

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta elektrotechnická
Katedra elektrotechniky a počítačového modelování

BAKALÁŘSKÁ PRÁCE

IoT systémy pro úsporu energie v bytových domech a
domácnostech

Autor práce: **Vojtěch Malík**
Vedoucí práce: **Ing. Jaroslav Podestát**

2022

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta elektrotechnická
Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Vojtěch MALÍK**
Osobní číslo: **E19B0018P**
Studijní program: **B2644 Aplikovaná elektrotechnika**
Studijní obor: **Aplikovaná elektrotechnika**
Téma práce: **IoT systémy pro úsporu energií v bytových domech a domácnostech**
Zadávací katedra: **Katedra výkonové elektroniky a strojů**

Zásady pro vypracování

1. Proveďte rešerši IoT systémů zaměřenou na oblast ekonomických úspor energií a jejich možnosti v oblastech bytových domů a domácností.
2. Realizujte návrh systému v oblasti energií s důrazem na ekonomické úspory elektrické a tepelné energie.
3. Zhodnoťte obdržené výsledky.


Rozsah bakalářské práce: **30 – 40**
Rozsah grafických prací: **dle doporučení vedoucího**
Forma zpracování bakalářské práce: **elektronická**


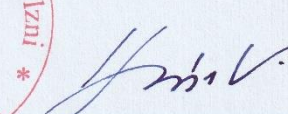
Seznam doporučené literatury:

1. MUHANJI, Steffi O., Alison E. FLINT a Amro M. FARID. IoT [online]. Cham: Springer International Publishing, 2019 [cit. 2021-04-19]. ISBN 978-3-030-10426-9. Dostupné z: doi:10.1007/978-3-030-10427-6.
2. MILENKOVIC, Milan. Internet of Things: Concepts and System Design [online]. Cham: Springer International Publishing, 2020 [cit. 2021-04-19]. ISBN 978-3-030-41345-3. Dostupné z: doi:10.1007/978-3-030-41346-0.

Vedoucí bakalářské práce: **Ing. Jaroslav Podestát**
Katedra elektrotechniky a počítačového modelování

Datum zadání bakalářské práce: **8. října 2021**
Termín odevzdání bakalářské práce: **26. května 2022**


Prof. Ing. Zdeněk Peroutka, Ph.D.
děkan



Prof. Ing. Václav Kůs, CSc.
vedoucí katedry

Abstrakt

Zadaná bakalářská práce se zabývá IoT systémy pro úsporu energií v bytových domech a domácnostech. Práce se nejprve zaměřuje na základní definici IoT systému, její historii, komunikační protokoly, zabezpečení a možnou úsporu energie. Věnuje se specificky úspoře především elektrické a tepelné energie. Dále práce pokračuje návrhem a praktickou implementací systému v apartmánu bytového domu. V závěru jsou porovnány úspory systému s předchozím stavem a jeho pořizovací náklady.

Klíčová slova

Internet věcí, chytrá domácnost, úspora energií, automatizace, ZigBee protokol, nízkoenergetická zařízení

Abstract

The assigned bachelor thesis deals with IoT systems for energy savings in apartment buildings and households. The work first focuses on the basic definition of the IoT system, its history, communication protocols, security, and possible energy savings. It is dedicated in particular to saving electricity and heat. The work continues with the design and practical implementation of the system in a flat of an apartment building. In the end, the savings of the system are compared with the previous state and its acquisition costs.

Key Words

Internet of Things, smart home, energy saving, automation, ZigBee protocol, low energy devices

Poděkování

Rád bych poděkoval svému vedoucímu bakalářské práce Ing. Jaroslavu Podestátovi za rady a vedení, které mi pomohli ve vytváření této práce.

Obsah

Úvod.....	- 9 -
1 Internet věcí	- 10 -
1.1 Definice internetu věcí	- 10 -
1.2 Historie IoT	- 10 -
1.3 Prvky IoT.....	- 11 -
1.4 Vrstvy architektury IoT	- 12 -
1.5 Přenos dat v IoT s nízkou spotřebou	- 14 -
1.5.1 Přenos s krátkým dosahem	- 14 -
1.5.2 Přenos s dlouhým dosahem.....	- 15 -
1.6 Protokoly	- 16 -
1.7 Zabezpečení IoT.....	- 19 -
1.8 Zařízení a procesy pro úsporu energie	- 23 -
1.8.1 Úspora elektrické energie	- 24 -
1.8.2 Úspora tepelné energie.....	- 24 -
2 Vlastní systém	- 26 -
2.1 Návrh systému.....	- 26 -
2.2 Jednotlivé komponenty	- 27 -
2.3 Řídící jednotky, huby a bridge	- 32 -
2.4 Rutiny a automatizace	- 34 -
2.5 Instalace zařízení	- 36 -
2.6 Zlepšení instalovaného systému.....	- 38 -
3 Vyhodnocení praktické části	- 40 -
3.1 Celková cena systému	- 40 -
3.2 Porovnání úspor a ztrát.....	- 41 -
4 Závěr.....	- 43 -
5 Zdroje	- 44 -

Seznam symbolů a zkratek

Zkratka	Popisek
<i>AMQP</i>	Advanced Message Queuing Protocol
<i>BLE</i>	Bluetooth Low Energy
<i>DDS</i>	Data Distribution Service
<i>DNS</i>	Domain Name System
<i>DNSSEC</i>	Domain Name System Security Extension
<i>HTTPS</i>	Hypertext Transfer Protocol Secure
<i>IaaS</i>	Infrastructure as a Service
<i>IoT</i>	Internet of Things
<i>ISM</i>	Industrial Scientific and Medical
<i>LoRaWAN</i>	Low-Power Wide Area Network
<i>MQTT</i>	Message Queueing Telemetry Transport
<i>PaaS</i>	Platform as a Service
<i>SaaS</i>	Software as a Service
<i>TCP</i>	Transmission Control Protocol
<i>TLS</i>	Transport Layer Security
<i>UDP</i>	User Datagram Protocol
<i>VM</i>	Virtual Machine
<i>VPN</i>	Virtual Private Network
<i>WAN</i>	Wide Area Network
<i>XML</i>	Extensible Markup Language
<i>XMPP</i>	Extensible Messaging and Presence Protocol

Úvod

Tato práce se zabývá návrhem a praktickou implementací systému pro úsporu energií v domácnostech a bytových domech. Veškerá použitá zařízení jsou komerčně dostupná a byla vybrána takovým způsobem, aby na instalaci a používání stačily běžné znalosti.

V první kapitole práce pojednává o definici IoT systému, jeho zabezpečení, komunikačních protokolech s jednotlivými prvky. Pojednává o možných úsporách energií za pomoci chytrých zařízení a rutin, které jsou s nimi spojeny.

Práce se dále zabývá doporučeními pro návrh obdobného systému a možnostmi dalšího zlepšení skrz instalaci dalších zařízení, modifikaci již stávajících zařízení a zabezpečení systému proti krádeži a ztrátě dat.

Popisovaný systém se zaměřuje na úspory v oblasti elektrické a tepelné energie. Systém využívá chytrých ZigBee senzorů a jejich požadovaný bridge. Automatizace systému je prováděna skrz aplikace výrobců zařízení. Ovládání je prováděno přes rutiny, fyzická tlačítka, nebo je možné celý systém ovládat pomocí příkazů přes hlasového asistenta Google.

Ve finální kapitole práce popisuje a hodnotí cenu celkového systému a úspory, popřípadě ztráty, kterých bylo dosaženo.

1 Internet věcí

Cílem této kapitoly je definovat pojem *internet věcí*, stručně popsat vznik, základní náležitosti, prvky, využití technologie pro zabezpečení, protokoly pro přenos dat a možné prvky pro integraci do domácností.

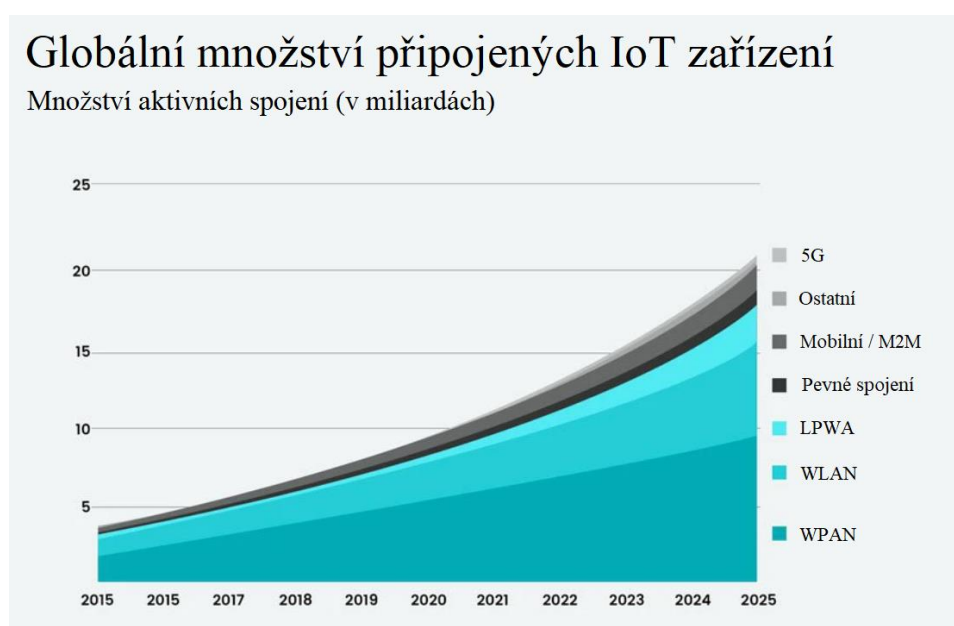
1.1 Definice internetu věcí

Jedná se o systém vzájemně propojených výpočetních zařízení, mechanických a digitálních přístrojů, objektů, zvířat nebo lidí, kteří jsou označeni jedinečnými identifikátory a mají schopnost odesílat a přijímat data přes síť spojení bez potřeby lidské interakce. [1]

1.2 Historie IoT

Pojem IoT je starý zhruba 16 let, ale nápad propojených zařízení existuje minimálně od 70. let 19. století. V té době byl tento koncept nazýván „embedded internet“, pojem IoT byl poprvé použit v prezentaci roku 1999 Kevinem Ashtonem, který pracoval na optimalizaci dodávek pro firmu Procter&Gamble za pomoci v té době nové technologie RFID. Navzdory tomu se IoT nedočkal širší pozornosti po příštích 10 let. [2]

Za opravdový vznik IoT společnost Cisco IBSG považuje časovou oblast mezi roky 2008 a 2009 kdy počet připojených zařízení přesáhl lidskou populaci díky dostupnosti mobilních zařízení. Zároveň s dostupností se rozrůstala mobilní síť pro jejich spojení a tím se i zlepšila přístupnost a cena IoT zařízení pro nekomerční uživatele jako jsou domácnosti. [3]



Obr. 1 Globální množství připojených zařízení a předpokládaný růst, překresleno z [4]

1.3 Prvky IoT

Prvek v IoT může být člověk s voperovaným srdečním monitorem, dobytek na farmě s implantovaným vysílacím čipem, automobil s integrovanými senzory pro upozornění řidiče na nízký tlak v pneumatikách nebo jakýkoliv jiný přírodní nebo syntetický objekt, kterému může být přidělena adresa v internetovém protokolu a je schopen přenášet data přes síť. [1]

Senzory a zařízení

Senzory a zařízení sbírají data z okolního prostředí. Data mohou mít různou složitost, může se jednat o jednoduchý senzor teploty nebo o komplexní záznam videa. Zařízení může mít větší množství senzorů, které mohou spolupracovat pro monitorování více než jedné věci. Jako příklad bych uvedl mobilní telefon, který má v sobě GPS senzory, akcelerometry a kamery. Hlavním účelem senzorů je posílat data k dalšímu zpracování na výpočetním zařízení. [5]

Propojení

Data ze senzorů se nějakým způsobem musí dostat ze senzorů do datového cloudu. Senzory mohou být propojeny více prostředky, jako jsou například mobilní síť, satelitní síť nebo síť WAN. Každá z možností propojení má svoje výhody a specifikace jako jsou spotřeba energie, dosah a šířka pásma. Výběr záleží na umístění a požadavcích daného IoT systému. [5]

Zpracování dat

Data z cloudu jsou zpracována a jsou prováděna potřebné výpočty. Může se jednat o něco jednoduchého jako je porovnání teplot pro klimatizace nebo topení, až po komplexní úkony jako vyhodnocování narušitelů na kamerovém systému. Nastávají však situace, kdy je vyžadována akce ze strany uživatele, například na určení, co má systém dělat, pokud je teplota moc vysoká. [5]

Cloud Computing

Cloud Computing je obecný výraz pro cokoliv, co zahrnuje doručování hostovaných služeb přes internet. Tyto služby se dělí do tří hlavních kategorií, IaaS, PaaS a SaaS. Cloud může být privátní nebo veřejný, Veřejný cloud poskytuje služby komukoliv na internetu. Privátní cloud je nesdílená síť nebo datové centrum, které poskytuje služby omezenému počtu uživatelů se specifickými povoleními. Ať už se jedná od privátní nebo veřejný cloud,

cílem je poskytnout jednoduchý a rozšiřitelný přístup k výpočetním prostředkům a IT službám. [6]

On-site Computing

V tomto modelu se uživatel spoléhá pouze na svoji výpočetní techniku, která se nachází ve stejném komplexu. Tyto servery se vyskytují ve dvou formách, fyzická a virtuální (VM). Fyzický server je určený pro jednoho uživatele, žádné výpočetní prostředky a komponenty nejsou sdíleny mezi více uživateli. Servery VM funguje na principu emulace skutečného fyzického zařízení. Více uživatelů sdílí výpočetní prostředky jednoho stroj, který rozdělený na více VM. Výhodami oproti cloud computing jsou lokální přístup k datům, fixní cena provozu, která se u cloud computing může časem zvedat a nezávislost na připojení k internetu. Nevýhodami jsou vyšší pořizovací cena, údržba, limitovaná rozšiřitelnost úložiště a obtížná obnova dat, při výpadku více disků v úložišti. [7, 8]

Uživatelské rozhraní

Uživatelské rozhraní se využívá k zobrazení relevantních dat, například spuštěním alarmů nebo zaslání upozornění na mobilní zařízení. Uživatel také může přes rozhraní kontrolovat plynulost chodu svého zařízení jako jsou kamerové systémy. Některé systémy dovolují uživateli upravovat nastavení jednotlivých zařízení, například upravit požadovanou teplotu v lednici přes aplikaci v mobilním telefonu. Jiné činnosti jsou prováděny automaticky bez zásahu uživatele pomocí předem definovaných pravidel a nastavení. [5]

1.4 Vrstvy architektury IoT

Architektura IoT se často popisuje jako čtyř etapový proces, ve kterém data cestují ze senzorů skrz síťové spojení až k úložišti na zpracování a zálohu dat. [9]

Vrstva vnímání

Tato základní vrstva je tvořena senzory a akčními členy, které shromažďují užitečná data. Hlavním účelem této vrstvy je získávat informace z okolního prostředí a předat data pro další zpracování. [10]

Síťová vrstva

Tato vrstva se o propojení jednotlivých součástí a vrstev IoT systému. Sbírá data z fyzických zařízení a převádí je z analogové na digitální podobu, formátuje data a posílá je

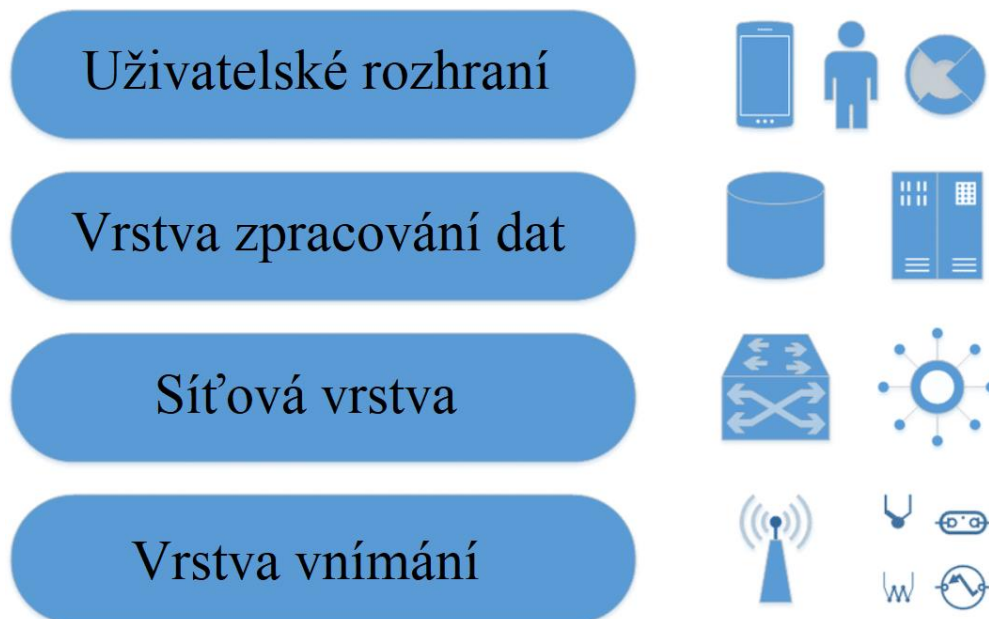
přes síťové spojení na zpracování. V tomto okamžiku se může jednat o velké množství dat, proto je nutné je filtrovat a komprimovat na optimální velikost k odeslání. [9]

Vrstva Edge

Vrstva se stará o základní zpracování odeslaných dat a redukci jeho objemu pro snazší zpracování dat. Stará se také o základní analýzu a jednoduché před zpracování. Strojové učení v tomto kroku může poskytovat zpětnou vazbu pro vylepšení procesu přenosu a zpracování dat, bez nutnosti příkazů z cloudu nebo řídicí jednotky. Zpracování dat tohoto typu se většinou odehrává na zařízení co nejbližší sensorům. [11]

Vrstva zpracování dat

V poslední vrstvě se na dedikovaných výpočetních zařízeních analyzují, spravují a bezpečně zálohují data. Tento proces se většinou odehrává v datovém centru firmy, která instalovala IoT systém nebo na síťovém úložišti, kde mohou být data ze sensorů sloučena pro poskytnutí širšího porozumění situace. Výhodou síťového úložiště je možnost zpracování dat kdekoli se zabezpečeným přístupem na internet. V této vrstvě se také odehrává hlubší analýza dat pro specifická odvětví. [5]



Obr 2.

Vrstvy IoT systému, překresleno z [12]

1.5 Přenos dat v IoT s nízkou spotřebou

Tyto typy sítí jsou vhodné pro aplikace, kde je dostačující krátká vzdálenost přenosu, jako jsou například domácnosti nebo kanceláře. Zařízení obvykle vyžadují malé množství energie, mohou tedy být napájeny baterií a jsou levné na provoz.

1.5.1 Přenos s krátkým dosahem

Wi-Fi

Wi-Fi je nejčastěji používaná komunikační technologie v domácnostech a kancelářích. Často se pro IoT využívá stávající infrastruktury, a i díky tomuto má jedny z nejnižších nákladů. Komunikuje na frekvenci 2,4 GHz a 5 GHz. Její nevýhodou je poměrně vysoká spotřeba energie ve srovnání s ostatními typy spojení a je často využívána u zařízení s přímým připojením na 230V síť domácnosti. [13]

Bluetooth

Bluetooth je bezdrátová technologie s krátkým dosahem hlavně využívaná pro výměnu dat mezi pevnými nebo mobilními zařízeními pomocí ultra krátkých rádiových vln v pásmu ISM. Má možnost využívat ostatních připojených zařízení pro předávání signálu mimo dosah odesílajícího. Tímto způsobem dokáže pokrýt celé budovy signálem [14]

Bluetooth Low Energy

BLE je varianta Bluetooth specificky navržená pro IoT systémy. Již z názvu lze vyčíst, že se jedná o nízkoenergetickou variantu. Technologie je často využívána u senzorů, které nepotřebují přenést větší množství dat. Využívá se ve fitness náramcích, chytrých hodinkách a lékařských zařízeních jako inzulinové pumpy. [15]

ZigBee

ZigBee je nízkonákladový a nízkoenergetický bezdrátový standard. Zařízení komunikují na frekvenci 2,4 GHz. Jeho hlavní vlastností je schopnost poskytnout zabezpečenou komunikaci, které je schopen dosáhnout za pomoci 128bitové kryptografické ochrany. Je založena na principu symetrických klíčů, to znamená, že stejný klíč musí mít, jak zařízení, které informaci odesílá, tak to, co je přijímá. Tyto klíče jsou buď předinstalovány, nebo jsou předávány za pomoci zabezpečeného zařízení v lokální síti. Jeho nevýhodou je častá nekompatibilita mezi výrobcí zařízení, je vhodné mít zařízení pouze od jednoho. [16]

Z-Wave

Z-Wave je smíšená síť používající nízkoenergetické rádiové vlny o frekvenci 868 kHz pro komunikaci mezi zařízeními a základnou. Signály jsou ze základny odesílány bezdrátově jiným zařízením a každé zařízení může fungovat jako opakovač signálu. Síť může obsahovat až 232 zařízení. Technologie je využívána hlavně pro automatizaci domácností například společností SmartLife nebo Honeywell. [17]

1.5.2 Přenos s dlouhým dosahem

Wi-Fi HaLow

Nově schváleným standardem je Wi-Fi HaLow, který má menší spotřebu energie než Wi-Fi a může být využit u bateriových zařízení. Využívá frekvence 900 MHz a dokáže vysílat data až do vzdálenosti 1 km. Nevýhodou je nižší maximální přenosová rychlost oproti přenosu Wi-Fi, která se pohybuje kolem 4 Mb/s. [18]

LoRaWAN

LoRaWAN je specifikace pro nízkoenergetický širokopásmový síťový protokol navržený pro bezdrátové spojení zařízení napájených baterií k internetu na velké vzdálenosti. Zařízení komunikují na frekvenci 868 MHz. Splňuje základní požadavky pro IoT jako jsou dvoucestná komunikace, koncové zabezpečení a mobilita. Technologii využívá firma Mikrotik pro výrobu svých produktů. [19]

NB-IoT

Úzkopásmové IoT je jeden z bezdrátových nízkoenergetických komunikačních standardů pro IoT. Používá podmnožinu standardu LTE a komunikuje na frekvenci 800 MHz. Používá se u zařízení, kterým dostačuje přenos pouze malého množství dat s dlouhou životností baterií a vysoké četnosti odeslaných dat. Zaměřuje se specificky na pokrytí vnitřních prostor. Roku 2019 globální asociace dodavatelů mobilních zařízení (GSA) oznámila, že přes 140 operátorů provozuje NB-IoT síť. [20]

Tabulka 1 Srovnání přenosových technologií

Název	Maximální dosah	Frekvence	Přenosová rychlost
Wi-Fi	100 m	2,4 GHz a 5 GHz	2 Gb/s
Bluetooth	100 m	2,4 GHz	2 Mb/s
BLE	100 m	2,4 GHz	1,5 Mb/s
ZigBee	100 m	2,4 GHz	250 kb/s
Z-Wave	100 m	908 MHz	100 kb/s
Wi-Fi HaLow	1 km	900 MHz	4 Mb/s
LoRaWAN	15 km	868 MHz	50 kb/s
NB-IoT	15 km	800 MHz	200 kb/s

1.6 Protokoly

IoT zařízení komunikují za pomoci protokolů, které zařízení chrání a zajišťují optimální přenos dat mezi zařízení a koncovým uživatelem. Některé protokoly jsou schopny provádět kontrolu úspěšného doručení dat a detekci autorizovaného uživatele. Konektivita mezi zařízeními může být drátová nebo za pomoci bezdrátových přenosových technologií.

CoAP

Jedná se o http protokol s nižší energetickou náročností vyvinutý specificky pro IoT pro činnost v zařízení s omezeným přístupem k síti. Byl vytvořen skupinou IETF Constrained RESTful Environments a spuštěn roku 2013. [21]

Protokol je navržen pro spolehlivý přenos dat v prostředí s velkou saturací přenosového pásma. Dokáže pracovat i v případech, kdy protokoly na bázi TCP selžou v přenosu dat a nedokážou komunikovat efektivně, jedním z důvodů je i kontrola doručení zpráv.

Jednou z funkcí CoAP je kontrola kvality, které je používána na kontrolu zpráv a jejich úspěšné doručení. Zprávy dělí na potvrditelné a nepotvrditelné v závislosti na obdržení zpětné vazby od příjemce. Pro bezpečné předávání dat v přenosové vrstvě používá DTLS. CoAP plně pokrývá nutnost extrémně nenáročného protokolu, který je potřeba na splnění požadavků bateriových zařízení. [22]

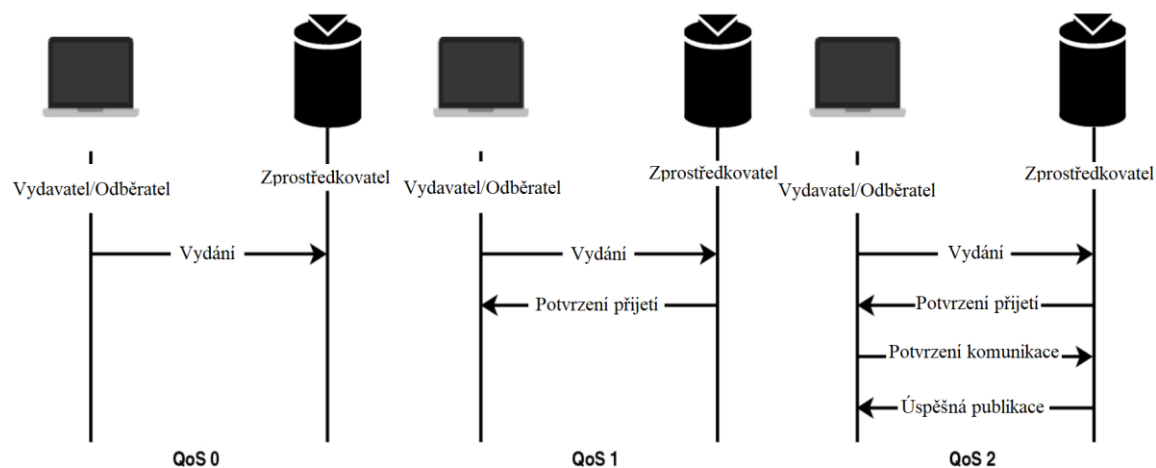
MQTT

Jedná se o nejvíce rozšířený protokol v průmyslovém IoT, byl vydán roku 1999 společností OASIS. Pracuje na základě TCP protokolu a byl specificky vytvořen pro činnost v oblastech se špatnou úrovní signálu jako odezva na v posledních letech se zvyšující počet malých a levných IoT zařízení. [23]

MQTT je nízkoenergetický protokol typu vydavatel/odběratel navržený pro bateriové zařízení. V tomto modelu je úkolem vydavatele shromažďovat data a odeslat je odběratelům skrz zprostředkovací vrstvu. Rolí sprostředkovatele je zajistit bezpečný přenos za pomoci kontroly autorizací a zpětné vazby vydavatele a odběratele, využívají se k tomu 3 hlavní typy kontrol, které se odkazují na [24]:

- QoS0 Nanejvýš jednou – Nejméně spolehlivá kontrola, ale nejrychlejší kontrola. Kontroluje, zda vydavatel odeslal data, ale potvrzení od odběratele už není zapotřebí
- QoS1 Alespoň jednou – Zajišťuje, že se zpráva dostala od vydavatele k odběrateli. V tomto typu se mohou objevit duplikáty.
- QoS2 Právě jednou – Nejspolehlivější, ale nejnáročnější na přenos. Stejný princip jako QoS1 s kontrolou duplikátů a zajištění, že je zpráva doručena jen jednou.

Navzdory charakteristikám MQTT mohou nastat problémy v některými omezenými zařízeními z důvodu přenosu zpráv přes TCP a dlouhých tematických názvů. Tento problém je vyřešen MQTT-SN, který využívá ke komunikaci UDP a podporuje indexování témat. [25]



Obr. 3 MQTT QoS, překresleno z [26]

XMPP

Protokol byl vyvinut roku 1999 open source komunitou Jabber a jeho původním účelem byla komunikace zprávami v reálném čase. Je založen na jazyku XML. Dovoluje výměnu dat v reálném čase mezi dvěma nebo více uživateli na síti. [27]

Už od jeho vzniku bylo XMPP široce využíváno jako komunikační protokol. Časem byla vytvořena odlehčená verze XMPP-IoT, která byla navržena pro zařízení v IoT. Jedná se o standard podporovaný open source komunitou. Jeho hlavními výhodami jsou schopnost adresování a škálovatelnosti, které jsou vhodné pro instalace se zaměřením na spotřebitele. Využívá se například pro komunikace více uživatelů (MUC). [28] Jedná se o rozšíření XMPP pro výměnu zpráv a dat v reálném čase v online místnosti. Protokol umožňuje velkou kontrolu nad uživateli, například vyhození uživatelů z místnosti nebo zákaz jejich opětovnému připojení. [29]

Nevýhodami využívání XMPP pro IoT komunikaci jsou neexistence QoS kontrol a nedisponuje end-to-end šifrováním. Kvůli těmto nevýhodám se předpokládá, že nebude zaveden jako standard v IoT systémech pro průmysl, na rozdíl od protokolů MQTT a LwM2M. [30]

AMQP

Jedná se o rozšiřitelný standard typu vydavatel/odběratel se zprostředkovatelem, který byl vyvinut roku 2003 společností JPMorgan Chase v Londýně. Jeho první použití bylo ve finančním sektoru. Protokol získal zázemí v informačních technologiích pro komunikaci, jeho využití v IoT průmyslu je poměrně limitované. Vlastnostmi AMQP jsou orientace zpráv, pořadník zpráv, přesměrování, spolehlivost a zabezpečení. Největší výhodou AMQP je robustní komunikační model, který garantuje úplnou výměnu dat. Ačkoliv, je to velmi užitečné, některé IoT aplikace tuto funkci ne vždy vyžadují. [31]

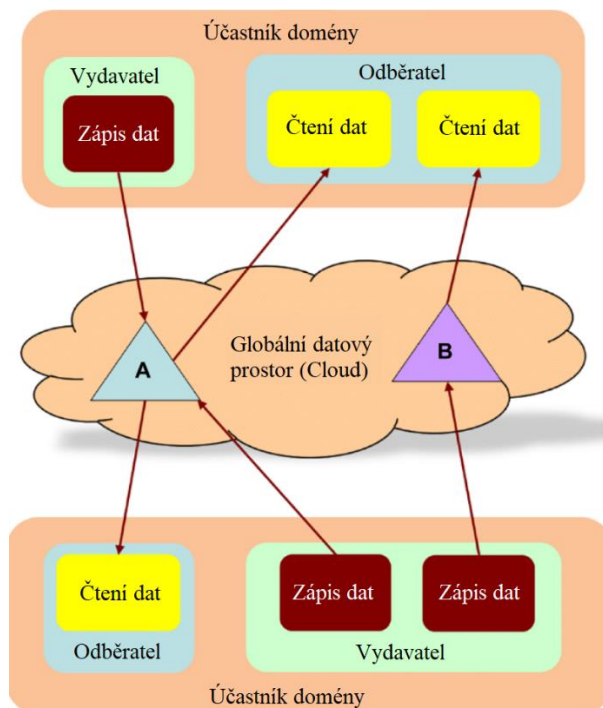
Vzhledem k náročnosti tohoto protokolu, není vhodný pro senzory s omezenou pamětí nebo šířkou pásma, ačkoliv v některých případech může být jediným použitelným protokolem pro end-to-end aplikaci jako například těžký průmysl nebo SCADA systémy, kde jsou systémy většinou velmi robustní. [32]

DDS

Protokol je založen na bázi vydavatel/odběratel. Byl vyvinut roku 2004 společností Object Management Group. Tento protokol pro komunikaci v reálném čase umožňuje rozšiřitelnou, spolehlivou, vysoko výkonovou a interoperabilní výměnu dat mezi připojenými zařízeními nezávisle na hardwaru a softwaru platformy. Podporuje architekturu bez zprostředkovatele a využívá multicasting pro kontrolu kvality. [33]

Architektura DDS protokolu je založena vrstvě zaměřenou na data typu vydavatel/odběratel (DCPS) a volitelně na vrstvě pro lokální rekonstrukci dat (DLRL). Vrstva DPCS je zodpovědná za přenos dat odběratelům zaměřený na rozšiřitelnost, efektivní

přenos s nízkou spotřebou energie. DLRL nabízí rozhraní pro funkce DCPS a umožňuje přenos dat mezi zařízeními připojenými do IoT sítě. Celkově lze DDS využít pro řízení výměny dat mezi nízkoenergetickými zařízeními a sítí propojených vysokovýkonových senzorů. Dokáže také přijímat a odesílat data z cloudu. [34]



Obr. 4 Síť DDS, překresleno z [35]

LwM2M

Lightweight M2M je protokol používaný v IoT, který byl vytvořen speciálně pro rozsáhlou výměnu dat zařízení s omezenými prostředky. Byl vytvořen roku 2014 společností Open Mobile Alliance na bázi CoAP, ale pozdější verze podporují i jiné přenosové protokoly. Poskytuje definovaný standard pro IoT komunikaci a správu zařízení. LwM2M vymezuje komunikační protokol mezi serverem a klientem bez použití připojených zařízení. [36]

1.7 Zabezpečení IoT

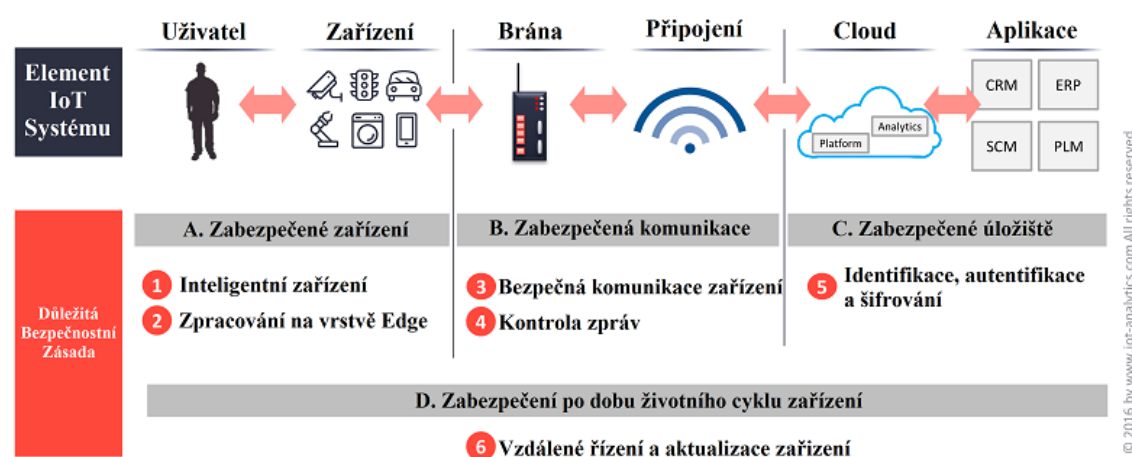
Nástroje pro zabezpečení IoT sítí slouží k odražení ohrožení, porušení bezpečnosti, identifikace a monitorování rizik, dokážou také opravit zranitelnosti.

Důležitost zabezpečení plyne z nutnosti chránit kritické IoT systémy jako jsou řídicí jednotky automobilů, domácnosti a senzory na silnicích, které dodávají cenná data pro zjednodušení a zlepšení pracovního a společenského života. Úspěch závisí na zajištění integrity a důvěrnosti IoT zařízení. [37]

Navzdory důležitosti a výhodám zabezpečení je mnoho domácností ani podniků nevyužívá, a to z důvodu pořizovací ceny a nejistoty při vybírání nejlepšího systému. Průzkum roku 2019 v Kanadě, Francii a Spojeném Království ukázal, že 63 % uživatelů vidí propojená zařízení jako nedůvěryhodná [38].

Každý prvek systému má svůj systém zabezpečení, můžeme je rozdělit do tří skupin, a to samotné zařízení, zařízení pro komunikaci se sítí a úložiště. Běžné zařízení v domácnosti jako je například chytrá žárovka nemá svoje vlastní zabezpečení, ale spoléhá na zabezpečení z domácí Wi-Fi sítě. Zařízení, která vyžadují centrální hub, nebo bridge, mohou za pomoci kontroly kvality monitorovat úspěšné doručení dat zároveň s kontrolou věrohodného zdroje. Nejdůležitějším prvkem je bezpečné úložiště, protože je irelevantní, jak bezpečný je přenos, pokud existuje jednoduchá cesta k finálním datům. [39]

6 zásad kybernetického zabezpečení v IoT systémech



Obr. 5 Rizika specifických IoT systémů, překresleno z [39]

VPN

Prostředek organizací pro propojení veškeré své informační infrastruktury pro IoT do jedné sítě. Tato privátní síť dovoluje bezpečnou komunikaci mezi zařízeními a infrastrukturou, která je monitoruje a sbírá z nich data. [40]

Díky pokroku v kryptografii, výpočetní technice a faktu, že internet pronikl do všech každodenních zařízení je možné zašifrovat data a odeslat je přes internet na server v privátní síti. Za pomoci VPN serveru jako řešení pro bezpečnost IoT jsou společnosti schopny si vytvořit svoji vlastní zabezpečenou privátní síť pro komunikaci s ostatními IoT zařízeními.

Tímto způsobem je možné zabránit útokům, které by potají monitorovala jejich data. Pouze zařízení autorizovaná společností mohou být součástí privátní sítě. [41]

Následující výhody a nevýhody vychází ze zdroje [42].

Výhody VPN:

- Skrytá IP adresa – IP adresa zařízení se změní na adresu používanou serverem VPN.
- Šifrování – Server VPN převádí data z prostého textu na zašifrovaný.

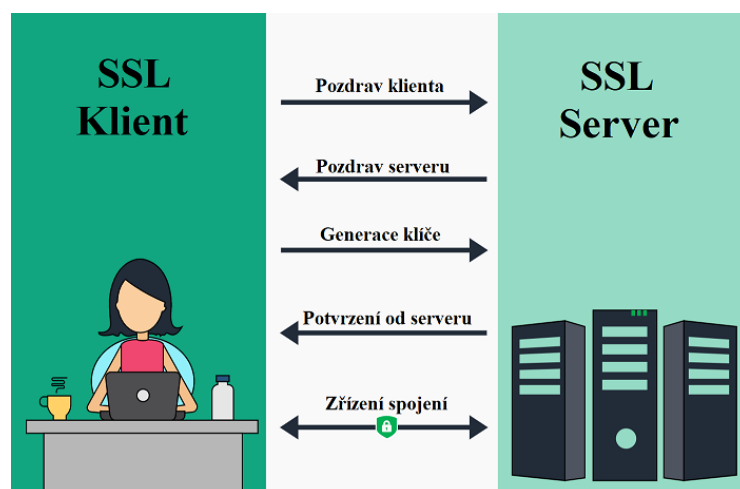
Nevýhody:

- Odezva – VPN jsou síťové technologie, důsledkem můžou být problémy s odezvou.
- Spolehlivost – Důvod nespolehlivosti je použití externí služby.
- Cena – Většina společností poskytující služby VPN mají placený obchodní model s ročním předplatným.
- Náročnost provedení – Sítě VPN vyžadují velké množství kódu k jejich správné funkci.

TLS

Jedná se o protokol, který využívá asymetrické šifrování k zabezpečení dat sdílenými mezi dvěma zařízeními na síti. TLS zajišťuje, že identity serveru nebo klienta jsou důvěryhodně potvrzené. Nejčastěji HTTPS server poskytne prohlížeči návštěvníka certifikát, který byl digitálně podepsán důvěryhodným vydavatelem certifikátů (CA) jako je například SSL.com. Matematický model, který vytváří protokoly, zabezpečuje, že daný certifikát je prakticky nemožné zfalšovat, pokud je dostatečně dlouhý klíčový řetězec. Veřejný CA verifikuje identitu žadatele před vydáním certifikátu. Zároveň podléhají přísným auditům, se stany poskytovatelů webových prohlížečů a operačních systémů, aby si udrželi důvěryhodný status v online obchodech. Seznam těchto certifikátů je nainstalován se softwarem prohlížečů a operačních systémů. [43]

Uživatelé, kteří se budou snažit připojit na stránky, které nemají důvěryhodný certifikát budou setkání s bezpečnostním varováním a dalšími zátarasy, skrz které se budou muset proklikat, aby bylo jasné, že na stránku opravdu chtějí dostat. Stejný princip funguje i pro emailové služby a zařízení v IoT. Další možností je přiřazení certifikátu klientům. Toto je často využíváno v průmyslu, kdy se dovolí pouze vybraným zaměstnancům přístup na specifické stránky. V tomto případě se SSL používá jako klíč s přístupem k privátní síti. [44]



Obr. 6 SSL komunikace, překresleno z [45]

DNS

Protokol využívající decentralizovaný, hierarchický systém doménových jmen. Každé IoT zařízení musí být identifikováno, inventarizováno, prověřeno, řízeno a zabezpečeno tak, aby nemohlo způsobit problémy pro zbytek zařízení v ekosystému, uživatelům nebo samotné společnosti. [46]

Podniky, nebo domácnosti, mohou zabránit zneužití bezpečnostních nedostatků v IoT zařízeních za pomoci řešení na principu DNS, které zabezpečuje komunikaci a takto limituje možný útok na IoT zařízení. Ochrana průmyslových IoT zařízení na síťové úrovni, ale i na úrovni DNS pomáhá zbavit se rizik jako je DNS Cache Poisoning, která zachycuje komunikaci mezi zařízeními a využívá všech jejich chyb. [47]

Zásadní je nedůvěřovat neproověřeným zařízením snažícím se připojit k síti za pomoci rekurzivní infrastruktury. Dobrou volbou je DNS filtrování žádostí, která spoléhá na whitelisting, což je seznam zařízení, které se můžou připojit. Toto izoluje veškerá ostatní zařízení od jakékoliv komunikace se serverem a jejich požadavky nejsou dále zpracovávány.

Nezbytnou součástí je zajištění integrity a věrohodnosti DNS informace za pomoci DNSSEC na DNS infrastruktuře. Ověřuje integritu všech záznamů, zjišťuje, zda záznam vychází z ověřeného DNS serveru a ujišťuje se, že je server určen jako důvěryhodný vyšší doménou v DNS hierarchii, tzv řetěz důvěry. [48]

DNS může být použito pro zvýšení přístupnosti a její kontroly do infrastruktury IoT zařízení, která mohou být používána v sítích s vysokou hustotou jako jsou například malá města nebo továrny až po rekreační zařízení nebo domácnosti. [49]

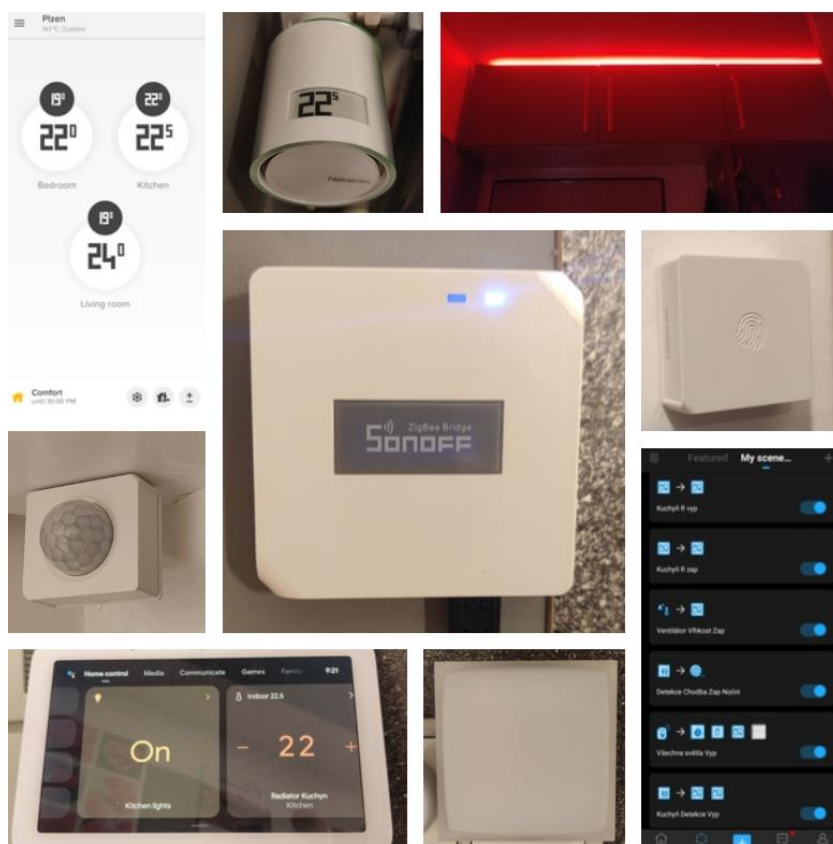
1.8 Zařízení a procesy pro úsporu energie

Definované rutiny

Rutiny v chytré domácnosti jsou seznamem činností, které se provedou v jednom okamžiku, místo spínání jednotlivých funkcí separátně. Sepnutí se většinou provádí hlasovým příkazem nebo specifickou akcí, jako je například zjištění pohybu v daný čas. Jako příklad rutiny bych uvedl jako podmět otevření dveří v obvyklý čas příchodu z práce, následné automatické zapnutí světel, spuštění hudby a nastavení vyšší teploty v obytných místnostech.

Centrální spínač

Jedním z důležitých prvků domácnosti je centrální spínač. Jeho účelem je při stisknutí vypnout, nebo obnovit funkci, veškerých ovládaných zařízení v domácnosti za účelem úspory energií. Spínač může být nastaven několika způsoby jako například režim odchodu při jednom stisknutí, kdy se vypnou veškerá zařízení a teplota ve všech místnostech se nastaví na nižší teplotu, zároveň můžou senzory na oknech upozornit, zda nejsou otevřena. V opačném případě po dvojitém stisknutí se obnoví funkce domácnosti. Využívá se hlavně v mimo rutinních případech jako je odjezd na dovolenou.



Obr. 7 Část zařízení a aplikací použitých v systému

1.8.1 Úspora elektrické energie

Automatická světla

Automatizace domácnosti dokáže za pomoci vypínání světel, které byly omylem ponechány zapnuté, šetřit elektrickou energií. Tohoto cíle lze dosáhnout za pomoci senzorů pohybu umístěných v místnostech, které zapínají světla při detekci pohybu a vypínají je, pokud v místnosti nezaznamenají pohyb. Další možností je nastavení senzorů podle množství přirozeného světla v místnosti a následná regulace jejich intenzity. Takto lze nastavit například noční režim, kdy se zapne pouze část světel na nižší jas. [50]

Odpojení spotřebičů

Mnoho spotřebičů odebírá nezanedbatelné množství energie, i když jsou vypnuty, jedná se o vše od strojků na vlasy až po televize. Energie spotřebovaná těmito zařízeními, které nejsou využívány, může zastupovat až 10 % měsíčních výdajů za elektřinu [51]. V minulosti bylo možné se této spotřebě vyhnout pouze přímým odpojením zařízení od sítě. Za pomoci chytrých zásuvek a vypínačů, které se připojují před spotřebiče, lze odpojit zařízení nevyužitá zařízení, dokud znovu nebudou zapotřebí. Toto lze jednoduše zařídit přes automatizační software.

1.8.2 Úspora tepelné energie

Automatické žaluzie

V letních měsících je výhodné zastínit okna, na které dopadá přímý sluneční svit, který zahřívá místnost a zbytečně se zapíná klimatizace. Automatické motorizované žaluzie lze nastavit na zavření v daném časovém intervalu, nebo na senzor teploty umístěný na vnější straně oken. Venkovní senzor reaguje na vysoký nárůst teploty, pokud se nachází ve slunečním svitu a vyšle signál žaluziím, aby se zavřely, po snížení teploty se zase otevrou, aby se zbytečně neplýtvala energie skrz svícení. [52]

Chytré termostaty

Termostaty jsou efektivním způsobem snížení spotřeby energie za klimatizaci a vytápění elektřinou. Většina moderních termostatů má zlepšenou funkcionalitu pro lepší regulaci teploty a tím pádem větší úspory, které se pohybují v rozmezí 10-15 % v závislosti na izolaci a návrhu domácnosti [53]. Senzory v domácnosti se dokážou naučit návyky jednotlivých uživatelů a upravovat teplotu podle obsazenosti místnosti a denních rutin. Měsíční shrnutí spotřeby energie mohou být využita k lepšímu pochopení modelů vytápění a chlazení. Tyto zprávy mohou nabídnout detailnější pohled na ovládání ventilace a teplotních zón.

Chytré ohřívače vody

Na rozdíl od konvenčních ohřívačů vody, které pouze udržují vodu při konstantní teplotě, mají chytré ohřívače schopnost odesílat data k dalšímu zpracování a optimalizaci ohřevu. Při spojení s průtokovým senzorem na zjištění spotřeby vody, dokáže centrální jednotka vytvořit model vaší spotřeby teplé vody a ohřívat vodu na vyšší teplotu pouze pokud je nutná, například při odchodu do práce, nočních hodinách nebo lze nastavit ohřev pár hodin před příjezdem z dovolené. Hlavní výhodou oproti konvenčním ohřívačům je schopnost se přizpůsobit měnícímu se životnímu rytmu uživatele a ovládání za pomoci mobilních zařízení.

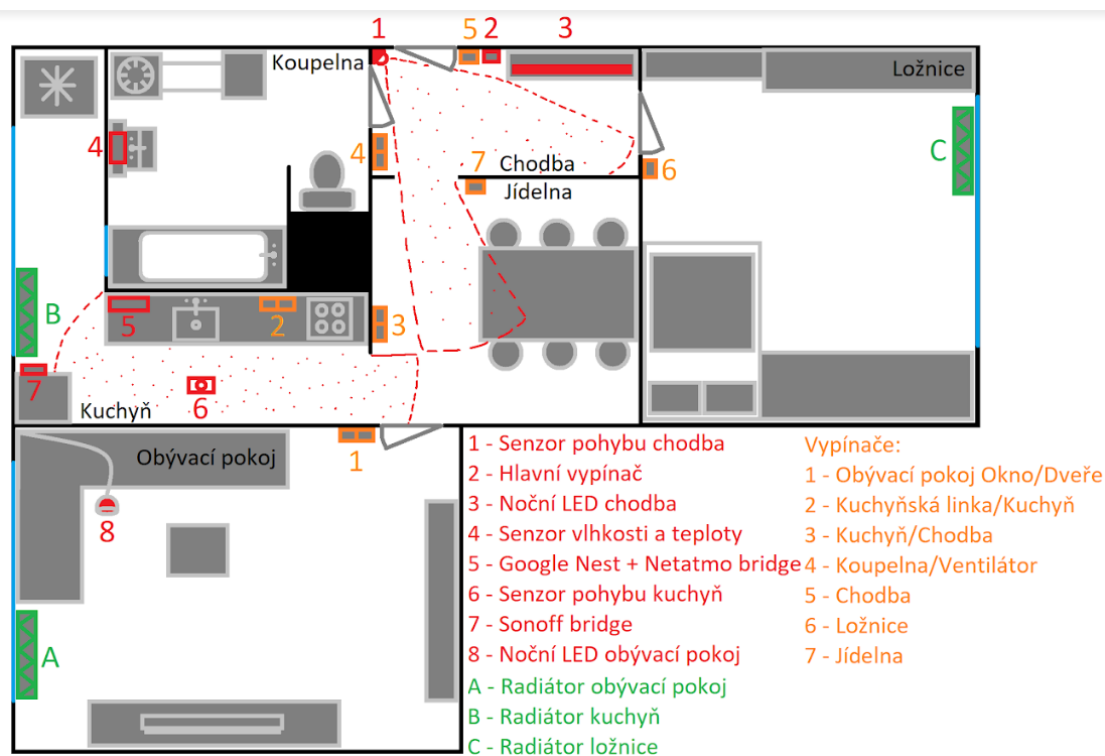
2 Vlastní systém

2.1 Návrh systému

Jedním z nejdůležitějších kritérií při výběru a návrhu systému je určení požadovaných funkcí a v závislosti na tom výběr požadovaných senzorů a zařízení. Nejlepší čas na návrh systému je zároveň s návrhem domácnosti, a to hlavně z důvodu výběru kompatibilních spotřebičů a uzpůsobení rozvodů v domácnosti vašemu IoT řešení. Pokud se jedná o již stávající obytný objekt, je možné IoT systémy dodělat, často je však potřeba vyměnit staré spotřebiče, nebo použít externí zařízení na ovládání spotřebičů.

Ať už se jedná o nový nebo stávající objekt, je důležité si vytvořit schématický náčrsek rozmístění jednotlivých senzorů a spotřebičů. Je mnohem jednodušší umístit zařízení do jasného náčrtu než do seznamu bez vizualizace, která napomáhá i ke zjištění nedostatků v možném pokrytí senzorů.

V mém případě se jedná o stávající byt a cílem je úspora energií a zlepšení kvality života. Plná automatizace domácnosti není prioritou, a proto se obejdu bez výměny drahých spotřebičů, nebo instalace externího řízení. Mým hlavním cílem je omezení plýtvání elektrické energie zbytečným svícením světel, omezení vytápění domácnosti v mé nepřítomnosti, nebo při otevření oken a ujištění, že jsou všechna světla opravdu vypnutá v mé nepřítomnosti za pomoci monitorovacích aplikací.



Obr. 8 Schéma mého systému

2.2 Jednotlivé komponenty

Sonoff T1 – spínač

Jedná se o chytrý Wi-Fi spínač v provedení s jedním až třemi tlačítky na vypínač. Jednotka je vyrobená z plastu s dotykovými tlačítky, komunikuje přes domácí Wi-Fi síť a ke své funkčnosti potřebuje 230 V s připojením na světlo. Tento typ vypínačů nevyžaduje žádný přídatný bridge ani baterie. Po jednoduchém spárování spínačů s aplikací eWelink nainstalovanou v mobilním telefonu je možné vytvořit schodišťový vypínač, přičemž jeden nebo více ze spínačů může být připojen pouze na elektrickou síť bez přímého spojení se světlem. V mém systému toho je využito u spínače Chodba, ve schématu číslo 5, a Kuchyň, ve schématu číslo 2. Tímto zapojením se eliminuje nutnost přídatného kabelu mezi vypínači a zjednodušuje se zapojení.



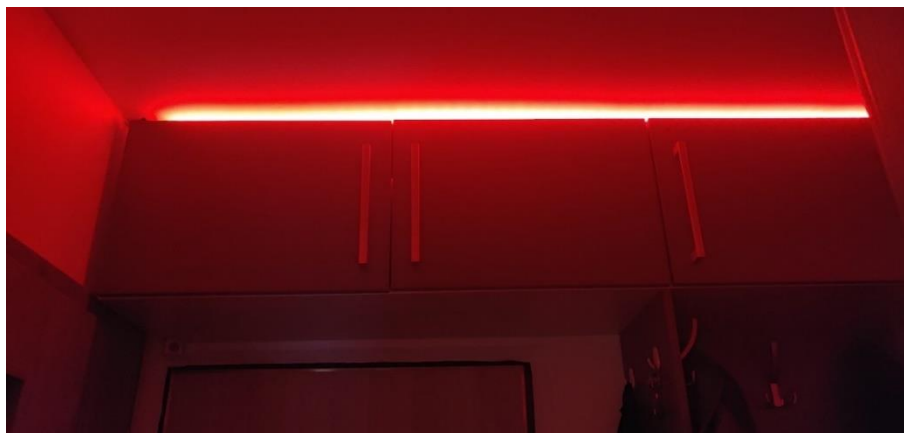
Obr. 9 Jedno/dvoutlačítkové spínače

Spínač je možné ovládat manuálně stiskem tlačítka na jednotce, rutinami za pomoci přídatných senzorů, prostřednictvím aplikace eWelink, nebo hlasových příkazů po integraci do aplikací jednoho z hlasových asistentů. Všechny jednotlivé spínače a jejich náležitá tlačítka je možné separátně pojmenovat dle jejich umístění a funkce. V mém případě jsou spínače v kuchyni a na chodbě výhradně řízeny přídatnými senzory, v ostatních místnostech se jedná o kombinaci hlasových příkazů a fyzického stisknutí tlačítka na jednotce. Tlačítka na vypínačích jsou podsvícena jemným modrým světlem pro jednoduchou operaci tlačítka v nočních hodinách. Indikátor připojení k Wi-Fi síti, který svítí mnohem jasněji a je poměrně rušivý, lze vypnout v aplikaci.

Sonoff L1 – LED pásek

Jedná se o inteligentní vodotěsný LED pásek s in-line transformátorem na 12 V, který je schopen dodat výkon 24 W. Disponuje světelným tokem 300 lumenů na metr, komunikuje přes domácí Wi-Fi síť nebo za pomoci IR ovladače, který je součástí balení. Pásek obsahuje RGB LED a oproti RGBW LED páskům nedokáže vytvořit dokonale bílé světlo. Stejně jako spínač je možné LED pásek ovládat přes aplikaci, rutiny nebo hlasovými příkazy. Jediný způsob ovládání, který využívám, je za pomoci rutin a přídavných senzorů.

LED pásek je v mém systému použit za účelem úspory energie v nočních hodinách, kdy není potřeba zapínat hlavní světlo na chodbě, ve schématu číslo 3, Noční LED chodba. Pásek je nastaven na čistě červené světlo, které není rušivé. V ideálním systému by nebylo zapotřebí přídavného pásku, ale bylo by využito tlumitelných LED v hlavním osvětlení, v mém případě by bylo nutné vyměnit světla v celém bytě.



Obr. 10 LED pásek v nočních hodinách

Sonoff B02-F-ST64 – LED žárovka

Inteligentní LED žárovka, která je schopna stmívat a má možnost změny teploty barvy. Po instalaci do klasické světelné objímky funguje na 230 V a komunikuje přes Wi-Fi. Světlo nevyžaduje žádný přídavný bridge a ke své základní funkčnosti nepotřebuje aplikaci. Na detailnější nastavení je zapotřebí nainstalovat aplikaci eWelink, která umožňuje řídit teplotu barvy, jas a dokáže žárovku spojit s chytrým vypínačem bez potřeby kabelového spojení. Žárovku je možné ovládat i klasickým vypínačem v domácnosti. Pokud chcete využívat jak chytrých funkcí, tak běžného vypínače, nastane problém, že při vypnutí žárovky vypínačem se odpojí od Wi-Fi sítě, jelikož již není napájena.

V mém systému se jedná o noční LED obývací, ve schématu číslo 8. Nainstalována byla z důvodu úspory energie, možnosti řízení domácím systémem a tím pádem i vypnutí v momentu odchodu z domu. V nočních hodinách je žárovka nastavena na teplé žluté světlo

a na vypínači v obýváku nahrazuje hlavní světlo, které lze zapnout pouze přes aplikaci nebo hlasovým příkazem.



Obr. 11 Inteligentní LED žárovka

Sonoff SNZB-03 – senzor pohybu

Jedná se o inteligentní senzor pohybu komunikující za pomoci ZigBee 3.0. Senzor ke své funkci potřebuje kompatibilní ZigBee hub, nebo bridge, pokud se v domácnosti budou používat pouze zařízení od jednoho výrobce, tak je nejjednodušší použít přímo jeho bridge. Propojení s bridgem zajišťuje aplikace eWelink, za pomoci které je možnost nastavit další parametry, jako je výchozí nastavení sepnutí při detekci pohybu nebo bez. Jelikož se jedná o zařízení s nízkou spotřebou energie, tak je senzor poháněn 3V baterií CR2450.

Senzor snímá prostor v úhlu 110° a zachycuje pohyb do vzdálenosti 6 m, je tedy zapotřebí uvažovat o umístění, aby senzor snímal požadovanou oblast. V mém případě je senzor pohybu kuchyň, ve schématu číslo 6, umístěn na stropě a zabírá tak mnou požadovanou oblast v celé délce kuchyňské linky. Senzor pohybu chodba, v diagramu číslo 1, je umístěn na stěně, tak aby snímal celou oblast chodby, pokud by tento senzor byl umístěn na stropě, tak by neobsáhl mnou požadovanou oblast. Oba senzory byly nainstalovány za účelem úspory energie a jsou hlavními spínači pro světla na chodbě a v kuchyni.



Obr. 12 Nainstalovaný senzor pohybu

Sonoff SNZB-01 – chytré tlačítko

Jde o inteligentní tlačítko, které komunikuje za pomoci ZigBee 3.0. Senzor ke své funkci potřebuje kompatibilní bridge. Propojení s bridgem zajišťuje aplikace eWelink, ve které se nastavují požadované funkce. Jedná se o zařízení s nízkou spotřebou energie a je tedy napájeno 3V baterií VR2450. Tlačítko dokáže rozeznat tři typy stisknutí, a to jedno kliknutí, dvojklik a dlouhé stisknutí.

Tlačítko, ve schématu číslo 2, je v mém systému umístěno u vchodových dveří do bytu. Je využito pro nastavení systému do režimu odchodu, za pomoci jednoho kliknutí, a zpět do režimu normálního chodu, za pomoci dvojkliku. Dalším neméně důležitým účelem tlačítka je ujištění odcházejícího člověka, že se nemusí strachovat, zda nenechal zapnuté nějaké světlo.



Obr. 13 Chytré tlačítko

Sonoff SNZB-02 – senzor teploty a vlhkosti

Jedná se o inteligentní senzor teploty a vlhkosti komunikující za pomoci ZigBee 3.0. Senzor ke své funkci vyžaduje kompatibilní bridge a aplikaci eWelink, bez které není v mém systému možné ho spárovat. Jelikož se jedná o nízkoenergetické zařízení, tak je napájeno 3V baterií CR2450. Senzor měří teplotu a vlhkost v místnosti s přesností na jedno desetinné místo.

V mém systému, ve schématu číslo 4, je senzor instalován v koupelně, kde je využit na spínání ventilátoru, při dané úrovni vlhkosti.



Obr. 14 Inteligentní senzor teploty a vlhkosti

Netatmo Smart Radiator Valve – chytrá hlavice topení

Jde o chytrou termostatickou hlavici komunikující za pomoci ZigBee 3.0. Ke své základní funkci nepotřebuje bridge, ale jakékoliv nastavení je prováděno po připojení k bridge přes aplikaci Netatmo Energy. Jedná se o zařízení s nízkou spotřebou energie, které je napájeno dvojicí 1,5V baterií. Po spárování termostatu s aplikací je možné nastavit denní cyklus vytápění, zapnout detekci otevřeného okna, při kterém se vypne vytápění, a zapnout režim odjezdu na dovolenou.

V mém systému jsou hlavice, ve schématu A/B/C, nainstalovány na každém topení v bytě. Každá hlavice má nastaven svůj separátní denní cyklus. Hlavice je možné ovládat za pomoci aplikace, hlasovými příkazy, nebo přímo na hlavici. Ovládání na hlavici na daný čas nastaví zvolenou teplotu a po čase, v mém případě 3 hodiny, se navrátí zpět do denního cyklu. Hlavice mají v sobě integrovaný senzor teploty a není nutné instalovat další senzor. V případě odchodu z bytu na delší dobu lze nastavit režim „dovolená“, který nastaví teplotu na celodenní udržování, v mém případě 16 °C.



Obr. 15 Chytrá hlavice topení

2.3 Řídící jednotky, huby a bridge

Sonoff ZigBee Bridge

Sonoff ZigBee Bridge je zařízení napájené 12V zdrojem přes Micro USB. Celé zařízení je vyrobeno z plastu, váží 35 g a má poměrně malé rozměry, přesněji 62x62x20 mm. Zařízení také disponuje dvojitou LED na indikaci propojení s Wi-Fi sítí a provedení akce přes ZigBee. Jeho funkcí je propojení zařízení komunikujících přes ZigBee 3.0 a jejich následné připojení k domácí 2,4GHz Wi-Fi síti, síť 5GHz není podporována. Výhodou tohoto typu spojení je to, že je uživatel schopen připojit nízkoenergetická zařízení k mnohem energeticky náročnější Wi-Fi síti. Bridge se z pohledu Wi-Fi sítě vždy tváří jako jedno zařízení, nezávisle na počtu zařízení, která jsou připojená přes ZigBee. S tímto bridgem jsou schopna komunikovat pouze kompatibilní zařízení od výrobce Sonoff. Je schopen propojit až 32 zařízení do vzdálenosti 75 m, každé další zařízení propojené na síť 230 V, které s bridgem komunikuje přes ZigBee funguje jako opakovač signálu a prodlužuje dosah o dalších 75 m. Se zabezpečením se spoléhá na domácí Wi-Fi síť. Uživatelské rozhraní zajišťuje aplikace eWelink, ve které se provádí párování se senzory.

V mém systému, na schématu číslo 7, je využit ke spojení senzorů pohybu, teploty a vlhkosti a inteligentního tlačítka, bez bridge by tato zařízení byla bezvýznamná.



Obr. 16 Sonoff ZigBee Bridge

Netatmo ZigBee Bridge

Netatmo ZigBee Bridge je zařízení napájené 230 V. Celé zařízení je vyrobeno z plastu, váží 95 g a jeho rozměry jsou 85x85x45 mm. Komunikuje přes ZigBee 3.0 a domácí 2,4GHz Wi-Fi síť. Funkce tohoto zařízení je spojení a řízení chytrých termostatických hlavic od výrobce Netatmo. Ke své funkci a spárování hlavic je zapotřebí nainstalovat aplikaci Netatmo Energy.

V mém systému, ve schématu číslo 5, nainstalován nad kuchyňskou linkou a je využit k ovládání termostatických hlavic nainstalovaných na radiátorech, na schématu A/B/C. Jednotka se stará o dodržování předem nastavených vyhřívacích cyklů v domácnosti.



Obr. 17 Netatmo ZigBee Bridge

Google Nest Hub

Google Nest Hub je zařízení napájené 230 V. Zařízení má integrovaný dotykový displej s úhlopříčkou 178 mm a rozlišením 1024x600 pixelů, celé zařízení má rozměry 178x118x67 mm. Obsahuje 2 mikrofony pro hlasové ovládání, 20W reproduktor a senzor pohybu. Komunikuje pouze přes domácí Wi-Fi síť a vyžaduje účet u společnosti Google pro

konfiguraci zařízení. Google Nest Hub disponuje vlastním operačním systémem na bázi Google Assistant, vyžaduje aplikaci Google Home k propojení s ostatními zařízeními a pro jejich následnou automatizaci. Zařízení spoléhá jak na zabezpečení domácí Wi-Fi sítě tak na TLS protokolu.

V mém systému, ve schématu číslo 5, je zařízení využíváno k jednotnému řízení zařízení, bridge a hubů od jiných výrobců, jako jsou Netatmo a Sonoff. Zároveň je to jediné zařízení v mém systému s displejem, který je využíván jako uživatelské rozhraní pro zobrazení dat z přiřazených zařízení. Celý systém je možno řídit hlasovými příkazy, nebo dotykově přes Google Nes Hub bez nutnosti mobilního zařízení.



Obr. 18 Google Nest Hub

2.4 Rutiny a automatizace

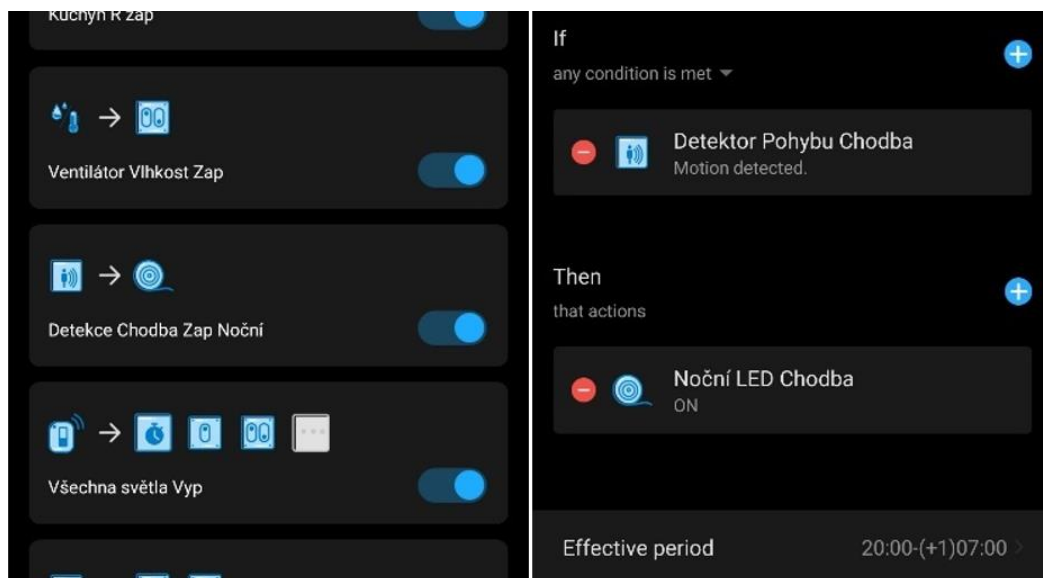
Automatizace elektrických spotřebičů

Rutiny v mém systému jsou využívány pro automatizaci zařízení pro úsporu energií a zlepšení kvality života v bytě. V aplikaci eWelink je za pomoci podmíněných příkazů na principu „if, then“, jednoduché definovat požadované akce. Jde nastavit cokoliv od zapnutí světel při stisknutí tlačítka v určitých denních hodinách po zapnutí hudby při příchodu z práce. Přes rutiny v této aplikaci je řízeno veškeré osvětlení v bytě a ventilace prostoru koupelny.

Jako příklad jsem vybral automatizaci světel na chodbě v nočních hodinách, o kterou se stará senzor pohybu na chodbě a noční LED pásek. Při detekci pohybu na chodbě senzor vyšle signál do Sonoff ZigBee Bridge, který signál zaregistruje, zkontroluje momentální čas a pokud se shoduje v nastaveném časovém intervalu, aktivuje noční LED pásek. Jakmile senzor pohybu po nastavenou dobu, v mém případě jedna minuta, nedetekuje žádný pohyb,

vyšle opět signál do bridge, který LED pásek vypne. Tato vypínací rutina je aktivní 24 hodin denně a funguje i pro denní osvětlení chodby. Veškeré rutiny jsou řízeny Sonoff bridgem bez nutnosti mobilního zařízení, které je potřeba pouze na konfiguraci a změny v rutinách.

Výše zmíněné rutiny přestávají fungovat, jakmile je stisknuto chytré tlačítko u vchodových dveří, které nastaví byt do režimu odchodu a zároveň vypne veškeré osvětlení. Rutiny jsou obnoveny po dvojitém stisknutí stejného tlačítka.



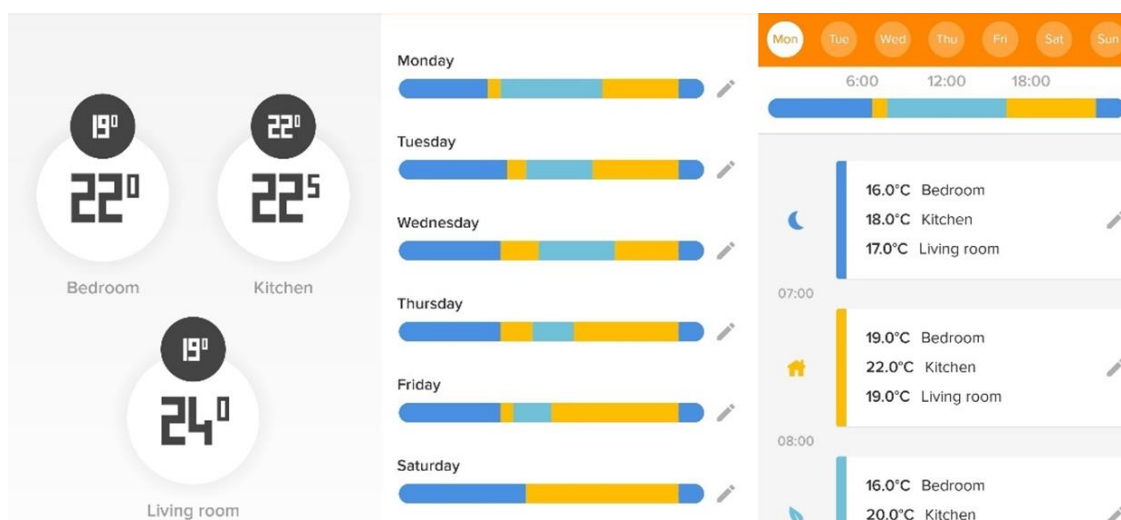
Obr. 19 Aplikace eWelink

Automatizace vytápění

Za pomoci aplikace Netatmo Energy je v mém systému ovládáno a automatizováno vytápění bytu. Chytré hlavice radiátorů jsou řízeny skrz Netatmo ZigBee Bridge, všechny hlavice mají svůj integrovaný termostat, za pomoci kterého regulují teplotu podle nastaveného denního cyklu. Hlavice dokážou detekovat otevření okna, tato funkce funguje na principu rychlého poklesu teploty na čidle teploty, pokud je tento pokles detekován, vytápění daného pokoje se pozastaví. Veškeré porovnávání teplot provádí přímo Netatmo bridge.

Aplikace je schopná upravovat denní cyklus vytápění podle častých manuálních změn teploty na samotné hlavici.

Vytápění lze nastavit do režimu „dovolené“, aneb odchodu na delší dobu z domácnosti, za pomoci chytrého tlačítka umístěného vedle vchodových dveří bytu, jedním stisknutím se se pozastaví normální cyklus a ve všech místnostech je nastavena teplota na 16 °C. Po návratu a dvojitým stisknutím tlačítka se obnoví normální vyhřívací cyklus.



Obr. 20 Aplikace Netatmo Energy

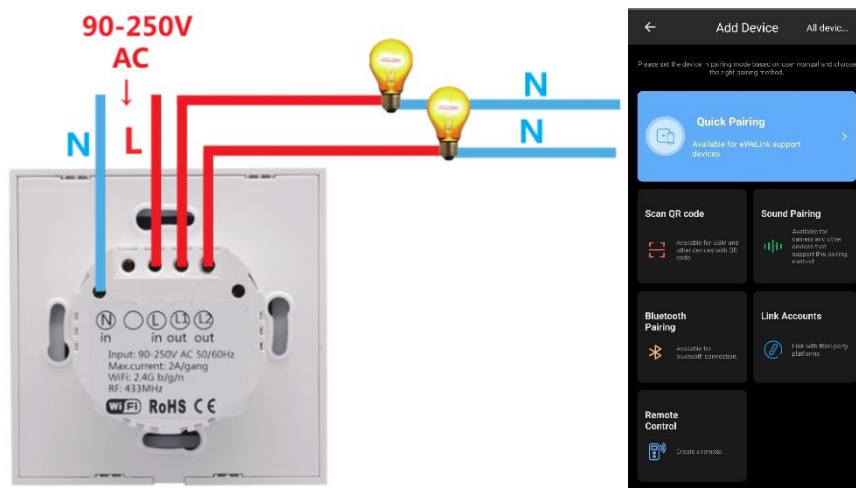
2.5 Instalace zařízení

Instalace veškerých zařízení probíhala podle návodů, které byly součástí balení všech zařízení, v případě Google Nest Hub je návod zobrazen po prvním zapnutí zařízení. Všechny příložené návody byly srozumitelné, přehledně napsané a graficky znázorněné i pro širokou veřejnost bez znalostí elektrických zařízení a domácí elektroinstalace.

Vypínače Sonoff

Instalace vypínačů probíhala bez větších problémů. Je zapotřebí se předem zjistit, zda máte na vypínače dostatek místa, jelikož jsou rozměrově větší (85x85 mm), než klasické vypínače a nevejdou se dva těsně vedle sebe. Dále je k funkčnosti zapotřebí nulového (modrého) vodiče, je to z důvodu napájení řídicího prvku vypínače pro spojení s Wi-Fi sítí.

Nastavení a párování s vypínači probíhá v příslušné aplikaci eWelink. Jedná se o velmi jednoduchý proces, ke kterému je zapotřebí mít staženou aplikaci eWelink a být připojen k domácí Wi-Fi síti na které budete chtít vypínač dále automatizovat. Aplikace vás srozumitelně provede procesem párování a přiřazení zařízení k vámi zvolené místnosti.



Obr. 21 Zapojení vypínače Sonoff T1 [54]

ZigBee zařízení

Zařízení komunikující přes ZigBee vyžadují k chodu velmi malé množství energie, a proto jsou většinou napájeny baterií. Instalace je tedy velmi jednoduchá, stačí vložit baterii, nebo odstranit bezpečnostní kryt, který vložené baterii brání v kontaktu se zařízením. Tato zařízení většinou automaticky přejdou do režimu párování, nebo je nutné je do něj nastavit. Většinou se jedná o stisknutí jediného tlačítka na zařízení.

Instalace zařízení na vámi zvolené místo se provádí přišroubováním do objímky, která je součástí balení, nalepením, nebo položením na požadované místo.

Párování probíhá v prostředí příslušných aplikací, v mém případě eWelink, pro výrobky Sonoff, a Netatmo Energy pro hlavice radiátoru. Vždy je nutné se nejprve spárovat s kompatibilním bridgem a následně pokračovat v párování ostatních zařízení dle pokynů aplikace.



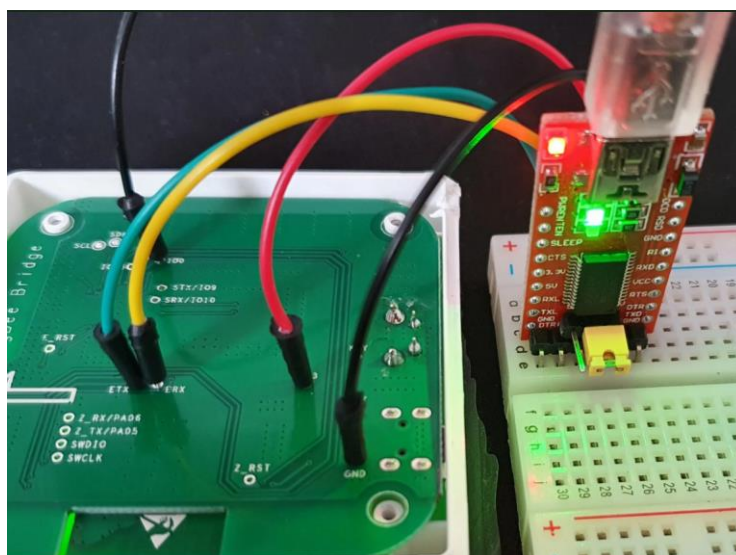
Obr. 22 Otevřený senzor teploty a vlhkosti s párovacím tlačítkem

2.6 Zlepšení instalovaného systému

Jednotný Hub

V momentální konfiguraci můj systém vyžaduje k plné funkčnosti 3 huby a bridge od různých výrobců. V ideálním případě by celý systém byl řízen jednou centrální jednotkou schopnou komunikovat se všemi senzory, provádět automatizaci a poskytovat jasné uživatelské rozhraní.

Jednou z možností je využít jedno z již nainstalovaných zařízení schopných komunikovat přes ZigBee a Wi-Fi, v mém případě bych vybral Sonoff bridge, vzhledem k jeho velikosti a způsobu napájení. Na bridge by bylo nutné přinstalovat firmware výrobce na námi vybraný. Pro instalaci je nutné rozebrat celý bridge, zakoupit specifický adaptér a napojit se přímo na základovou desku bridge, což není pro normálního uživatele jednoduché. Existuje více možností systémů, mým výběrem byl firmware Tasmota MQTT, který disponuje kontrolou kvality přenesených dat a má rozsáhlejší možnost automatizace.



Obr. 23 Sonoff ZigBee Bridge připravený na instalaci firmware [55]

Instalace přídavných senzorů

Můj systém by pro optimální funkci vyžadoval větší množství senzorů, než je momentálně nainstalováno. V ideálním případě by každá místnost obsahovala svůj vlastní senzor teploty pro přesnější ovládání vyhřívání, protože senzory na hlavicích radiátorů jsou zkreslovány z důvodu jejich těsné blízkosti ke zdroji tepla. Každé okno, které je často otevřeno, by vyžadovalo senzor otevření, aby se nespolehalo na detekci otevřeného okna, integrovanou v hlavicích.

Bezpečnostní prvky

Aktuální systém se spoléhá na zabezpečení domácí Wi-Fi sítě a TLS, v případě Google Nest Hub. Ideální variantou pro zlepšení zabezpečení by bylo zakoupení VPN pro řízení systému. Jedná se o nejjednodušší způsob, který nevyžaduje žádné hardwarové změny v systému. Nevýhodou je měsíční poplatek za její využívání.

Zabezpečení se netýká jen dat ale i osob, z tohoto důvodu bych nainstaloval senzor otevření hlavních dveří a kameru na chodbě namířenou na vchodové dveře do bytu. Jednalo by se o senzor Sonoff SNZB-04 a kameru Sonoff GK-200MP2-B. Obě zařízení jsou kompatibilní s momentálními řídicími jednotkami a nebylo by zapotřebí provádět změny v systému.

Záloha dat

Záloha dat na externím úložišti je důležitá pro obnovu dat v případě poruchy kteréhokoliv z hubů, bridge nebo senzorů. V případě Google Nest Hub se záloha provádí v automaticky nastavených intervalech, většinou jednou týdně, na cloud propojený s vaším Google účtem. V případě použití jednotného hubu, jako Tasmota, je nutné vytvořit zařízení schopné ukládat data a nastavit automatické zálohování. V nejlepším případě by se úložiště na zálohu mělo nacházet v jiné lokaci a na jiné síti než zálohované zařízení. Důvod je lepší zabezpečení dat a v případě zničení zařízení, například při požáru, nebude poškozena i záloha.

Vlastní zařízení

Další možností by byla výroba vlastního zařízení od základů, za pomoci jednotlivých modulů s požadovanou funkcí, jako jsou například teplotní čidla, závory s infračervenou detekcí a moduly pro komunikaci pomocí protokolů jako jsou Wi-Fi a ZigBee. Výhodou výroby vlastního zařízení je vysoká modularita a nižší cena zařízení. Nevýhodou je nutnost vytvoření, popřípadě jen nahrání, firmware, potřeba hlubší znalosti programování, vlastní pájecí stanice a nízká podpora ze strany výrobců, zejména u čínských výrobků, které většinou disponují manuálem jen v čínském jazyce. Tímto tématem se zabývá zdroj [56].

3 Vyhodnocení praktické části

3.1 Celková cena systému

Jednotlivé komponenty byly zakoupeny po návrhu systému, včetně DPH, který byl proveden za pomoci informací dostupných z internetových stránek výrobců. Veškerá instalace byla prováděna mnou a není možné započítat cenu systému v případě návrhu a instalace specializovanou společností.

Některá zařízení byla zakoupena ve slevě, nebo ve výhodném balíčku. Veškeré ceny uvedené v následující tabulce budou odkazovat na specifické datum a prodejce.

Výběr prodejce

Při výběru prodejce jsem se zaměřil především na příznivou cenu, dostupnost a možnost vrácení zboží v případě nekompatibility se zbytkem systému.

Většinu zařízení jsem zakoupil u prodejce Alza.cz kvůli příznivé ceně a dopravě zdarma, která mi byla poskytnuta programem Alza Premium, jehož jsem součástí. Dalším důvodem byla jednoduchost vyzvednutí, nejbližší výdejní místo se nachází asi 200 metrů od bytu, do kterého jsem systém instaloval. V neposlední řadě jsem prodejce vybral kvůli široké síti prodejen a tedy snadné výměny, nebo vrácení, zboží z důvodu nekompatibility po dobu 14 dnů od zakoupení zboží.

Prodejce Smart-Switch.cz jsem zvolil z důvodu nedostupnosti některých potřebných zařízení u prodejce Alza.cz a možnosti zakoupení výhodného balíčku Sonoff Zigbee Set, ve kterém se nacházel Sonoff ZigBee Bridge, a 4 nízkoenergetická bateriová zařízení dle mého výběru. Vrácení zboží by u tohoto prodejce bylo nutné provést zasláním zařízení zpět k prodejci za pomoci přepravní služby, jelikož se jedná pouze o e-shop.

Žádný z vybraných prodejce neposkytuje instalaci zařízení ani prvotní návrh systému. Pro návrh a instalaci by bylo zapotřebí výběru specializované společnosti, která by mnohonásobně navýšila potřebný rozpočet. Součástí instalace systému by nejspíše byl i zásah do stávajících elektrických rozvodů v domácnosti.

Tabulka 2 Cena zakoupených zařízení se slevami a balíčky

Název zařízení	Název v systému	Množství	Místo zakoupení	Datum	Cena [Kč]			
Sonoff Zigbee Set	Sonoff ZigBee Bridge	1	Smart-Switch.cz	14.03.2022	1 899			
	Senzor pohybu	2						
	Chytré tlačítko	1						
	Senzor teploty a vlhkosti	1						
Netatmo Smart Radiator Valves Starter Pack	Netatmo ZigBee Bridge	1	Alza.cz		14.03.2022	4 239		
	Chytrá hlavice topení	2						
Netatmo Additional Smart Radiator Valve	Chytrá hlavice topení	1				Alza.cz	14.03.2022	1 919
Google Nest Hub (2nd gen)	Google Nest Hub	1						2 289
Sonoff T1EU1C-TX	Spínač jednotlačítkový	2						1 018
Sonoff T1EU2C-TX	Spínač dvoutlačítkový	4						2 116
Sonoff T1EU1C-TX-rozbalené zboží	Spínač jednotlačítkový	1		433				
Sonoff B02-F-ST64	LED žárovka	1		17.03.2022				399
Sonoff L1 5m	LED pásek	1						639
Celková cena								14 951

3.2 Porovnání úspor a ztrát

Měření úspor systému jsem prováděl po dobu měsíce dubna. Spotřebu elektrické energie jsem odečetl z elektroměru bytu. Tepelnou energii jsem měřil za pomoci Q calorics 5.5 měřičů nainstalovaných na veškerých radiátorech v bytě. Měřiče zaznamenávají počet hodin, při kterých byla teplota média uvnitř radiátoru vyšší než 41 °C.

Úspora elektrické energie

Spotřeba elektrické energie za stejné období minulého roku činila dle faktury od společnosti GEEN a.s. 187 kWh. Po instalaci systému jsem naměřil spotřebu 175 kWh, to znamená že systém uspořil 12 kWh za měřené období, tedy 7 %. S průměrnou cenou 4.095 Kč/kWh, včetně DPH, se jedná o úsporu **49 Kč měsíčně**. Cena zařízení na úsporu energií činila 8.703 Kč, to znamená že návratnost systému je 14 let.

Spotřeba tepelné energie v jednotlivých místnostech

Spotřeba v různých místnostech bytu se razantně liší z důvodu rozdílných velikostí místností, množství oken, jejich nasměrování a rozdílných návyků jednotlivých sousedů.

V celém bytě byla před čtyřmi lety provedena rekonstrukce, při které se instalovala dodatečná izolace na stropěch všech místností. Z tohoto důvodu je v místnostech směřujících na jih, ložnice a obývací pokoj, které jsou během roku v přímém slunečním svitu, mnohem nižší spotřeba energie na vytápění. Ložnice a obývací pokoj sousedí dvěma stěnami, podlahou a stropem s byty nájemníků, kteří vytápí na poměrně vysokou teplotu a sálavé teplo ze stěn je dostačující na udržení teploty 22 °C v těchto místnostech, bez potřeby vytápění, z tohoto důvodu je v tabulce značena nulová spotřeba.

Nejvyšší spotřeba je v místnosti směřující na sever, v tomto případě kuchyň, která se nachází přímo pod prázdným bytem, který není vytápěn. Všechny tyto faktory přispívají k rozdílu ve spotřebě energie, především mezi kuchyní a obývacím pokojem.

Ztráta tepelné energie

Tabulka 3 Hodnoty výhřevu z měřičů Q caloric 5.5

Umístění měřiče	Spotřeba za stejné období minulého roku [hodin]	Spotřeba za měřené období [hodin]
Kuchyň	49	54
Obývací pokoj	0	0
Ložnice	2	4
Celková hodnota [hodin]	51	58

Z tabulky je vidět, že systém za měřené období spotřeboval o 12 % více energie než ve stejném období minulého roku, i přes vyšší průměrnou teplotu venkovního vzduchu.

Ztrátu vyvažuje zvýšený komfort v bytě, po instalaci systému se zlepšila kvalita mého spánku, díky automatickému snížení teploty v nočních hodinách a následné vyhřívání, především v oblasti kuchyně, hodinu před plánovaným vzbuzením.



Obr. 23 Vyhřívací graf pro kuchyň z aplikace Netatmo Energy

4 Závěr

Hlavním cílem této práce bylo vytvořit systém, který by byl schopen úspory energií. Aktuální systém splňuje stanovený cíl v oblasti elektrické energie, úspora za měřené období činila 7 %, oproti stejnému období minulého roku. Systém tedy lze z tohoto hlediska doporučit.

Pro úsporu elektrické energie byla zvolena zařízení od společností Sonoff a Google, která spolu po konfiguraci a nastavení rutin komunikovala prostřednictvím domácí Wi-Fi sítě, automatizace tedy byla bezproblémová. Byly vybrány senzory pohybu, chytrá tlačítka, senzory teploty a vlhkosti, LED pásky a žárovky, spínače, ZigBee bridge a centrální řídicí jednotka s uživatelským rozhraním na displeji.

V oblasti tepelné energie naopak stoupla spotřeba o 12 %, pořízení tohoto systému lze doporučit pouze v případě, že uživatel touží po zvýšení komfortu. O regulaci teploty se stará hlavice topení a centrální bridge společnosti Netatmo, pro úsporu energie v aktuálním systému by bylo výhodnější zařízení odinstalovat. Ztráta je vyvážena subjektivním zlepšením kvality života v domácnosti.

Instalace byla provedena samostatně bez pomoci specializovaných firem, nebo dodavatelů. Celý systém byl automatizován skrze příslušné aplikace daných výrobců a je možné ho řídit za pomoci hlasových příkazů, nebo fyzických tlačítek. Pro dodatečné zvýšení úspor v aktuálním systému bych instaloval přídatné senzory teploty v místnostech pro přesnější regulaci teploty, senzory pohybu a zařízení se schopností měření odebrané energie jednotlivých komponent systému.

5 Zdroje

- [1] *What is IoT (Internet of Things) and How Does it Work?* - Alexander S. Gillis, TechTarget, 2022 [online]. [cit. 2022-04-29]. Dostupné z: <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>
- [2] *Why it is called Internet of Things: Definition, history, disambiguation* - Knud Lasse Lueth, IoT Analytics, 2014 [online]. [cit. 2022-05-02]. Dostupné z: <https://iot-analytics.com/internet-of-things-definition/>
- [3] *The Internet of Things How the Next Evolution of the Internet Is Changing Everything.* - Dave Evans, Cisco Internet Business Solutions Group, 2011. [online]. [cit. 2022-05-02]. Dostupné z: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- [4] *Why Bluetooth IoT? Bluetooth technology has been integrated into IoT* – MokoBlue, 2020 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.mokoblue.com/why-bluetooth-iot/>
- [5] *Introduction to IoT | How Does an IoT System Work* – Leverage, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.leverage.com/iot-ebook/how-iot-systems-work>
- [6] *What is Cloud Computing? Everything You Need to Know* – Wesley Chai, TechTarget, 2021 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing>
- [7] *What Is the Difference Between Physical Servers and VMs?* – Jessie Reed, Nakivo, 2018 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.nakivo.com/blog/physical-servers-vs-virtual-machines-key-differences-similarities/>
- [8] *Pros and Cons of Cloud Servers vs Onsite Servers* – Atlasps, 2021 [online]. [cit. 2022-05-04]. Dostupné z: <https://atlasps.com/2021/05/cloud-servers-vs-onsite-servers/>
- [9] *The 4 Stages of IoT Architecture | Digi International* – Alec Jahnke, Digi, 2020 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.digi.com/blog/post/the-4-stages-of-iot-architecture>

- [10] *5 Layer Architecture of Internet of Things – GeeksforGeeks, 2020* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.geeksforgeeks.org/5-layer-architecture-of-internet-of-things/>
- [11] *7 IOT Layers That You Should Know in 2021 – Ajay Sarangam, Jigsaw Academy Education, 2018* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.jigsawacademy.com/4-layers-of-the-internet-of-things/>
- [12] *IoT Architecture Layers | HIOTRON – hIoTron, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.hiotron.com/iot-architecture-layers/>
- [13] *WiFi IoT Protocol - Popular choice for IoT development – Naval Allurwar, IoTDunia.com, 2021* [online]. [cit. 2022-05-04]. Dostupné z: <https://iotdunia.com/wifi/>
- [14] *Bluetooth | Definition, Uses, History, & Facts – Erik Gregersen, Britannica, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.britannica.com/technology/Bluetooth>
- [15] *Bluetooth Low Energy (BLE) and the Internet of Things (IoT) – Mohammad Afaneh, LinkedIn, 2017* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.linkedin.com/pulse/bluetooth-low-energy-ble-internet-things-iot-mohammad-afaneh>
- [16] *What is ZigBee? – Techopedia, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.techopedia.com/definition/4390/zigbee>
- [17] *What is Z-Wave? – Techopedia, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.techopedia.com/definition/27782/z-wave>
- [18] *Wi-Fi HaLow is now certified and ready for action - Stacey Higginbotham, Stacey on IoT, 2021* [online]. [cit. 2022-05-04]. Dostupné z: <https://staceyoniot.com/wi-fi-halow-is-now-certified-and-ready-for-action/>
- [19] *What is LoRaWAN® Specification - LoRaAlliance, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://lora-alliance.org/about-lorawan/>
- [20] *NB-IoT explained: a complete guide to Narrowband-IoT – i-scoop, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.i-scoop.eu/internet-of-things-iot/lpwan/nb-iot-narrowband-iot/>
- [21] *CoAP Protocol: Definition, Architecture – Wallarm, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.wallarm.com/what/coap-protocol-definition>

- [22] *CoAP - Constrained Application Protocol – Radiocrafts*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://radiocrafts.com/technologies/coap-constrained-application-protocol/>
- [23] *What is MQTT and How Does it Work? - Corinne Bernstein, TechTarget*, 2021 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.techtarget.com/iotagenda/definition/MQTT-MQ-Telemetry-Transport>
- [24] *What is MQTT? Definition and Details – Paessler*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.paessler.com/it-explained/mqtt>
- [25] *MQTT - The Standard for IoT Messaging – MQTT*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://mqtt.org/>
- [26] *QoS Levels – Springernature*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: https://media.springernature.com/original/springer-static/image/chp%3A10.1007%2F978-3-030-15032-7_58/MediaObjects/473249_1_En_58_Fig1_HTML.png
- [27] *What does XMPP mean? – Definitions*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.definitions.net/definition/XMPP>
- [28] *What is Extensible Messaging and Presence Protocol (XMPP)? - Techopedia*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.techopedia.com/definition/396/extensible-messaging-and-presence-protocol-xmpp>
- [29] *XEP-0045: Multi-User Chat – XMPP*, 2021 [online]. [cit. 2022-05-04]. Dostupné z: <https://xmpp.org/extensions/xep-0045.html>
- [30] *An Overview of XMPP – XMPP*, 2021 [online]. [cit. 2022-05-04]. Dostupné z: <https://xmpp.org/about/technology-overview/>
- [31] *Definition of Advanced Message Queuing Protocol (AMQP) – Gartner*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.gartner.com/en/information-technology/glossary/advanced-message-queuing-protocol-amqp>
- [32] *AMQP is the Internet Protocol for Business Messaging – AMPQ*, 2022 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.amqp.org/about/what>
- [33] *What's in the DDS Standard? – DDS-foundation*, 2021 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.dds-foundation.org/omg-dds-standard/>

- [34] *The Data Distribution Service The Communication Middleware Fabric for Scalable and Extensible Systems-of-Systems.* - Angelo Corsaro, Douglas C. Schmidt, Vanderbilt University. [online]. [cit. 2022-05-04]. Dostupné z: <https://www.dre.vanderbilt.edu/~schmidt/PDF/dds-sos.pdf>
- [35] *Data Distribution Service Converter Based on the Open Platform Communications Unified Architecture Publish-Subscribe Protocol.* – Woongbin Sim, ByungKwen Song, Junho Shin, Taehun Kim, MDPI, 2021 [online]. [cit. 2022-05-04]. Dostupné z: <https://www.mdpi.com/2079-9292/10/20/2524/htm>
- [36] *Lightweight M2M (LWM2M) – OMA Spec Works, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/>
- [37] *IoT Security Issues, Threats, and Defenses – Trendmicro, 2021* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses>
- [38] *The trust opportunity: Exploring Consumers' Attitudes to the Internet of Things.* – InternetSociety, ConsumersInternational, 2019 [online]. [cit. 2022-05-04]. Dostupné z: https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf
- [39] *Understanding IoT Security Part 1 of 3: IoT Security Architecture - Padraig Scully, IoTAnalytics, 2016* [online]. [cit. 2022-05-04]. Dostupné z: <https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/>
- [40] *What Is a VPN? - Virtual Private Network – Cisco Systems, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>
- [41] *Creating A Secure IoT Private Network With Access Server – OpenVPN, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://openvpn.net/for/iot-secure-network/>
- [42] *VPN For IoT Devices - Pros & Cons - Carsten Gregersen, Nabto, 2021* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.nabto.com/vpn-for-iot-devices-pros-and-cons/>
- [43] *TLS protocol overview – IBM, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.ibm.com/docs/en/sdk-java-technology/7.1?topic=provider-tls-protocol-overview>

- [44] *Securing the Internet of Things (IoT) with SSL/TLS – SSL.com, 2021* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.ssl.com/article/securing-the-internet-of-things-iot-with-ssl-tls/>
- [45] *What is an SSL certificate? – ManageEngine, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.manageengine.com/key-manager/information-center/what-is-ssl-certificate.html>
- [46] *What is DNS? | How DNS works – Cloudflare, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.cloudflare.com/learning/dns/what-is-dns/>
- [47] *What is DNS? – MyraSecurity, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.myrasecurity.com/en/what-is-dns/>
- [48] *What is the Domain Name System (DNS)? – Techopedia, 2017* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.techopedia.com/definition/24201/domain-name-system-dns>
- [49] *Protecting IoT devices requires a DNS-based solution – Ronan David, Help Net Security, 2021* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.helpnetsecurity.com/2021/09/23/protecting-iot-dns/>
- [50] *Automatic Home Light Control System – Which Home Automation, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.whichhomeautomation.com/automatic-home-light-control-system.php>
- [51] *Identifying and tracking Your Home's Phantom Power - Independent Electricity System Operator, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://saveonenergy.ca/For-Your-Home/Advice-and-Tips/Phantom-power>
- [52] *Best smart shades and blinds 2022 – Michael Brown, TechHive, 2022* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.techhive.com/article/578738/best-smart-shades.html>
- [53] *Is a Smart Thermostat a Worthwhile Investment for Your Home? – Smart Energy* [online]. [cit. 2022-05-04]. Dostupné z: <https://www.whatissmartenergy.org/featured-article/is-a-smart-thermostat-a-worthwhile-investment-for-your-home>
- [54] *Sonoff T1 EU User Guide – 店长, eWelink, 2017* [online]. [cit. 2022-05-04]. Dostupné z: <https://ewelink.coolkit.cc/?p=1359>

- [55] *Setting up a Zigbee WiFi bridge using Tasmota and Sonoff hardware - Rudy Dullier, Stuff Blog, 2021* [online]. [cit. 2022-05-04]. Dostupné z: <https://stuffblog.dullier.eu/2020/12/21/setting-up-a-zigbee-wifi-bridge-using-tasmota-and-sonoff-hardware/>
- [56] *Internet of Things Zařízení s Podporou Bluetooth a COAP – Ondřej Fuchs, Petr Musil, Vysoké učení technické v Brně, 2016* [online]. [cit. 2022-05-04]. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=132237