkům sdílena.

Jako první vrcholová událost byla analyzována pomocí metody FTA nefunkční regulace teploty (viz graf č. 4). K vrcholové události vede chyba v topné soustavě systému nebo chyba ve stínění a chlazení. Chyba topení může být způsobena chybou termostatu, termostatických hlavic nebo poruchou kotle. Chyba stínění a chlazení může být způsobena chybou žaluzií nebo chybou klimatizace. Tyto chyby mohou být způsobeny nejčastěji mechanickým poškozením, chybou sítě nebo vybitou baterií.



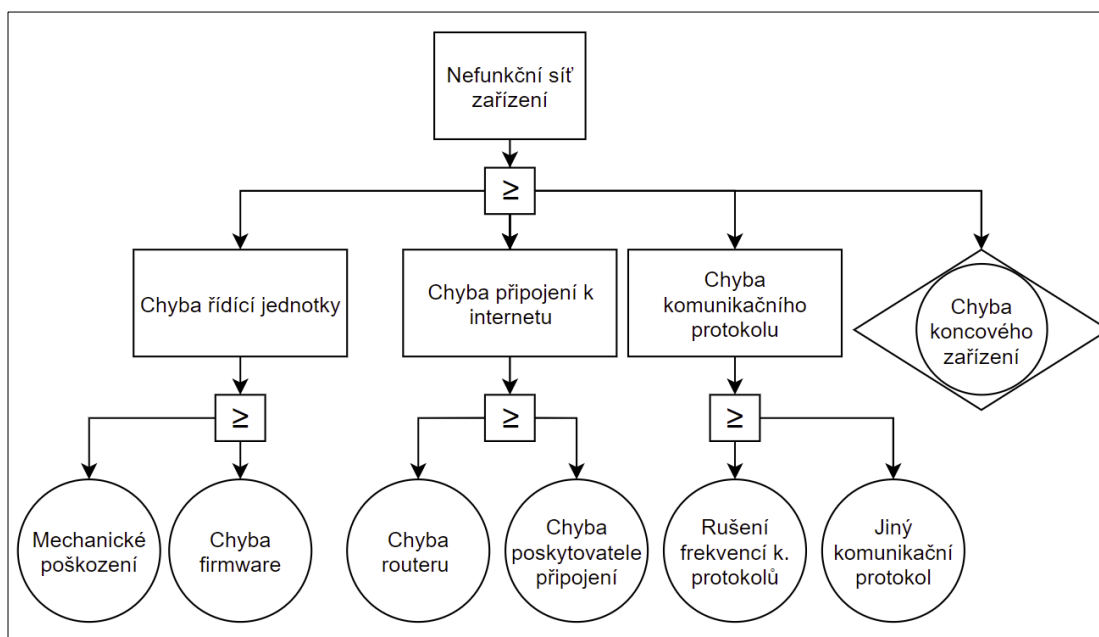
Graf č. 4 – FTA 1 – Nefunkční regulace teploty v domě [vlastní]

Druhou analyzovanou vrcholovou událostí metodou FTA je nefunkční regulace osvětlení (viz graf č. 5). Tato vrcholová událost může být způsobena chybou LED svítidel, chybou žaluzií nebo chybou elektroinstalace. Nejvíce příčin je identifikováno u chyby LED svítidel, jsou to chyba nebo poškození LED diod, chyba napájení LED pásek, chybné nastavení osvětlení nebo chyba sítě. Příčiny chyb žaluzií v kontextu vrcholové události, jsou především v jejich připojení k síti.



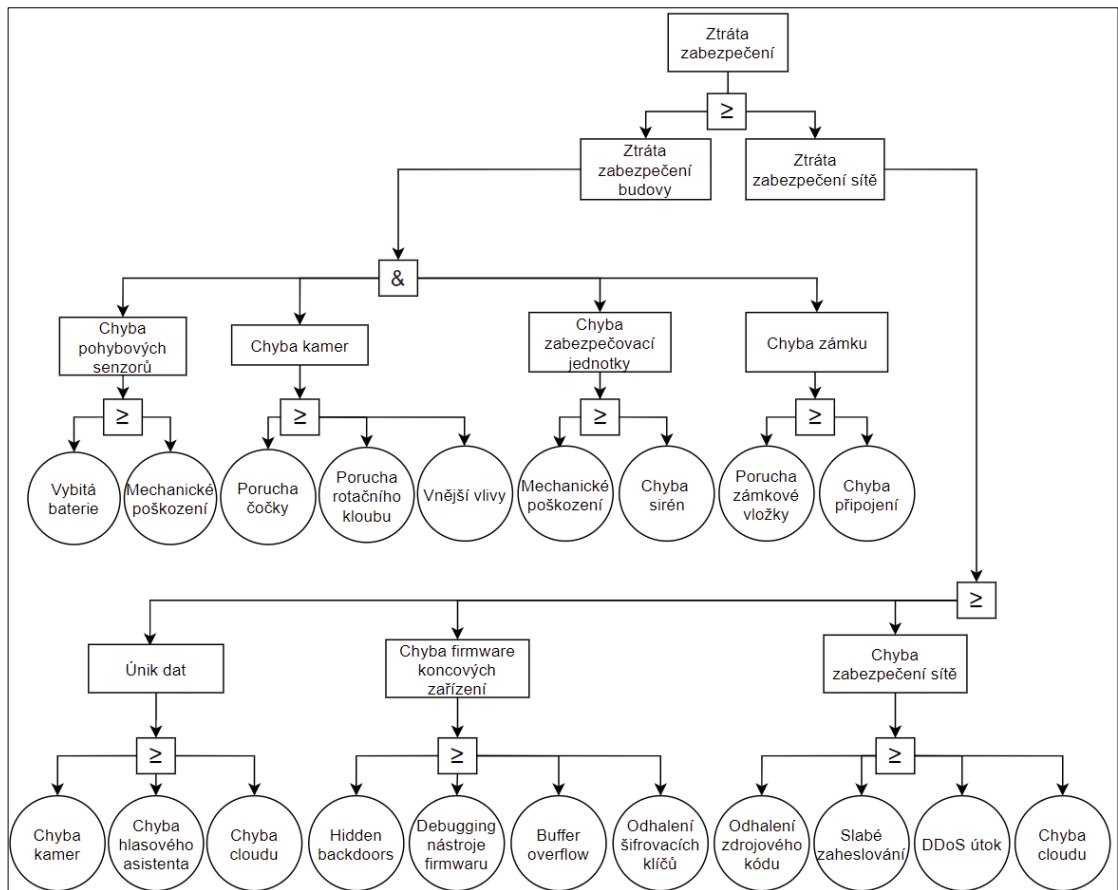
Graf č. 5 – FTA 2 – Nefunkční regulace osvětlení [vlastní]

Třetí vrcholová událost, která byla analyzována metodou FTA se týká nefunkční sítě zařízení (viz graf č. 6). Tato síť může být internetová nebo síť komunikačních protokolů zařízení. Chyby vedoucí k vrcholové události mohou být v řídicí jednotce, v připojení k internetu, v komunikačním protokolu nebo v samotném koncovém zařízení. Příčinami chyb může být chyba firmwaru řídicí jednotky, chyba routeru, chyba poskytovatele připojení. V úvahu připadá také rušení rádiových frekvencí různými komunikačními protokoly.



Graf č. 6 – FTA 3 – Nefunkční síť zařízení – ovládání a komunikace [vlastní]

Poslední vybranou vrcholovou událostí je ztráta zabezpečení (viz graf č. 7). Ke ztrátě zabezpečení může dojít vlivem ztráty zabezpečení budovy nebo ztrátou zabezpečení sítě. Ztráta zabezpečení budovy může být způsobena chybou pohybových senzorů, chybou kamer, chybou zabezpečovací jednotky nebo chybou elektronických zámků. Nejčastějšími příčinami těchto chyb může být mechanické poškození nebo porucha daných zařízení, nedají se vyloučit ani vnější vlivy, jako je počasí nebo lidský faktor a chyba připojení elektronického zámku. Ztráta zabezpečení sítě může být způsobena chybou firmware koncových zařízení, chybou zabezpečení sítě anebo únikem dat. Příčinou úniku dat bývá nezabezpečený přístup ke kamerovému systému, sběr dat výrobcem hlasových asistentů nebo nezabezpečený přístup ke cloudovému výpočetnímu prostředí. Příčinou chyby firmware koncových zařízení a chyby zabezpečení sítě, bývá využití slabých míst v jejich zabezpečení, hlavní příčinou chyby je vnější útok na systém pro získání neoprávněného přístupu. Typy takových útoků se nazývají například: Hidden Backdoors, ponechané nástroje vývojářů pro debugging firmware jednotlivých zařízení, Buffer Overflow, Odhalení šifrovacích klíčů, odhalení zdrojových kódů, DDoS útoky a další. Vysvětlení jednotlivých pojmů se nachází v kapitole 2.2.7 Bezpečnost chytrých domácností. Ke ztrátě zabezpečení může dojít i vlivem využití slabých hesel pro zabezpečení sítě.



Graf č. 7 – FTA 4 – Ztráta zabezpečení

6 DISKUZE / ANALÝZA VÝSLEDKŮ ŘEŠENÍ

Na základě přechozí kapitoly (kapitola 5) byly stanoveny odpovědi na výzkumné otázky. Při zpracování výzkumných otázek bylo využito dat, která byla získána z různých zdrojů, například se jedná o ceny vybavení, ceny tarifů dodávané elektřiny a další položky. Specifikace vybraného vybavení má vliv na celkovou cenu vybavení, a tedy i na vstupní investice. Náklady na vybavení domácnosti se odvíjejí od výběru typu zboží, výrobce, prodejce, množství a podobně. Zvolený modelový dům byl nadefinován autorem a analýzy se tedy vztahují pouze k tomuto modelu. V domech s jinými rozměry, jinými typy vybraného vybavení v odlišné klimatické oblasti apod. by analýzy vycházely z jiných vstupních dat. Teplotní ztráta objektu, množství a specifika obyvatel, způsob větrání a další, mají vliv na spotřebu energií dané domácnost a na návratnost vstupních investic.

Pro zjednodušení výpočtu návratnosti investic byla uvažována konstantní spotřeba modelového domu. Reálná spotřeba by se odvíjela od dané aktuální situace v určitém časovém úseku. Na proměnlivost spotřeby má vliv mnoho faktorů, jako je například počet přítomných osob, jejich zvyklosti, měnící se okolí a další. Na cenu spotřebovaných energií má zase vliv například měnící se výše tarifu dodávané energie poskytovatelem. Reálné ceny za spotřebu by tedy byly proměnlivé a ovlivnily by tak návratnost investic. Výše úspor se odvíjí od maximálního využití technologií, které mají za úkol snížit energetickou spotřebu domácnosti. V příkladu modelového domu bylo počítáno s plným využitím těchto technologií, což ve skutečnosti není realizovatelné.

Do výpočtu elektrické spotřeby využívané na vytápění nebyla uvažována hystereze otopných soustav. Jelikož se jedná o vytápění domu pomocí teplovodního elektrokotle a radiátorů, mohlo by docházet k hysterezi. To znamená k nadměrnému nebo nedostatečnému topení, před nebo po dosažení požadované přednastavené hodnoty na termostatu. Pro řešení se využívá nastavení spínání topení při dosažení určitých přednastavených teplot, které zajistí dostatečné topení a včasné vypnutí topení. Nastavení by mělo být vztaženo pro danou otopnou soustavu, protože má každá svá specifika.

Do celkových nákladů na vybavení jsou započítána všechna dodaná zařízení chytré domácnosti, ačkoliv některá z nich nepřinášejí energetické úspory. Tato zařízení mohou plnit například bezpečnostní funkce nebo zvyšují komfort bydlení, a jsou proto součástí vybavení. Na druhou stranu mohou představovat opatření proti možným finančním a bezpečnostním rizikům, jako je například krádež majetku.

Návratnost investic do vybavení modelové domácnosti chytrými technologiemi je vypočtena na zhruba 13,5 let. Otázkou je, jaká je životnost jednotlivých vybraných zařízení. Jelikož se jedná o poměrně nová zařízení s chytrými technologiemi, není výrobcem většinou udávána jejich životnost. Záruka od

prodejce na výrobky tohoto typu bývá často pouze 2 roky. Je tedy pravděpodobné, že před navrácením vložených investic mohou některé výrobky přestat fungovat.

Některá zavedená opatření v rámci rizikové analýzy a metody FMEA by mohla znamenat zvýšení nákladů na zajištění chodu domácnosti. Tyto náklady se vztahují například k vytvoření záložní sítě, pořízení vlastního serveru pro zabezpečení komunikace jednotlivých zařízení, záložní zdroje pro napájení bezpečnostních prvků a serveru. Náklady na pořízení vlastního serveru by se mohly pohybovat v rozmezí 6 000 až 50 000 a více Kč. Cena serveru by se odvíjela od vlastní technické specifikace. Náklady na pořízení záložního zdroje se pohybují v řádu tisíců Kč. Další opatření se vztahují především na kontrolu jednotlivých zařízení, jejich údržbu a případné opravy. Kromě placených opatření jsou zavedena i opatření bezplatná, která vyžadují znalosti a čas, potřebný pro jejich provedení, i když je uživatel schopen, zajistit si je sám.

Náklady na vybavení chytré domácnosti jsou poměrně vysoké a člověk musí mít pro toto vybavení dostatečný počáteční kapitál. Od výše finančních zdrojů se většinou odvíjí i kvalita a množství funkcí vybraných zařízení. Dražší zařízení mohou mít i delší životnost a zvyšovat více kvalitu života uživatelů a komfort bydlení. Na druhou stranu technika zastarává a vývoj jde kupředu. Je tedy možné, že po určité době bude nutné zařízení vyměnit za novější modely s modernější technologií, protože vývoj v této oblasti jde rychle kupředu. Starší zařízení nemusí být s postupem času kompatibilní s novými technologiemi.

Shrnutím předcházejících úvah lze formulovat určitá doporučení pro praxi. Důležitým doporučením pro zajištění funkčnosti celého systému je výběr vzájemně kompatibilních zařízení. I přes vyšší náklady na pořízení může uživatel upřednostnit zařízení šetrná k ekologickému prostředí a ta, která přinášejí úspory v energetické spotřebě. Je důležité uvažovat o různých typech paliv pro vytápění a různých typech otopných soustav pro zajištění minimálních nákladů a optimálního výkonu. V případě řešeného modelového domu je vytápění a ohřev teplé vody zajištěn elektrickou energií. Využitím jiných paliv, jako je například zemní plyn, by se mohla snížit finanční náročnost vytápění a ohřevu teplé vody.

Dle mého subjektivního názoru se v souvislosti se zaváděním chytrých technologií do domácnosti nedá počítat s návratností investic. Především z důvodu životnosti jednotlivých zařízení a jejich poměrně vysoké pořizovací ceny. Pořízení těchto technologií se dle mého názoru finančně nevyplatí, ale přináší některá pozitiva, která hrají roli při rozhodování o vybavení domácnosti chytrými technologiemi. Těmito pozitivy může být například zlepšení kvality života uživatelů, komfortu bydlení, snížení ekologické zátěže pro okolí a zvýšení zabezpečení objektu.

7 ZÁVĚR

Hlavním cílem této diplomové práce bylo analyzovat a ohodnotit rizika spojená se zapojováním a využíváním technologií, používaných pro propojení chytrých domácností, které jsou součástí oblasti Internetu věcí. Nejdříve byla popsána teoretická východiska pro řešení problematiky. Následně byly formulovány problémy a výzkumné otázky. Pro zodpovězení výzkumných otázek byly vybrány postupy a metody identifikace, analýzy a ohodnocení rizik.

Teoretická část práce, nazvaná současný stav, se zabývala konceptem Internetu věcí. Popsáno bylo složení IoT sítí, jejich architektura a oblasti využití. Součástí tohoto konceptu jsou i chytré domácnosti, v rámci kterých lze vymezit několik typů komunikačních technologií. Nejvyužívanějšími komunikačními technologiemi v rámci chytrých domácností jsou komunikační technologie s krátkým dosahem. Takovou technologií může být například Wi-fi, Bluetooth, Zigbee, Z – Wave a další. Pro správu chytrých domácností bývá využíváno řešení od společností Google, Apple, Amazon a dalších. Uživatel si však může vytvořit i vlastní rozhraní pro správu chytré domácnosti, například pomocí programovatelného hardwaru, jako je Arduino nebo Raspberry Pi. Mezi koncová zařízení chytrých domácností patří vybavení pro regulaci teploty, vlhkosti, osvětlení, stínění, dále zařízení pro zábavu, provoz a zabezpečení. Teoretická část se zabývá i automatizací chytrých domácností, hospodařením se zdroji a jejich bezpečností.

Ve výzkumné části práce byly zvoleny metody pro zodpovězení pěti výzkumných otázek, které byly naformulovány na základě problémů, popisovaných v odborné literatuře o této problematice. Otázky byly rozděleny do tří oblastí podle typu rizik na: finanční, technická a bezpečnostní rizika. Pro finanční rizika byly formulovány dvě otázky: 1. Jak vysoké finanční investice jsou potřeba na vybavení modelové chytré domácnosti ve srovnání s domácností bez chytrých technologií? 2. Za jakou dobu, při maximálním využití chytrých technologií, které přinášejí energetické úspory, jsou investice návratné? Odpověď na první výzkumnou otázku byla stanovena na základě vytvoření modelového domu a vytvoření seznamu zařízení pro standardní a chytrou domácnost. Náklady na vybavení standardního domu jsou 40 690 Kč. Náklady na vybavení chytré domácnosti jsou 223 247 Kč. Rozsah a ceny vybavení obou domácností je možno zjistit v přílohách č. 1 a č. 2. Rozdíl nákladů činí 182 557 Kč.

Odpověď na druhou výzkumnou otázku byla formulována na základě metody finančního plánu spotřeby energií obou typů domácností. Celková částka ročních nákladů na spotřebu domácnosti bez chytrých vybavení činila 87 433 Kč. Celková částka ročních nákladů na spotřebu domácnosti s chytrými technologiemi byla nižší a činila 73 930 Kč. Rozdíl mezi ročními náklady na elektrickou spotřebu obou typů domácností je 13 503 Kč. Počet let návratnosti investice do chytrých vybavení se pohybuje okolo 13,5 let. Výsledek byl diskutován a relativizován v závislosti na vstupních proměnných.

Pro technická rizika byly také formulovány dvě výzkumné otázky (očíslovány jako 3. a 4. otázka): „Které činnosti v procesu zavádění chytrých technologií do domácností jsou kritické z hlediska plánování?“ a „U kterých prvků chytré domácnosti dochází nejvíce k častým poruchovým stavům?“ Odpověď na třetí výzkumnou otázku byla vytvořena pomocí výsledků síťové analýzy, která se skládá ze sestavení síťového grafu a metody PERT. Jako kritické body v procesu zavádění chytrých technologií do domácnosti lze označit činnosti ležící na kritické cestě procesu. Tyto body byly pracovně označeny písmeny a jejich posloupnost je následující: A, B, C, F, G, H, CH, J, K, L, M, O, P, Q, U, V, W, X. Přiřazení jednotlivých písmen k činnostem je uvedeno v příloze č. 7. Celková doba trvání procesu zavedení chytrých technologií do domácnosti je 828 hodin.

Odpověď na čtvrtou otázku o poruchovosti jednotlivých prvků zařízení chytré domácnosti byla formulována na základě rizikové analýzy pomocí metod FMEA a FTA. Pro celý systém a jeho jednotlivé prvky se podařilo identifikovat určitá rizika z hlediska častých poruchových stavů. Nejrizikovější jsou ta zařízení, u kterých byla zjištěna vysoká hodnota rizikového prioritního čísla. Z kvalitativního zpracování analýz vyplývá, že k nejčastějším poruchám dochází v rámci připojení jednotlivých prvků do systému, ale nebylo možno určit konkrétní přístroje, u kterých dochází nejčastěji k poruchovým stavům. Přesnou odpověď na tuto otázku nelze formulovat, protože nejsou přístupná spolehlivostní data jednotlivých zařízení pro kvantitativní zpracování metod.

Třetí oblastí rizik jsou rizika bezpečnostní. Zde byla formulována jedna výzkumná otázka (očíslována jako 5. otázka): „Představují chytré technologie bezpečnostní rizika pro uživatele z hlediska zabezpečení objektu a bezpečí uživatelů samotných, například vnějšími vlivy, vlivem úniku osobních dat nebo technické poruchy?“ Odpověď na otázku byla také zpracována v rámci rizikové analýzy s využitím metod FMEA a FTA. Chytré technologie představují bezpečnostní riziko z hlediska úniku osobních dat. Osobní data mohou být odcizena několika způsoby. Osobní data uživatelů mohou sbírat výrobci jednotlivých zařízení, například hlasový asistent a může tak dojít k jejich zneužití, další možností úniku dat je jejich odcizení neoprávněným přístupem do sítě. Rizika plynoucí z technických poruch mohou způsobit například požár nebo poranění uživatele. Z hlediska zabezpečení objektu, mohou tyto technologie přinášet zvýšení zabezpečení, avšak rizikem je možný neoprávněný přístup do sítě, výpadek sítě nebo elektrického proudu. Konkrétní výsledky analýzy jsou v příloze č. 10 a v kapitole 5.2.2 Analýza technických a bezpečnostních rizik.

Pomocí využitých metod analýz se podařilo najít odpovědi na všechny otázky. Odpověď na čtvrtou otázku však není kvantifikována a odpověď tak není zcela konkrétní, vzhledem k tomu, že výrobci nezveřejňují spolehlivostní data jednotlivých zařízení pro chytré domácnosti. Celkově lze říct, že rizika spojená se zapojováním a využíváním chytrých technologií byla v této diplomové práci analyzována a posouzena různými metodami a byly formulovány odpovědi na všechny výzkumné otázky.

SEZNAM POUŽITÝCH ZDROJŮ

- [1] *Průmysl 4.0, Vzdělávání 4.0, Práce 4.0 a Společnost 4.0: učební text*. Praha: SONDY, 2017. ISBN 978-80-86809-23-6. Dostupné z: <https://dnnt.mzk.cz/uuid/uuid:51feb690-0299-11e9-a5a4-005056827e52>
- [2] XU, Li Da, Eric L XU a Ling LI. Industry 4.0: state of the art and future trends. *International Journal of Production Research* [online]. Taylor & Francis, 2018, **56**(8), 2941 [cit. 2021-6-10]. ISSN 0020-7543. Dostupné z: [doi:10.1080/00207543.2018.1444806](https://doi.org/10.1080/00207543.2018.1444806)
- [3] ALI, Zainab H, Hesham A. ALI a M. MAHMOUD. Internet of Things (IoT): definitions, challenges and recent research directions. *International Journal of Computer Applications*. 2015, **128**(1), 37-47.
- [4] MACAULAY, Tyson. *RIoT Control: Understanding and Managing Risks and the Internet of Things*. Morgan Kaufmann, 2016. ISBN 978-0-12-419971-2.
- [5] Transforma Insights: Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by communications technology (in millions). *Statista* [online]. Statista, 2020 [cit. 2020-11-10]. Dostupné z: <https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology/>
- [6] BURHAN, Muhammad, Rana Asif REHMAN, Bilal KHAN a Byung-Seo KIM. *IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey* [online]. 2018 [cit. 2020-11-15]. Dostupné z: [doi:10.3390](https://doi.org/10.3390)
- [7] ANTAO, Liliana, a . Requirements for testing and validating the industrial internet of things. In: *IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)* [online]. Västerås, Sweden, 2018 [cit. 2020-11-15]. Dostupné z: [doi:10.1109](https://doi.org/10.1109)
- [8] DEMIRIS, George, van HOOFF a Eveline WOUTERS. *Handbook of smart homes, health care and well-being*. 2016. ISBN 9783319015828, 9783319015842. Dostupné z: [doi:10.1007/978-3-319-01583-5](https://doi.org/10.1007/978-3-319-01583-5)
- [9] SURESH, P, J. Vijay DANIEL, V PARTHASARATHY a R. H ASWATHY. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In: *2014 International Conference on Science Engineering and Management Research (ICSEMR)* [online]. IEEE, 2014, s. 1-8 [cit. 2020-11-20]. Dostupné z: [doi:10.1109/ICSEMR.2014.7043637](https://doi.org/10.1109/ICSEMR.2014.7043637)

- [10] HUA, Goh Bee. *Smart cities as a solution for reducing urban waste and pollution*. Hershey: Information Science Reference, An Imprint of IGI Global, 2016, xxi, 362 stran ; 27 cm. ISBN 978-1-5225-0302-6.
- [11] SAAD AL-SUMAITI, Ameena, Mohammed Hassan AHMED a Magdy M. A SALAMA. Smart Home Activities: A Literature Review. *Electric power components and systems* [online]. Taylor & Francis Group, 2014, **42**(3-4), 294-305 [cit. 2020-11-16]. ISSN 1532-5008. Dostupné z: doi:10.1080/15325008.2013.832439
- [12] Chytrý dům a byt. *Loxone* [online]. [cit. 2020-11-22]. Dostupné z: <https://www.loxone.com/cscz/chytry-dum/>
- [13] Number of Smart Homes forecast worldwide from 2017 to 2025 (in millions). *Statista* [online]. Statista, 2020 [cit. 2020-11-23]. Dostupné z: <https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-worldwide>
- [14] NATH, R.K., R. BAJPAI a H. THAPLIYAL. IoT based indoor location detection system for smart home environment. In: *2018 IEEE International Conference on Consumer Electronics, ICCE 2018* [online]. Institute of Electrical and Electronics Engineers, 2018, s. 1-3 [cit. 2020-11-25]. ISBN 9781538630259. Dostupné z: doi:10.1109/ICCE.2018.8326225
- [15] MA, Yongsun, Gang ZHOU a Shuangquan WANG. WiFi Sensing with Channel State Information: A Survey. *ACM computing surveys* [online]. ACM, 2019, **52**(3), 1-36 [cit. 2020-11-27]. ISSN 03600300. Dostupné z: doi:10.1145/3310194
- [16] KIRAVUO, Timo, Mikko SARELA a Jukka MANNER. A Survey of Ethernet LAN Security. *IEEE Communications Surveys & Tutorials* [online]. IEEE, 2013, **15**(3), 1477-1491 [cit. 2020-11-27]. Dostupné z: doi:10.1109/SURV.2012.121112.00190
- [17] LONZETTA, Angela, Peter COPE, Joseph CAMPBELL, Bassam MOHD a Thaier HAYAJNEH. Security Vulnerabilities in Bluetooth Technology as Used in IoT. *Journal of Sensor and Actuator Networks* [online]. Basel: MDPI, 2018, **7**(3) [cit. 2020-11-27]. Dostupné z: doi:10.3390/jsan7030028
- [18] KHANJI, S., F. IQBAL a P. HUNG. ZigBee Security Vulnerabilities: Exploration and Evaluating. In: *2019 10th International Conference on Information and Communication Systems, ICICS 2019* [online]. Institute of Electrical and Electronics Engineers, 2019, s. 52-57 [cit. 2020-11-27]. ISBN 9781728100456. Dostupné z: doi:10.1109/IACS.2019.8809115

- [19] BADENHOP, Christopher W, Scott R GRAHAM, Benjamin W RAMSEY, Barry E MULLINS a Logan O MAILLOUX. The Z-Wave routing protocol and its security implications. *Computers & security* [online]. Elsevier, 2017, **68**, 112-129 [cit. 2020-11-27]. ISSN 0167-4048. Dostupné z: doi:10.1016/j.cose.2017.04.004
- [20] RFID handbook; applications, technology, security, and privacy. *Scitech Book News* [online]. Portland: Ringgold, 2008, **32**(2) [cit. 2020-11-27]. ISSN 01966006. Dostupné z: <http://search.proquest.com/docview/200176119/>
- [21] AL-SARAWI, Shadi, Mohammed ANBAR, Kamal ALIEYAN a Mahmood ALZUBAIDI. Internet of Things (IoT) communication protocols: Review. In: *2017 8th International Conference on Information Technology (ICIT)* [online]. IEEE, 2017, s. 685-690 [cit. 2020-11-27]. Dostupné z: doi:10.1109/ICITECH.2017.8079928
- [22] ANDY, Syaiful, Budi RAHARDJO a Bagus HANINDHITO. Attack scenarios and security analysis of MQTT communication protocol in IoT system. In: *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)* [online]. IEEE, 2017, s. 1-6 [cit. 2020-11-27]. ISBN 9781538605486. ISSN 2407439X. Dostupné z: doi:10.1109/EECSI.2017.8239179
- [23] ZHILENKOV, Anton A, Dinis D GILYAZOV, Ilya I MATVEEV a Yanina V KRISHTAL. Power line communication in IoT-systems. In: *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)* [online]. IEEE, 2017, s. 242-245 [cit. 2020-12-10]. Dostupné z: doi:10.1109/EIConRus.2017.7910538
- [24] STERGIOU, Christos, Kostas E PSANNIS, Byung-gyu KIM a Brij GUPTA. Secure integration of IoT and Cloud Computing. *Future generation computer systems* [online]. Elsevier B.V, 2018, **78**, 964-975 [cit. 2021-12-10]. ISSN 0167-739X. Dostupné z: doi:10.1016/j.future.2016.11.031
- [25] POLIANYTSIA, A., O. STARKOVA a K. HERASYMENKO. Survey of hardware IoT platforms. *Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*. Kharkiv, 2016, 150-155. Dostupné z: doi:10.1109/INFOCOMMST.2016.7905364.
- [26] Arduino UNO Wi-fi Rev2. *Distrelec* [online]. [cit. 2020-12-10]. Dostupné z: <https://www.distrelec.cz/cs/arduino-uno-wifi-rev2-arduino-abx00021/p/30117100>

- [27] DINKAR R PATNAIK PATNAIKUNI. A Comparative Study of Arduino, Raspberry Pi and ESP8266 as IoT Development Board. *International Journal of Advanced Research in Computer Science* [online]. Udaipur: International Journal of Advanced Research in Computer Science, 2017, **8**(5), 2350-2352 [cit. 2021-6-10]. Dostupné z: doi:10.26483/ijarcs.v8i5.3959
- [28] Raspberry Pi 4 Model B. *Alza* [online]. [cit. 2021-1-10]. Dostupné z: <https://www.alza.cz//raspberrypi-4-model-b-4gb-ram>
- [29] Quarterly unit shipments of smart speaker with intelligent personal assistant worldwide from 2016 to 2019, by vendor (in millions): Strategy analytics. *Statista* [online]. Statista, 2020 [cit. 2021-1-10]. Dostupné z: <https://www.statista.com/statistics/792598/worldwide-smart-speaker-unit-shipment/>
- [30] PENG, Chen-yen a Rung-chin CHEN. Voice recognition by Google Home and Raspberry Pi for smart socket control. In: *2018 Tenth International Conference on Advanced Computational Intelligence (ICACI)* [online]. IEEE, 2018, s. 324-329 [cit. 2021-1-10]. Dostupné z: doi:10.1109/ICACI.2018.8377477
- [31] Chytrý reproduktor Google Home Mini. *Alza* [online]. [cit. 2020-12-10]. Dostupné z: <https://www.alza.cz//google-home-mini>
- [32] DOAN, Tam Thanh a et al. Towards a resilient smart home. *Proceedings of the 2018 Workshop on IoT Security and Privacy*. Hungary, 2018, , 15-21.
- [33] Chytrý reproduktor Apple Homepod Mini. *Alza* [online]. [cit. 2021-1-10]. Dostupné z: <https://www.alza.cz//apple-homepod-mini-bily>
- [34] JACKSON, Catherine a Angela OREBAUGH. A study of security and privacy issues associated with the Amazon Echo. *International Journal of Internet of Thing and Cyber-Assurance*. 2018, (1.1), 91-100. Dostupné z: doi:<https://doi.org/10.1504/IJITCA.2018.090172>
- [35] Amazon Echo Dot 3. generace. *Alza* [online]. [cit. 2021-1-10]. Dostupné z: <https://www.alza.cz/amazon-echo-dot-3-generace-charcoal>
- [36] XU, Ke, Xiaoliang WANG, Wei WEI, Houbing SONG a Bo MAO. Toward software defined smart home. *IEEE communications magazine* [online]. IEEE, 2016, **54**(5), 116-122 [cit. 2021-1-10]. ISSN 0163-6804. Dostupné z: doi:10.1109/MCOM.2016.7470945

- [37] CHEN, Weili, Mingjie MA, Yongjian YE, Zibin ZHENG a Yuren ZHOU. IoT Service Based on JointCloud Blockchain: The Case Study of Smart Traveling. In: *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)* [online]. IEEE, 2018, s. 216-221 [cit. 2021-1-10]. ISBN 9781538652060. Dostupné z: doi:10.1109/SOSE.2018.00036
- [38] ADNAN, Nursyazwani, Noorfazila KAMAL a Kalaivani CHELLAPPAN. An IoT Based Smart Lighting System Based on Human Activity. In: *2019 IEEE 14th Malaysia International Conference on Communication (MICC)* [online]. IEEE, 2019, s. 65-68 [cit. 2021-3-10]. Dostupné z: doi:10.1109/MICC48337.2019.9037601
- [39] WANG, Yuan a Partha DASGUPTA. Designing an adaptive lighting control system for smart buildings and homes. In: *2015 IEEE 12th International Conference on Networking, Sensing and Control* [online]. IEEE, 2015, s. 450-455 [cit. 2020-12-10]. Dostupné z: doi:10.1109/ICNSC.2015.7116079
- [40] ADIONO, Trio, Maulana Yusuf FATHANY, Syifaul FUADA, Irfan Gani PURWANDA a Sinantya Feranti ANINDYA. A portable node of humidity and temperature sensor for indoor environment monitoring. In: *2018 3rd International Conference on Intelligent Green Building and Smart Grid (IGBSG)* [online]. IEEE, 2018, s. 1-5 [cit. 2021-3-10]. Dostupné z: doi:10.1109/IGBSG.2018.8393575
- [41] NACER, A., B. MARHIC a L. DELAHOUCHE. Smart Home, Smart HEMS, Smart heating: An overview of the latest products and trends. In: *2017 6th International Conference on Systems and Control, ICSC 2017* [online]. Institute of Electrical and Electronics Engineers, 2017, s. 90-95 [cit. 2021-3-10]. ISBN 9781509039609. Dostupné z: doi:10.1109/ICoSC.2017.7958713
- [42] SALMAN, Ayman Dawood, Osamah Ibrahim KHALAF a Ghaida Muttasher ABDULSAHEB. An adaptive intelligent alarm system for wireless sensor network. *Indonesian Journal of Electrical Engineering and Computer Science*. 2019, **15**(1), 142-147. ISSN 2502-4760. Dostupné z: doi:10.11591/ijeecs.v15.i1.pp142-147
- [43] PANDYA, Sharnil, Hemant GHAYVAT, Ketan KOTECHA, Mohammed AWAIS, Saeed AKBARZADEH, Prosanta GOPE, Subhas MUKHOPADHYAY a Wei CHEN. Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol. *Applied System Innovation*. 2018, **1**(4). ISSN 2571-5577. Dostupné z: doi:10.3390/asi1040042

- [44] POTHITOU, Mary, Richard F HANNA a Konstantinos J CHALVATZIS. ICT entertainment appliances' impact on domestic electricity consumption. *Renewable & sustainable energy reviews* [online]. Elsevier, 2017, **69**(C), 843-853 [cit. 2021-3-12]. ISSN 1364-0321. Dostupné z: doi:10.1016/j.rser.2016.11.100
- [45] GUO, Xiao, Zhenjiang SHEN, Yajing ZHANG a Teng WU. Review on the Application of Artificial Intelligence in Smart Homes. *Smart Cities*. 2019, **2**(3), 402-420. ISSN 2624-6511. Dostupné z: doi:10.3390/smartcities2030025
- [46] MACHORRO-CANO, Isaac, Giner ALOR-HERNÁNDEZ, Mario Andrés PAREDES-VALVERDE, Lisbeth RODRÍGUEZ-MAZAHUA, José Luis SÁNCHEZ-CERVANTES a José Oscar OLMEDO-AGUIRRE. HEMS-IoT: A Big Data and Machine Learning-Based Smart Home System for Energy Saving. *Energies*. 2020, **13**(5). ISSN 1996-1073. Dostupné z: doi:10.3390/en13051097
- [47] AL-ALI, A.R., Imran A. ZUALKERNAN, Mohammed RASHID, Ragini GUPTA a Mazin ALIKARAR. A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics*. 2017, **63**(4), 426-434. ISSN 0098-3063. Dostupné z: doi:10.1109/TCE.2017.015014
- [48] KODRA, Suela, Danilo GLIGOROSKI, Marie MOE a Dominique UNRUH. *Smart Home Hacking*. NTNU, 2016.
- [49] KANG, Won Min, Seo Yeon MOON a Jong Hyuk PARK. An enhanced security framework for home appliances in smart home. *Human-centric Computing and Information Sciences*. 2017, **7**(1). ISSN 2192-1962. Dostupné z: doi:10.1186/s13673-017-0087-4
- [50] DOSKOČIL, Radek. *Kvantitativní metody: studijní text pro prezenční a kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2011, 160 s. : il., grafy, tab. ISBN 978-80-214-4247-4.
- [51] RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007, 152 s. : il. ISBN 978-80-214-3510-0.
- [52] ADAMEC, Vladimír, Danuše PROCHÁZKOVÁ a Barbora SCHÜLLEROVÁ. *Analýza rizik: Učební text* [online]. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2019 [cit. 2021-4-12]

- [53] VYMAZAL, Tomáš; MIKA, Otakar Jiří; MISÁK, Petr. *Analýza, posouzení a ošetření rizik technických systémů*. Brno: Vysoké učení technické v Brně, Fakulta stavební, 2015.
- [54] URBÁNEK, Michal. *Metoda FTA* [online prezentace]. Vysoké učení technické v Brně, 2020 [cit. 2021-04-15]. Dostupné z: <https://moodle.vutbr.cz/>
- [55] Porovnání nákladů na vytápění, teplou vodu a elektrickou energii: Výpočet a grafické porovnání včetně investičních a provozních nákladů. *TZB – info* [online]. [cit. 2021-4-20]. Dostupné z: <https://vytapani.tzb-info.cz/tabulky-a-vypocty/138-porovnani-nakladu-na-vytapani-teplou-vodu-a-elektrickou-energii-tzb-info>
- [56] *Honeywell* [online]. [cit. 2021-4-20]. Dostupné z: <https://www.honeywell.com/cz/en>
- [57] *Emos* [online]. [cit. 2021-4-21]. Dostupné z: https://www.emos.cz/?gclid=Cj0KCQjw8laGBhCHARIsAGIRRYpWgKGk0Aq-leiJxpFnimcy6m-a2DFzj64xhbjoF85Y95c-sb3a_QMaAIKEEALw_wcB
- [58] *Samsung* [online]. [cit. 2021-4-25]. Dostupné z: https://www.samsung.com/cz/?cid=cz_paid_ppc_google_brand_hot_lt-ecommerce_text_search_search_1SAM0008|01|txt|src|
- [59] *Broadling* [online]. [cit. 2021-4-25]. Dostupné z: <https://www.ibroadlink.com/>
- [60] *IGet* [online]. [cit. 2021-4-25]. Dostupné z: <http://www.iget.eu/>
- [61] *Hutermann* [online]. [cit. 2021-4-26]. Dostupné z: <https://www.hutermann.cz/>
- [62] *EVVA* [online]. [cit. 2021-4-30]. Dostupné z: <https://www.evva.com/cz-cz/?from=guardcz>
- [63] *Somfy* [online]. [cit. 2021-4-30]. Dostupné z: <https://www.somfy.cz/o-somfy/technologie-a-kompatibilita>
- [64] *TP-Link* [online]. [cit. 2021-4-30]. Dostupné z: <https://www.tp-link.com/cz/>
- [65] *Phillips* [online]. [cit. 2021-5-5]. Dostupné z: <https://www.philips.cz/>
- [66] *Selax: prodejce* [online]. [cit. 2021-5-5]. Dostupné z: <https://www.selax.cz/>

[67] Alza: *prodejce* [online]. [cit. 2021-5-5]. Dostupné z: <https://www.alza.cz/google-home-hub>

SEZNAM TABULEK

Tabulka č. 1 - Stanovené stupnice hodnocení intervalů výskytu, dopadu a odhalení vady [vlastní]	44
Tabulka č. 2 - Stanovené intervaly rizikového prioritního čísla [vlastní]	44
Tabulka č. 3 – Použité grafické symboly pro metodu FTA [54] (upraveno autorem)	45
Tabulka č. 4 – Srovnání celkových nákladů na vybavení v Kč [vlastní]	47
Tabulka č. 5 – Roční energetické náklady domácnosti bez chytrých technologií [55] (upraveno autorem)	49
Tabulka č. 6 – Roční energetické náklady domácnosti s chytrými technologiemi [55] (upraveno autorem)	49
Tabulka č. 7 – Srovnání nákladů na vybavení, energie a stanovení počtu let návratnosti [vlastní]	50

SEZNAM GRAFŮ

Graf č. 1 – Celosvětový počet připojených IoT zařízení podle komunikační technologie v letech 2019 až 2030 (předpoklad) [5] (upraveno autorem)	18
Graf č. 2 – Celosvětový počet chytrých domácností v letech 2017 až 2025 [13] (upraveno autorem).....	24
Graf č. 3 - Počty prodaných chytrých reproduktorů s hlasovým asistentem podle výrobce, celosvětově, čtvrtletně v letech 2016 až 2019 (v milionech kusů) [29] (upraveno autorem).....	30
Graf č. 4 – FTA 1 – Nefunkční regulace teploty v domě [vlastní].....	52
Graf č. 5 – FTA 2 – Nefunkční regulace osvětlení [vlastní]	53
Graf č. 6 – FTA 3 – Nefunkční síť zařízení – ovládání a komunikace [vlastní].....	54
Graf č. 7 – FTA 4 – Ztráta zabezpečení.....	55

SEZNAM OBRÁZKŮ

Obrázek č. 1 – Vrstvená architektura IoT sítí [6] (upraveno autorem)	20
Obrázek č. 2 – Pětivrstvá architektura IoT sítě s koncovými zařízeními a funkcemi vrstev [7] (upraveno autorem).....	21
Obrázek č. 3 - Topologie zapojení WSN [8] (upraveno autorem).....	22
Obrázek č. 4 – Příkladové schéma vybavení chytré domácnosti [12]	24
Obrázek č. 5 – Arduino UNO Wi-fi Rev2 [26]	28
Obrázek č. 6 – Raspberry Pi 4 Model B [28].....	29
Obrázek č. 7 – Chytrý reproduktor Google Home Mini [31].....	31
Obrázek č. 8 – Chytrý reproduktor Apple HomePod Mini [33]	32
Obrázek č. 9 – Chytrý reproduktor Amazon Echo Dot 3. generace [35].....	33

SEZNAM ZKRATEK

IoT – Internet of Things

IoS – Internet of Services

CPS – Cyber Physical Systems

WSN – Wireless Sensor Network

Wi-fi – Wireless fidelity

SH – Smart Home

QoL – Quality of Life

IEEE – Institute of Electrical and Electronics Engineers

MIMO – Multiple – Input, Multiple – output

OFMD – Orthogonal Frequency – Divison Multiplexing

TWT – Target Wake Time

BLE – Bluetooth Low Energy

RFID – Radio Frequency Identification

NFC – Near Field Communication

MQTT – Message Queuing Telemetry Transport

PLC – Power Line Communication

AI – Artificial Inteligence

DDoS – Denial of Service

PERT – Program Evaluation and Review Technique

FMEA – Failure Mode and Effect Analysis

FTA – Failure Tree Analysis

SEZNAM PŘÍLOH

Příloha č. 1 - Finanční plán vybavení modelové domácnosti bez chytrých technologií [vlastní].....	71
Příloha č. 2 – Finanční plán vybavení modelové domácnosti s chytrými technologiemi [vlastní].....	72
Příloha č. 3 – Vstupní hodnoty výpočtu energetické spotřeby modelové domácnosti bez chytrých technologií [55] (upraveno autorem)	73
Příloha č. 4 – Vstupní hodnoty výpočtu energetické spotřeby spotřebičů a dodaného vybavení modelové domácnosti bez chytrých technologií [55] (upraveno autorem)	74
Příloha č. 5 – Vstupní hodnoty výpočtu energetické spotřeby modelové domácnosti s chytrými technologiemi [55] (upraveno autorem)	75
Příloha č. 6 – Vstupní hodnoty výpočtu energetické spotřeby spotřebičů a dodaného vybavení modelové domácnosti s chytrými technologiemi [55] (upraveno autorem).....	76
Příloha č. 7 – Metoda PERT – výpis činností, jejich označení, trvání a statistické ukazatele [vlastní]	77
Příloha č. 8 – Metoda PERT – Posloupnost činností, určení začátků možných a přípustných, určení konců možných a přípustných, určení časové rezervy [vlastní]	79
Příloha č. 9 – Hranově definovaný síťový graf [vlastní]	81
Příloha č. 10 – Metoda FMEA [vlastní].....	82

Příloha č. 1 - Finanční plán vybavení modelové domácnosti bez chytrých technologií [vlastní]

Skupina prvků	Prvky domácnosti bez chytrých technologií	Počet ks	Cena za 1 ks [Kč]	Cena vybavení [Kč]
Vytápění, ohřev teplé vody a chlazení	Termostatická hlavice Honeywell Thera 3 [56]	8	182	1456
	Termostat EMOS P5614 (2 baterie 1,5 V AAA - 1 rok) [57]	1	1249	1249
	Klimatizace Samsung Luzon (3,5 kW) [58]	1	20 590	20590
Osvětlení	Emos LED žárovka Classic A60 806 lm (9 W) [57]	20	69,9	1398
	BROADLINK LED RGB žárovka 720 lm, 2700ch, dálkové ovládání (9 W) [59]	5	340	1700
	BROADLINK RGB LED PÁSEK 2 m, dálkové ovládání (21 W) [59]	3	300	900
Zabezpečení	-			0
	-			0
	iGET HOMEGUARD HGNVK88304 FHD, 1080 p, 6 W [60]	4	2250	9000
	iGET PIR bezdrátové pohybové čidlo – HG-PIR5 (2x1.5 V (AAA), cca 1 rok (podle četnosti pohybu před čidlem)) [60]	6	253	1518
	Siréna interní HG-S03 HUTERMANN (5 W) [61]	1	590	590
	OS-350 Venkovní siréna HUTERMANN (3 W) [61]	1	1290,00	1290
	Zabezpečovací jednotka (alarm)HUTERMANN HG-430-EN 5 W [61]		3 399	0
	GUARD G330 NVL 46/51 Ni vložka cylindrická [62]		949	0
Stínící technika	Venkovní žaluzie s motorem Somfy J406 WT Protect 95 W stanby <0,5 W [63]		3232	0
Elektroinstalace	-			
Síťové a řídicí jednotky	TP-Link Archer C6 (12 W) [64]	1	999	999
	-			
Celkem Kč, -				40690

Příloha č. 2 – Finanční plán vybavení modelové domácnosti s chytrými technologiemi [vlastní]

Skupina prvků	Prvky chytré domácnosti	Počet ks	Cena za 1 ks [Kč]	Cena vybavení [Kč]
Vytápění, ohřev teplé vody a chlazení	Termostatické hlavice Somfy (2x baterie AA LR03 – 2 roky) [63]	8	2190	17520
	Termostat: Somfy Termostat (2x baterie AA LR03 – 2 roky) [63]	1	4 190	4190
	Klimatizace Samsung CEBU smart wifi (3,5 kW) [58]	2	22290	44580
Osvětlení	Žárovky: Philips Hue White 806 lm (9 W)	20	400,5	8010
	Philips Hue White and Color ambiance 806 lm 6300ch (9 W) [65]	5	1374,5	6872,5
	Led pásy: Philips Hue LightStrip Plus 25 W 2metry (25 W) [65]	3	2199	6597
Zabezpečení	Kamery: TD-9583E2AZF – Face Detection IR Dome (4,5-6,5 W, dle režimu) [66]	1	7383,42	7383,42
	Vnitřní: Somfy One+ (5 W) [63]	1	8990	8990
	Venkovní kamera: Somfy IP, 1080 p (10 W) [63]	4	6289	25156
	Pohybové senzory: Somfy vnitřní pohybové čidlo, (1× CR123A (životnost 2 roky)) [63]	6	1 799	10794
	Čidla dveří a oken: Somfy čidlo IntelliTAG (3x 1× AAA (životnost 1 rok)) [63]	3	1 290	3870
	Venkovní siréna: Somfy (4x baterie LR20 - 2 roky) [63]	1	3865	3865
	Zabezpečovací jednotka(alarm): Somfy Home Alarm (3x 1× AAA (životnost 1 rok)), (5 W) [63]	1	8 713	8713
	Zámek dveří: Somfy Connected Doorlock (4x baterie AAA LR03 2 roky), (5W připojení jednotky) [63]		9269	0
Stínící technika	Venkovní žaluzie s motorem Somfy J4 io Protect ((95 W) stáby <0,5 W) [63]	6	5853	35118
Elektroinstalace	Zásuvky: Somfy ON-OFF Plug io [63]	10	1790	17900
Síťové a řídicí jednotky	TP-Link Archer AX73 (15 W)	1	3499	3499
	Somfy Tahoma (2,5 W) [63]	1	7990	7990
	Google Home Nest Hub (5 W) [67]	1	2199,00	2199
Celkem Kč, -				223247

Příloha č. 3 – Vstupní hodnoty výpočtu energetické spotřeby modelové domácnosti bez chytrých technologií [55] (upraveno autorem)

Lokální klimatická data		
Klimatická oblast	Brno	
Venkovní výpočtová teplota t_e	-12	°C
Délka otopného období d	232	dnů
Vlastnosti budovy		
Celková tepelná ztráta	7,5	kW
Podlahová plocha A	180	m ²
Objem budovy V	486	m ³
Intenzita výměny vzduchu n	0,4	h ⁻¹
Ohřev TV		
Počet osob n (rodina s dětmi)	4	osoby
Množství ohřivané vody	50 l/osoba/den	
Počet dnů přípravy teplé vody N	365	dnů
TV je ohřívána energií na vytápění		
Spotřebiče a zařízení		
Distribuční území	EG.D (E.ON)	
Tarif	D02d	
Jistič nad 3x16 A do 3x20 A včetně		
VT (vyšší tarif)	4,86223	Kč/kWh
Vytápění a ohřev TV		
Teplovodní elektrokotel		
Účinnost přeměny energie	95 %	
Tarif	D57d	
Jistič nad 3x20 A do 3x25 A včetně		
VT (vyšší tarif)	3,04826	Kč/kWh
NT (nižší tarif)	2,78875	Kč/kWh
Spotřeba paliva na rok	17817	kWh/rok
Potřeba tepla na vytápění a ohřev TV	16926	kWh/rok

Příloha č. 4 – Vstupní hodnoty výpočtu energetické spotřeby spotřebičů a dodaného vybavení modelové domácnosti bez chytrých technologií [55] (upraveno autorem)

Zařízení	Příkon [W]	Doba provozu [h/den]	Roční spotřeba [kWh]	Tepelný zisk [kWh]
Elektrický sporák	2000	1	730	371
Elektrická trouba	2000	0,5	365	186
Rychlovarná konvice	2000	0,12	88	45
Mikrovlnná trouba	600	0,3	66	33
Kombinovaná chladnička	120	6	263	134
Myčka nádobí	650	1,5	356	181
Pračka	600	1,5	329	167
Sušička prádla	750	2	548	278
Televize	70	6	153	78
Osobní počítač	80	6	175	89
Internet (modem, router)	12	24	105	53
Klimatizace	3500	3	3833	-
Celkem	12382	52	7010	1615
Dodané základní vybavení				
Osvětlení 1 (LED žárovky) x 25	9	8	657	-
Osvětlení 2 (LED pásky) x 3	21	4	92	-
Kamery venkovní x4	6	24	210	-
Zabezpečovací jednotka	5	24	44	-
Venkovní žaluzie – motor	95	0,3	62	-
Celkem	136	60	1065	
Baterie	[Kč/rok]			
Termostat	12			
Pohybová Čidla	72			
Celkem	84			

Příloha č. 5 – Vstupní hodnoty výpočtu energetické spotřeby modelové domácnosti s chytrými technologiemi [55] (upraveno autorem)

Lokální klimatická data		
Klimatická oblast	Brno	
Venkovní výpočtová teplota t_e	-12	°C
Délka otopného období d	185,6	dnů
Vlastnosti budovy		
Celková tepelná ztráta	7,5	kW
Podlahová plocha A	180	m ²
Objem budovy V	486	m ³
Intenzita výměny vzduchu n	0,4	h ⁻¹
Ohřev TV		
Počet osob n (rodina s dětmi)	4	osoby
Množství ohřivané vody	50 l/osoba/den	
Počet dnů přípravy teplé vody N	292	dnů
TV je ohřívána energií na vytápění		
Spotřebiče a zařízení		
Distribuční území	EG.D (E.ON)	
Tarif	D02d	
Jistič nad 3x16 A do 3x20 A včetně		
VT (vyšší tarif)	4,86223	Kč/kWh
Vytápění a ohřev TV		
Teplovodní elektrokotel		
Účinnost přeměny energie	95 %	
Tarif	D57d	
Jistič nad 3x20 A do 3x25 A včetně		
VT (vyšší tarif)	3,04826	Kč/kWh
NT (nižší tarif)	2,78875	Kč/kWh
Spotřeba paliva na rok	14936	kWh/rok
Potřeba tepla na vytápění a ohřev TV	14189	kWh/rok

Příloha č. 6 – Vstupní hodnoty výpočtu energetické spotřeby spotřebičů a dodaného vybavení modelové domácnosti s chytrými technologiemi [55] (upraveno autorem)

Zařízení	Příkon [W]	Doba provozu [h/den]	Roční spotřeba [kWh]	Tepelný zisk [kWh]
Elektrický sporák	2000	1	730	297
Elektrická trouba	2000	0,5	365	148
Rychlovarná konvice	2000	0,12	88	36
Mikrovlnná trouba	600	0,3	66	27
Kombinovaná chladnička	120	6	263	107
Myčka nádobí	650	1,5	356	145
Pračka	600	1,4	307	125
Sušička prádla	750	1,9	520	212
Televize	70	5	128	52
Osobní počítač	80	5	146	59
Internet (modem, router)	15	20	110	45
Klimatizace	3500	1,5	1916	-
Celkem	12385	44	4993	1253
Dodané chytré vybavení				
Osvětlení 1 (LED žárovky) x 25	9	5	411	-
Osvětlení 2 (LED pásy) x 3	25	3	82	-
Kamery venkovní x4	10	24	350	-
Kamera Face Recognition	5,5	0,5	1	-
Kamera vnitřní	5	0,5	1	-
Zámek dveří	5	0,5	1	-
Zabezpečovací jednotka	5	24	44	-
Venkovní žaluzie – motor	95	0,5	104	-
Řídící jednotka	2,5	24	22	-
Google Home Hub	5	2	4	-
Celkem	167	84	1019	
Baterie	[Kč/rok]			
Termostat	6			
Termostatické hlavice	48			
Zabezpečovací čidla	36			
Siréna venkovní	100			
Pohybová čidla	168			
El. Zámek	12			
Celkem	358			

Příloha č. 7 – Metoda PERT – výpis činností, jejich označení, trvání a statistické ukazatele [vlastní]

Označení činností	Činnosti	Trvání (hodiny)				Trvání (zaok.)	Statistické ukazatele	
		a	m	b	t(ij)	t(ij)	σ^2	σ
A	Výběr vybavení – kompatibilita, funkčnost, cena	95	168	300	177,833	178	1167,36	34,17
B	Elektroinstalace kabelového vedení pro osvětlení a kamerový systém	12	18	34	19,667	20	13,44	3,67
C	Osvětlení – montáž jednotlivých svítidel, nastavení	42	68	86	66,667	67	53,78	7,33
D	Kamerový systém – montáž kamer, nastavení	15	24	32	23,833	24	8,03	2,83
E	Nastavení připojení kamer – konfigurace sítě, uživatelská nastavení	3	5	10	5,500	6	1,36	1,17
F	Zámky dveří a motory brán – montáž, nastavení	16	24	32	24,000	24	7,11	2,67
G	Pohybové a závěrové senzory – montáž senzorů, nastavení	12	28	36	26,667	27	16,00	4,00
H	Zabezpečovací centrální jednotka – konfigurace sítě	4	10	20	10,667	11	7,11	2,67
CH	Klimatizace – montáž/úprava, nastavení	2	10	15	9,500	10	4,69	2,17
I	Vytápění – výměna termostatických hlavíc, nastavení komunikace s kotlem	3	5	12	5,833	6	2,25	1,50
J	Termostat – montáž a konfigurace sítě pro kontrolu teploty	4	8	16	8,667	9	4,00	2,00
K	Elektroinstalace kabelového vedení pro žaluzie a požadované spotřebiče	6	12	20	12,333	12	5,44	2,33
L	Stavební úpravy – příprava pro montáž žaluzií a spotřebičů	16	24	30	23,667	24	5,44	2,33
M	Žaluzie a rolety – montáž, nastavení	12	24	72	30,000	30	100,00	10,00
N	Spotřebiče a zábava – montáž, nastavení	4	7	15	7,833	8	3,36	1,83
O	Zapojení a nastavení routeru – vytvoření internetové sítě	3	7	12	7,167	7	2,25	1,50
P	Zapojení a nastavení centrální řídicí jednotky – síť komunikačních protokolů	2	4	8	4,333	4	1,00	1,00
Q	Nastavení a připojení jednotlivých zařízení	6	10	24	11,667	12	9,00	3,00
R	Testování funkčnosti a propojení jednotlivých zařízení	1	3	10	3,833	4	2,25	1,50

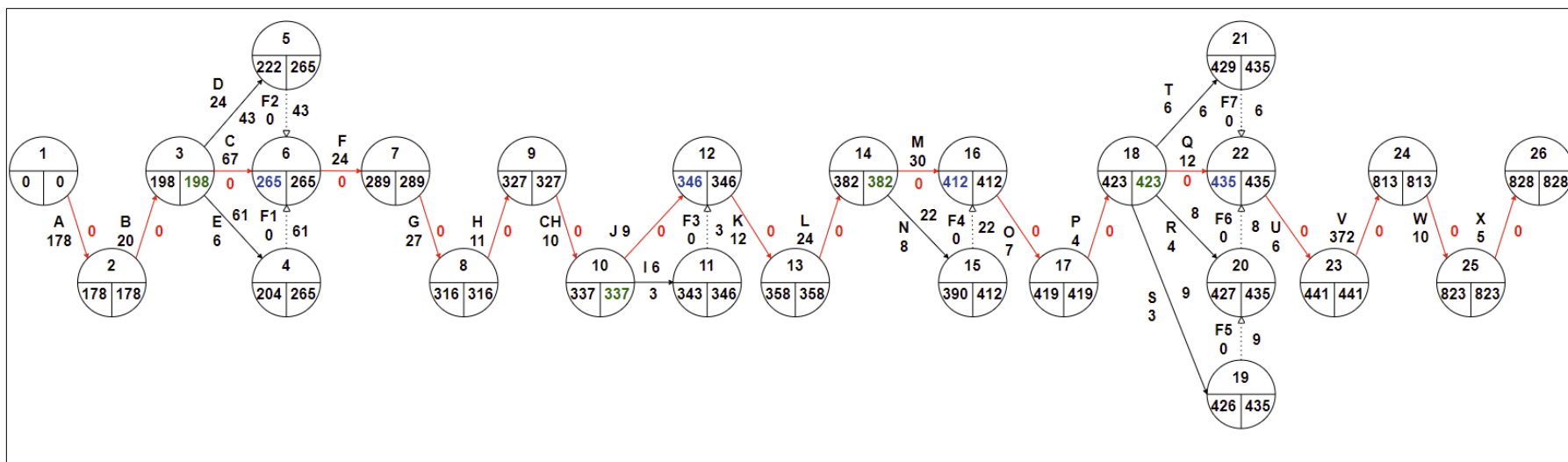
Označení činností	Činnosti	Trvání (hodiny)				Trvání (zaok.)	Statistické ukazatele	
		a	m	b	t(ij)	t(ij)	σ^2	σ
S	Instalace aplikace do chytrých zařízení, konfigurace sítě	1	3	5	3,000	3	0,44	0,67
T	Vytvoření uživatelských profilů	3	5	12	5,833	6	2,25	1,50
U	Manuální vytvoření scénářů pro nastavení domácnosti	2	6	12	6,333	6	2,78	1,67
V	Sběr dat o uživatelích a využití jednotlivých zařízení	168	336	720	372,000	372	8464,00	92,00
W	Vyhodnocení dat ze senzorů – využití místností a zařízení	4	10	16	10,000	10	4,00	2,00
X	Vytvoření scénářů pro automatické nastavování domácnosti	2	5	10	5,333	5	1,78	1,33

Příloha č. 8 – Metoda PERT – Posloupnost činností, určení začátků možných a přípustných, určení konců možných a přípustných, určení časové rezervy [vlastní]

Předchůdci - i	Následovníci - j	Ozn. činnosti	Uzly i_j	Termíny zahájení a ukončení činností				Rezerva RC
				ZM	KM	ZP	KP	
-	B	A	1_2	0	178	0	178	0
A	C, D, E	B	2_3	178	198	178	198	0
B	F	C	3_6	198	265	198	265	0
B	F	D	3_5	198	222	241	265	43
		F2	5_6	222	222	265	265	43
B	F	E	3_4	198	204	259	265	61
		F1	4_6	204	204	265	265	61
C, D, E	G	F	6_7	265	289	265	289	0
F	H	G	7_8	289	316	289	316	0
G	CH	H	8_9	316	327	316	327	0
H	I, J	CH	9_10	327	337	327	337	0
CH	K	I	10_11	337	343	340	346	3
		F3	11_12	343	343	346	346	3
CH	K	J	10_12	337	346	337	346	0
I, J	L	K	12_13	346	358	346	358	0
K	M, N	L	13_14	358	382	358	382	0
L	O	M	14_16	382	412	382	412	0
L	O	N	14_15	382	390	404	412	22
		F4	15_16	390	390	412	412	22
M, N	P	O	16_17	412	419	412	419	0
O	Q, R, S, T	P	17_18	419	423	419	423	0
P	U	Q	18_22	423	435	423	435	0
P	U	R	18_20	423	427	431	435	8
		F6	20_22	427	427	435	435	8
P	U	S	18_19	423	426	432	435	9
		F5	19_20	426	426	435	435	9
P	U	T	18_21	423	429	429	435	6
		F7	21_22	429	429	435	435	6

Předchůdci - i	Následovníci - j	Ozn. činnosti	Uzly i_j	Termíny zahájení a ukončení činností				Rezerva RC
				ZM	KM	ZP	KP	
Q, R, S, T	V	U	22_23	435	441	435	441	0
U	W	V	23_24	441	813	441	813	0
V	X	W	24_25	813	823	813	823	0
W	-	X	25_26	823	828	823	828	0

Příloha č. 9 – Hranově definovaný síťový graf [vlastní]



Příloha č. 10 – Metoda FMEA [vlastní]

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
Vytápění a chlazení	Termostatické hlavice	Odpojení od řídicí jednotky	Chyba připojení, výpadek sítě	Omezení ovládání topení	6	6	3	108	Kontrola připojení, záložní síť	4	6	3	72
			Chyba v komunikačním protokolu	Omezení ovládání topení	2	6	5	60	-	2	6	5	60
		Porucha materiálu	Stáří materiálu	Ztráta funkčnosti	5	7	2	70	-	5	7	2	70
			Mechanické poškození	Ztráta funkčnosti	3	7	3	63	-	3	7	3	63
		Nefunkční ovládání	Vybitá baterie	Znemožnění dálkového ovládání	5	5	3	75	-	5	5	3	75
		Zatuhnutí ventilu	Usazeniny, nepoužití ventilu	Znemožnění regulace teploty	4	5	5	100	Pravidelná údržba otopné soustavy	4	5	3	60
	Klimatizace	Odpojení od řídicí jednotky	Chyba připojení k řídicí jednotce	Znemožnění dálkového ovládání	5	5	3	75	-	5	5	3	75

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
Termostaty		Chybné nastavení teploty	Chyba výrobce	Znemožnění regulace teploty	2	4	3	24	-	2	4	3	24
		Odpojení od řídicí jednotky	Chyba připojení, výpadek sítě	Znemožnění regulace teploty a ohřevu TV	6	6	3	108	Kontrola připojení, záložní síť	4	6	3	72
		Chyba komunikace s kotlem	Chyba připojení, výpadek sítě	Znemožnění regulace teploty a ohřevu TV	6	6	3	108	Kontrola připojení, záložní síť	4	6	3	72
		Chyba komunikace s čidly pokojů	Chyba připojení, výpadek sítě	Znemožnění regulace teploty	6	5	3	90	-	6	5	3	90
			Chyba čidel pokojů	Znemožnění regulace teploty	5	5	3	75	-	5	5	3	75
Osvětlení	Žárovky	Porucha svícení	Životnost žárovky	Ztráta funkčnosti osvětlení	5	4	5	100	Kontrola žárovek, výměna	4	4	4	64
			Chybné zapojení kabeláže	Ztráta funkčnosti osvětlení	4	4	6	96	-	4	4	6	96

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních				
					P	D	O	RPN		P	D	O	RPN	
			Chyba výrobce	Ztráta funkčnosti osvětlení	3	4	2	24	-	3	4	2	24	
		Závada na měniči chromatičnosti	Chybné nastavení uživatelem	Omezení funkčnosti	7	2	3	42	-	7	2	3	42	
			Chyba výrobce	Omezení funkčnosti	3	2	7	42	-	3	2	7	42	
		Chyba komunikace s řídicí jednotkou	Chyba sítě	Ztráta dálkového ovládání světel	4	3	3	36	-	4	3	3	36	
	LED pásy	Přehřívání	Nevhodný zdroj (transformátor)	Poškození svítidla, požár	2	9	5	90	-	2	9	5	90	
		Blikání	Chybné napětí, porušení vedení	Ztráta funkčnosti	4	3	2	24	-	4	3	2	24	
		Chyba komunikace s řídicí jednotkou	Chyba sítě	Ztráta dálkového ovládání pásků	3	2	3	18	-	3	2	3	18	
	Stínění	Žaluzie	Chyba naklápění	Chybné přednastavení naklopení	Omezení ovládání	5	4	3	60	-	5	4	3	60

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
		Nemožné vytažení/zatažení žaluzií	Závada motoru	Znemožnění ovládání	2	7	4	56	-	2	7	4	56
			Chyba montáže	Ztráta funkčnosti, poškození výrobku	3	8	4	96	-	3	8	4	96
			Chyba připojení k řídicí jednotce	Znemožnění ovládání	3	7	4	84	-	3	7	4	84
Elektroinstalace	Zásuvky	Chyba v přenosu energie	Chybné zapojení uživatelem	Ztráta funkčnosti	5	6	2	60	-	5	6	2	60
			Chyba výrobce	Ztráta funkčnosti	3	6	2	36	-	3	6	2	36
		Chyba komunikace s řídicí jednotkou	Mechanická závada zásuvky	Znemožnění dálkového ovládání	4	5	4	80	-	4	5	4	80
			Chyba v komunikačním protokolu	Znemožnění dálkového ovládání	2	5	4	40	-	2	5	4	40
Zabezpečení	Pohybové senzory	Chyba pohybového senzoru	Porucha pohybového senzoru	Ztráta funkčnosti pohybové	1	6	5	30	-	1	6	5	30

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
				ho senzoru									
			Vybitá baterie	Ztráta funkčnosti pohybového senzoru	5	6	3	90	-	5	6	3	90
		Chybná detekce pohybu	Chyba uživatele	Omezení zabezpečení	5	7	3	105	Kontrola čidel a prostoru	3	7	2	42
			Chyba senzoru	Omezení zabezpečení	3	7	4	84	-	3	7	4	84
	Kamery	Chyba uploadu	Výpadek proudu, připojení	Ztráta záznamu kamer	4	6	5	120	Vlastní server, síť	2	6	5	60
			Chyba serveru s cloudem	Ztráta záznamu kamer	5	6	5	150	Vlastní server, síť	2	6	5	60
		Chybná rotace kamer	Vadný kloub, chybná kalibrace	Ztráta funkčnosti, omezené ovládání	3	6	5	90	-	3	5	2	30
		Nekvalitní kamerový záznam	Nečistoty na čočce kamery	Nemožné využití záznamu	4	6	4	96	-	4	4	2	32
		Chybné rozpoznání obličeje	Chyba uživatele	Nemožné odemčení obličejem	6	3	3	54	-	6	3	3	54

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních				
					P	D	O	RPN		P	D	O	RPN	
	Elektronické zámky a čidla	Chybné rozpoznání obličejů	Chyba čočky	Nemožné odemčení obličejem	5	3	4	60	-	5	3	4	60	
		Nefunkční zámek	Mechanická porucha zámku (vločky)	Nemožné odemčení zámku	3	5	3	45	-	3	5	3	45	
			Chyba připojení	Nemožné odemčení zámku	5	5	4	100	Kontrola připojení, manuální klíč	4	4	4	64	
		Nefunkční čidlo	Vybitá baterie	Omezené zabezpečení	5	6	2	60	-	5	6	2	60	
			Špatné nastavení	Omezené zabezpečení	4	6	5	120	Kontrola funkčnosti, nastavení	2	6	3	36	
		Zabezpečovací jednotka	Chyba uzamčení/odemčení prostoru	Chyba uživatele	Falešný poplach	6	3	5	90	-	6	3	5	90
				Chyba čidel	Falešný poplach	3	3	8	72	-	3	3	8	72
			Chyba komunikace s řídicí jednotkou	Chyba připojení, výpadek sítě	Ztráta funkčnosti	4	7	5	140	Vlastní server, síť	2	7	3	42
				Chyba řídicí jednotky	Ztráta funkčnosti	3	7	5	105	Kontrola funkčnosti ř. j.	3	7	3	63

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
Připojení	Wifi router	Nefunkční připojení	Chyba poskytovatele připojení	Nefunkční internetová síť	5	6	3	90	-	5	6	3	90
			Chyba uživatele	Nefunkční internetová síť	4	6	2	48	-	4	6	2	48
		Výpadek připojení	Rušení radiofrekvenčních vln jinou sítí (2.4 GHz)	Omezení funkčnosti sítě	6	5	5	150	Využití protokolů o nižší fq	3	5	4	60
	Řídicí jednotka	Chyba ovládání řídicí jednotky	Výpadek internetové sítě	Ztráta funkčnosti, omezené ovládání	3	6	3	54	-	3	6	3	54
		Chyba komunikace se zařízeními	Chyba připojení, rušení sítě	Ztráta funkčnosti, omezené ovládání	6	6	5	180	Vlastní server, nastavení sítě	3	6	5	90
			Chyba jednotlivých zařízení	Ztráta ovládání a dat daného zařízení	6	7	5	210	Kontrola funkčnosti zařízení	6	7	2	84
		Nefunkční řídicí jednotka	Chyba software (zamrznutí, update)	Ztráta kontroly nad zařízeními	5	6	4	120	Vlastní server, síť	3	6	4	72

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
	Ovládání		Mechanické poškození	Ztráta funkčnosti	3	7	2	42	-	3	7	2	42
		Nefunkční aplikace	Chyba software	Ztráta funkčnosti	5	6	3	90	-	5	6	3	90
		Nefunkční ovládací jednotka	Chyba Homekit zařízení	Ztráta funkčnosti	3	6	3	54	-	3	6	3	54
		Nefunkční hlasový asistent	Chyba připojení	Omezení ovládání	5	4	3	60	-	5	4	3	60
Bezpečí uživatelů	Zavedené technologie	Neoprávněný přístup k zařízením	Nedostatečné zabezpečení sítě	Ztráta zabezpečení	6	10	5	300	Vlastní server, síť, zabezpečení	3	10	3	90
		Přístup třetích stran k sbíraným datům	Nezabezpečená data na cloudovém úložišti	Únik osobních dat	5	8	5	200	Vlastní server, síť, zabezpečení	3	8	3	72
			Sběr dat výrobcem	Únik osobních dat	5	8	7	280	Nastavení preferencí sběru dat	5	8	2	80
		Zneužití kamer	Umístění vnitřních kamer	Psychická újma uživatelů	4	8	4	128	Klapka čoček vnitřních kamer	3	8	4	96
	Vnější vlivy	Mechanické poškození zařízení	Neoprávněný přístup do objektu	Újma na zdraví,	5	10	4	200	Využití zabezpečo	3	10	3	90

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
				finanční újma					vacích prvků				
			Vlivy počasí (meteorologické jevy)	Újma na zdraví, finanční újma	3	10	3	90	-	3	10	3	90
	Sít	Prolomení komunikačních protokolů	Chyba sítě	Únik osobních dat	4	8	7	224	Vlastní server, síť	2	8	6	96
Bezpečnost budovy	Elektronický zámek	Neúspěšné uzamčení	Chyba software zámků	Omezení zabezpečení	3	7	5	105	Kontrola uzamčení	3	7	3	63
			Nepovolený přístup	Omezení zabezpečení	4	7	6	168	Využití zabezpečovacích prvků	4	7	3	84
	Zabezpečení prostoru	Neúspěšné zakódování/odkódování místností	Chyba uživatele	Ztráta zabezpečení	6	9	3	162	Kontrola zabezpečení	4	9	2	72
			Chyba senzorů pohybu	Ztráta zabezpečení	4	9	5	180	Kontrola senzorů, zón	4	9	2	72
			Chyba připojení k síti	Omezení zabezpečení	5	7	5	175	Kontrola připojení a zakódování	5	7	2	70
			Nefunkční sirény	Chyba připojení k síti	Omezení zabezpečení	4	7	5	140	Testování funkčnosti, kontrola	4	7	3

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
			Vybitá baterie	Omezení zabezpečení	3	7	5	105	Testování funkčnosti, kontrola	3	7	3	63
	Kamerový systém	Zneužití kamer	Neoprávněný přístup	Krádež majetku	6	9	5	270	Vlastní server, síť, zabezpečení	2	9	5	90
		Neoprávněné vypnutí kamer	Neoprávněný přístup	Ztráta záznamu kamer	6	8	5	240	Vlastní server, síť, zabezpečení	2	8	5	80
	Firmware zařízení	Přístup do sítě bez autentikace/slabá hesla	Chyba uživatele	Ztráta zabezpečení sítě	5	8	6	240	Vytvoření silných hesel	2	8	6	96
			Chyba výrobce	Ztráta zabezpečení sítě	3	8	6	144	Vytvoření silných hesel	2	8	6	96
		Prolomení přednastavených hesel	Chyba uživatele	Ztráta zabezpečení sítě	6	8	5	240	Změna přednastavených hesel	2	8	5	80
		Hidden Backdoors ("skrytá vrátka")	Chyba výrobce	Omezení zabezpečení sítě	5	7	7	245	Výběr bezpečných zařízení, zjištění možností přístupu	3	7	4	84

Prvek, funkce, systém, znak	Rozčlenění prvků	Potenciální chyba	Předpokládaná příčina chyby	Předpokládané důsledky chyby	Stávající stav				Opatření	Stav po opatřeních			
					P	D	O	RPN		P	D	O	RPN
		DDoS útok	Vnější útok na zabezpečení systému	Ztráta zabezpečení sítě	5	8	7	280	Vlastní server, síť, zabezpečení	2	8	6	96
		Odhalení šifrovacích klíčů	Vnější útok na zabezpečení systému	Ztráta zabezpečení sítě	4	8	7	224	Vlastní server, síť, zabezpečení	2	8	5	80
		Buffer overflow (překročení hranic vyrovnávací paměti)	Vnější útok na zabezpečení systému	Umožnění neoprávněného přístupu	5	8	6	240	Development softwaru, hranice vyrovnávací paměti	3	8	3	72
		Zneužití zdrojového kódu	Využití komunikace zařízení s cloudem	Umožnění neoprávněného přístupu	5	8	7	280	Vlastní server, síť, zabezpečení	2	8	6	96
		Přístupné debugging nástroje pro zařízení	Chyba výrobce	Umožnění neoprávněného přístupu	5	8	5	200	Výběr bezpečných zařízení, zjištění možností přístupu	3	8	4	96

Vysvětlivky k hlavičce tabulky: P – Pravděpodobnost výskytu vady, D – Dopad vady, O – Pravděpodobnost odhalení vady, RPN – Rizikové prioritní číslo