Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Moderní domácnost

Bakalářská práce

Autor: Jan Pokorný
Studijní obor: Aplikovaná informatika

Vedoucí práce: prof. RNDr. Peter Mikulecký, PhD.

Hradec Králové Duben 2020

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 30.4.2020 Jan Pokorný

Poděkování:

Děkuji vedoucímu bakalářské práce prof. RNDr. Peteru Mikuleckému, PhD. za metodické vedení práce, užitečné rady a ochotu při vytváření této práce. Také děkuji své rodině a přátelům za podporu při studiu.

Anotace

Cílem této bakalářské práce je popsání moderní, přesněji chytré domácnosti neboli smart home. Teoretická část se zaobírá funkcionalitou zařízení, způsobem komunikace, technologiemi a mírou rizik chytré domácnosti. V praktické části je provedena analýza dotazníkového šetření a dále se pak práce zaměřuje na systémy Apple HomeKit a Loxone, které patří k velice oblíbeným systémům pro chytrou domácnost. Práce zkoumá možnosti využití daných systémů, jejich pozitivními, ale i negativními faktory a jejich vzájemným porovnání. Součástí praktické části bude také návrh domácnosti s použitím zkoumaných systémů za stejných podmínek. Důraz bude kladen zejména na pořizovací náklady, způsob obsluhy a náročnost rozšíření domácnosti o další chytrá zařízení.

Klíčová slova: domácnost, chytrý, internet, internet věcí, standard, systém, zařízení

Annotation

Title: Modern Household

The aim of this thesis is to describe a modern, more precisely smart, household or smart home. The theoretical part deals with the functionality of the device, the way of communication, technologies and risk level of a smart home. In the practical part, the analysis of the questionnaire survey is performed and then the work focuses on Apple HomeKit and Loxone systems, which are very popular systems for smart homes. It also examines the possibilities of using the given systems, their positive but also negative factors and possible comparison. The practical part will also include a design of households applying the given systems under the same conditions. Emphasis will be placed especially on the purchase costs, the way of operation and the difficulty of extending the home with other smart devices.

Keywords: device, home, internet, Internet of things, smart, standard, system

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Chytrá domácnost je aktuálním trendem při zařizování bytu, či domu, který usnadňuje a zpříjemňuje každodenní konfrontaci se zařízeními v domácnosti. Pojem chytrá domácnost zahrnuje jakousi podmnožinu k takzvanému internetu věcí. Právě zařízení internetu věcí umožnují předávání informací a ovládání zařízení bezdrátově pomocí internetu a tvoří tak nedílnou součást chytré domácnosti. Chytrou domácností budeme v této práci rozumět domácnost vybavenou pomocí vzájemně propojenými zařízeními internetu věcí, které nabízejí bezpečnost, komfort a úsporu energie domácnosti a je možné je ovládat pomocí jednotné aplikace v chytrém zařízení. Práce pojednává o struktuře a možnostech chytré domácnosti. Popisuje, jaké jsou způsoby implementace chytré domácnosti a vzájemná komunikace a kompatibilita zařízení této domácnosti.

Práce je rozdělena do dvou částí. Teoretická část se věnuje původu a technologiím použitých u zařízení internetu věcí, či v chytrých domácnostech. Rozebírá jejich výhody a nedostatky a možnou vzájemnou kompatibilitu těchto technologií. Praktická část je zaměřená na výsledky dotazníkového šetření, návrh moderního domu, implementaci a na porovnání dvou systémů chytré domácnosti. Konkrétně se jedná o systém Loxone od stejnojmenné společnosti a systém HomeKit od společnosti Apple.

2 Cíl práce

Cílem bakalářské práce je objasnit, co je to chytrá domácnost a jak chytré domácnosti, které pro svůj chod využívají moderních technologií, fungují. V práci se zkoumá aktuální dostupnost a kompatibilita vhodných chytrých zařízení a také je provedena analýza systémů Loxone a HomeKit sloužící k zjištění, pro jaké cílové skupiny je určitý systém zaměřený. Tato bakalářská práce se také věnuje finanční náročnosti a možnostem použití chytré domácnosti.

3 Metodika zpracování

K dosažení hlavního cíle je nutné nejdříve splnit cíle ostatní. Nejprve jsou vyvozena východiska z dotazníkového šetření. Poté je vytvořen návrh moderní domácnosti a následně provedena analýza problematiky inteligentních domácností založených na systémech Loxone a Apple HomeKit. Je proveden výběr jednotlivých komponent a průzkum tuzemského trhu pro tyto dva systémy. Výběr a implementace jednotlivých zařízení jsou zpracovány přehledně dle skupin zaměření daných zařízení a doplněny schématem a tabulkou vybraných zařízení, jejich počtem a cenou. Hlavním cílem je identifikace rozdílů systémů Loxone a Apple HomeKit.

4 Internet věcí

4.1 Co je to IoT?

Internetem věcí - „Internet of things“, dále již IoT, lze rozumět zařízení v oblasti kontroly a vzájemné komunikace mezi předměty s jinými předměty nebo člověkem, a to pomocí moderních technologií s použitím bezdrátového přenosu dat a internetu [1].

Tato IoT technologie je tedy nadřazeným pojem pro připojené digitální a fyzické komponenty, které dokážou přenášet data i bez pomoci lidských zprostředkovatelů. Každá tato komponenta, můžeme ji označit i jako zařízení IoT, má svůj unikátní identifikátor (Unique Identifier – UID), díky němuž je rozpoznatelná. Zařízení IoT umožňují sběr velkého objemu dat, jejich zpracování a vyhodnocení. V současnosti dělíme aplikaci IoT do pěti typů:

- **Consumer IoT** – (Spotřební) Do této oblasti spadá celá sféra zařízení chytrých domácností. Řadí se sem chytré osvětlení, reproduktory, zámky dveří, kamery, různé chytré spotřebiče a jiná spotřební zařízení IoT.
- **Commercial IoT** – (Komerční) Zařízení IoT a jejich implementace ve zdravotnictví a dopravě. Jsou to například různé monitorovací systémy, či inteligentní kardiostimulátory.
- **Industrial IoT** – (Průmyslový) Obsahuje statistické vyhodnocování, monitorovací systémy nebo organizační struktury automatických agentů. Průmyslový internet věcí je úzce spjat s pojmem Průmysl 4.0.
- **Infrastructure IoT** – (Infrastruktury) To zejména zahrnuje pojem smart cities neboli chytrých měst.
- **Military IoT** – (Vojenská) Do armádní oblasti spadají různé výzkumné zařízení od speciálních čidel a kamer, přes nositelné zařízení až k vojenským dronům [2].

4.2 Vývoj internetu věcí

Pojem internet věcí v sobě zahrnuje širokou škálu technologií, bez kterých by nemohl vzniknout. Prvním pomyslným milníkem lze označit polovinu 19. století a návrh Charlese Babbage „Analytical Engine“ aneb výpočetního stroje, který

disponoval částmi sloužícími jako paměť a procesor, které můžeme nalézt i u dnešních počítačů. Důležitá pro vývoj byla také publikace Heinricha Herze z roku 1887, ve které popisoval objev rádiových vln. O půl století později John V. Atanasoff a Clifford Berry postavili oficiálně první počítač, konkrétně se jednalo o rok 1937 a počítač Atanasoff-Berry Computer (ABC). Tento počítač se řadí do takzvané nulté generace počítačů, které se datuje do roku 1946. V období počítačů 1. generace 1947–1962 docházelo k velkému rozmachu nových programovacích jazyků, přičemž vzniklo více než 100 nových programovacích jazyků. Od roku 1963 do současnosti se datuje 3. generace počítačů neboli počítačů s integrovaným obvodem. Díky integrovanému obvodu se počítače staly výkonnější, menší a spolehlivější [3][4][5].

Vývoj internetu věcí však nejvíce souvisí s vývojem internetu. Jeho počátky se datují od konce 60. let 20. století, kdy došlo ve Spojených státech Amerických k vytvoření experimentální sítě ARPANET (Advanced Research Projects Agency Network). Později roku 1983 ARPANET přijal internetový protokol TCP/IP (Transmission Control Protocol/Internet Protocol). Podobu blízkou internetu dnešní doby přinesl až rok 1990, kdy Tim Berners-Lee vynalezl World Wide Web (WWW), který je často zaměňován za celý internet, ovšem jedná se pouze o nejběžnější online přístup k datům pomocí webových stránek a hypertextových odkazů.

Termín „Internet of Things“ (Internet věcí) byl poprvé použit v roce 1999 jako marketingově zajímavý titulek k prezentaci Kevina Ashtona o technologii RFID a internetu. S postupným vývojem technologií přibývalo také množství zařízení připojených k internetu. Dle skupiny Cisco Internet Business Solution Group (IBSG) byl internet věcí zrozen v roce 2008 ve chvíli, kdy bylo k internetu připojeno více zařízení než lidí [6][7].

Od té doby získal internet věcí celosvětové pokrytí, neboť stále více společností pracovalo na jeho postupném zdokonalování a uplatňování ve výrobních procesech. V minulosti lidé označovali IoT pouze jako „embedded internet“, neboli zabudovaný internet, ale v dnešní době je již technologie IoT zakotvena v mnoha aspektech našeho života [2].

Vzestup zařízení IoT je pevně svázán nejen s objevováním nových technologií, ale také s vývojem stávajících technologií a postupně snižující se cenou součástek nutných pro výrobu těchto zařízení. Již před několika lety bylo možné některá chytrá zařízení vyrobit. Taková zařízení by však byla značně rozměrnější, energeticky náročnější, objem dat, se kterým by zařízení pracovala, by byl naopak mnohem nižší, stabilita spojení horší a výrobní náklady mnohonásobně vyšší. V neposlední řadě nebylo ani uzpůsobené prostředí pro taková zařízení. Dnes je již možné vyrobit téměř jakékoliv zařízení. Zařízení mohou být velice malá, energeticky nenáročná a disponující kvalitní a stabilní komunikací mezi sebou. S novými technologiemi se snižují také náklady na výrobu a je možné zvyšovat počty zařízení a tím utvářet prostředí pro možné další připojení nových IoT zařízení. Mezi dnes již běžná chytrá zařízení lze řadit mobilní telefony, tablety, PC, televizory, tiskárny, kamery, zámky dveří, různé detektory pohybu, kouře, vlhkosti, ale také chytré hodinky, či jiná nositelná elektronika [8].

Internet věcí mění způsob, jakým se pracuje i žije. Skutečná hodnota a úspěch internetu věcí vycházejí ze stále většího počtu připojených IoT komponentů. Podle zprávy o mobilitě společnosti Ericsson bude do roku 2023 celosvětově připojeno více než 30 miliard zařízení, z nichž přibližně dvě třetiny zařízení budou pracovat na principu přímého připojení k internetu. Dle prozatímních prognóz se mezi roky 2017 a 2023 bude tento počet meziročně zvyšovat průměrně o 19 %, což je způsobeno rychlým vývojem IoT technologie v posledních letech a stále větší oblibou mezi běžnými uživateli. V současné době řada inteligentních zařízení IoT využívá mobilní sítě, jako je třetí generace (3G), či LTE neboli čtvrtá generace mobilní sítě (4G), aby se udržely ve spojení s internetovými datovými středisky, takzvanými cloudy, nebo jinými zařízeními. Pro stále větší množství chytrých zařízení postupně začíná být čtvrtá generace mobilních sítí nedostatečná a tím pádem hraje internet věcí zásadní roli ve vývoji nové, páté generace mobilních sítí (5G), která dle předpokladů bude disponovat zejména vysokým výkonem, nízkou latencí, zvýšenou škálovatelností a vysokou spolehlivostí přenosu dat. S příchodem tohoto nového standartu vznikají nové možnosti v oblasti autonomně řízených

vozů, robotické chirurgie, či průmyslu 4.0, chytrých domácnostech a v mnoha dalších odvětvích [9].

4.3 Komunikace

Jak již bylo výše zmíněno, tak zařízení internetu věcí mohou být takto označována, pokud dokáží získávat data z internetu a také je tam odesílat, a to ať přímým spojením (zařízení-internet), nebo předáním dat jinému zařízení, které již dokáže odeslat data na internet. Jelikož ale existuje veliké množství způsobů, jak data přeposlat, kdy každý způsob má v porovnání s ostatními určité výhody a nevýhody, tak vznikají zařízení, která disponují několika způsoby komunikace, ale také zařízení, která podporují pouze jeden způsob komunikace. Tyto způsoby komunikace se obecně označují jako komunikační standardy. Aby dvě zařízení mohla spolu navzájem komunikovat, tak je nutné, aby obě podporovala stejný standard komunikace [8].

Tyto standardy lze rozlišit na:

- Drátová připojení
- Bezdrátová připojení

4.3.1 Drátová připojení

Dříve bylo propojení dvou zařízení pomocí kabelu jediným komunikačním standardem pro přenos většího objemu dat. Při propojování kabelem je nutné, aby obě zařízení podporovala přenos dat přes daný kabel. Kabelů existuje veliké množství. Z hlediska komunikace zúžíme výběr pouze na sdělovací kabely [10].

Ty mohou být stíněné, či nestíněné, kabely s kroucenou dvojlinkou, telefonní, koaxiální, datové, nebo také optické kabely. Pro připojení k internetu se velice často využívají optické kabely, které disponují vysokou přenosovou rychlostí. Ty se však využívají na propojení vzdálenosti od 500 m až po 1600 m. Na kratší vzdálenosti se využívají kabely s kroucenou dvojlinkou, a to buď stíněné (STP), kde každá dvojlinka má své stínění, nebo kabely nestíněné (UTP), či FTP kabely, u kterých je jedna vrstva stínění pro všechny dvojlinky dohromady. Každý kabel spadá, dle svých vlastností, do určité kategorie. Tyto vlastnosti jsou například šířka pásma frekvence,

maximální možná délka kabelu a také přenosová rychlost. Momentálně existuje více než 13 kategorií, přičemž nejnovější je kategorie cat8, která disponuje šířkou pásma až 2 GHz, délkou kabelu až 30 m a maximální přenosovou rychlostí dokonce až 40 Gb/s. V domácnostech se běžně využívají zejména kabely kategorie Cat 5E, které dosahují přenosové rychlosti až 1 Gb/s, nebo také kabely kategorie Cat 6A, které v porovnání s Cat 5E mají 10x vyšší přenosovou rychlost, ale cena za metr kabelu Cat 6A je dvojnásobně vyšší než cena za kabel Cat 5E [11].

Při každém přenosu se musí brát v potaz rušení přenosu. Právě proti rušení se u kabelů využívá různé druhy stínění kabelů. Přenos dat pomocí kabelu může být sice rušen, ale v porovnání s bezdrátovou komunikací je kabelový přenos dat mnohem méně ztrátový a je rychlejší, stabilnější a kvalitnější [12].

4.3.2 Bezdrátová komunikace

Bezdrátová komunikace, nebo také komunikace bez použití kabelů spočívá ve spojení dvou zařízení jiným než mechanickým způsobem. Bezdrátové komunikace můžeme rozlišit do tří typů na:

- Optickou – Přenosové médium je světlo
- Sonickou – Přenos je zajištěn pomocí zvuku
- Rádiovou – Přenos pomocí rádiových vln, která je v současnosti nejčastějším typem [13].

4.3.2.1 Optická bezdrátová komunikace

Jedná se o přenos informací pomocí světla. Tato technologie je historicky velice stará a sahá až do starověku, kdy si lidé dle získaných poznatků předávali informace pomocí signálů, jako bylo zapalování ohňů a různé odlesky přes vodní hladinu. S postupným vývojem technologií se využívá optická komunikace i v dnešní elektrotechnice [13][14].

Mezi optické bezdrátové technologie pro přenos informací se řadí tyto typy komunikace:

a. Laserová komunikace

Laserová komunikace je označována za budoucnost vesmírné komunikace a postupně bude nahrazovat komunikaci rádiovou. Výhody laserové komunikace jsou zejména ve vysoké přenosové rychlosti s minimálními ztrátami, a to i při velikých vzdálenostech. Její nevýhodou však je, že mezi vysílačem a přijímačem laserového paprsku nesmí být žádná překážka. V takovém případě se nepřenáší žádná data [15].

b. Infračervené záření

Dalším typem optické bezdrátové komunikace je pomocí infračerveného záření. Jedná se o přenos na krátké vzdálenosti. Tento typ přenosu se využívá zejména v ovladačích. Pro přenos informací se využívá LED dioda emitující infračervené záření s vlnovou délkou v rozmezí 840 nm – 960 nm a fotodioda, která záření přijímá. Přenosová vzdálenost se pohybuje v mezích od několika centimetrů až po několik metrů v závislosti na zářivosti led diody. IrDA je standardem pro přenos dat pomocí infračerveného záření. U technologie IrDA se využívá modulované infračervené záření o vlnové délce 875 nm. Tato technologie se často vyrábí jako set přijímače (LED diody) a vysílače (fotodiody) a používá se u počítačů, mobilních telefonů, ale také u některých senzorů a jiných zařízení. Mezi hlavní výhody IrDA je nízká energetická náročnost. Nevýhodou však je potřeba přímé viditelnosti. Z toho důvodů bývá tato technologie postupně nahrazována Bluetooth technologií [16].

4.3.2.2 Sonická komunikace

Tento typ bezdrátové technologie komunikuje pomocí vytváření a rozpoznání zvuku. Je to nejpřirozenější typ mezilidské komunikace a jedná se o řeč. V podobě ultrazvuku se zase využívá pro echolokaci, či sonografii.

Dlouhou dobu byla sonická komunikace pro většinu elektronických zařízení nevhodná. Tvorba zvuku je nejen náročná na komponenty, ale také spotřebuje mnoho energie. Dalším negativem je náročnost sledovaný zvukový signál rozpoznat, očistit od okolního hluku a ideálně identifikovat informace, které daný signál předává. Proto se pro komunikaci mezi zařízeními, dále již (M2M – Machine to machine), nevyužívá.

Během posledních 10 let však technologičtí giganti, jako jsou firmy Samsung, Apple, Huawei a mnoho dalších, investovali miliony dolarů na vývoj této technologie, kterou implementují do svých zařízení pro zprostředkování komunikace mezi uživatelem a zařízením, či celou skupinou zařízení. Často jsou tato zařízení také doplněna o takzvaného virtuálního asistenta, díky kterému dokáží tato zařízení reagovat i na složitější příkazy od uživatele [13][17].

4.3.2.3 Rádiová komunikace

Rádiová komunikace je momentálně nejrozšířenější bezdrátová technologie. Tato technologie je založená na principu přenosu informací pomocí rádiových vln. Rádiové vlny se dělí na různá vlnová pásna, která se od sebe liší šířkou pásma neboli rozsahem jeho frekvencí, a vlnovou délkou. Pomocí rádiové komunikace se přenáší například televizní vysílání, které spadá do pásem vysoké a ultra vysoké frekvence a má tedy celkovou šířku pásma od 30 MHz až po 3 GHz a vlnovou délku od 10 metrů až 100 milimetrů. Na principu rádiových vln pracuje také Wi-Fi, které spadá do pásem ultra vysoká a super vysoká frekvence a má tedy šířku pásma od 300 MHz až po 30 GHz a vlnovou délku od 1 m až 10 mm. Typem rádiové komunikace je například FM rádio, telefonní signál, ale také většina radarů komunikuje pomocí této technologie. Do této kategorie spadají také přenosové standardy jako jsou Bluetooth, ZigBee, Z-Wave, RFID, UWB, LoRaWan a mnoho dalších [13][18].

4.4 Komunikační protokoly

Jak již bylo zmíněno výše, rádiová komunikace využívá rádiové vlny o různých frekvencích a vlnových délkách pro přenos dat. K uskutečnění přenosu je však důležité, aby přijímače vysílaného signálu dokázaly přijmout signál, který vysíláme a ne jiný. Nejen z tohoto důvodu existují pro přenos informací různé standardy s odlišnými vlastnostmi. Velmi důležité je také zmínit povolení pro vysílací pásma. Vysílání signálu na určitých frekvencích je limitováno pomocí regulí Českého telekomunikačního úřadu (ČTU), či obdobnými úřady v jiných státech. Na některých pásmech je vysílání zcela zakázáno. Mezi taková pásma patří například pásmo o vysílacích frekvencích 230 MHz – 400 MHz, které je vyhrazeno pro účely obrany státu. Existují také takzvaná licencovaná pásma. Vysílání na těchto pásmech

je zpoplatněno a je nutné mít platnou generální licenci od ČTU. Třetím typem pásem jsou takzvaná ISM pásma (Industrial, Scientific and Medical). Jedná se o pásma určená pro použití v průmyslovém, vědeckém a zdravotnickém oboru. Jsou to pásma volná, což znamená, že je v nich dovolen, při použití homologovaného (schváleného) zařízení, provoz bez licenčních poplatků. Mezi ISM pásma spadá například nejčastěji užívané pásmo 2,4 GHz, které se využívá u Bluetooth, Wi-Fi, či u vysílaček RC modelů (drony, auta na ovládání atd.). Mezi volná pásma se řadí také pásmo o frekvenci 5 GHz, které nejčastěji využívá u Wi-Fi a které má jiné přenosové vlastnosti než pásmo 2,4 GHz. Nejčastěji se však využívá Wi-Fi router, který podporuje obě pásma a umožňuje uživateli si volit pásma dle momentální výhodnosti. Od poloviny ledna roku 2020 uvolnil ČTU pásmo 60 GHz (57–66 GHz) pro volné užití i pro venkovní stanice. Aby se předešlo vzájemnému rušení stanic, je nutné každou stanici zdarma registrovat na registračním portálu ČTU. Pásmo 60 GHz umožňuje vysokorychlostní připojení k internetu bez využití pokročilých technologií jako je například technologie MIMO [18].

4.4.1 Bluetooth

Standard pro bezdrátovou komunikaci s označením Bluetooth byl založen v roce 1994 Jaapem Haartsenem a Svenem Mattissonem, kteří tehdy pracovali pro firmu Ericsson. Název Bluetooth byl odvozen od příjmení dánského krále Haralda Blåtanda, českém překladu Modrozuba a v anglickém překladu jako Harald Bluetooth, který vládnul v 10. století našeho letopočtu. Modrozub byl znám svou skvělou diplomacií a komunikací, což byl důvod, pro použití jeho jména pro označení komunikačního standardu. Bluetooth je založeno na standardu IEEE 802.15.1. Původně byla technologie Bluetooth navržena pro komunikaci s nízkou spotřebou, krátkým dosahem, využívající všesměrový režim vysílání, či jako bezdrátová náhrada k sériovému portu RS 232 a spadá mezi takzvané osobní počítačové sítě (Personal Area Network – PAN). Dalším významným rokem pro Bluetooth je rok 1998, kdy byla založena skupina Bluetooth Special Interest Group (SIG). Mezi její zakladatelé se řadí firmy IBM, Toshiba, Intel, Ericsson a Nokia. Skupina SIG se stará o aktualizace a vývoj tohoto standardu. První certifikované Bluetooth zařízením byl bezdrátový headset GN 9000, který byl představený v roce 2000. Později téhož roku

byl představen také první telefon s touto technologií a obě zařízení se dostala do prodeje v roce 2001 [19][20].

Bluetooth pracuje na aplikační vrstvě síťového modelu ISO/OSI ve frekvenčním pásmu 2,4 GHz. Kvalita a dosah signálu se s počtem překážek zhoršuje. Přenosové rychlosti pro nejnovější verzi 5.2 tohoto standardu jsou 125 kb/s, 500 kb/s, 1 Mb/s a 2 Mb/s. Dosah signálu může být až 240 m v otevřeném prostoru, či 40 m v prostoru uzavřeném a úzce souvisí s přenosovou rychlostí, kdy čím nižší je rychlost přenosu, tím vyšší je dosah signálu. Protože tento standard pracuje ve veřejném frekvenčním pásmu, je vysoká pravděpodobnost rušení od jiných vysílačů. Pro minimalizaci rušení se využívá technologie FHSS (Frequency Hopping Spread Spectrum). Tato technologie zajišťuje změnu frekvencí v určitém časovém úseku. Dochází až k tisíce přeladění za sekundu mezi několika desítkami kanálů o šířce 1 MHz. Bluetooth podporuje dva typy komunikace. Dvoubodovou (point to point), neboli přímé

Obr. 1 Logo Bluetooth
Zdroj: [20]

spojení dvou zařízení a vícebodovou (multi-point) komunikaci, která má jedno zařízení statusem master (pán) a poté až 7 zařízení se statusem slave (otrok). Zařízení se statusem master slouží jako přístupový bod, ke kterému lze následně připojit až 7 dalších zařízení se statusem slave. Takovéto seskupení se nazývá piconet (pikosíť). Vzájemným propojením více pikosítí může vzniknout takzvaný scatternet. Scatternet může obsahovat až 10 pikosítí. Každé Bluetooth zařízení má své identifikační číslo, tzv. Bluetooth Device Adrress, což je jakýsi ekvivalent MAC adresy [19][21].

Zabezpečení

Pro zabezpečení Bluetooth využívá metodu párování, kdy obě zařízení musí být nastavená do párovacího módu. Žádost o párování se obvykle odešle od uživatele, vyžadujícího spojení. Při párování se vygeneruje 48bitový párovací klíč, díky němuž mohou být přenášená data šifrována, tedy chráněna proti odposlechu [19][20].

Vývoj Bluetooth technologie

Verze 1.0a byla uveden na trh v polovině roku 1999 a na konci téhož roku vyšla verze 1.0b. Tyto verze však trpěly řadou nepřesností a chyb, a tak nebyly příliš komerčně využívány. V roce 2002 vyšla oprava předešlých chyb pod označením verze 1.1, která navíc umožňovala implementaci pikosítí, či indikátor síly signálu. Verze 1.2 z roku 2003 byla zpětně kompatibilní se verzí 1.1., nově nabízela vyšší přenosové rychlosti, podporu technologie přeskakování frekvencí (Adaptive Frequency Hopping – AFH), která zmírňovala okolní rušení a také nabízela možnost rychlého vytvoření připojení. Standard Bluetooth 2.0 byl schválen roku 2005 a přinášel technologii EDR, díky níž bylo možné dosáhnout přenosové rychlosti až 2,2 Mbit/s. O dva roky později byla představena verze 2.1 + EDR, jejímž hlavním rysem bylo bezpečné a jednoduché párování díky protokolu (Secure Simple Paring – SSP), který usnadňoval párování a také zvyšoval bezpečnosti přenosu. Verze 2.1 také přinesla režim nízké energie (Bluetooth Low Energy – Bluetooth LE, či BLE), rozšíření informací o zařízeních v okolí, či podporu NFC. Bluetooth 3.0 + HS byla přijata v roce 2009. Používá široko pásmovou technologii (Ultra Wide Band – UWB), která zajišťuje přenosovou rychlost až 24 Mbit/s. Této rychlosti dosahuje díky spojení a souběžnému přenosu s technologií Wi-Fi [19][20].

Dalším standardem je Bluetooth 4.0, který byl schválen v polovině roku 2010. Tato verze se rozděluje na tři typy. Prvním typem je klasické Bluetooth, které nově nabízí vyšší přenosové rychlosti, vyšší dosah a podporu 128bitového šifrování. Dalším typem je Bluetooth Smart, které slouží pro nízkoenergetické připojení k různým měřičům tepu a jiným senzorům, ale již není kompatibilní s klasickým Bluetooth. Posledním typem je Bluetooth Smart Ready, které je kompatibilní s oběma předchozíma typy. Verze 4.1 vyšla v koncem roku 2013 a vylepšovala většinu dosavadních přenosových vlastností a nově nabízela také podporu ipV6 a lepší

koordinaci ve spojení s LTE. O rok později vychází verze 4.2, která zásadně vylepšuje sdílení internetu přidáním protokolu IPv6/6LoWPAN. Také přichází s úsporou energie u zařízení Bluetooth Smart a samozřejmě opět dochází ke zlepšení přenosových rychlostí. V roce 2018 přichází standard Bluetooth 5.0, který přináší možné volby přenosových rychlostí: 2Mb/s, 1Mb/s, 500 kb/s a 125 kb/s, zatímco dříve bylo možné mít pouze jednu přenosovou rychlost. Tato možnost zvyšuje celkový dosah, neboť s nižší přenosu rychlostí se zvyšuje maximální dosah [20].

Bluetooth 5.1 vychází v lednu 2019. Tato technologie nabízí možné vyhledávání zařízení s přesností na centimetry díky dvou metodám detekce zařízení. Metoda příchozího úhlu (Angle of Arrival – AoA) a metoda odchozího úhlu (Angle of Departure – AoD) [22].

Zatím nejnovější verzí je verze 5.2, která byla představena v lednu 2020. Tato technologie je v porovnání s předchozími již čistě na technologii Bluetooth LE a již nedochází k změnám u přenosových rychlostí, ale zejména u úspory energie a kvalitě přenosu. Další novinkou je také takzvané true wireless stereo (TWS), které značně vylepšuje poslech hudby. Doposud pracoval bezdrátový přenos hudby tak, že se odesílal dvou kanálový signál do hlavního zařízení a z něj pak šel ještě jednokanálový přenos do zařízení druhého. Vzniklý časový posun byl upraven softwarem, ale celé to bylo energeticky náročnější a docházelo také ke ztrátám kvality při přenosu. Nová technologie umožňuje přeposílání signálu do obou zařízení najednou, což vyrovnává výdrž baterií obou zařízení a celková spotřeba energie je také nižší. Tato technologie také umožňuje sdílení audia s více zařízeními. Například dva lidé mohou poslouchat hudbu z jednoho zařízení pomocí bezdrátových sluchátek, což dříve nebylo s Bluetooth 5.1 možné. Tato technologie však není zcela nová. Již dříve vyvinula společnost Apple svůj komunikační čip U1, který tyto funkce také umožňoval, avšak tento čip byl kompatibilní pouze s produkty značky Apple a dceřiné společnosti, pro ostatní firmy byla tedy tato technologie uzavřená [23][24].

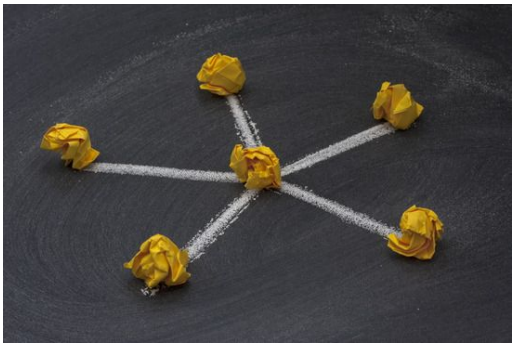
Pro různé činnosti Bluetooth se využívá jiný profil a každé zařízení obsahuje odlišnou sadu profilů dle jeho účelu. Profil je jakýsi soubor instrukcí, pomocí nichž

propojená zařízení komunikují. Existuje mnoho profilů a každý musí být schválen skupinou Bluetooth SIG. Mezi nejznámější profily se řadí:

- A2DP (Advanced Audio Distribution Profile) – bezdrátový přenos zvuku
- AVRCP (Audio/Video Remote Control Profile) – ovládání hudby a videa
- BIP (Basic Imaging Profile) – práce s obrázky, jejich přesuny, tisk a zálohování
- DID (Device ID Profile) – nástroj pro identifikaci připojených zařízení
- DUN (Dial-up Networking Profile) – sdílení internetu
- FTP (File Transfer Profile) – přístup k adresářům a složkám jiného zařízení
- HFP (Hands-Free Profile) – ovládání handsfree
- HID (Hands-Free Profile) – připojení periferií k osobnímu počítači, vyznačuje se nízkými prodlevami a spotřebou energie
- LAP (LAN Access Profile) – sdílení internetu se zařízeními (obdoba Wi-Fi, výjimečné řešení)
- OPP (Object Push Profile) – snadné posílání menších souborů jako jsou obrázky, či vizitky
- VDP (Video Distribution Profile) - streamování videa
- PBAP (Phone Book Access Profile) – přístup k telefonním kontaktům zařízení [20].

4.4.2 Wi-Fi

Wi-Fi je označením pro bezdrátovou komunikaci v místní síti (Wireless Local Area Network – Wireless LAN, či WLAN). Nejčastěji využívanou topologií této sítě je takzvaná topologie do hvězdy. V síti do hvězdy každé koncové zařízení komunikuje přímo jen a pouze s centrálním zařízením. Pokud je koncové zařízení mimo dosah centrálního, pak nebude součástí sítě [25].



Obr. 2 Topologie do hvězdy
Zdroj: [25]

Stejně jako technologie Bluetooth i Wi-Fi pracuje na volném ISM pásmu 2,4 GHz, ale na rozdíl od Bluetooth se Wi-Fi nachází na linkové vrstvě v ISO/OSI modelu a pro bezdrátovou komunikaci se u Wi-Fi využívá protokol CSMA/CA. Pro usnadnění vzájemné bezdrátové komunikace různých zařízení od různých výrobců institut IEEE (Institute of Electrical and Electronic Engineers) schvaluje vyvinuté standardy. Pokud obě zařízení splňují daný standard, pak jsou navzájem kompatibilní. Každé síťové zařízení má svůj identifikátor, který se nazývá MAC adresa. Tento identifikátor se skládá ze 48 bitů a uvádí se v podobě šestice dvojciferných hexadecimálních čísel a je továrně přiřazený ke konkrétnímu zařízení. Pro zařízení podporující Internetový protokol vzniká při připojení takzvaná IP adresa, která slouží k identifikaci síťového rozhraní a aktuálně se využívají protokoly IPv4 a IPv6. IPv4 tvoří 32bitové číslo, které se zapisuje v dekadickém tvaru, jako čtyři osmibitové pole oddělené tečkou. Novější protokol IPv6 je tvořen 128bitovým číslem a zapisuje v hexadecimálním tvaru, jako osm šestnácti bitových polí navzájem oddělených dvojtečkou. Tento protokol vznikl z důvodů rychlého vyčerpávání adresního prostoru IPv4. Každá bezdrátová síť má také svůj identifikátor (Service Set Identifier – SSID), často označován jako název sítě, který je tvořen 32 ASCII znaky a slouží k identifikaci dané sítě. Sítě mohou být buď Ad-hoc, či infrastrukturní. V Ad-hoc sítích jsou spojovaná zařízení navzájem rovnocenná a vzájemná identifikace probíhá pomocí SSID. Příkladem může být například bezdrátové spojení PC, mobilních telefonů, či tiskáren. Na rozdíl od Ad-hoc sítí, tak infrastrukturní sítě obsahuje alespoň jeden přístupový bod, takzvaný access point, který vysílá své SSID a dle kterého si klient vybere síť, ke které se připojí. Přístupovým bodem může být v domácí síti například router [26][27][28][29].

Zabezpečení

Proti nechtěnému narušení sítě se využívá Firewall, který omezuje přístup do sítě, či ke konkrétnímu zařízení sítě. Firewall je konfigurovatelný a má různé stupně zabezpečení. Existuje mnoho způsobů pro zabezpečení sítě. Jedním z nich je použití statických klíčů WEP, které jsou však pomocí speciálních programů snadno prolomitelné. Další možností je zabezpečení WPA. Je to podobné zabezpečení jako WEP, jen využívá doprovodný program pro dynamické měnění klíčů. Nástupcem WPA je WPA2, které využívá kvalitní šifrování pomocí šifry AES. Dalším možným způsobem zabezpečení sítě je pomocí protokolu 802.11.1X. Toto zabezpečení pracuje na přístupovém bodu a to tak, že po připojení k síti je nutné pro přístup projít autorizací. Například zadat speciální klíč, či přihlašovací jméno a heslo. Než se klient autorizuje, přístupový bod blokuje jeho datový provoz na síti. Mezi další způsob zabezpečení se řadí kontrola MAC adresy. Přístupový bod má k dispozici seznam MAC adres, takzvaný whitelist, či blacklist. Whitelist omezuje přístup pouze na MAC adresy uvedené na seznamu, zatímco blacklist zamezuje přístup konkrétním MAC adresám uvedených na seznamu. Zabezpečit lze bezdrátovou síť také skrytím SSID, kdy skryté SSID nebude vidět v seznamu sítí, ale po ručním zadání přesného SSID se lze k síti připojit [29][30].

Původ Wi-Fi

Hlavní standardizační autorita Institute of Electrical and Electronics Engineers založila v únoru 1980 novou rodinu standardů IEEE 802 pro lokální a metropolitní sítě. Kdy číslo 802 je složeninu roku 1980 a 2. měsíce. Skupiny standardů pak přicházeli s označením složeným z prefixu IEEE 802., který byl pro všechny standardy stejný a k němu doplněným o postfix složený z označení dané skupiny standardů a jejím konkrétním typem standardu. Běžné drátové sítě LAN a MAN spadají pod skupinu 802.3, což je Ethernet. Jejich bezdrátovou alternativou je 802.11 (Wireless LAN) a 802.16 (MAN). Bezdrátové sítě PAN spadají do skupinu 802.15, kam patří například Bluetooth, či ZigBee. Skupina 802.16 splňuje standardy technologie WiMAX, což je obdobná technologie jako Wi-Fi, ovšem Wi-Fi je rozuměna standardem pro vnitřní sítě, zatímco WiMAX je standard pro bezdrátovou komunikaci venkovních sítí. Standard Wi-Fi tedy spadá pod označení skupiny

802.11. Její vývoj započal v září 1990 a první oficiální standard byl schválen o sedm let později v roce 1997. Jednalo se o standard s označením 802.11. Protože tento první WLAN standard ještě neměl žádné dodatečné značení, zpětně se označuje jako 802.11-1997. Tento standard pracoval na frekvenci 2,4 GHz a maximální rychlost přenosu byla 2 MB/s, zatímco Ethernet měl v této době rychlost 10 MB/s.

Dva nové standardy se byly představeny v roce 1999. Konkrétně se jednalo o 802.11a a 802.11b. Zatímco standard 802.11a pracoval na frekvenci 5 GHz s široko pásmovou modulací OFDM až 64-QAM a s přenosovými rychlostmi až 54 MB/s, tak druhý standard 802.11b pracoval na frekvenci 2,4 GHz s rychlostí přenosu do 11 Mb/s. Oba tyto standardy nabízeli šířku kanálu až 20 MHz. V této době ještě neexistovalo označení Wi-Fi. Pro kontrolu kompatibility zařízení podporující standard 802.11b vznikla nezisková organizace Wireless Ethernet Compatibility Aliance (WECA), které mimo jiné zvolila z marketingového hlediska název Wi-Fi jako náhradu za označení 802.11b. Později téhož roku bylo marketingově použito toto označení s dodaným sloganem Wireless fidelity, neboli bezdrátová věrnost, avšak jednalo se pouze o slogan a označení Wi-Fi není zkratkovým názvem. V roce 2001 byl vydán nový standard 802.11g, jehož přenosová rychlost byla 54 Mb/s na frekvenci 2,4 GHz, jehož šířka kanálu byla 20 MHz a modulace OFDM 64-QAM. O rok později se nechala přejmenovat celá organizace WECA na Wi-Fi Alliance [28][31].

Od 802.11g se na další standard čekalo sedm let, když v roce 2009 vyšel standard 802.11n. Ten fungoval na obou dosavadních pásmech, jak na 2,4 GHz, tak i na 5 GHz. Využíval modulaci 64-QAM a šířka kanálů byla 20 MHz a 40 MHz, což byl dvojnásobek oproti standardu 802.11g, ale také bylo umožněno více cestné vysílání, neboli „multiple-input, multiple-output“ (MIMO). Tato technologie dokáže efektivněji využít pásmo a s více anténami násobit teoretickou přenosovou rychlost. Tedy za předpokladu, že přenos s jednou anténou má přenosovou rychlost 150 Mb/s, tak s použitím čtyř antén, což je maximální počet pro daný standard, může být teoretická propustnost až 600 Mb/s. Na konci roku 2012 byl představen standard 802.11ad, který nese obchodní označení WiGig a pracuje na pásmech 2,4 GHz, 5 GHz a 60 GHz a jeho přenosová rychlost dosahuje až 7 Gb/s pro pásmo 60 GHz. Šířka kanálu je 2160 MHz a modulace je OFDM až 64-QAM. Nevýhody této

technologie jsou však téměř neproniknutelnost stěnami při frekvenci 60 GHz a nízká přenosová vzdálenost [31][32].

Na začátku roku 2014 byl schválen standard 802.11ac. Ten pracuje na frekvenci 5 GHz a podporuje kanály o šířce 80 MHz až 160 MHz a možnost komunikace až na osmi MIMO prostorových kanálech a modulací s vysokou hustotou až 256-QAM. S příchodem tohoto standardu také přišla podpora režimu multi-user MIMO, neboli MU-MIMO. Pro lepší představu lze označit dosavadní technologii MIMO, jako SU-MIMO, neboli single-user. SU-MIMO dokáže komunikovat pouze s jedním zařízením současně. To znamená, že pro router s rychlostí 1300 Mb/s, ke kterému se připojí tři telefony o maximální přenosové rychlosti 433 Mb/s, které budou chtít stáhnout stejný soubor bude stahování trvat 3krát pomaleji, než pro telefon samotný a router bude pracovat pouze na 1/3 své kapacity. Zatímco MU-MIMO pro stahování dokáže obsluhovat až 4 zařízení současně a pracovat tak na maximální kapacitu routeru. Koncem roku 2018 vydala Wi-Fi Alliance rozhodnutí o přejmenování názvů pro Wi-Fi standardy. Každému standardu zůstává i jeho dosavadní označení, ale získává i komerční označení. Wi-Fi 1 je označením standardu 802.11a, Wi-Fi 2 pro standard 802.11b, Wi-Fi 3 pro 802.11g, Wi-Fi 4 pro 802.11n a Wi-Fi 5 pro standard 802.11ac [28][31][33].

Nejnovějším standardem je Wi-Fi 6, který byl představen v roce 2019 a jeho nekomerční označení je 802.11ax. Tento nový standard pracuje na pásmech 2,4 GHz i 5 GHz a přichází se zvýšením počtu MIMO streamů na 8. Nově je také zvýšení přenosové rychlosti pro jeden kanál z 433 Mb/s na 600 Mb/s, ale šířka kanálu zůstává stejná jako u Wi-Fi 5, tedy do 160 MHz. Teoreticky je možné dosahovat maximální propustnosti až 9,6 Gb/s. Technologie MU-MIMO se nově uplatňuje i u nahrávání dat na internet, zatímco doposud se využívala pouze u stahování. Wi-Fi 6 nově podporuje modulační schéma OFDMA až 1024-QAS pro zvýšení kapacity sítě, které se využívá také u LTE, či 5G. V rámci OFDMA se logický komunikační blok dokáže rozdělit až na desítky menších částí, které se dynamicky přidělí jednotlivým zařízením. Tato technologie je vhodná pro místa s vyšší koncentrací připojených zařízení, jako jsou například koncerty, či fotbalové zápasy, kde by již s použitím této technologie nemělo docházet k takzvaným komunikačním

zácpám a mohlo být každé připojené zařízení rychle obslouženo. Ačkoliv Wi-Fi 6 zatím podporuje pouze pásma o frekvencích 2,4 a 5 GHz, tak je již tento standard uzpůsobený na budoucí začlenění také pásma o frekvenci 6 GHz, přesněji pro spektrum od 5,925 GHz až po 7,125 GHz. Toto pásmo prozatím nepatří mezi bezlicenční pásma, ale úřady již pracují na změnách, které by dané pásmo uvolnily a bylo by možné ho začlenit mezi podporované pásma standardu Wi-Fi 6 [33][34][35].

4.4.3 Zigbee

Jedná se o významný otevřený bezdrátový komunikační standard pro nízkorychlostní komunikaci v takzvané personální bezdrátové síti (Low-Rate Wireless Personal Area Network – LR-WPAN). V roce 2002 byla založena aliance ZigBee Alliance, která sdružovala firmy podílející se na vývoji tohoto standardu. Mezi tyto firmy patří například Motorola, Siemens, či Samsung. Technologie je založena na standardu IEEE 802.15.4. a od roku 2004 je uznána platným standardem. Tento standard umožnuje multiskokové ad-hoc směrování, které dokáže komunikovat i bez přímé radiové viditelnosti jednotlivých zařízení. Jedná se o topologii typu mesh. Tento standard je běžně využíván IoT zařízeními, která se používají například v chytrých domácnostech, ale také v průmyslu a senzorových sítích. Sítě typu ZigBee mají dosah většinou do 100 metrů, avšak při použití multiskokového ad-hoc směrování umožňuje dosah až 300 metrů [36][37].

Obr. 3 Logo ZigBee
Zdroj: [25]

U fyzické vrstvy a vrstvy řízení přístupu (MAC), vychází ZigBee ze standardu 802.15.4. Další vrstvy jsou bezpečnostní vrstva, aplikační vrstva a aplikace, kde první dvě definuje ZigBee Alliance a třetí vrstva je uživatelská. Ve fyzické vrstvě (PHY) z důvodu přiřazení různých pásem v Evropě a Americe, ZigBee podporuje jiné pásmo výlučné pro Evropu, konkrétně pásmo 868 MHz s jedním kanálem o šířce 600kHz a rychlostí přenosu 20 kb/s, a jiné pro Ameriku, kde podporuje pásmo

915 MHz s 10 kanály o šířce 2 MHz a přenosovou rychlostí 40 kb/s. Celosvětově ZigBee podporuje, stejně jako Bluetooth a Wi-Fi, bezlicenční pásmo 2,4 GHz, na kterém dosahuje rychlosti přenosu až 250 kbit/s a také zde umožňuje využít 16 kanálů, přičemž šířka jednoho kanálu je 5 MHz. Také modulace signálu jsou různé, kdy pro Evropu se využívá dvoustavového fázového klíčování (Binary Phase Shift Keying – BPSK) a pro ostatní pásma se využívá čtyřstavového fázového klíčování s offsetem (Offset-Quadrature Phase Shift Keying – O-QPSK). Rozprostření signálu pracuje na technologii DSSS neboli přímého rozprostření spektra. Na vrstvě řízení přístupu se stejně jako u Wi-Fi i u ZigBee využívá protokol CSMA/CA pro přístup k fyzickému médiu. Na této vrstvě se užívají 4 typy rámců. Konkrétně jde o datový ráme (Data Frame), neboli rámec pro přenos užitečných dat. Dalším typem je potvrzovací rámec (Acknowledge Frame) sloužící pro přenos potvrzovací informace. Třetím typem je MAC příkazový rámec (MAC Command Frame) pro centrální konfiguraci a poslední je synchronizační rámec (Beacon Frame), který slouží pro synchronizaci zařízení v síti [37][38].

Bezpečnostní vrstva je již vrstvou definovanou ZigBee Alliance. Každé zařízení má přiřazený jedinečný adresovací kód, který slouží pro adresaci zařízení. Zařízení může mít buď dlouhý 64bitový kód, či zkrácený 16bitový kód. Přičemž v jedné síti je možné adresovat až 65535 zařízení, zatímco u technologie Bluetooth je možné mít na jedné síti maximálně 7 uzlů. Technologie ZigBee dělí moduly dle funkčnosti na koordinátora sítě (Coordinator PAN), zařízení s plnou funkčností (Full Functionality Device – FFD) a zařízení s omezenou funkčností (Reduced Functionality Device – RFD). Přičemž Koordinátor je zároveň zařízení FFD. Dle standardu IEEE 802.15.4 podporuje ZigBee tři topologie. Nejznámější topologií je hvězdicová topologie. Tuto topologii využívá také Wi-Fi, kdy veškerá komunikace v síti probíhá přes centrální uzel. Další je smíšená topologie, známější pod anglickým označení mesh. Tato topologie je typická právě pro technologii ZigBee a spočívá v možnosti propojit dvě zařízení více způsoby pomocí dalších zařízení a zajišťuje tak vyšší stabilitu sítě. Posledním typem je takzvaná stromová topologie, u které se zařízení mohou na sebe navzájem propojovat, ale vždy existuje jen jedna cesta ke koordinátorovi sítě. Výhodou této topologie je vyšší celkový dosah

sítě, ale mezi nevýhody se řadí například transportní zpoždění u vzdálenějších zařízení, či výpadek více zařízení při poruše jednoho uzlu. Tento typ topologie není doporučovaný. Pro zabezpečení na přenosové trase se data šifrují pomocí kryptografického standardu AES ve třech úrovních. Mohou se volit klíče délky 32 bitů, 64 bitů anebo až 128 bitů. Aplikační vrstva se dělí na pomocnou aplikační vrstvu, vrstvu ZigBee objektů a vrstvu uživatelských aplikačních objektů [25][36][37][38].

Obr. 4 Topologie typu mesh
Zdroj: [25]

4.4.4 Z-Wave

Z-Wave je bezdrátovým komunikačním protokolem vytvořeným primárně pro automatizaci domácnosti. Vyvinula ho dánská společnost Zensys v roce 1999. Technologie je založená na „system on chip“ (SoC) protokolu pro automatizaci domácnosti. V průběhu let společnost zdokonalovala chip sety, které nabízely nižší spotřebu energie a vyšší výkon. V roce 2005 se ke společnosti Zensys přidružily další společnosti a utvořili Z-Wave Alliance, ke které se později přidaly také firmy jako Intel, či Cisco. V roce 2016 aliance představila Z-CIT neboli Z-Wave Certified Installer Toolkit, který byl jakýmsi nástrojem pro testování a vývoj zařízení s technologií Z-Wave. Od roku 2018 vlastní společnost Silicon Labs zaměřující se na zařízení IoT zařízení, která technologii koupila za 240 miliónů dolarů. V porovnání s předchozími standardy je Z-Wave privátní technologií na rozdíl od Bluetooth, Wi-Fi, či ZigBee, které jsou otevřenými technologiemi. Každé zařízení pracující

s touto technologií musí získat dvě certifikace. Technickou certifikaci od společnosti Silicon Labs a marketingovou od Z-Wave Alliance [39][40][41].

Obr. 5 Logo Z-Wave
Zdroj: [41]

Z-Wave stejně jako ZigBee používá topologii mesh neboli smíšenou topologii. Na rozdíl od ZigBee však povoluje mnohonásobně méně připojených zařízení k síti, kdy Z-Wave umožňuje připojení 232 zařízení a ZigBee více než 65 tisíc zařízení. Dalším rozdílem těchto dvou standardů je kvalita propojení zařízení a možný počet přeskoků mezi zařízeními k centrálnímu zařízení, kdy Z-Wave poskytuje stabilnější propojení s delším dosahem, ale zatím co ZigBee umožňuje neomezený počet přeskoků mezi zařízeními, tak Z-Wave podporuje pouze 4 přeskoky. Tedy mezi koncovým zařízením a centrálním hubem může být maximálně 3 zařízení, přes které bude přenos probíhat. Stejně jako ZigBee má i Z-Wave nízkofrekvenční pásma různé dle lokace a odlišné od ZigBee. Příkladem frekvence dle lokací: EU (868,4 MHz, 868,42 MHz, 869,85 MHz), USA (908,4 MHZ, 908,42 MHz, 916 MHz), Rusko (869 MHz) a například Indie (865,2 MHz). Rozdílem mezinárodně velice důležitým je, že na rozdíl od Z-Wave, ZigBee navíc podporuje i mezinárodní pásmo 2,4 GHz, a tedy výrobky Z-Wave, které nejsou určeny pro daný trh také nejsou kompatibilní se zařízeními určenými pro daný trh a zároveň jsou v dané oblasti z většiny zakázané, neboť využívají nepovolené vysílací frekvence [25][40][41][42].

4.4.5 LoRaWan

Technologie LoRaWan (Long Range Wide Area Network) se řadí mezi nízkopříkonové bezdrátové síťové protokoly vytvořené pro snadnou a zabezpečenou komunikaci zařízení IoT. Vznik je datován k roku 2015 a tento komunikační standard spadá pod organizaci LoRa Alliance. Zabezpečení probíhá na dvou úrovních, konkrétně na internetové a aplikační a využívá šifrování AES. Podobně jako Z-Wave operuje na frekvenčním pásmu 868 MHz pro Evropu a odlišných pro ostatní lokace. Využívá modulaci SS chrip – FSK s technologii

rozprostřeného spektra a rozprostírá signál na celý vysílací kanál s frekvencemi 125 kHz, 250 kHz a 500 kHz, přičemž podporuje až 10 kanálů a přenosové rychlosti jsou od 0,25 kb/s do 50 kb/s. Jak název „long range“, neboli dlouhý dosah, napovídá, tak výjimečností této technologie je dosah od 2 km až po 40 km v závislosti na prostředí.

LoRaWan rozlišuje zařízení do 3 tříd.

- Třída A – koncová zařízení podporující obousměrnou komunikaci
- Třída B – zařízení otevírají přijímací okna pouze v určitou dobu
- Třída C – přijímací okna jsou otevřená, krátkodobě se zavírají pouze po dobu vysílání

Pro maximalizování životnosti baterie koncového zařízení, síťový server LoRaWAN spravuje pro každé koncové zařízení individuálně jeho přenosovou rychlost a RF výstup, prostřednictvím systému adaptivní rychlosti přenosu dat (ADR). Zařízení komunikující pomocí této technologie nabízí výdrž baterie od 5 až do 15 let v závislosti na konfiguraci zařízení a hustotě komunikace. Tato technologie je díky svým vlastnostem často využívaná při tvorbě chytrých domácností, chytrých měst a celkově u zařízení internetu věcí [43][44].

4.4.6 Sigfox

Sigfox je názvem francouzské firmy, ale také názvem jimi vydané technologii pro bezdrátové spojení nízkopříkonových zařízení. Sigfox využívá technologii ultra nízkého pásma (UNB, Ultra-narrow Band) s modulací DBSPK (Differential Phase-Shift Keying). Tato technologie stejně jako LoRaWan, či Z-Wave pracuje na frekvenčním pásmu 868 MHz pro Evropu s přenosovou rychlostí do 100 bitů za sekundu s dobou přenosu a zpracování okolo 5 sekund. Využívá také vícecestné vysílání MIMO bez synchronizace. Všechna zařízení musí obsahovat komunikační čip, který poskytuje možnost komunikovat na síti Sigfox. Čip využívá pro identifikaci unikátní 32bitové Sigfox ID, které se přiřadí zařízení při výrobě.

Zařízení smí denně odeslat maximálně 144 zpráv, přičemž jedna zpráva může dosahovat velikosti maximálně 96 bitů. Tím zajišťuje malou spotřebu energie a životnost baterie 5 až 15 let. Obousměrná komunikace je aktivovaná pouze

na vyžádání koncovým zařízením. Tudíž se Sigfox hodí spíše na jednosměrnou komunikaci. Velkou nevýhodou je tedy složitější aktualizace firmware u koncových zařízení [39].

4.4.7 UWB

UWB (Ultra-Wide Band) pracuje na širokém frekvenčním pásmu s více než 500 MHz a lze jej využívat s různou frekvencí pulzů. Od 1 MHz až po 2 GHz. UWB dokáže velice přesně určovat vzdálenost mezi vysílačem a přijímačem, přičemž v závislosti na konfiguraci může dosahovat přesnosti 5 mm, ale také 10 cm. Tato technologie se využívá u standardu bezdrátového USB (Wireless USB), nebo také je využíván společností Apple u čipů U1, které společnost Apple využívá u bezdrátových sluchátek AirPods a které umožňují mimo jiné sdílení audia s jiným zařízením s čipem U1, či novější generace [23][45].

4.4.8 RFID a NFC

Technologie RFID neboli radiofrekvenční identifikace, jde takzvaně o novou generaci čárových kódů, kterou nechal patentovat v roce 1983 Charles Walton. Zařízení pracují na komunikaci mezi kontrolním zařízením a čipem. Existují dva typy čipů, aktivní a pasivní. Pasivní čipy nepotřebují žádný zdroj energie. Při komunikaci vysílá kontrolní zařízení elektromagnetické pulsy, které v případě nálezu RFID čipu nabijí jeho kondenzátor a následně čip odešle zpět odpověď, což může být například elektronické číslo produktu (EPC), nebo některé čipy mohou disponovat dodatečnou pamětí pro další informace. Aktivní zařízení mají navíc zdroj v podobě baterie a jsou schopny samy vysílat svou identifikaci [8][46].

Zařízení RFID pracuje na různých frekvencích, které se liší oblastí (Evropa, Amerika, …), ale také dle využití. Frekvence mohou být nízkofrekvenční (LF), které pracují na 124 kb/s a 135 kb/s a mají dosah až 0,5 metru. Dalším typem je vysokofrekvenční (HF) komunikace. Jedná se o nejčastěji využívané RFID s frekvencí 13,56 MHz a dosahem do 1 metru. Ultra frekvenční (UHF) nabízí dosah až 3 metry a podporuje různé frekvence pro Evropu (868 MHz), USA (915 MHz) a jiné frekvence pro další oblasti. I technologie RFID podporuje frekvenci 2,45 GHz s dosahem do 2 metrů,

avšak takto vysoká frekvence je mnohonásobně energeticky náročnější a využívá se pouze u mohutných a vysoce náročných systémů [8][47].

Novou generací RFID lze nazvat technologii NFC (Near Field Comunication), která ze standardu RFID vychází. Nejedná se o kompletní náhradu RFID za NFC zejména kvůli dosahu komunikace, kdy dosah NFC je se pohybuje okolo 4 cm maximálně však do 10 cm. NFC pracuje na frekvenci 13,56 MHz s přenosovými rychlostmi od 106 kb/s do 424 kb/s. Stejně jako RFID i NFC existuje v podobě aktivních a pasivních čipů. Pasivní NFC čipy se nazývají tagy a jsou programovatelné pro uchování a sdílení určitých informací. Aktivní čipy mají přístup ke zdroji energie a jsou součástí elektronických zařízení. NFC se vyznačuje zejména rychlostí připojení kratší než 1 milisekunda. Z hlediska zabezpečení, šifrování neprobíhá na NFC čipu a je nutná další implementace v zařízení. Tato technologie také podporuje režim emulace karty. V tomto režimu se aktivní NFC emuluje do podoby pasivního. Emulace se využívá při NFC platbách elektronickým zařízením, které se emulací NFC dokáže proměnit v bezkontaktní platební kartu. Použití této technologie je časté také u chytrých zařízení, jako jsou bezkontaktní zámky dveří, či přenos souborů mezi dvěma zařízeními, nebo také pro snadné spárování zařízení. Právě snadné párování je často využito při připojování zařízení do systému chytrých domácností [8][46][48].

4.4.9 Mobilní sít

Také mobilní sít spadá pod rádiovou komunikaci, přičemž se může jednat o satelitní, nebo celulární síť. Satelitní komunikace se využívá zejména v oblastech, ve kterých není dostatečná infrastruktura celulární sítě. Zařízení se v takových případech připojují ke stacionárním satelitům na oběžných dráhách planety Země. Pro oba typy sítí je pro připojení nutná identifikace účastníka v mobilní síti. K identifikaci slouží fyzická karta SIM (Subscriber Identity Module), kterou je nutné vložit do mobilního zařízení, či elektronická SIM (E-SIM) zabudovaná na základové desce mobilního zařízení a která vyžaduje registraci u operátora. Operátor je poskytovatel mobilního připojení, přičemž za využívání jeho služeb může vyžadovat poplatky [49].

Celulární rádiová síť neboli buněčná, je tvořena pomocí vysílačů signálu v určité kruhové oblasti. Tato oblast může být označována jako buňka mobilní sítě. Různé oblasti se navzájem překrývají a docilují tak kontinuální dostupnosti mobilního signálu. Mobilní signál umožňuje přeposílání zpráv, uskutečňování telefonních hovorů, ale také možnost připojení k internetu. Za počátky komerční mobilní sítě lze považovat přelom 60. a 70. let 20. století, kdy vznikala takzvaná nultá generace bezdrátové telefonní technologie (0G). 0G se v té době využívala zejména v automobilech. V 80. letech přichází 1. generace (1G) této technologie, přičemž se jednalo o analogový signál a již sloužil pro mobilní telefony. Od roku 1991 můžeme datovat 2. generaci bezdrátové telefonní technologie (2G) založenou na GSM (Global Systém for Mobile Comunications) standardu, jejíž největší odlišností od 1G byl přechod na digitální signál. 2G umožňovalo odesílání textových zpráv (SMS), ale i odesílání obrázků (MMS). Díky digitalizaci bylo také možné hovory i zprávy digitálně šifrovat. Nástupcem 2G bylo takzvané 2.5G neboli GPRS (General Packet Radio Service), která umožňovala uživatelům připojení k internetu a umožňovala přenos dat rychlostí až 80 kb/s. Nástupcem GPRS byla technologie EDGE (Enhanced Data rates for GSM Evolution) s označením 2.75G. EDGE nabízí 3krát efektivnější osmistavovou modulaci 8-PSK, zatímco předchozí generace (GMS a GPRS) využívali modulaci GMSK. Zlepšení přináší EDGE také v přenosové rychlosti, která se pohybovala okolo 100 až 120 kb/s. Třetí generace (3G) zahrnuje také technologii UMTS (Universal Mobile Telecommunication Service) a přináší nárůst přenosové rychlosti až k 3 Mb/s. Jako 3.5G se označuje technologie HSPA (High-Speec Down-Link Packet access) a nabízející rychlost až 14 Mb/s. Takzvaná vylepšená HSPA, neboli HSPA+ umožňuje rychlost přenosu dat více než 42 Mb/s. Dosavadní rychlostní zlom nastal v roce 2010 a uvedení 4. generace (4G) o rychlosti přenosu 100 Mb/s až po 1 Gb/s. Do kategorie 4G se řadí LTE (Long-term Evolution), avšak nejedná se o synonyma. Rychlost LTE značně závisí na operátorovi, ale také na vzdálenosti od vysílače a přenosové rychlosti dosahují rozmezí od 100 Mb/s až 300 Mb/s. Roky 2019 a 2020 se nesou ve znamení nástupu nové technologie, která dle všeho změní svět. Jedná se o 5. generaci bezdrátové telefonní technologie (5G). Výjimečností této technologie je vysoká přenosová rychlost, která dosahuje od 50 Mb/s až k 2 Gb/s, ale také minimální latence, která by měla činit pouhých

8-12 milisekund. Latence je doba mezi udáním pokynu a reakcí na daný pokyn. Právě díky takto nízké latenci se mluví o přelomové technologii zejména pro zařízení IoT, konkrétněji například pro autonomní řízení vozů, či pro robotickou chirurgii [50][51].

Mobilní signál je typem rádiové komunikace a samozřejmě i on smí pracovat pouze na některých frekvencích. Nejen že s přicházejícími generacemi bezdrátové telefonní technologie se podporovaná frekvenční pásma měnila, ale také pomyslný seznam podporovaných pásem je odlišný pro různé oblasti. Například telefony dovezené z USA, či Číny mohou podporovat pouze některá, nebo dokonce nemusí podporovat žádná frekvenční pásma v České republice.

Pásma v České republice jsou:

- Band 1 s frekvencí 2,1 GHz technologiemi LTE a UMTS
- Band 3 s frekvencí 1,8 GHz a technologiemi GSM a LTE
- Band 7 s frekvencí 2,6 GHz a technologiemi LTE
- Band 8 s frekvencí 900 MHz a technologiemi GSM a LTE
- Band 20 s frekvencí 800 MHz a technologiemi LTE [52][53].

S příchodem 5G se projednává uvolnění nových pásem pro tuto technologii. Zatím se uvažuje o uvolnění pásem 700 MHz, 3,5 GHz a 42 GHz [54].

4.5 Aplikační protokoly

Aplikační protokol je na vrcholku TPC (Transmission Control Protocol) vrstvy. Aplikační protokol využívá TPC jako transportní vrstvu pro specifickou aplikační komunikaci [8].

4.5.1 MQTT

Protokol MQTT (Message Queuing Telemetry Transport) je založený společností IBM a jedná se o protokol pro předávání zpráv pomocí centrálního bodu, takzvaného brokeru. Přenos informací probíhá pomocí TPC (Transmission Control Protocol), což je nejvyužívanější protokol transportní vrstvy OSI modelu internetové sítě a využívá návrhového vzoru publisher – subscriber (vydavatel a odběratel). Tento

protokol je vytvořený snazší komunikací mezi více zařízeními. Základním kamenem je broker, někdy také přímo označovaný jako server. Ten přijímá (subscribe) všechny informace a také je vysílá (publish) do dalších zařízení. Snazší je uvědomit si jeho výhody při vzájemném propojení více zařízení. V situaci bez využití brokeru musí uživatel komunikovat se zařízeními či skupinou zařízení zvlášť [8][55].

Při využití MQTT protokolu a brokera tedy dochází k sjednocování zpráv od koncových zařízení do brokeru, ten následně informace může odeslat do databáze a jednomu, či více odběratelům. Každý uživatel tedy komunikuje pouze s brokerem, který následně komunikuje s koncovými zařízeními. Důležité je také porozumění, kdo je vydavatel (publischer) a kdo je odběratel. Například senzorická zařízení jsou pouze vydavatelé, kteří vysílají získané informace z okolí. Některá zařízení mohou být vydavatelé i odběratelé zároveň, kdy odebírají různé instrukce a vysílají informace o svém stavu. MQTT také nabízí možnost jakýchsi témat. Tématem může například být teplota v místnosti, kdy teplotní senzor vysílá informace o aktuální teplotě do tohoto tématu a ovladač topení a klimatizace se přihlásí k jeho odběru, kdy pro vysoké teploty se spustí chlazení pomocí klimatizace, zatím co pro nízké se sepne topení [55].

Zabezpečení a identifikace uživatelů probíhá prvotním přihlášením uživatele pomocí jeho ID, či přihlašovacím jménem a heslem, nebo také uživatelským certifikátem. Zabezpečení komunikace poskytuje kryptografický protokol TLS (Transport Layer Security) a také lze nastavit různé úrovně šifrování dle MQTT protokolu pro TPC kanály. Kanál 1883 slouží pro nešifrovaný přenos informací. 8883 je pro šifrovaný přenos pomocí TLS a 8884 je opět šifrovaný přenos pomocí TLS, který ovšem navíc vyžaduje certifikát o autenticitě.

Protokol MQTT je nejužívanějším komunikačním protokolem IoT. Existuje také typ protokolu MQTT-SN, který vychází z MQTT a je primárně určen pro komunikaci se sítí senzorů. Tento protokol pracuje na UDP (User Datagram Protocol), který je označován v porovnání s TCP, jako protokol bez garance doručení. Tento prvek je důležitý právě pro komunikaci s nízko příkonovými zařízeními, jako jsou senzory, u kterých možná ztrát není brána jako chyba [8][55].

4.5.2 CoAP

Protokol CoAP (Constrained Application Protocol), neboli omezený aplikační protokol, je vytvořený pro zařízení a sítě omezené na zdroje. Tento protokol je uzpůsoben pro použití M2M (Machine to machine) komunikace zařízení. Vychází z konceptu HTTP (Hypertext Transfer Protocol), což je internetový protokol určený pro komunikaci s WWW servery a přenos hypertextových dokumentů ve formátech HTML, XML a dalších. CoAP pracuje na principu žádost/odezva (request/response) stejně jako HTTP, ale s nižším objemem dat a na rozdíl od HTTP, CoAP pracuje na transportní vrstvě UDP. Protokol využívá client-server model a nabízí podporu REST (Representational State Transfer) příkazů, jako jsou GET, POST, PUT a DELETE. Protokol CoAP také podporuje asynchronní komunikaci pomocí zpráv [8].

4.5.3 AMQP

Protokol rozšířených frontových zpráv (Advance Message Queuing Protocol) je dalším často využívaným protokolem zpráv pro IoT. Tento protokol podporuje obousměrnou komunikaci a operuje na protokolu TPC a zajišťuje spolehlivé doručení zpráv. AMQP dokáže také komunikovat s různými druhy programovacích jazyků [8].

4.6 Struktura IoT

Internet věcí je úzce spjat se zařízeními. Každé zařízení kolem nás má do budoucna potenciál pro připojení k internetu a sdílení dat získaných pomocí senzorů, či ovládání zařízení a sdílení informací o jejich stavu. Co však by mělo takové zařízení, integrované do oblasti zařízení IoT, mělo splňovat? Každé IoT zařízení obsahuje mikrokontrolér, což je jednočipový počítač, či integrovaný obvod. Nutností jsou prvky potřebné pro napájení, ovládání zařízení a téměř vždy tato zařízení obsahují paměťový čip, integrovaný procesor, často také síťový port, zařízení mohou mít také malý operační systém Linux, který umožňuje jejich správu. Součástí jsou i IO prvky (vstupy a výstupy). Nutností pro IoT zařízení je podpora určitého komunikačního standardu, a to ať se jedná propojení pomocí Ethernet kabelu, či bezdrátovou technologií jako jsou Wi-Fi, Bluetooth, ZigBee, Z-Wave, LoRaWan

a mnoho dalších. IoT zařízení musí tedy podporovat alespoň jeden takový komunikační standard, ale některá zařízení dokáží podporovat hned několik těchto standardů. Při budování IoT sítí je důležité vždy ověřit vzájemnou kompatibilitu zařízení. Výrobci zařízení internetu věcí u každého zařízení ve specifikacích produktu uvádí typy podporované komunikační standardy a často pro snazší orientaci uvádí také loga těchto standardů. Pro připojení nového zařízení IoT do systému probíhá mnoha způsoby. Některá zařízení podporují usnadňující párování pomocí NFC, či RFID tagů, nebo také pomocí QR kódů. Pro všechna zařízení však platí, že musí být v zapnutém stavu a v párovacím módu. Konfigurace jiných zařízení, než centrálních jednotek již probíhá přes centrální jednotky. Funkce zařízení jsou udávána pomocí jejich senzorů a aktuátory [8].

4.6.1 Aktuátory

Jedná se o takzvané vykonavače akce. Přesněji jsou fyzickou vrstvou zařízení. Dokáží pohybovat se zařízením, vydávat zvuk, světlo, či odemykat a zamykat dveře a měnit tak prostředí. Tyto aktuátory lze dělit do tří kategorií na elektrické, hydraulické a pneumatické. Pneumatické využívají stlačeného vzduchu, hydraulické kapaliny a elektrické energie [8].

4.6.2 Senzory

Senzorem je zařízení, které slouží jako informační prvek na detekci událostí a změn v jeho prostředí. Získávají informace, které jsou pro uživatele nebo pro celý systém důležité. Tato zařízení obsahují čidla, ta vnímají své okolí a dle své funkce z něj získávají data. Může se jednat například o senzory pohybu, senzory teploty, nebo také o senzor vlhkosti [8].

4.7 Architektura IoT

Běžnější typem architektury je 3 vrstvá architektura skládající se z:

- Application layer – aplikační vrstvy
- Network layer – síťové vrstvy
- Perception layer – vnímací vrstvy

Vnímací vrstva je fyzickou vrstvou, která obsahuje senzory pro získávání informací z okolí. Síťová vrstva je odpovědná za propojování chytrých zařízení, síťových zařízení a k serveru. Tato vrstva je také využívaná k přenosu a zpracování dat ze senzorů. Třetí vrstvou je aplikační vrstva, která je zodpovědná za doručování konkrétních aplikačních služeb uživateli. Definuje různé aplikace, ve kterých může být internet věcí nasazen, například inteligentní domy, inteligentní města a inteligentní zdraví.

Třívrstvá architektura je základním kamenem pro internet věcí, ale nedostatečná pro výzkum. Proto existují vícevrstvé architektury. Jednou z nich je pěti vrstvá architektura, která se skládá z:

- Business layer – obchodní vrstva
- Application layer – aplikační vrstva
- Processing layer – procesní vrstva
- Transport layer – transportní vrstva
- Perception layer – vnímací vrstva

V porovnání s 3vrstvou architekturou jsou tedy tři nové vrstvy, nahrazující původní síťovou vrstvu. Obchodní vrstva řídí celý systém internetu věcí včetně aplikací, obchodních a ziskových modelů uživatelů. Procesní vrstva také známa jako takzvané middleware. Ukládá, analyzuje a zpracovává obrovské množství dat, která pocházejí z transportní vrstvy. Může spravovat a poskytovat rozmanitou sadu služeb pro spodní vrstvy. Využívá mnoho technologií, jako jsou databáze, cloudová úložiště a velké moduly pro zpracování dat. Poslední novou vrstvou je transportní vrstva, která přenáší data senzorů, prostřednictvím bezdrátových sítí, jako jsou 3G, LAN, Bluetooth, RFID a NFC, z vrstvy vnímání do vrstvy procesní a naopak.

V poslední době se přechází k takzvanému mlhovému zpracování (Fog computing), kde senzory a síťové brány provádějí část zpracování a analýzy dat. Mlhová architektura představuje vrstvený přístup, který vkládá monitorovací vrstvu, před vrstvy procesní, ukládací a také přidává bezpečnostní vrstvu mezi vrstvu fyzickou a transportní. Monitorovací vrstva monitoruje výkon, zdroje, odpovědi a služby. Předběžná procesní vrstva provádí filtrování, zpracování a analýzu dat ze senzorů. Vrstva dočasného úložiště poskytuje funkce úložiště, jako je replikace, distribuce

a ukládání dat. Nakonec bezpečnostní vrstva provádí šifrování a dešifrování a zajišťuje integritu dat a soukromí. Monitorování a předzpracování se provádí na okraji sítě před odesláním dat do cloudového úložiště [56].

4.7.1 Brány (Gateways)

Důležitým prvkem IoT systémů jsou takzvané brány, které slouží k vzájemnému propojení jinak nekompatibilním sítím, či protokolům a poskytují připojení na internet. Příkladem je například připojení několika senzorů k bráně pomocí protokolů jako jsou ZigBee, či Z-Wave, které nejsou schopny komunikovat přímo s internetem. Brána přeloží příchozí data na IP data, které mohou být poslány na internet. Brána může být využita také jako firewall a ochraňovat tak zařízení před škodlivými útoky.

Smart Gateway (chytrá brána) je typem brány, která má své vlastní lokální úložiště a zabudovanou aplikaci, která provádí analýzu dat odesílaných z připojených zařízení. Tyto brány se také označují jako edge brány (Edge Gateways). Použití těchto bran u IoT systémů se nazývá také mlhovým výpočtem (Fog computing), který znatelně redukuje síťový provoz a zvyšuje efektivitu při zpracování základních dat v reálném čase. Bránou může být i chytrý telefon, který se spojí se zařízením pomocí Bluetooth protokolu a následně může zpracovat data nebo je odesílat například pomocí mobilní sítě [8][56].

4.7.2 Zařízení pro tvorbu prototypů

Velké společnosti na výrobu zařízení IoT vyrábí své vlastní minipočítače, které distribuují již jako hotová zařízení, nebo je prodávají svým odběratelů, kteří zařízení zkompletují. Nicméně většinou neumožňují prodej konkrétních čipů, či součástek pro běžné uživatele, kteří by si chtěli vytvořit svá vlastní zařízení. Pro tyto uživatele se vyrábí řada minipočítačů, které slouží zejména pro tvorbu prototypů IoT zařízení. Mezi známé se řadí Arduino, Rasberry Pi, AMD Gizmo Board, BeagleBone, Intel Galileo a mnoho dalších. Tyto minipočítače jsou, zjednodušeně řečeno, základové desky, na které lze nahrát operační systém a které je možné připojit k senzorům a aktuátorům. Tyto minipočítače se řadí mezi IoT zařízení a lze je připojit některým chytrým domácnostem, či různým IoT sítím [8].

5 Chytré domácnosti

5.1 Úvod do chytrých domácností

Chytré domácnosti jsou jednou z několika aplikací konceptu IoT, kam se řadí také chytré zemědělství, chytrá města, průmysl 4.0 a další [57].

V chytrých domácnostech je využíváno zařízení IoT k vytvoření uceleného snadno ovladatelného systému, zohledňujícího tři důležité aspekty:

- Úspora
- Komfort
- Zabezpečení

Chytré domácnosti mohou dosahovat různého stupně vybavení, kdy domácnost lze označit za chytrou, pokud obsahuje navzájem komunikující chytrá zařízení. S větším počtem zařízení v síti chytré domácnosti přibývají možnosti vytváření scénářů automatizace. Automatizace chytré domácnosti umožňuje ovládání zařízení bez nutnosti pokynu uživatele, tedy automaticky. Automatizace vychází z webového nástroje IFTTT (If This Than This), neboli pokud se něco stane, pak něco udělej. V rámci chytrých domácností automatizaci tvoří různé scénáře. Jedná se o sled pokynů pro některá zařízení domácnosti. Tyto scénáře mohou být triviální a zahrnovat pouze ovládání jediného zařízení, ale také se může jednat o velice složité scénáře, které zpracováním informací získaných od dalších zařízení nepřetržitě nastavují odpovídající nastavení. Častým scénářem chytrých domácností je scénář, který se spustí ve chvíli, kdy opustí poslední osoba domácnost. Například se zhasnou světla, spustí senzory pohybu a třeba se také aktivuje zabezpečení alarmem [58][59][60].

Zabezpečení domácností může nabývat dvou forem. První formou jsou fyzická zařízení, která slouží pro uživatele dané domácnosti. Do této kategorie se řadí zejména chytré zámky dveří, či oken, ale také senzory kouře, či vody, kdy právě senzory dokáží včasně upozornit nebo zcela zamezit možnému nebezpečí. Druhou formou je zabezpečení systému proti vnějším útokům. Tato část je závislá na zvoleném systému chytré domácnosti a zabezpečení každého IoT zařízení

připojeného do chytré domácnosti. Existuje mnoho výrobců chytrých zařízení a s tím přichází i mnoho způsobů implementace ochrany u daných zařízení. Pro bezpečnost celé domácnosti je nutné používat zařízení aktualizovaná na nejnovější firmware, neboť s technologickým vývojem se mohou vyskytovat nové mezery v zabezpečení, jež mohou aktualizace eliminovat. Pokud v síti zařízení chytré domácnosti se nachází nezabezpečené zařízení, pak útočníkům stačí jediný útok na takové zařízení a pomoci ním ovládnout celou domácnost. Zabezpečení mohou snižovat také snadno odhalitelné přihlašovací údaje k internetovým účtům chytrých domácností nebo k Wi-Fi routerům. V neposlední řadě může zabezpečení domácnosti ohrozit používání nelicencovaných IoT zařízení. Některé systémy chytrých domácností omezují možnosti připojení zařízení, které nedisponují konkrétními licencemi [61][62].

5.2 Historie

Počátkem chytré domácnosti se dá považovat rok 1957, kdy společnost Disney společně se společností Monsanto Plastic Company představili v Tomorowlandu koncept domu budoucnosti. Přesněji se jednalo o vizi bydlení v roce 1987 a tento koncept se nazýval „Monsanto Home of the Future“ a mezi futuristické prvky této domácnosti se řadila například automatická myčka nádobí, elektrické ovládání skřínek, a dokonce i centrální ovládání pro klimatizaci v domě. Vynálezci se zaměřili na technologie domácí automatizace a roku 1966 byl vyvinut první inteligentní automatizační systém Echo IV. Toto zařízení umožnilo spotřebitelům vytvářet počítačové nákupní seznamy, regulovat teplotu domu a zapínat a vypínat zařízení. Kuchyňský počítač byl vytvořen v roce 1969 a mohl vytvářet recepty, ale díky své ceně se zařízení nikdy nestalo komerčně úspěšné [63].

Postupný vývoj mikrokontroléru v roce 1971 vyústil ve snížení cen elektronických zařízení, čímž se technologie staly dostupnější. Dalším významným milníkem je rok 1984, kdy americká národní asociace stavitelů domů („National Assotiation of Home Builders“) uznala termín „smart home“ pro dům vybavený moderními elektrickými zařízeními. Jako zajímavost lze také uvést, že právě tento rok byl v Americe považován, po technologické stránce, za přelomový, neboť společnost Apple představila svůj první osobní počítač Macintosh [63].

K historii chytré domácnosti lze také přiřadit rok 1991 a takzvanou Gerontechnologii, která kombinuje gerontologii (nauka o starých lidech) s technologií a usnadňuje život seniorů. V této době vznikají první komunikační bezdrátové standardy. Na přelomu 2. tisíciletí začala popularita domácí automatizace rychle stoupat a chytré domy se najednou staly dostupnější alternativou, a tedy životaschopnou technologií pro spotřebitele. Na pultech obchodů se začaly objevovat moderní technologie, domácí sítě a další zařízení [64].

Paralelně probíhá také vývoj internetu věcí. Se vstupem do nového tisíciletí již lze chytré domácnosti a internet věcí považovat za dvě navzájem propojená témata. Technologie chytrých domů a domácnosti je jednou z nejrychleji rostoucí technologií ve stavebnictví. Z hlediska zastoupení společností na trhu zařízení pro chytré domácnosti byly pro rok 2018 nejoblíbenější společností Amazon, na druhém místě byla společnost Google a na třetím místě společnost Samsung [65].

V roce 2019 bylo celosvětově prodáno 814,8 milionů zařízení chytré domácnosti, přičemž téměř 42 % zařízení bylo pro multimédia, více než 19 % tvořila zařízení pro monitoring a zabezpečení, 16,5 % byly zastoupeny chytré reproduktory a zbylých 22,5 % zařízení z kategorie ostatní. Z dané studie vychází i prognóza pro rok 2023, která říká, že počet zařízení chytrých domácností dosáhne počtu 1 396 miliónů. U produktů se očekává vyrovnanější rozložení, kdy multimédia budou zastoupena 30 %, monitoring a zabezpečení 22 %, chytré reproduktory 14,3 % a ostatní chytrá zařízení budou tvořit 33,7 % [66].

5.3 Budování chytré domácnosti

Existuje mnoho způsobů, jak chytrou domácnost zařídit. Při výběru daného způsobu vždy hraje roli mnoho faktorů, jako jsou například rozměry dané domácnosti, nebo také jestli se jedná o implementaci chytré domácnosti do již postaveného domu, či bytu, nebo jestli se jedná o zakomponovanou chytrou domácnost do stavebního plánu před započetím stavby [67].

5.3.1 Elektroinstalace

V případě stavby nového domu je nutné dopředu rozhodnout, jestli má být daný dům v budoucnu chytrým domem, nebo ne. Domy, u kterých se očekává zařízení chytré domácnosti, nemusí být po dostavení rovnou chytrými domy. Rozdíl je zejména v elektroinstalacích. Pro elektroinstalace použité v obyčejných bytech se používá termín konvenční elektroinstalace, zatímco v komplexních chytrých domech se jedná o systémovou elektroinstalaci, někdy také označovanou za inteligentní. Rozdíl v elektroinstalacích je v pouhém doplnění rozvodů o další kabely v závislosti na použití topologie systémové elektroinstalace. Náklady na systémovou elektroinstalaci jsou přibližně o 20 až 45 % vyšší než na konvenční, v závislosti na poskytovateli instalace. Použití systémové elektroinstalace samo o sobě ještě netvoří chytrou domácnost, ale umožňuje mnohonásobně levnější její pozdější implementaci. Dokud nebude tato systémová elektroinstalace vybavená o chytré prvky, nebude mít řídící jednotku a další zařízení, pak její ovládání bude stejné, jako u konvenční. Systémové elektroinstalace se dělí na centralizované a decentralizované. Někdy se však využívá elektroinstalace hybridní, která využívá oba typy systémových instalací [68][69][70].

5.3.1.1 Centralizovaná systémová elektroinstalace

Tato systémová instalace je specifická svou hierarchií. Každý vypínač, různé snímače, kamery a termostaty, prostě každý prvek systému má svedené kabely do centrální řídící jednotky, která má elektronické spínače pro každý okruh zvlášť. Řídící jednotka je připojená k internetu v zásadě pomocí Ethernet kabelu a již je standardem bezdrátové ovládání domácnosti pomocí aplikace v tabletu, nebo v chytrém telefonu. Topologie centralizované elektroinstalace může být do hvězdy, která je nejstabilnější, ovšem nejnáročnější po stránce kabelové. Další topologie je například stromová topologie [71].

5.3.1.2 Decentralizovaná systémová elektroinstalace

Decentralizovaná systémová instalace se používá spíše u nemovitostí s užitnou plochou větší než 600 m^2. Při porovnání s centralizovanou instalací je zásadní přidání rozložení prvku sběrnic, kde pro každý okruh, jako jsou vypínače, světla,

termostaty a další části, existuje jedna sběrnice. Do takové sběrnice jsou zapojeny všechny spínače z daného okruhu a z toho důvodu lze v jeden okamžik ovládat vždy maximálně jedním spínačem jedno světlo. Výhodou oproti centralizované instalaci je omezení kabeláže, a naopak nevýhodou je nutnost použití systémový tlačítek KNX, která jsou o poznání dražší než tlačítka konvenční, která lze použít u typu hvězda. Nicméně tlačítka standardu KNX mají garantovanou zpětnou kompatibilitu i pro následující roky. Topologie decentralizované jsou například liniové, lineární anebo kruhové topologie [71].

5.3.1.3 Konvenční elektroinstalace

V případě implementace chytré domácnosti do bytů, či již postavených domů bez systémové elektroinstalace, pak je nutné využít jiných chytrých zařízení pro danou domácnost. Kompletní předělání rozvodů elektroinstalace na systémovou je velice nákladné a doporučuje se provádět pouze v situacích, kdy je stávající elektroinstalace nevhodná. Mezi nevýhody chytré domácnosti vybudované bez systémové elektroinstalace patří nutnost každé zařízení připojit ke zdroji energie, a to ať do elektrické zásuvky, kdy onu moderní domácnost ohyzdí nevzhledné kabely, nebo zařízení disponuje vlastní baterií, kterou je ale nutné u mnoha zařízení dobíjet, či vyměňovat. Další nevýhodou je horší míra zabezpečení, kdy na rozdíl od systémových elektroinstalací kde je vše řízeno přes centrální jednotku, či komunikační sběrnici, jenž jsou zabezpečeny a aktualizovat firmware stačí provádět u jediného zařízení, zatím co u zařízení připojených bezdrátově je nutné hlídat aktualizace pro každé zařízení. Také kvalita a spolehlivost přenosu je lepší u systémové chytré domácnosti a v neposlední řadě je cena každého zařízení, zejména kvůli podpoře bezdrátového přenosu dat, znatelně vyšší. Naopak velikou výhodou u bezdrátové chytré domácnosti je jednoduché připojení nových chytrých zařízení, které často zvládne uživatel domácnosti sám. Právě u systémů se systémovou elektroinstalací je implementace nového zařízení mnohdy tak náročná, že se neobejde bez přizvání specializovaného technika [69].

5.4 Systémy chytrých domácností

Systémy pro chytré domácnost vyvíjí mnoho společností. Nejčastěji využívanou společností na českém trhu je společnost Loxone se stejnojmenným systémem chytré domácnosti.

5.4.1 Loxone

Společnost Loxone byla založena v Rakousku v roce 2008 Thomasem Moserem. Tato společnost nabízí vytvoření chytré domácnosti na míru založenou na vlastním operačním systému Loxone. Technologie pro podporu systému Loxone je otevřenou technologií, která je pravidelně aktualizována. Loxone nabízí možnost výběru z velkého množství produktů, které mohou být také kompatibilní i s jinými společnostmi. Důležitým prvkem speciálně od této společnosti je miniserver Loxone. Do tohoto prvku jsou svedená všechna zařízení chytré domácnosti pomocí systémové centralizované elektroinstalace. V případě potřeby do systému implementovat bezdrátové zařízené komunikující na standardu Bluetooth, ZigBee, Z-Wave, či jiných, pak je nutné použít speciální přijímač podporující daný standart a který je pomocí kabelů sveden do minserveru. Výhody tohoto systému jsou stabilita, minimální náklady, mimo těch počátečních, a propracovaný systém, který nabízí strojové učení a navrhuje uživateli začlenění určitých scénářů, které odpovídají jeho dosavadní rutině. Specialitou Loxone je také jejich tlačítkový standard, který lze zakomponovat do tlačítek na zdi, ale také do kuchyňské linky, nebo do sprchy. Tento standard tlačítek využívá čtvercové plochy s pěti body dotyku.

Obr. 6 Logo Loxone
Zdroj: [72]

Loxone nenabízí svého hlasového asistenta, ale nabízí otevřené uživatelské rozhraní a s použitím vhodných rozšiřujících zařízení a osobní naprogramováním podpory lze v k tomuto systému připojit i asistenty Google Assistant, Amazon Alexa i Siri. Toto zpřístupnění podpory i jiných zařízení však společnost Loxone nenabízí a musí tedy tento úkon vykonat uživatel sám, či s přizváním odborného technika [72].

5.4.2 TaHoma®

TaHoma® je systém chytré domácnosti od společnosti Somfy. Jedná se o společnost, která vznikla v roce 1969 a v té době byla specializovanou na předokenní rolety a markýzy. Od roku 1997 implementovala do svých rolet rádiové zařízení pro dálkové ovládání. Po odkoupení firmy Domis v roce 2001 se již Somfy začíná starat o ovládání prvků domácnosti, a to od garážových vrat, přes bezpečnostní senzory až po světla a stává se tak firmou specializující se na chytré domácnosti. V roce 2007 vytváří alianci se společností Velux a zároveň představují komunikační protokol io-homecontrol. Od roku 2010 došlo k podpoře cloudového úložiště a komunikaci s PC, mobilním telefonem, či tabletem pomocí speciální aplikace. Od té doby až dodnes zaznamenává tato společnost meziroční růst a postupně skupuje a vytváří společenství s dalšími značkami z oblasti produktů chytré domácnosti.

Systém TaHoma® je složen z řídící jednotky a dalších zařízení, která se k této jednotce připojují pomocí bezdrátových rádiových standardů, mezi které patří io-homecontrol, Somfy RTS, EnOcean, ZigBee a Z-Wave. Řídící jednotka vyžaduje kabelové připojení do elektrické sítě a k pomocí ethernet kabelu k internetu. Také nabízí USB port, který slouží pro párování některých zařízení. Systém je také kompatibilní s hlasovými asistenty Amazon Alexa a Google Assistant. Společnost Somfy plánuje do budoucna možnou integraci Apple HomeKit zařízení a hlasového asistenta Siri [73].

5.4.3 Apple HomeKit

Také společnost Apple nabízí svou verzi systému pro chytrou domácnost. Tento systém se nazývá Apple HomeKit a jedná se o plnohodnotný systém chytré domácnosti, který je schopen nabídnout stejné možnosti ovládání, jako výše zmíněné systémy. Je však ve spoustu aspektech odlišný.

Apple nabízí jedinečně propracovanou komunikaci svých produktů. Tyto produkty vytváří takzvaný ekosystém Apple. Zásadním rozdílem je sortiment produktů. Zatímco společnosti Loxone, či Somfy nabízí vlastní sortiment zařízení, který dokáže pokrýt veškeré potřeby při zařizování chytré domácnosti, a ještě k tomu podporují

možnost implementace kompatibilních zařízení třetích stran, tak Apple nabízí pouze základní zařízení k ovládání chytré domácnosti a ostatní zařízení pochází od výrobců třetích stran. Právě v podpoře výrobků se nachází další rozdíl. Ostatní společnosti umožňují připojení zařízení dle podpory komunikačních protokolů, jako jsou Bluetooth, ZigBee, Z-Wave a další, ale Apple umožňuje připojení pouze těch zařízení, které jsou certifikované licencí Works with Apple HomeKit. Pro získání této licence musí zařízení splnit minimální požadavky zadané společností Apple. Každé licencované zařízení má na spodu speciální logo „Works with Apple HomeKit“ společně s identifikačním číslem a QR kódem zařízení [74].

Obr. 7 Logo certifikace pro Apple HomeKit
Zdroj: [74]

Pro zařízení chytré domácnosti od společnosti Apple je potřeba těchto zařízení:

- Wi-Fi router
- Řídící jednotku
- Chytré zařízení pro ovládání domácnosti

Nejsou definované žádné nároky na Wi-Fi routery, pouze doporučení, které varuje uživatele, že v případě nízké rychlosti internetového připojení, či využívání routeru s nízkým výkonem, může systém HomeKit pracovat pomaleji [75][76].

Řídící jednotkou může být jakékoliv zařízení od společnosti Apple s aplikací Domácnost. Nutností pro provoz systému je, aby řídící jednotka byla připojená k lokální síti domácnosti v zapnutém stavu. Z tohoto důvodu je řídící jednotkou nejčastěji využíváno Apple TV připojené do sítě ethernet kabelem a podporou probuzení po síti (Wake On Lan – WOL), pro úsporu energie. Pro ovládání domácnosti je možné využít zařízení pouze od společnosti Apple, konkrétně iPhone (telefon), iPad (tablet), MacBook (notebook), Apple Watch (hodinky), iMac (PC), či iPod (multimediální zařízení) a dané zařízení musí mít přístup k internetu. Zařízení pro ovládání domácnosti a řídící jednotka může být totéž zařízení.

Apple HomeKit podporuje komunikační protokoly Bluetooth LE (Bluetooth Low Power) a IP (Internet Protocol). Pro připojení zařízení, které nepodporuje ani jeden z uvedených standardů je nutné využít komunikační hub, který daný standard podporuje. Takový hub musí splňovat certifikaci Works with Apple HomeKit a umožňuje připojení více zařízení do systému domácnosti.

Stejně, jako předchozí systémy i Apple HomeKit podporuje virtuálního asistenta s názvem Siri, kterou je možné ovládat pomocí jakéhokoliv zařízení z aktuálního sortimentu společnosti Apple [75].

5.4.4 Microsoft HomeOS

Projekt vývoje systému chytré domácnosti započala společnost Microsoft v roce 2010 a ani o deset let později nebyl projekt dokončen a vydán pro veřejnost. V současné době Microsoft uvádí jedenácti členný tým, který pracuje na tomto projektu. Během posledních let však projektu nevykazuje pro veřejnost žádnou aktivitu. Tento systém z hlediska pevné základny na poli operačních systémů počítačů, kde tvoří většinové zastoupení, může být silným konkurentem do budoucna pro ostatní systémy chytrých domácností [77].

5.5 Virtuální asistenti

5.5.1 Amazon – Alexa

Virtuální asistentka Alexa byla představena v roce 2014 jako součást zařízení Amazon Echo. Tato asistentka je kompatibilní s operační systémy Android i iOS a dokáže rozpoznat významy vět v různých jazycích. Hlasová aktivace spouští tuto asistentku oslovením „Alexo“, či „Alexa“. Samotný asistent ještě nenabízí podporu češtiny. Amazon plánuje uvedení češtiny mezi podporované jazyky, ale prozatím neurčil žádné konkrétní datum. Firma Amazon aktuálně figuruje jako společnost s největším počtem chytrých zařízení a díky tomu je i Alexa nejvyužívanější virtuální asistentka [78][79][80].

5.5.2 Google – Google Assistant

Google Assistant byl představen v roce 2016 společně s chytrým reproduktorem Google Home. Tento asistent vychází z prvního virtuálního asistenta Google Now, který vyšel v roce 2012. Google Assistant je dostupný na každém chytrém telefonu s operačním systémem Android 6.0 a novější. Hlasová aktivace asistenta proběhne vyslovením „Ok Google“. Google již v průběhu roku 2018 slíbil podporu českého jazyka do konce roku 2018, ale ani v roce 2020 tato podpora nedorazila. Prozatím však Google Assistant dokáže v češtině přijmout jasné povely, u kterých nemusí rozhodovat o složitějším významu vět [78][80].

5.5.3 Microsoft – Cortana

Momentálně nejhorším virtuálním asistentem, v porovnání asistentů Cortana, Siri, Alexa a Google Assistant, je dle několika testů asistent Cortana od společnosti Microsoft. Cortana se nachází na mobilních telefonech s operačním systémem Windows Phone 8.1 a novějším, herních konzolích Xbox a největší zastoupení má Cortana na osobních počítačích, neboť je součástí operačního systému Windows 10. Cortanu lze aktivovat pomocí příkazu „Hey Cortana“ nebo lze nastavit aktivační příkaz dle přání uživatele [81][82][83].

5.5.4 Apple – Siri

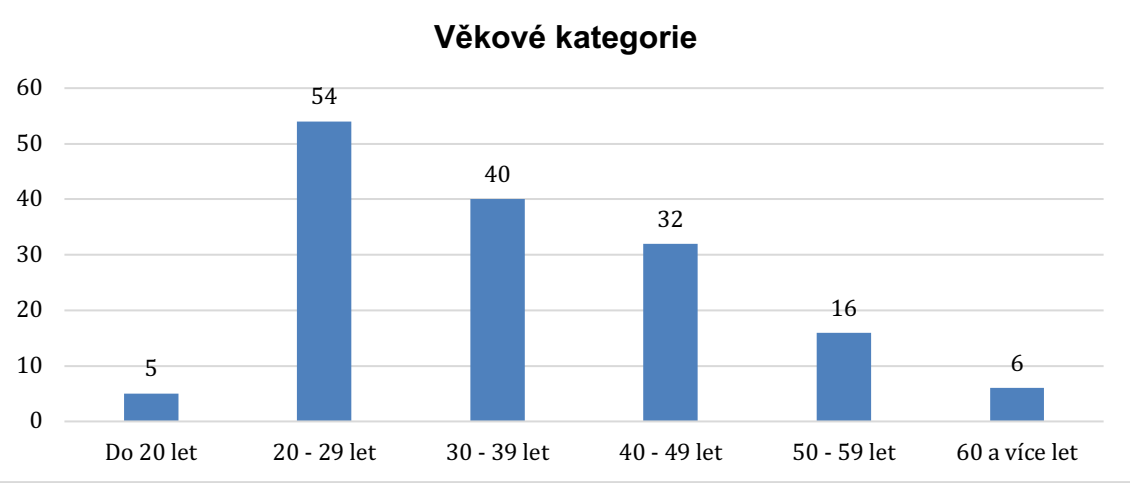
Tato virtuální asistentka je dostupná pouze na zařízeních Apple. Jedná se o asistentku představenou v roce 2010 a je zároveň nejstarší z této čtveřice virtuálních asistentů. Hlasová aktivace probíhá vyslovením „Hey Siri“. Prvním zařízením, které podporovala Siri byl iPhone 4s. Siri je velice oblíbenou virtuální asistentkou, která dokáže porozumět i složitějším příkazům k ovládání chytrého zařízení, či celé domácnosti. Nevýhodou Siri, zejména pro české uživatele, je prozatímní absence podpory českého jazyka [78][84].

6 Dotazníkové šetření

Dotazníkové šetření vychází z dat získaných v období od ledna do dubna roku 2020. Sběr dat probíhal online formou a celkem se výzkumu zúčastnilo 153 respondentů, přičemž 128 odpovědělo skrze odkaz ze sociálních sítí a zbylých 25 respondentů reagovalo na přímo adresovaný odkaz. Výsledky jsou zpracovány do grafů a doplněny o slovní komentáře.

6.1 Výsledky dotazníkového šetření

Ze 153 respondentů jsou muži zastoupeni z více než dvou třetin. Největší zastoupení má věková kategorie od 20 do 29 let s 54 respondenty. Více než čtvrtina všech respondentů odpovídá kategorii mezi 30 a 39 léty. Třetí nejpočetnější kategorií jsou respondenti ve věkovém rozmezí od 40 do 49 let, kteří jsou zastoupeni 21 hlasy. Padesátníci čítají 16 hlasů tedy 10,5 % a zbývající dvě kategorie, do 20 let a starší 60 let, dosahují obě méně než 4 %, respektive 5 a 6 hlasů. Nejčastěji zastoupeným typem respondenta je muž žijící v bytě ve městě s více než 150 000 obyvateli a při omezení výběru pouze na ženy jsou nejpočetnější skupinou respondentky bydlící v domě na vesnici.

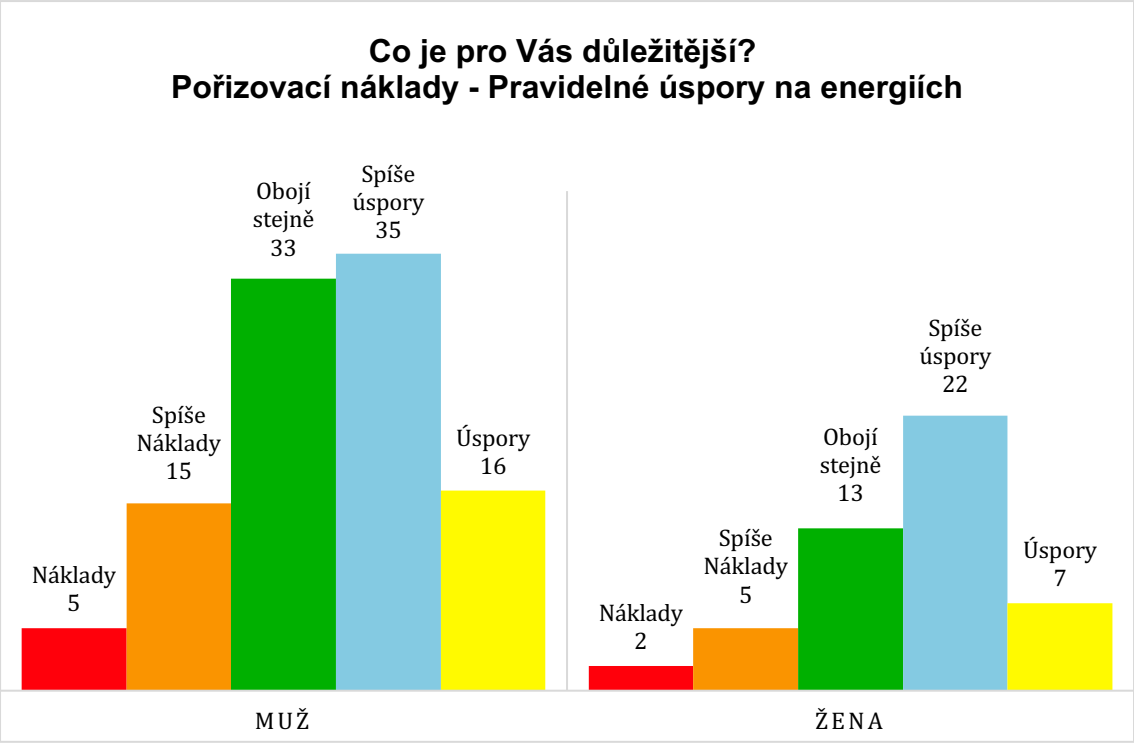


Obr. 8 Graf rozložení věkových kategorií
Zdroj: Vlastní zpracování

Na otázku, zdali je Vaše domácnost chytrá, odpovědělo kladně 37,9 % respondentů. Tedy již více než jedna třetina z dotazovaných mají chytrou domácnost. Tento fakt

do jisté míry značí, že v dnešní době bydlet v chytré domácnosti ještě není zcela přirozené, ale již to lze označit za běžné.

Z následujících tří grafů je možné zjistit velice zajímavé informace. První graf znázorňuje preference respondentů při výběru mezi výší pořizovacích nákladů na chytrou domácnost a výší pravidelných úspor na energiích dosažených díky zavedení chytré domácnosti. Z grafu je patrné, že pro muže i ženy je důležitějším aspektem úspora na energiích. V případě této otázky odpověděli muži i ženy velice podobně, kdy extrémní varianty zvolili maximálně s 1,5 % odchylkou a celkově se pro úspory více přikláněly ženy. Zajímavostí je také fakt značící dobrou představu o této problematice, neboť muži bydlící v chytré domácnosti odpovídali téměř totožně, jako uživatelé, kteří chytrou domácností nedisponují.

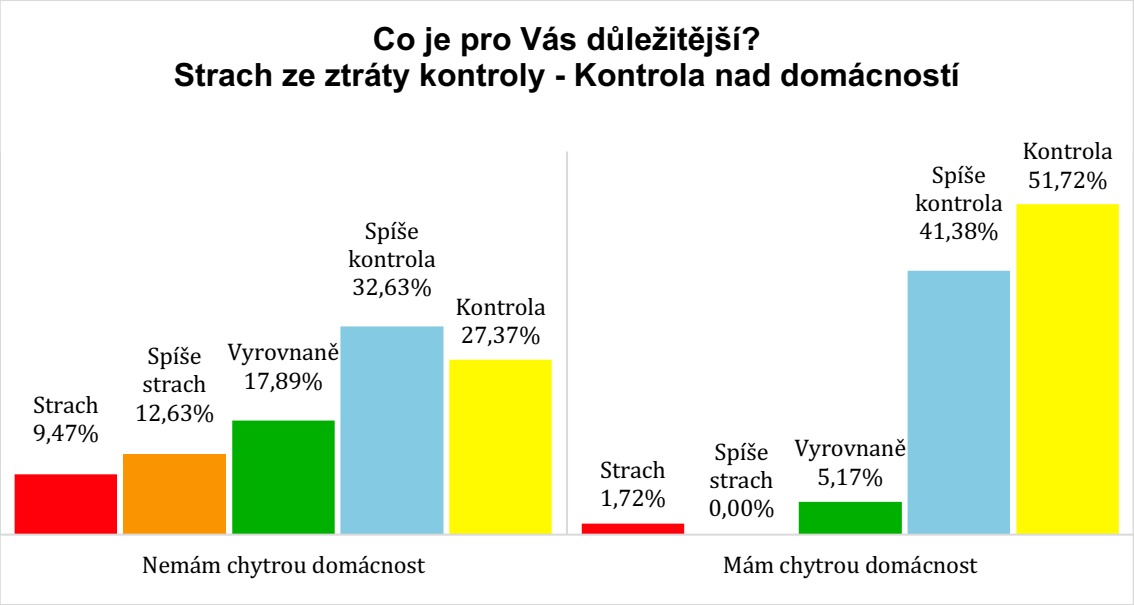


Obr. 9 Graf preferencí mezi náklady a úspory
Zdroj: Vlastní zpracování

Ve druhém srovnávacím grafu, který zjišťuje závislosti strachu ze ztráty kontroly nad informacemi dané domácnosti a jejím ovládáním, vůči kontrole nad domácností, kterou díky systému chytré domácnosti můžou vzdáleně sledovat, či ji ovládat. Ačkoliv respondenti při odpovídání na tuto otázku obecně inklinovali k možnosti

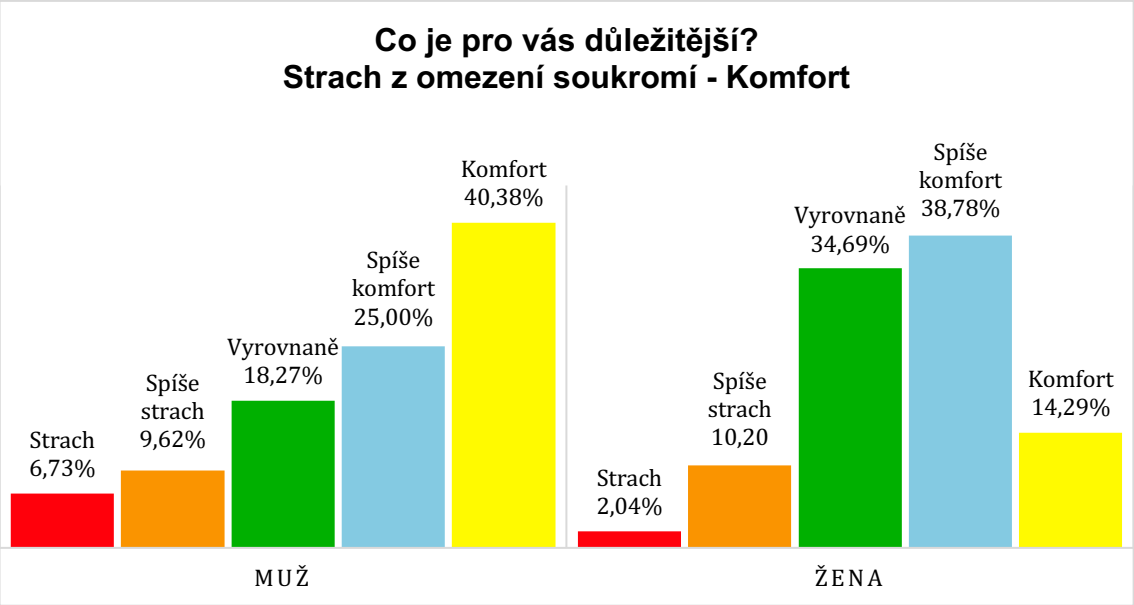
zvýšené kontroly nad domácností. Zřetelněji je vidět, že ti, kteří takovou domácností nedisponují, přeci jen projevují drobné obavy ohledně kontroly domácnosti, zatímco respondenti s chytrou domácností prakticky strach ze ztráty kontroly nemají, kdy převládající strach nad kontrolou pociťuje jediný z 58 respondentů, kteří vlastní chytrou domácnost, a naopak v této skupině se celkem 93,1 % respondentů přiklání ke větší kontrole domácnosti nad strachem ze ztráty této kontroly, například při napadení hackerem.

Z dat také vyplývá, že se nejvíce bojí ztráty kontroly ženy ve věku mezi 20 a 29 lety, a naopak nejmenší strach mají muži ve věkové kategorii od 30 do 39 let.



Obr. 10 Graf preferencí mezi strachem a kontrolou
Ztroj: Vlastní zpracování

Třetí graf znázorňuje vztah mezi strachem z omezení soukromí a komfortem, který chytrá domácnost nabízí. Zvolil jsem také porovnání mezi pohlavím respondentů. Muži celkově nemají strach z omezení soukromí, přičemž jejich nejčastější odpovědí byla „komfort“ a druhou nejčastější volba byla „spíše komfort“, jenž dohromady tvořily 65,38 % dotazníků od mužských respondentů, a naopak u pouhých 16,35 % mužů převládal faktor strachu nad komfortem. Na rozdíl od mužů, ženy volily opatrněji. Nicméně i u nich znatelně převládá komfort nad strachem z omezení soukromí.



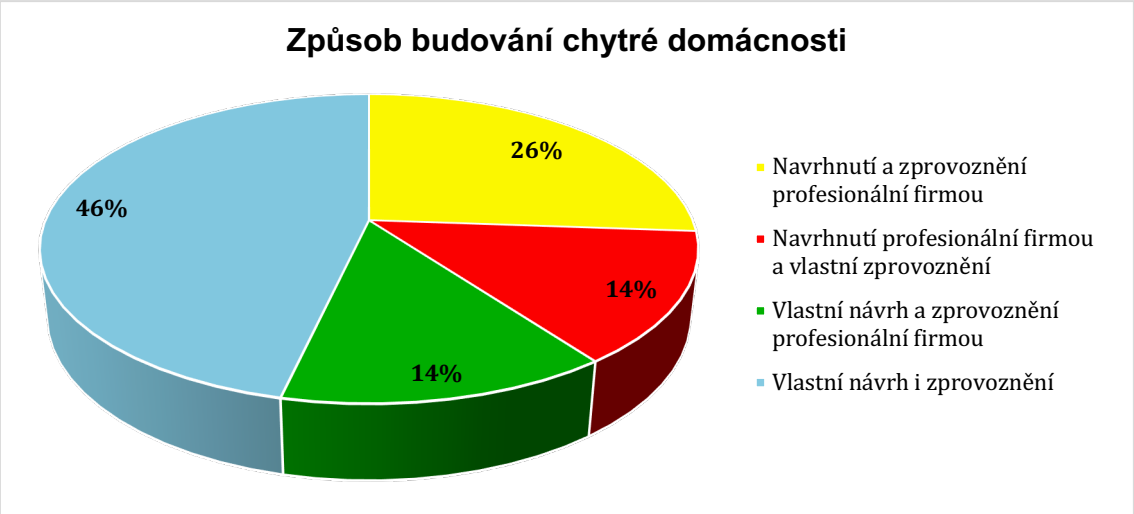
Obr. 11 Graf preferencí mezi strachem z omezení soukromí a komfortem
Zdroj: Vlastní zpracování

Pokud bychom se podívali na získaná data rozřazená dle věkových kategorií, tak největší strach je patrný u respondentů z kategorie od 50 do 59 let, a naopak velice nízký strach z omezení soukromí projevují respondenti do 39 let.

Další otázka směřovala na způsob budování chytré domácnosti. Ze 153 respondentů by 71 zvolilo vlastní návrh i zprovoznění. To prokazuje zejména nízký strach z moderních technologií, a i jakýmsi technologickým sebevědomím těchto respondentů. Profesionální firmu by o spolupráci požádalo 56 % tedy 82 dotazovaných, přičemž 21 z nich by využilo pouze návrhu od dané firmy a zprovoznění by již prováděli sami. Stejný počet dotazovaných by naopak zvolilo vlastní návrh a zprovoznění pomocí specializované firmy a nakonec 40 respondentů by využilo jak na návrh, tak i na zprovoznění firmu specializující se na chytré domácnosti.

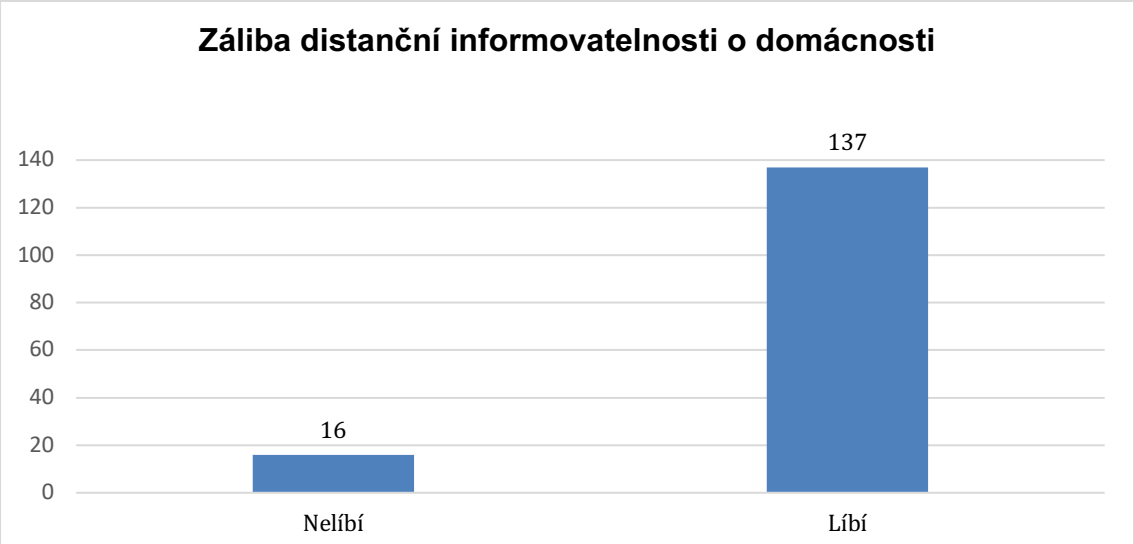
Z hlediska pohlaví se však odpovědi znatelně liší. Muži, kteří tvoří 68 % respondentů, nejčastěji zvolili možnost vlastního návrhu i implementace, přičemž se k této variantě přikláněl0 58 % mužů. 20 % mužů by využilo vždy pouze jedné služby od specializované firmy, ať návrh, či implementaci a nakonec 22 % mužů by využilo i návrhu i zprovoznění od odborné firmy. Za to nejčastější volbou žen bylo právě kompletní využití firmy, kdy tuto možnosti zvolilo 36 % žen. Naopak vlastní

implementaci i zprovoznění vybralo nejméně žen, konkrétně 20 %. Částečné zprovoznění firmou vybralo dohromady 44 % žen, přesněji shodně po 22 % pro každou z variant částečné výpomoci od specializované firmy.



Obr. 12 Graf způsobu budování chytré domácnosti
Zdroj: Vlastní zpracování

Z dat také vyplývá, že téměř 90 % respondentů by se líbilo, kdyby měli informace o své domácnosti, i když by se nacházeli mimo ni. Odpovědi respondentů jsou přibližně stejné nehledě na pohlaví, věku, bydlišti, či velikosti domácnosti.



Obr. 13 Graf obliby distanční informovatelnosti
Zdroj: Vlastní zpracování

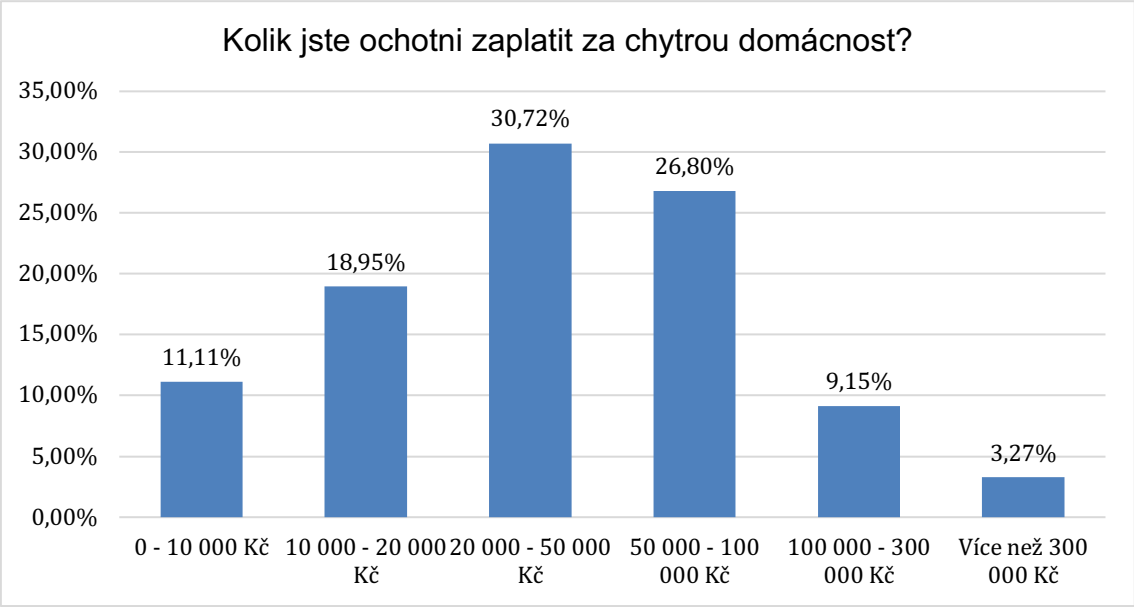
V tomto dotazníkovém šetření více než jedna čtvrtina, přesněji 28,76 %, respondentů odpověděla, že neví, či nevěděla o možnosti ovládání chytré domácnosti pomocí scénářů. Tato funkce vytváří samo o sobě podstatu chytré domácnosti, kdy bez této funkce by se dala domácnost nazývat pouze domácností s moderními zařízeními a univerzálním ovládačem v podobě chytrého telefonu, či tabletu.

Obr. 14 Graf znalosti funkce scénářů
Zdroj: Vlastní zpracování

Při volbě zařízení, která by neměla chybět v chytré domácnosti zvolilo 82 % respondentů světla a zařízení na ovládání teploty. 102 tedy rovné dvě třetiny dotazovaných vybralo senzory pohybu, kouře či záplavové senzory. Taktéž dvě třetiny respondentů vybraly rolety k oknům jako zařízení, která by neměla chybět v chytré domácnosti. Zabezpečující zařízení však zvolilo podstatně méně respondentů. Čidla otevřených dveří, či oken 59 % dotazovaných, kamery pouhých 50 %, zámky dveří 49 % a uzávěry vody, či plynu 46 %, přitom právě tyto prvky jsou mnohdy velice důležité pro vzdálenou správu chytré domácnosti a její zabezpečení.

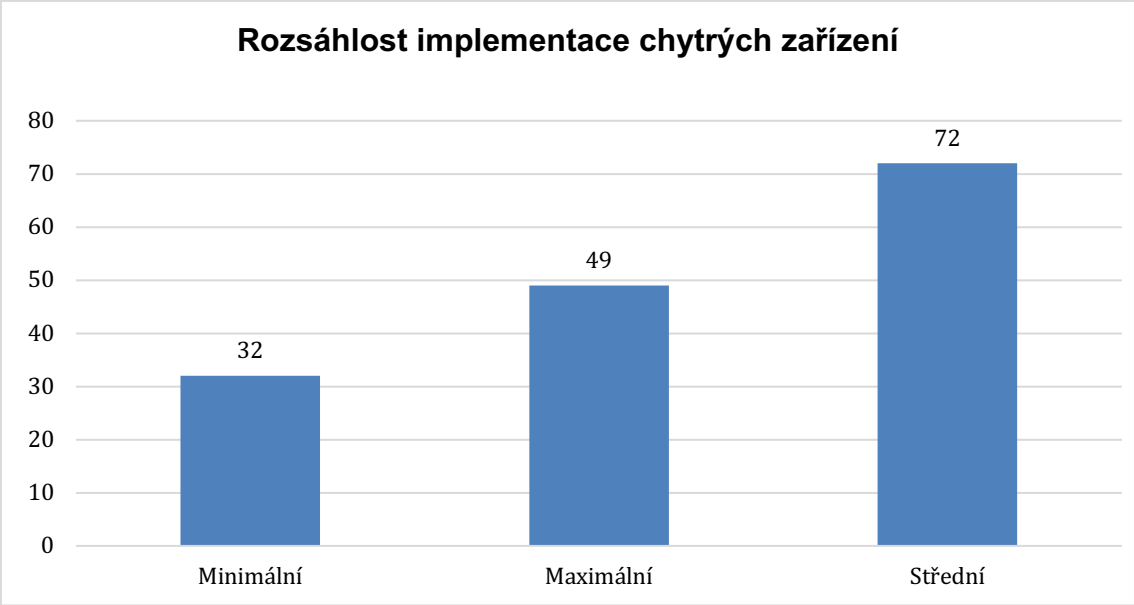
Poslední dva grafy znázorňují představu, či ochotu respondentů utratit za pořízení chytré domácnosti a rozsáhlost implementace chytrých zařízení do domácnosti. Nejvíce, konkrétně 47 respondentů odpovědělo, že na chytrou domácnost jsou ochotní vynaložit od 20 000 Kč do 50 000 Kč. Na druhém místě je rozmezí

od 50 000 Kč do 100 000 Kč, kterou zvolilo 41 dotazovaných a 29 tázaných by zaplatilo peněžní částku v rozmezí od 10 000 Kč do 20 000 Kč. Pouhých 19 respondentů by bylo ochotno zaplatit více než 100 000 Kč, přičemž jen 5 z nich by zaplatilo i více než 300 000 Kč. Naopak nic, či do 10 000 Kč by bylo ochotno investovat17 respondentů. Přitom okolo 10 000 Kč se pohybují často pouze samotné řídící jednotky, které jsou nutné pro zařízení chytré domácnosti.



Obr. 15 Graf akceptovatelnosti nákladů na chytrou domácnost
Zdroj: Vlastní zpracování

Z rozsáhlosti implementace domácnosti chytrými zařízeními si respondenti nejvíce, přesněji 47 % z nich vybralo střední implementaci, dále 32 % maximální a 21 % minimální implementaci. V porovnání s částkami, které jsou ochotni dotazovaní vynaložit, rozsáhlost implementace částečně odpovídá, ale je spíše mírně posunutá k nižším částkám. Ačkoliv pro každou domácnost jsou finální náklady, i při použití stejných zařízení, odlišné, tak následující cenové kategorie je možné přibližně přiřadit k rozsáhlosti implementace chytrých zařízení. Na maximální implementaci je většinou nutné vynaložit více než 100 000 Kč. Střední implementace odpovídá nákladům v rozmezí od 20 000 Kč do 100 000 Kč a minimální implementaci je možné zařídit do 20 000 Kč.



Obr. 16 Graf rozsáhlosti implementace chytré domácnosti
Zdroj: Vlastní zpracování

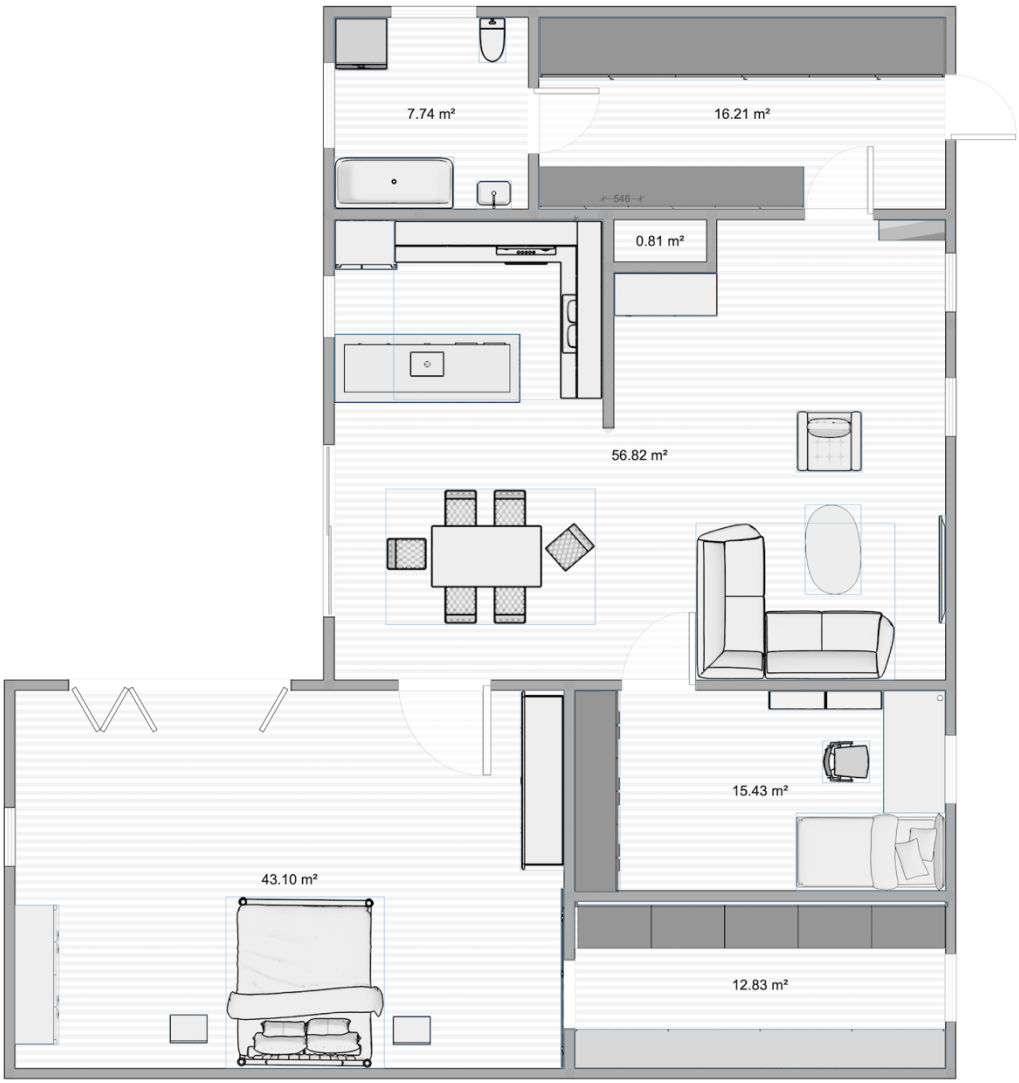
6.2 Shrnutí dotazníkového šetření

Z dat získaných tímto šetřením. Je možné vyvodit, že oblíbenost chytrých domácností stále roste a jejím začlenění se již nebrání většina obyvatel. Dochází tak ke snížení strachu z technologií, které lidé umí ovládat, ale již nutně nemusí rozumět, jak zařízení fungují. Tento fakt je velice pozitivní z hlediska budoucnosti chytrých domácností, avšak může docházet ke snížení bezpečnosti. Právě snížení bezpečnosti vychází v tomto šetření ze skutečnosti, že mnoho dotazovaných by rádo si svou domácnost navrhlo i zprovoznilo, což může vést k zásadnímu vynechání, či špatnému zvolení chytrých zařízení, popřípadě i k nevhodné instalaci. Právě takové domácnosti mohou vykazovat mnoho bezpečnostních nedostatků, které mohou umožňovat snazší vniknutí vnějších útočníků, takzvaných hackerů.

Data také znázorňují rozdíly v představách žen a mužů ohledně chytrých domácností. Ženy jsou v porovnání s muži v oblasti soukromí a bezpečnosti obezřetnější a méně suverénní. U respondentů je také zpozorováno, že ačkoliv by si většina přála zařízení chytré domácnosti, tak jejich cenová představa na náklady je mnohdy nižší, než možná teoretická cena za domácnost s rozsáhlou implementací chytrých zařízení, dle jejich přání.

7 Návrh chytré domácnosti

Pro návrh chytré domácnosti jsem zvolil jednopodlažní dům o velikosti 3+kk a rozměrech 155 m^2. Hlavní vstup vede do předsíně, kde se nachází botníky a skříně na oblečení. Z předsíně lze projít do koupelny a obývacího pokoje. Obývací pokoj je spojen s jídelní částí a s kuchyní, se kterou je částečně oddělen příčkou. V obývacím pokoji jsou dvě okna, lze z něj vstoupit do pracovny, ložnice a prosklenými francouzskými dveřmi na terasu. K ložnici patří také šatna s jedním oknem. I ložnice nabízí velké francouzské dveře na terasu a jedno klasické okno.



Obr. 17 Návrh domu
Zdroj: Vlastní zpracování

7.1 Vybavení domácnosti

a) Zabezpečení

O zabezpečení se starají 4 venkovní kamery, které jsou rozmístěny na rozích domu. K dispozici je také 5. kamera, sloužící pro snímání tváří v oblasti vchodových dveří. Součástí zabezpečení jsou také rolety, které jsou na všech oknech a francouzských dveřích. Hlavní vstup je možné odemknout bezkontaktně z jakéhokoliv místa, kde je připojení k internetu. Záplavový senzor je nainstalován v kuchyni a v koupelně a detektory kouře jsou v obývacím pokoji, ložnici, pracovně a v předsíni. Pro ochranu proti vytopení disponuje domácnost také chytrým centrálním uzávěrem vody.

b) Osvětlení

Osvětlení řeší chytrá světla, která lze ovládat pomocí mobilní aplikace. Venkovní světla, světla v koupelně, šatně, kuchyni a předsíni jsou bílá světla, zatímco v ostatní místnostech disponují světla navíc možností změny barvy.

c) Další prvky

Každý pokoj má svůj senzor teploty, regulátor topení a klimatizaci. Domácnost obsahuje také chytré reproduktory, elektrické zásuvky, detektory pohybu, čidla otevřených dveří a oken a v domácnosti se nachází také její řídící jednotka.

7.2 Apple HomeKit

Důvodem zvolení chytré domácnosti od společnosti Apple je bezpečnost tohoto systému. Do aplikace Domácnost, což je aplikace pro chytrou domácnost od společnosti Apple, lze přidat pouze produkty s certifikací „Works with Apple HomeKit“. Pro licencování touto certifikací musí zařízení splňovat náročné normy. Tento proces licencování trvá okolo 6 měsíců. Pro mnoho uživatelů je však nevýhodou, že tuto chytrou domácnost lze ovládat pouze ze zařízení od společnosti Apple. Na ostatních chytrých telefonech, tabletech a ani na počítačích nelze systém HomeKit, a jeho aplikaci Domácnost, využívat.

7.2.1 Zařízení pro domácnost

a. Zabezpečení

V navržené domácnosti jsem zvolil venkovní kamery Circle 2 od firmy Logitech, které nabízí 180° pozorovací úhel, Full HD kvalitu obrazu, jsou voděodolné umožňují zdarma 24hodinovou zálohu dat a komunikují s chytrou domácností pomocí Wi-Fi na pásmech 2,4 GHz i 5 GHz. Jinou možností byla kamera Smart Outdoor camera od společnosti Netatmo. Ta navíc disponuje osvětlením a identifikací událostí. Bohužel tato kamera je téměř dvakrát dražší než Circle 2, což se mi zdálo nevýhodné. Pátou kamerou sledující prostor hlavních dveří je Ring video doorbell 1. Ta se oproti předchozím kamerám liší v kvalitě obrazu, kdy podporuje pouze HD kvalitu, ale také v možnosti volby napájení buď z elektrické sítě, nebo z baterie. Také nabízí noční vidění, senzor pohybu, mikrofon s reproduktorem a tlačítko pro aktivování zvonku. Tento dveřní zvonek s kamerou však nelze nativně připojit do chytré domácnosti a komunikuje s chytrým zařízením pouze přes svou vlastní aplikaci. Doposud není na českém trhu žádný dveřní zvonek s kamerou, který by bylo možné připojit do aplikace Domácnost. HomeKit podporuje prozatím pouze chytrý zvonek od Holandské firmy Robin, který se ovšem v České republice neprodává a v přepočtu vychází na více než 15 tisíc korun. Nicméně společnost Netatmo již disponuje chytrým dveřním zvonkem s certifikací „Works with Apple HomeKit“, který plánuje uvést na trh v průběhu roku 2020.

U zámků vchodových dveří jsem volil mezi Danalock V3, jehož výhodou je snadná montáž a možnost odemknutí klasickým klíčem v případě vybití telefonu, či baterií v zámku. Další možností byl zámek Nuki Smart Lock 2.0, který umožňuje připojovat další rozšíření v podobě dálkových ovladačů, či číselných panelů pro odemčení zámku, ale právě možnost odemčení obyčejným klíčem nenabízí, což v případě vybití baterií může být fatální. Jako nejlepší chytrý zámek bych označil Reagle Smart Lock, který také komunikuje s aplikací domácnost a nabízí možnosti vzdáleného ovládání, či odemknutí při přiblížení telefonu a také disponuje klávesnicí pro odemknutí zámku pomocí číselného kódu. Nevýhodou tohoto zámku

je nedostupnost na českém trhu a možné objednání pouze od firmy Amazon s dovozem z Ameriky. Celková cena zámku, z důvodu drahého poštovného, vysoce převyšuje ceny předchozích chytrých zámků a z toho důvodu jsem nakonec vybral zámek Danalock V3.

HomeKit podporuje jen velice malé množství rolet, či žaluzií, ke kterým je navíc zapotřebí spojovací brány (Gateway). Na českém trhu se jedná oficiálně pouze o značku VELUX, která však nabízí chytré rolety jen pro střešní okna, a IKEA. Ta však disponuje jen malým sortimentem a nabízí pouze interiérové rolety, které neumožňují absolutní zatmění a ani nijak nepřispívají pro zvýšení bezpečnosti. Společnost Somfy, která se specializuje na chytré domácnosti se systémem TaHoma a zejména na stmívací zařízení oken, prozatím oficiálně neoznámila konektivitu s aplikací Domácnost od firmy Apple, ale toto oznámení se očekává během roku 2020. Právě z důvodu této mezery na trhu existují zařízení jako spínací modul FIBARO. Toto zařízení může být připojeno k libovolné elektrické zásuvce, či ovladači a zapínat/vypínat i ta zařízení, která nepodporují žádný bezdrátový přenos. Tento modul umožňuje připojení klasických bezpečnostních rolet do chytré domácnosti a jeho funkcí je také možnost sledovat spotřebu elektrické energie. Pro zvýšení bezpečnosti a možnosti dosáhnout absolutní tmy jsem zvolil bezpečnostní rolety od firmy Almma, která pro navrženou domácnost na můj dotaz vytvořila kalkulaci na 78 000 Kč. Ta zahrnuje i instalaci a zprovoznění těchto rolet.

Důležitým prvkem zabezpečení jsou také čidla indikující stav otevřených/zavřených dveří, či oken. Do domácnosti jsem vybíral ze senzorů Eve DOOR & WINDOW a FIBARO Door/Window, kdy oba typy senzorů podporují HomeKit. Sentor Eve stojí 949 Kč a senzor Fibaro 1499 Kč, ale senzory Fibaro navíc disponují také indikátorem baterie a senzorem teploty a díky těmto bonusovým prvkům jsem pro navrženou domácnost použil dražší senzory od společnosti Fibaro.

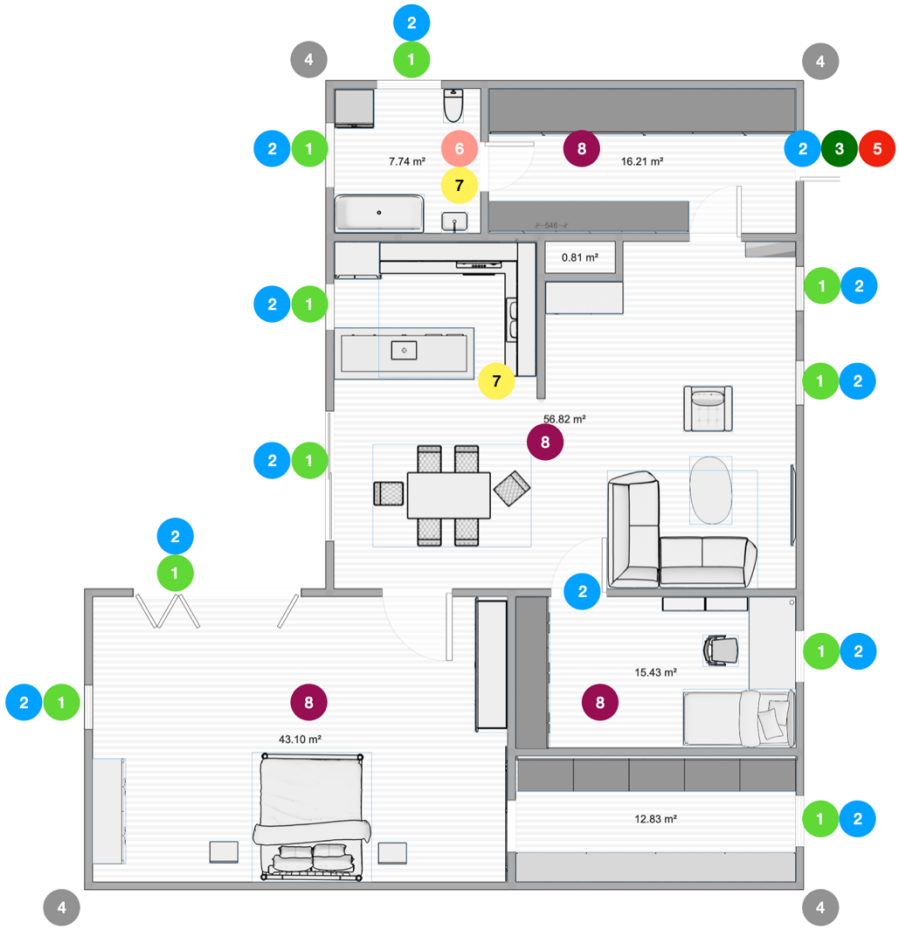
Senzor kouře je prvkem, který je vhodné mít v každé větší místnosti. Chytré detektory kouře podporující Apple HomeKit jsou Netatmo Smart Smoke Alarm a Eve Smoke. Oba detektory jsou vizuálně i funkčně téměř stejné a jediným rozdílem je cena, kdy Netatmo stojí okolo 2500 Kč a Eve stojí přibližně o 500 Kč více. Zvolil

jsem tedy levnější variantu od společnosti Netatmo. Také záplavový senzor disponuje vysokým stupněm užitečnosti. Jeho užitečnost se však odvíjí zejména od skutečnosti, zda domácnost obsahuje nějaký aktuátor, který dokáže vzniklou situaci vyřešit. Mezi záplavové senzorů podporující systém HomeKit sice patří Fibaro Flood senzor a Eve Water Guard, ale bohužel již nedisponují chytrým uzávěrem vody. Uzávěr vody je v mém návrhu uzávěr ventilů eWeLink, ačkoliv tento chytrý uzavírač není kompatibilní se systémem HomeKit a na Apple zařízeních je možné ho ovládat pouze skrze speciální aplikaci. Uzávěr podporuje pouze záplavové čidlo 433MHz Detekce vody a technologii IFTTT. Tedy v případě, že nějaké čidlo zaznamená únik vody, pak uzávěr uzavře přívod vody a podá uživateli skrze aplikaci eWeLink notifikaci.

Tabulka 1 Zařízení pro zabezpečení domácnosti

Číslo	Název	Popis	Cena / Ks	Počet
4	Logitech Circle 2	Venkovní kamera	4489 Kč	4
3	Ring video doorbell 1	Zvonek s kamerou	2799 Kč	1
5	Danalock V3	Zámek dveří	4879 Kč	1
1	Fibaro spínací modul	Reléový spínací modul	1399 Kč	11
2	Fibaro Door/Window	Dveřní/okenní senzor	1499 Kč	13
8	Netatmo Smart Smoke Alarm	Detektor kouře	2499 Kč	4
6	eWeLink uzavírač ventilů	Chytrý uzávěr vody	1699 Kč	1
7	433MHz Detekce vody	Detektor vody	629 Kč	2

Zdroj: Vlastní zpracování



Obr. 18 Rozložení zařízení sloužících k zabezpečení
Zdroj: Vlastní zpracování

b. Osvětlení

Veškeré osvětlení je připojeno k chytré domácnosti s pomocí Philips Hue Bridge. Barevná světla jsem použil v obývacím pokoji ve formě jednoho hlavního světla, 4 žárovek a 2 metry dlouhého led pásku, v ložnici, kde jsou 4 žárovky a 2 m dlouhý led pásek, a v pracovně. Tam jsou instalovány pouze dvě barevné žárovky. Z bílých světel jsou 3 bodová v kuchyni a jedno v koupelně. Nakonec jsem zvolil po jednom bílém světle v šatně, nad jídelním stolem a v předsíni. Světla jsou umístěna také mimo dům, kdy jedno venkovní světlo je u vchodových dveří a dvě jsou na terase. Všechna tato světla jsem vybral díky výborné kompatibilitě s Apple HomeKit přes Philips Hue Bridge, který zaručuje stabilitu a kvalitní provedení. Cena v porovnání se světly jiných značek, než Philips Hue je sice vyšší, ale levnější světla většinou

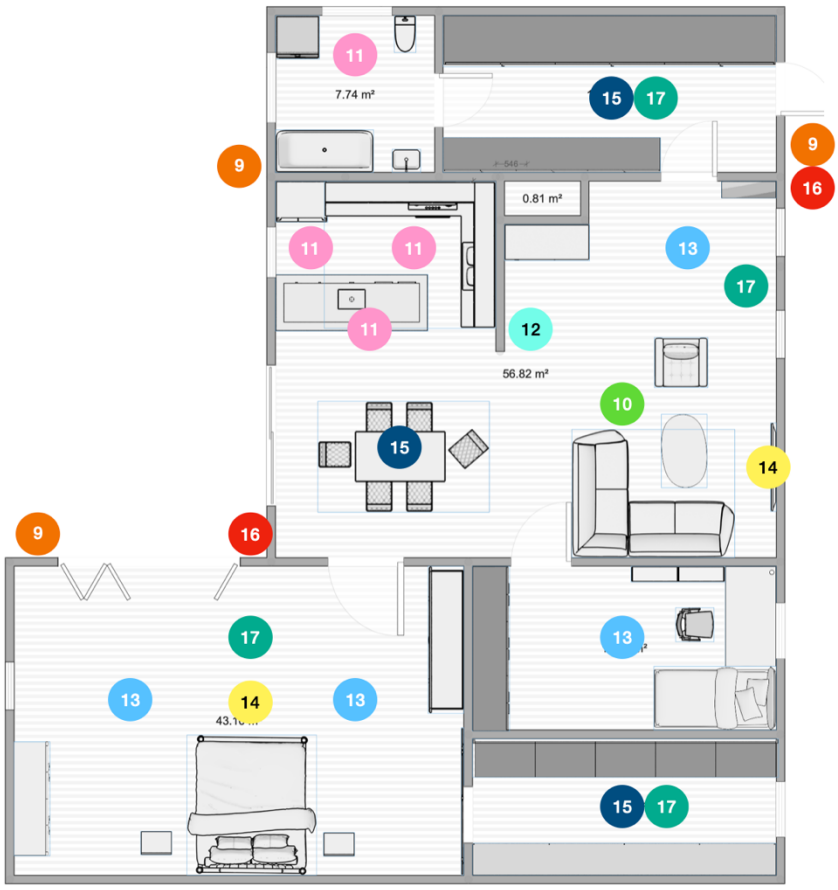
mívají větší poruchovost, či nedokáží komunikovat s chytrou domácností od společnosti Apple. Venkovní světla disponují detektory pohybu. Cena obyčejných senzorů pohybu začíná již na 200 Kč. V případě chytrých senzorů podporujících Apple HomeKit je cena pohybují se v rozmezí od 900 Kč k více než 2000 Kč. Při volbě senzoru jsem vybíral mezi Eve Motion a senzorem Philips Hue ve venkovní verzi a ve verzi vnitřní, které patří z dané kategorie k nejlevnějším. Ačkoliv Eve Motion umožňuje komunikovat přímo s domácností Apple a nevyžaduje žádnou bránu (Gateway), tak navržená domácnost z velké míry využívá technologie Philips Hue, která dokáže snadno komunikovat mezi senzory a světly připojenými ke stejnému zařízení a z toho důvodu jsem vybral od značky Philips i pohybové senzory, a to v obou verzích, kdy venkovní senzory navíc disponují ochranou IP54, tedy základní ochranou proti dešti a povětrnostním podmínkám.

Ceny těchto prvků jsou:

Tabulka 2 Osvětlení domácnosti

Číslo	Název	Popis	Cena / ks	Počet
12	Philips Hue Bridge + 2 barevné žárovky	Set	2399 Kč	1
14	Philips Hue LightStrips Plus	LED pásek – 2 m	2099 Kč	2
13	Philips Hue White and color ambiance (2ks)	Barevné žárovky	2074 Kč	4
11	Philips Hue Milliskin	Bodové světlo	1049 Kč	4
15	Philips Hue White	Bílá žárovka	486 Kč	3
10	Philips Hue Cher	Stropní světlo	5199 Kč	1
9	Philips Hue White Turaco	Venkovní lampa	1799 Kč	3
17	Philips Hue Motion Senzor	Vnitřní senzor	990 Kč	4
16	Philips Hue Outdoor Motion Senzor	Venkovní senzor	1299 Kč	2

Zdroj: Vlastní zpracování



Obr. 19 Osvětlení domácnosti
Zdroj: Vlatní zpracování

c. Další prvky

Pro kontrolu vytápění jsem použil chytré termostatické hlavice. Těchto chytrých hlavic je na trhu větší množství, ale většina z nich nepodporují Apple HomeKit. Mezi kompatibilní zařízení se řadí termo hlavice Eve Thermo, Fibaro Radiator Thermostat a Netatmo thermo hlavice. Ceny uvedených hlavic jsou si velice podobné a pohybují se okolo 2000 Kč. Hlavice Netatmo jsem vyřadil z důvodu nutnosti centrální jednotky sloužící také jako bridge pro propojení s chytrou domácností. Ze zbývajících thermo hlavic jsem zvolil Fibaro Radiator Thermostat, která stejně jako Eve Thermo nabízí přímé spojení s domácností pomocí technologie Bluetooth LE, ale navíc ještě disponuje malým termostatem pro přesnější určení teploty v místnosti. K ovládání teploty v domě je využito také klimatizace. Nejsnadnějším

způsobem zařízení chytré klimatizace do systému HomeKit, je pořízení klasické klimatizace, která pro navržený dům v závislosti na volbě poskytovatele služeb vychází přibližně na 80 tisíc korun a ke každé klimatizační jednotce dokoupit chytrý ovladač klimatizace. Jediný ovladač klimatizace pro Českou republiku s podporou Apple HomeKit je Tado° Smart AC Control. Toto zařízení podporuje infračervené ovládaní, stejně jako ovladač ke klimatizaci, který stačí se zařízením spárovat a ovladač Tado° již bude schopen komunikovat s klimatizací pomocí svého IR ovladače a s chytrou domácností pomocí Wi-Fi. Bonusem tohoto ovladače je také intuitivní dotykové ovládání.

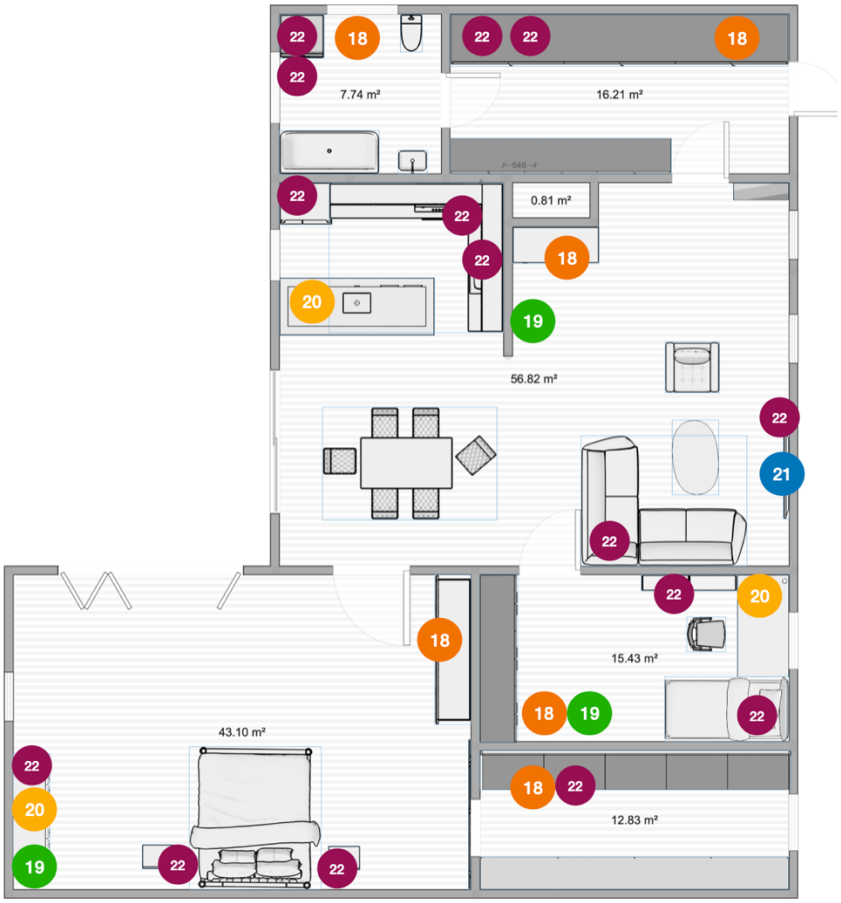
Při interakci s chytrou domácností jsou důležité také reproduktory. Některé reproduktory umožnují připojení přímo do chytré domácnosti, ale zle použít i klasické reproduktory, které jsou připojeny k jinému chytrému zařízení. V navržené domácnosti jsem použil dva reproduktory Apple HomePod. HomePod je pro Apple domácnost více než reproduktor. Kromě produkce kvalitního zvuku může být i hlavní řídící jednotkou domácnosti a také disponuje virtuální asistentkou Siri, kterou je možné kdykoliv aktivovat vyslovením „Hey Siri“ a následně tak ovládat i celou domácnost. HomePody jsem umístil na rozmezí kuchyně a jídelny, do pracovny a do ložnice. V obývacím pokoji je k dispozici soustava reproduktorů, které jsou připojeny k domácnosti přes Apple TV, jenž je v této domácnosti použitá jako hlavní řídící jednotka. Apple TV je připojena pomocí HDMI kabelu k televizi a Ethernet kabelem k internetu. Z chytrých zařízení nakonec použijeme opět spínací modul Fibaro, který vložíme do každé zásuvky v domácnosti a získáme tak možnost spínání těchto zásuvek, ale i přehled o energetickém vytížení každé zásuvky.

Tabulka 3 Ostatní zařízení domácnosti

Číslo	Název	Popis	Cena/Ks	Počet
18	Fibaro Radiator Thermostat	Termo hlavice	1974 Kč	6
19	Tado° Smart AC Control	Chytrý ovladač klimatizace	2599 Kč	3
20	Apple HomePod	Chytrý reproduktor	7999 Kč	3

21	Apple TV 4K	Řídící jednotka domácnosti a multimediální centrum	5190 Kč	1
22	Fibaro spínací modul	Reléový spínací modul	1399 Kč	15

Zdroj: Vlastní zpracování



Obr. 20 Ostatní zařízení domácnosti
Zdroj: Vlastní zpracování

Výsledná cena za pořízení chytré domácnosti pracující na systému Apple HomeKit s použitím uvedených zařízení vychází na 180 977 Kč.

7.3 Loxone

Tento systém stejně jako HomeKit vychází z jedné řídící jednotky. Zde se jedná o Miniserver. Loxone nabízí Miniserver Go, který komunikuje se zařízeními chytré domácnosti pouze bezdrátově, a reléový Miniserver, který navíc umožňuje i připojení pomocí systémové elektroinstalace. Po konzultaci se specialistou

od firmy Loxone jsme utvořili rozvržení chytré domácnosti s použitím zařízení Loxone. V návrhu jsou navíc použity speciální prvky, jako je Loxone tlačítkový standard či multi-room audio systém. Domácnost je založená na systémové elektroinstalaci s reléovým miniserverem. V návrhu nechybí ani barevné osvětlení a různé jeho režimy, pohybové senzory, termostaty, klimatizace, stínění oken, či zvonek s kamerou.

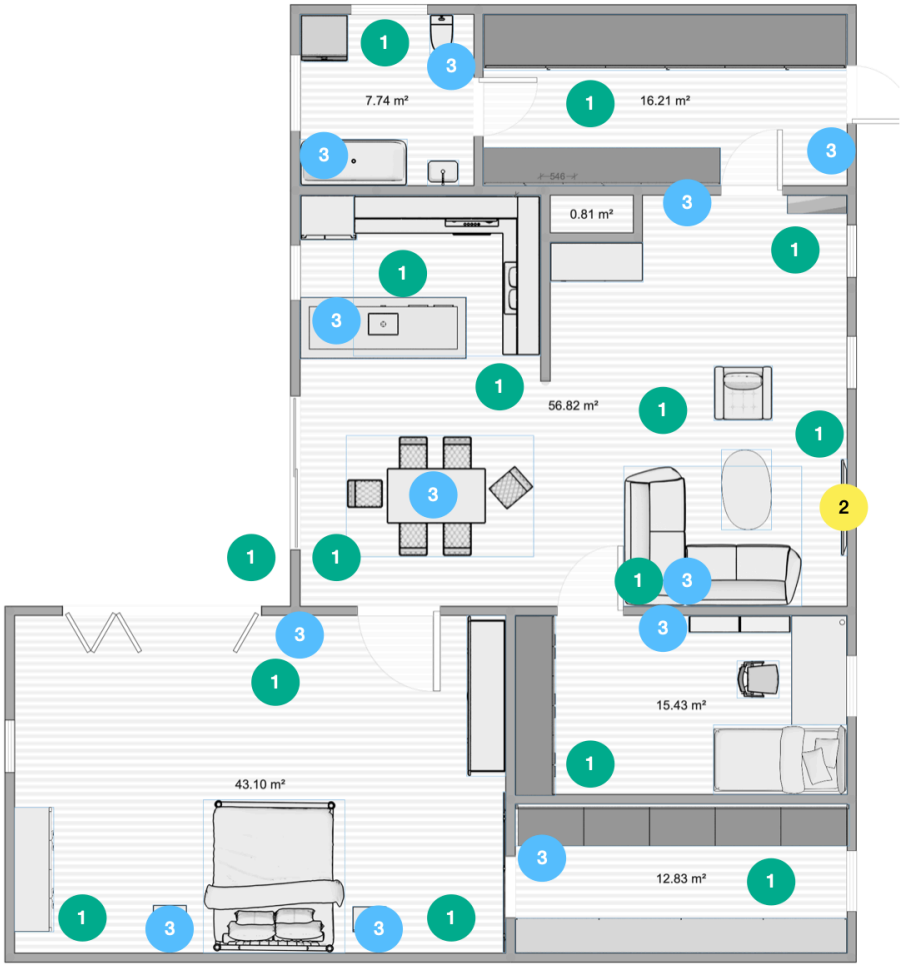
Pro snazší porovnání jsem většinu zařízení usadil na stejné místo v domě, jako u rozvržení domácnosti Apple, jen se jedná o produkty Loxone. V Loxone domácnosti tedy jsou stejně použité senzory otevřených oken, či dveří, ovládání rolet, ale i venkovní kamery, uzávěr přívodu vody, záplavové senzory, detektory kouře, senzory pohybu, interkom, IR ovladače klimatizace, chytré termo hlavice, a i chytré zásuvky. Naopak rozdílné řešení nastalo u audio zařízení, kde není použito přenosných reproduktorů, ale jednoho centrálního Music serveru a k němu připojené vestavěné reproduktory. Ty se nachází po jednom v koupelně, předsíni, šatně a pracovně a na terase. Tři reproduktory jsou v ložnici a v prostoru kuchyně a jídelny a na závěr čtyři reproduktory v obývacím pokoji. Tento Music server dokáže v jeden okamžik přehrávat v různých částí domu různé písničky a využívat i různá média najednou. Osvětlení domu je doplněné o navigační LED pásky sloužící pro navigaci ve tmě, které jsou použity po celém domě. A celá domácnost navíc disponuje tlačítkovým standardem, jenž umožňuje jednoduché ovládání domácnosti. Tento standard se nachází ve formách jako klasický vypínač na zdi. Je ale také zabudovaný do kuchyňské linky, kde mu neuškodí ani rozžhavený hrnec a rovněž je vestavěný do stěny u vany v koupelně. Standard je tvořen pěti dotykovými body, kterými lze ovládat světla, stínění oken a i hudbu. Loxone si také zakládá na důkladných a přehledných statistikách o spotřebě energií v domácnosti.

Velikou nevýhodou je absence podpory virtuálního hlasového asistenta. Protože je Loxone otevřenou technologií, již je možné dohledat neoficiální návody pro úpravu systému a zaimplementováním virtuálních asistentů, jako jsou Siri, Alexa, či Google Assistant. V případě pořizování domácnosti u firmy Loxone a implementací pomocí odborných zaměstnanců této firmy, však zřízení daného virtuálního asistenta prozatím není možné.

Tabulka 4 Odlišné prvky u domácnosti Loxone

Číslo	Produkt	Počet
1	Vestavěný reproduktor	15
2	Multi-audio server	1
3	Tlačítkový standard	12

Zdroj: Vlastní zpracování



Obr. 21 Odlišné prvky u domácnosti Loxone
Zdroj: Vlastní zpracování

Celkové náklady na navrženou chytrou domácnost vyčíslil pracovník firmy Loxone na 260 000 Kč.

8 Shrnutí výsledků

Oba systémy chytrých domácností, ať Loxone, či Apple HomeKit, jsou schopny nabídnout plně vybavenou chytrou domácnost. Obě společnosti však cílí na odlišné skupiny uživatelů. Systém Loxone cílí na zákazníky, kteří mají rádi moderní technologie, vyžadují kompletní řešení, ale nemají čas na zjišťování dalších informací o technologiích, které chytré domácnosti nabízí. Tedy cílí na zákazníky, kteří využijí služeb Loxone, návrh i implementaci nechají na specializovaných technicích a obdrží chytrou domácnost jako hotový produkt. Tento produkt bude správně nastaven, ale v případě rozšíření o další zařízení bude zapotřebí opět technik firmy Loxone. Naopak HomeKit cílí na uživatele, kteří již vlastní zařízení Apple, ať už chytrý telefon, tablet, či počítač. Tedy na uživatele, kteří jsou s produkty Apple spokojeni a věří této firmě ohledně zabezpečení a postupně chtějí rozšiřovat svou domácnost o chytrá zařízení.

Cenové náklady na zřízení těchto chytrých domácností se pro navržený dům liší o téměř 80 tisíc korun. Znatelný rozdíl ceny tvoří zejména integrace systémové elektroinstalace pro systém Loxone. Ovládání pomocí aplikace mají oba systémy velice přehledné a snadné. Pokud však uživatel momentálně nedisponuje zařízením s danou aplikací, pak se ovládání liší. Loxone nabízí panely s tlačítkovým standardem, které jsou rozmístěny ve všech pokojích, ale umožňují pouze ovládání světel, rolet a hudby. Systém HomeKit sice nabízí ovládání v každém pokoji pouze pomocí fyzických tlačítek s jedinou funkcí (například zapínaní světla), ale domácnost lze ovládat i přes chytrý reproduktor Apple HomePod pomocí virtuální asistentky. Pokud je zařízení HomePod v místnosti, lze snadno aktivovat virtuální asistentku Siri vyřknutím „Hey Siri“ a následně příkazem v anglickém, či jiném podporovaném jazyce dát jasné instrukce, co se má stát. Pomocí virtuálního asistenta lze ovládat veškerá zařízení v domácnosti, nebo se jen dotazovat na jejich aktuální stav.

Dle mého názoru právě absence virtuálního hlasového asistenta pro systém Loxone a náročnost rozšíření o další produkty nejvíce odlišuje sympatie uživatelů k daným systémům.

9 Závěry a doporučení

Ačkoliv chytré domácnosti poskytují komfort, míru bezpečí i úsporu na energiích a uživatelům těchto domácností tím přináší mnoho pozitiv, je také nutností disponovat jistou mírou potřebných vědomostí a schopností, bez kterých by mohlo docházet k nevhodným reakcím chytrých zařízení.

U chytrých domácností je důležité využívat kvalitní zařízení, která nabízí dobrou konektivitu s jinými zařízeními a disponují zabezpečujícími prvky. Tyto zařízení jsou však mnohdy dražší než zařízení nižší kvality, která sice nabízejí stejné funkce, ale mohou obsahovat nebezpečné bezpečnostní mezery, které se mohou stát oknem do celé domácnosti pro počítačové útočníky.

Pro zařízení chytrých domácností je tedy možné využít specializovaných firmem, jako je například firma Loxone, či jiné firmy. Taková chytrá domácnost sice pravděpodobně bude dražší, než při samostatném budování bez firmy, ale velice pravděpodobně bude disponovat všemi důležitými prvky a bude dostatečně zabezpečená.

Pokud se však uživatel rozhodne zařídit domácnost sám, tak se nabízí další možnosti. Bezpečnější možností je využití speciálních systémů, které umožňují připojení pouze omezené množině zařízení a nepodporují tak každé zařízení komunikující určitým komunikačním standardem, ale vyžadují také určité certifikace. Takovým systémem je například Apple HomeKit, který lze označit za bezpečný systém, avšak jeho poněkud slabší stránkou je nedostatečný sortiment kompatibilních zařízení.

10 Seznam použité literatury

[1] IoT portál, 2020. *Co je to IoT?* [online]. [cit. 2020-01-27]. Dostupné z: https://www.iot-portal.cz/co-je-iot/

[2] MAAYAN, Gilad David, 2020. *The IoT Rundown For 2020: Stats, Risks, and Solutions*. Security today [online]. [cit. 2020-03-03]. Dostupné z: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=1

[3] MALCOVÁ, Barbora, 24.3.2001. *Maxwellova duha.* MFF UK [online]. [cit. 2020-04-03]. Dostupné z: http://utf.mff.cuni.cz/vyuka/OFY016/F2000/Malcova2.html

[4] Mendelova univerzita v Brně, 2018. *Historie počítačů* [online]. [cit. 2020-01-27]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=20692

[5] STEITZ, Beverley, 2006. *A BRIEF COMPUTER HISTORY* [online]. [cit. 2020-02-18]. Dostupné z: http://people.bu.edu/baws/brief%20computer%20history.html

[6] ANDREWS, Evan, 2019. *Who Invented the Internet?.* A&E Television Networks [online]. [cit. 2020-02-13]. Dostupné z: https://www.history.com/news/who-invented-the-internet

[7] HARWOOD, Trevor, *11.12.2019. Internet of Things (IoT) Histor.* Postscapes [online]. [cit. 2020-03-01]. Dostupné z: https://www.postscapes.com/iot-history/

[8] BALANI, Naveen, 2015. *Enterprise IoT*. Great Britain: Amazon. 155 s. ISBN 9781535505642.

[9] WU, Yulei, Haojun HUANG, Cheng-xiang WANG a Yi PAN, 2019. *5G-enabled internet of things*. Boca Raton, FL: Taylor & Francis, CRC Press. ISBN 978-0-367-19010-1.

[10] FILKA, Miloslav, 2014. *Kabely a technologie informačního přenosu pro integrovanou výuku VUT a VŠB-TUO.* Brno: VUT [online]. [cit. 2020-03-04]. ISBN: 978-80-214-5063-9. Dostupné z: http://optolab.utko.feec.vutbr.cz/wp-content/uploads/SKRIPTA_14_Kabely-a-technologie-informačn%C3%ADho-přenosu-pro-integrovanou-výuku.pdf

[11] LINKBASIC POLAND. *Jak vybrat počítačovou dvojlinku k výstavbě sítě LAN?.* Linkbasic [online]. [cit. 2020-03-03]. Dostupné z: https://www.linkbasic.eu/cs/jak-vybrat-pocitacovou-dvojlinku-k-vystavbe-site-lan

[12] DOBEŠ, Jakub, 6.2.2019. *WiFi vs LAN – bezdrát vs kabel.* J2D Solution [online]. [cit. 2020-04-03]. Dostupné z: https://www.j2ds.cz/wifi-vs-lan-bezdrat-vs-kabel/

[13] PORTÁŠIK, Tomáš, 2018. *Komerční jednotky pro bezdrátovou komunikaci na krátké vzdálenoti* [online]. Plzeň. Bakalářská práce. Západočeská univerzita v Plzni. Fakulta elektrotechnická [cit. 2020-04-03]. Dostupné z: https://otik.uk.zcu.cz/bitstream/11025/32168/1/BP_Tomas_Portasik.PDF

[14] PETERKA, Jiří, 2015. *Z historie sdělovací techniky* [online]. [cit. 2020-03-03]. Dostupné z: https://www.earchiv.cz/a94/a404c501.php3

[15] MAJER, Dušan, 24.10.2017. *Komunikace od kovového světa přes lasery.* Kosmonautix.cz [online]. [cit. 2020-04-03]. Dostupné z: https://www.kosmonautix.cz/2017/10/komunikace-od-kovoveho-sveta-pres-lasery/

[16] BORDÁCZ, Balázs, 2010. *Dálkové ovládání televizního přijímače* [online]. Brno. Diplomová práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií [cit. 2020-03-16]. Vedoucí práce Jiří HERMANY. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=26991

[17] COMPUTERWORLD, 24.4.2017. *Budou se stroje mezi sebou dorozumívat lidskou řečí?* [online]. [cit. 2020-03-03]. Dostupné z: https://computerworld.cz/internet-a-komunikace/budou-stroje-mezi-sebou-hovorit-lidskou-reci-53834

[18] ČTU, 2018. *Využívání vymezených rádiových kmitočtů* [online]. [cit. 2020-03-15]. Dostupné z: https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu

[19] *KOVAŘÍK, David, 18.12.2011. Bluetooth – modrozub pod drobnohledem.* Mobilizujeme.cz [online]. [cit. 2020-03-05]. Dostupné z: https://mobilizujeme.cz/clanky/bluetooth-modrozub-pod-drobnohledem-vedecke-okenko

[20] ŠKOPEK, Pavel, 24.5.2013. *Techbox: Bluetooth sjednotilo bezdrátovou komunikaci.* 24net [online]. [cit. 2020-02-16]. Dostupné z: https://mobilenet.cz/clanky/techbox-bluetooth-sjednotilo-bezdratovou-komunikaci-12085

[21] KILIÁN, Karel, 20.12.2018. *Bluetooth 5: jaké jsou největší výhody proti starší verzi 4.2?.* SvetAndroida.cz [online]. [cit. 2020-03-05]. Dostupné z: https://www.svetandroida.cz/bluetooth-5/

[22] *HOFFMAN, Chris, 31.1.2019. Bluetooth 5.1: What's New and Why It Matters.How-To Geek* [online]. [cit. 2020-03-05]. Dostupné z: https://www.howtogeek.com/403606/bluetooth-5.1-whats-new-and-why-it-matters/

[23] TILMAN, Maggie, 11.10.2019. *How Apple's U1 chip adds 'amazing' new capabilities to the iPhone. Pocket-lint* [online]. [cit. 2020-04-03]. Dostupné z: https://www.pocket-lint.com/phones/news/apple/149336-how-apple-s-u1-chip-adds-amazing-new-capabilities-to-the-iphone

[24] WOOLLEY, Martin, 6.1.2020. *Bluetooth Core Specification Version 5.2 Feature Overview* [online]. [cit. 2020-04-01]. Dostupné z: https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf

[25] THE Smart Cave, 2019. *Z Wave Vs ZigBee: Which Is Better For Your Smart Home?.* Thesmartcave.com [online]. [cit. 2020-02-18]. Dostupné z: https://thesmartcave.com/z-wave-vs-zigbee-home-automation/

[26] IEEE, 2020. *Technologies & Initiatives* [online]. [cit. 2020-02-15]. Dostupné z: https://standards.ieee.org

[27] *MONÍK, Jakub, 30.10.2017. Co je to vlastně WiFi? Jaké jsou možnosti bezdrátových sítí.* Kvalitní internet [online]. [cit. 2020-03-03]. Dostupné z: https://www.kvalitni-internet.cz/co-je-vlastne-wifi-jake-jsou-moznosti-bezdratovych-siti

[28] Wi-Fi Alliance 2020. *Specifications* [online]. [cit. 2020-03-03]. Dostupné z: https://www.wi-fi.org/discover-wi-fi/specifications

[29] Wi-Fi u nas. *SSID* [online]. [cit. 2020-03-03]. Dostupné z: http://wi-fi.unas.cz/ssid.php

[30] INTERNETEM BEZPEČNĚ, 2018. *Zabezpečení připojení k internetu* [online]. [cit. 2020-02-15]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/navody/router-zabezpeceni-pripojeni-k-internetu/

[31] Wireless Excellence, 2019. *The History of WiFi: 1971 to Today* [online]. [cit. 2020-01-27]. Dostupné z: https://www.cablefree.net/wireless-technology/history-of-wifi-technology/

[32] ELECTRONICS NOTES. *WiGig: IEEE 802.11ad 60GHz Microwave Wi-Fi* [online]. [cit. 2020-04-03]. Dostupné z: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ad-wigig-gigabit-microwave.php

[33] Actiontec Electronics, 2020. *The evolution of WiFi standards: a look at 802.11a/b/g/n/ac* [online]. [cit. 2020-03-17]. Dostupné z: https://www.actiontec.com/wifihelp/evolution-wi-fi-standards-look-802-11abgnac/

[34] TP-Link Technologies, 2020. *Wi-Fi 6* [online]. [cit. 2020-02-16]. Dostupné z: https://www.tp-link.com/cz/wifi6/?utm_medium=select-local

[35] VÁCLAVÍK, Lukáš, 3.10.2018. *Čísla místo písmenek. Wi-Fi sítě mění značení na 4, 5, 6.* [online]. [cit. 2020-03-02]. Dostupné z: https://www.cnews.cz/wi-fi-wifi-cislovani-80211-ac-ax

[36] ITHAVLINA, 2020. *ZigBee.* Ithavlina.cz [online]. [cit. 2020-03-18]. Dostupné z: https://ithavlina.cz/2018/09/16/zigbee/?cli_action=1585568761.579

[37] MILOŠ, Jiří, 2010. *Zpracování signálů v systému ZigBee* [online]. Brno. Diplomová práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. [cit. 2020-03-03]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=26532

[38] Zigbee Alliance, 2020. *What is Zigbee?* [online]. [cit. 2020-03-12]. Dostupné z: https://zigbeealliance.org/solution/zigbee/

[39] AVSystem, 2020. *Simplifying IoT with Sigfox and data orchestration* [online]. [cit. 2020-04-03]. Dostupné z: https://www.avsystem.com/static/avssite/files/brochure/Simplifying_IoT_with_Sigfox.pdf

[40] Silicon Laboratories, 2020. *Safer, smarter homes start with Z-Wave* [online]. [cit. 2020-03-18]. Dostupné z: https://www.z-wave.com

[41] Z-Wave Alliance, 2020. *About Z-Wave Technology* [online]. [cit. 2020-03-13]. Dostupné z: https://z-wavealliance.org/about_z-wave_technology/

[42] SMARTHOME, 2020. *What Is Z-Wave?* [online]. [cit. 2020-03-18]. Dostupné z: https://www.smarthome.com/sc-what-is-zwave-home-automation

[43] LINK LABS, 2020. *What Is LoRaWAN?* [online]. [cit. 2020-03-16]. Dostupné z: https://www.link-labs.com/blog/what-is-lorawan

[44] Lora Alliance, 2015. *A technical overview of LoRa® and LoRaWANTM.* [online]. [cit. 2020-03-03]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf

[45] *Sewio Networks, 2020. UWB Technology* [online]. [cit. 2020-04-03]. Dostupné z: https://www.sewio.net/uwb-technology/

[46] Smart-TEC, 2020. *Technologie RFID* [online]. [cit. 2020-02-20]. Dostupné z: https://www.smart-tec.com/cs/auto-id-svet/technologie-rfid

[47] VOJÁČEK, Antonín, 1.9. 2015. *Používané RFID frekvence a jejich vliv na čtení a zápis tagu* [online]. HW server s.r.o. [cit. 2020-01-27]. Dostupné z: https://automatizace.hw.cz/komponenty-prumyslove-sbernice-a-komunikace/vice-i-mene-bezne-rfid-frekvence-a-jejich-vliv-na-vlastnosti-tagu.html

[48] Smart-TEC, 2020. *Technologie NFC* [online]. [cit. 2020-02-20]. Dostupné z: https://www.smart-tec.com/cs/auto-id-svet/technologie-nfc

[49] SUMMERSON, Cameron, 8.11.2017. *What Is an eSIM, and How Is It Different From a SIM Card?* [online]. LifeSavvy [cit. 2020-01-27]. Dostupné z: https://www.howtogeek.com/331442/what-is-an-esim-and-how-is-it-different-from-a-sim-card/

[50] Brainbridge BVBA, 2019. *From 1g to 5g: a brief history of the evolution of mobile standards* [online]. [cit. 2020-02-16]. Dostupné z: https://www.brainbridge.be/news/from-1g-to-5g-a-brief-history-of-the-evolution-of-mobile-standards

[51] Jisc. Ac.uk. *Mobile networking: 1G to 4G* [online]. [cit. 2020-02-21]. Dostupné z: https://community.jisc.ac.uk/library/advisory-services/mobile-networking-1g-4g

[52] Cestování po USA, 2009 – 2020. *Mobilní telefon v USA* [online]. [cit. 2020-03-14]. Dostupné z: https://www.cestovani-po-usa.cz/mobilni-telefon-v-usa/

[53] RYŠÁNEK, F., 2020. *Pásma lte/umts/edge/gsm používaná v České republice* [online]. FCC průmyslové systémy s.r.o, [cit. 2020-01-27]. Dostupné z: http://www.fccps.cz/pasma-lteumtsedgegsm-pouzivana-v-ceske-republice-1379

[54] REJZEK, Jakub, 2019. *5G se netýká jen mobilních operátorů, milimetrové pásmo přinese nové možnosti* [online]. Internet Info, s.r.o. [cit. 2020-01-20]. Dostupné z: https://www.lupa.cz/clanky/5g-se-netyka-jen-mobilnich-operatoru-milimetrove-pasmo-prinese-nove-moznosti/

[55] VOJÁČEK, Antonín, 21.1.2017. *IoT MQTT prakticky v automatizaci - 1.díl – úvod* [online]. HW server s.r.o. [cit. 2020-01-24]. Dostupné z: https://automatizace.hw.cz/iot-mqtt-prakticky-v-automatizaci-1dil-uvod.html

[56] SETHI, Palavi a R. Smruti SARANGI, 2017. Internet of Things: Architectures, Protocols, and Aplications. *Journal of Electrical and Computer Engineering* [online]. New Delhi(India): Department of Computer Science [2020-02-24]. 2090-0147. Dostupné z: https://doi.org/10.1155/2017/9324035

[57] VOŘÍŠEK, Lukáš, 30.7.2016. *Kde najde IoT největší využití? 10 oblastí, které pravděpodobně ovlivní nejvíce* [online]. CDR server s.r.o. [cit. 2020-01-24]. Dostupné z: https://cdr.cz/clanek/kde-najde-iot-nejvetsi-vyuziti-10-oblasti-ktere-pravdepodobne-ovlivni-nejvice

[58] Connect GmbH. *Protože každý z nás je jedinečný: Vaše vlastní aplikace s technologiemi IFTTT a Home Connect* [online]. [cit. 2020-02-23]. Dostupné z: https://www.home-connect.com/cz/cs/pripojeni-partneri/pripojena-zarizeni-a-sluzby/ifttt

[59] Loxone Electronics GmbH, 2020. *Chytrý dům nebo byt s Loxone* [online]. [cit. 2020-02-20]. Dostupné z: https://www.loxone.com/cscz/chytry-dum/

[60] MINÁŘOVÁ, Ivana, 2020. SMART HOME jako standard moderního bydlení [online]. Geniální dům [cit. 2020-02-20]. Dostupné z: https://www.genialnidum.cz/smart-home-jako-standard-moderniho-bydleni/

[61] Chytré domácnosti, 2020. *Jak vytvořit chytrou domácnost?* [online]. [cit. 2020-02-20]. Dostupné z: https://www.chytredomacnosti.cz/chytra-domacnost/co-potrebujete-vedet-o-chytre-domacnosti/

[62] Loxone Electronics GmbH, 2020. *Inteligentní zabezpečení od Loxone* [online]. [cit. 2020-01-27]. Dostupné z: https://www.loxone.com/cscz/produkty/zabezpeceni/

[63] GAURAV, Sinha G., 11.4.2018. *The Evolution of Smart Home Technology* [online]. BCC Research [cit. 2020-01-27]. Dostupné z: http://blog.bccresearch.com/the-evolution-of-smart-home-technology

[64] HENDRICK, Drew, 22.4. 2014. *The History of Smart Homes* [online]. IoT Evolution [cit. 2020-02-22]. Dostupné z: https://www.iotevolutionworld.com/m2m/articles/376816-history-smart-homes.htm

[65] LÁSKA, Jan, 12.4.2019. *Zájem o zařízení chytré domácnosti v Evropě roste. Jen chytrých reproduktorů se prodalo 7,5 milionu* [online]. Czech news center a.s. [cit. 2020-02-20]. Dostupné z: https://www.mobilmania.cz/clanky/zajem-o-zarizeni-chytre-domacnosti-v-evrope-roste-jen-chytrych-reproduktoru-se-prodalo-75-milionu/sc-3-a-1344825/default.aspx

[66] PETROCK, Victoria, 16.12.2019. *Smart Homes 2020: The End of Interruptive Marketing as We Know It (Part 1 of a 2-Part IoT Series)* [online]. eMarketer Inc. [cit. 2020-02-20]. Dostupné z: https://www.emarketer.com/content/smart-homes-2020

[67] HL system group. *Inteligentní nebo konvenční?* [online]. [cit. 2020-02-20]. Dostupné z: https://www.hlsystemgroup.cz/novinky/inteligentni-nebo-konvencni/

[68] Narrative Media s.r.o., 2018-2019. *Je lepší inteligentní elektroinstalace, nebo bezdrátová chytrá domácnost?* [online]. Nalezeno.cz [cit. 2020-02-25]. Dostupné z: https://www.nazeleno.cz/je-lepsi-inteligentni-elektroinstalace-nebo-bezdratova-chytra-domacnost/

[69] PRŮCHA, Jan, 18.9.2012. *Chytré bydlení: inteligentní dům* [online]. Insight home, a.s. [cit. 2020-03-20]. Dostupné z: http://www.insighthome.eu/Chytre-bydleni/Chytre-bydleni.pdf

[70] RK elektro. *Porovnání ceny běžný x inteligentní dům* [online]. [cit. 2020-03-20]. Dostupné z: http://www.rkelektro.cz/inteligentni-domy/porovnani-ceny-bezny-x-inteligentni-dum

[71] VECKA Jiří, 2018. *Návrh inteligentní elektroinstalace rodinného domu* [online]. Plzeň. Diplomová práce. Západočeská univerzita v Plzni. Fakulta elektrotechnická [cit. 2020-01-27]. Vedoucí práce Jakub JIŘINEC. Dostupné z: https://otik.uk.zcu.cz/bitstream/11025/31538/1/DP_Jiri%20Vecka.pdf

[72] Loxone Electronics GmbH, 2020. *Create Automation* [online]. [cit. 2020-02-16]. Dostupné z: https://www.loxone.com/cscz/

[73] Somfy, 2020. *Somfy, partner pro vaši propojenou domácnos*t [online]. [cit. 2020-01-27]. Dostupné z: https://www.somfy.cz

[74] Apple Inc., 2020. *Your home at your command* [online]. [cit. 2020-02-13]. Dostupné z: https://www.apple.com/ios/home/

[75] Apple Inc., 2020. *HomeKit Accessory Protocol Specification* [online]. [cit. 2020-02-13]. Dostupné z: https://developer.apple.com/homekit/specification/

[76] CLOSE, Chistopher, 27.2.2020. *HomeKit Routers: Everything you need to know* [online]. Future US, Inc. [cit. 2020-02-14]. Dostupné z: https://www.imore.com/homekit-routers-everything-you-need-know

[77] Microsoft, 2020. HomeOS: Enabling smarter homes for everyone [online]. [cit. 2020-04-03]. Dostupné z: https://www.microsoft.com/en-us/research/project/homeos-enabling-smarter-homes-for-everyone/

[78] DE LOOPER, Christian, 3.3. 2020. *We compared Google Assistant, Amazon Alexa, and HomeKit to see which smart home platform is the best — and Alexa wins when it comes to device support* [online]. [cit. 2020-04-03]. Dostupné z: https://www.businessinsider.com/homekit-vs-google-assistant-vs-amazon-alexa

[79] Home Connect GmbH. *Amazon Alexa: Pomoc a podpora* [online]. [cit. 2020-04-03]. Dostupné z: https://www.home-connect.com/cz/cs/pomoc-podpora/amazon-alexa

[80] CHROBOK, Michael, 12.1.2020. *Google Assistant vs. Alexa: který chytrý asistent vyhraje bitvu o českou domácnost?* [online]. SMARTmania s.r.o. [cit. 2020-03-20]. Dostupné z: https://smartmania.cz/google-assistant-vs-alexa-ktery-chytry-asistent-vyhraje-bitvu-o-ceskou-domacnost/

[81] Deccan Chronicle, 24.12.2018. *Cortana scores worst in most voice assistant categories: Report* [online]. [cit. 2020-03-27]. Dostupné z: https://www.deccanchronicle.com/technology/in-other-news/241218/cortana-scores-worst-in-most-voice-assistant-categories-report.html

[82] Microsoft, 2020. *Your personal productivity assistant* [online]. [cit. 2020-04-03]. Dostupné z: https://www.microsoft.com/en-us/cortana

[83] Wondershare, 2020. *Jak používat Microsoft Cortanu v systému Windows 10* [online]. [cit. 2020-01-27]. Dostupné z: http://cs.wondershare.com/windows10/microsoft-cortana-on-windows-10.html#Part2

[84] Apple Inc., 2020. *Siri does more than ever. Even before you ask* [online]. [cit. 2020-02-13]. Dostupné z: https://www.apple.com/siri/

11 Přílohy

1) Dotazník

Dotazník

Na téma:
Moderní domácnost

1. Jaké je Vaše pohlaví? (Zvolte jednu odpověď.)

Muž	Žena

2. Do jaké věkové kategorie spadáte? (Zvolte jednu odpověď.)

Do 20 let	20 – 29 let	30 – 39 let	40 – 49 let	50 – 59 let	60+ let

3. Jaké je velikost Vaší obce? (Zvolte jednu odpověď)

Vesnice	Městys	Město do 50 000 obyvatel	Město s 50 000 – 150 000 obyvateli	Město s více než 150 000 obyvateli

4. V jakém obydlí bydlíte? (Zvolte jednu odpověď.)

V domě	V bytě

5. Jaká je velikost Vaší domácnosti? (Zvolte jednu odpověď.)

1+kk	1+1	2+kk	2+1	3+kk	3+1	4+1	5+1
Jiná……..							

6. Máte chytrou domácnost? (Domácnost lze považovat za chytrou, pokud obsahuje systém, který sjednocuje chytrá zařízení a měnit nastavení bez pokynů uživatele. Zvolte jednu odpověď.)

Ano	Ne

7. Chtěl/a byste v budoucnu bydlet v chytré domácnosti? (Zvolte jednu odpověď.)

Ano	Spíše ano	Spíše ne	Ne

8. V případě pořízení chytré domácnosti byste volil/a? (Zvolte jednu odpověď.)

Maximální implementaci	Střední implementaci	Minimální implementaci

9. Jaké jsou Vaše preference ohledně chytré domácnosti? (Pro každý řádek zvolte Vaše preference. 3 označuje vyrovnané preference ohledně daných aspektů.)

Pořizovací náklady	1	2	3	4	5	Pravidelné úspory na energiích
Strach ze ztráty kontroly	1	2	3	4	5	Kontrola nad domácností
Omezení soukromí	1	2	3	4	5	Komfort

10. Jaký způsob budování chytré domácnosti byste zvolil? (Zvolte jednu odpověď.)

Navrhnutí i zprovoznění profesionální firmou
Navrhnutí profesionální firmou a vlastní zprovoznění
Vlastní návrh a zprovoznění profesionální firmou
Vlastní název i zpracování

11. Jaká chytrá zařízení byste chtěli mít ve své domácnosti? (Zvolte jednu nebo více odpovědí.)

Termostaty, Klimatizace	Vysavače, sekačky	Světla
Detektory kouře, vody, pohybu	Uzávěry vody, plynu	Kamery
Rolety, žaluzie, záclony, závěsy	Zámky dveří	Alarmy
Ovládání dveří, garážových vrat	Žádná	Jiná ….

12. Líbí/líbilo by se Vám mít informace o domácnosti, i když se nacházíte mimo ni? (Zvolte jednu odpověď.)

Ano	Ne

13. Víte, že chytré domácnosti umožňují ovládání pomocí scénářů, kdy zařízení dokáží spolu komunikovat a měnit nastavení bez pokynů uživatele? (Zvolte jednu odpověď.)

Ano	Ne

14. Kolik byste byl/a ochotný/á investovat do chytré domácnosti? (Zvolte jednu odpověď.)

Do 10 000 Kč
10 000 – 20 00 Kč
20 000 – 50 000 Kč
50 000 – 100 000 Kč
100 000 Kč – 300 000 Kč
300 000 Kč a více

Oskenované zadání práce

Zadání bakalářské práce

Autor:	**Jan Pokorný**
Studium:	I1700128
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Moderní domácnost**
Název bakalářské práce AJ:	Modern Household

Cíl, metody, literatura, předpoklady:

Cílem bakalářské práce je popsat moderní domácnost, založenou na rozsáhlém využití moderních informačních a komunikačních technologií, výsledků výzkumu ambientní inteligence a internetu věcí. Bude zkoumána aktuální dostupnost a kompatibilita vhodných chytrých zařízení a bude provedeno porovnání zařízení založených na ekosystému od společnosti Apple se zařízeními od jiných producentů. Bude navržen a podrobně charakterizován koncept ideální moderní domácnosti a provedeno porovnání s aktuálně dostupnou domácností.

Literatura bude doporučena zadavatelem.

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	prof. RNDr. Peter Mikulecký, Ph.D.
Oponent:	RNDr. Petr Tučník, Ph.D.
Datum zadání závěrečné práce:	21.10.2014