ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Fakulta elektrotechnická
Katedra aplikované elektroniky a telekomunikací

Bakalářská práce

IoT technologie pro Smart City

Autor práce: Kryštof Vaněk
Vedoucí práce: Ing. Karel Šíma

Plzeň 2018

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Kryštof VANĚK**
Osobní číslo:	**E15B0031P**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Elektronika a telekomunikace**
Název tématu:	**IoT technologie pro Smart City**
Zadávající katedra:	**Katedra aplikované elektroniky a telekomunikací**

Zásady pro vypracování:

1. Popište aktuální problematiku technologie Internet of Things (IoT) využitelnou v oblasti Smart City.
2. Navrhněte a realizujte měřicí systém vybraných environmentálních parametrů integrovatelný do IoT technologií.
3. Navržený měřicí systém otestujte a zhodnoťte dosažené výsledky.

Rozsah grafických prací: **podle doporučení vedoucího**

Rozsah kvalifikační práce: **30 - 40 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **The internet of things, Samuel Greengard, ISBN 978-0-262-52773-6**
2. **Designing the internet of things,Adrian McEwen, ISBN 978-1-118-43062-0**
3. **Internetové zdroje**

Vedoucí bakalářské práce: **Ing. Karel Šíma**
Katedra technologií a měření

Datum zadání bakalářské práce: **10. října 2017**

Termín odevzdání bakalářské práce: **7. června 2018**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Dr. Ing. Vjačeslav Georgiev
vedoucí katedry

V Plzni dne 10. října 2017

Abstrakt

Práce je zaměřená na aktuálně využitelné technologie v oblasti Internetu věcí se zaměřením na aplikace ve Smart City. Obsahuje přehled aktuálně dostupných síťových řešení vhodných jak pro zařízení s přístupem k síťovému napájení, tak pro zařízení s omezenými energetickými prostředky. Dále je rozebrán výběr některých metod přenosu a zpracování získaných dat, společně s přehledem běžně sledovaných parametrů prostředí a principů jejich měření.

V praktické části je realizován vývoj detekčního systému atmosferické výbojové aktivity, založeného na integrovaném senzoru blesků AS3935. Řízení systému je realizováno ARM mikrokontrolérem. Vzhledem k málo detailní dokumentaci bylo nutné mnoho vlastností čipu AS3935 zjišťovat experimentálně. S ohledem na to byla platforma připojena k embedded počítači RaspberryPI, který umožnil monitorování většího množství dat v reálném čase. Po odladění byl systém upraven pro použití s modemem umožnujícím přístup k Internetu prostřednictvím sítě LoRaWAN.

Klíčová slova

IoT, Smart City, IoT telekomunikace, protokoly, environmentální parametry, detekce blesků

Abstract

Vaněk, Kryštof. *IoT technology for Smart City* [*IoT technologie pro Smart City*]. Pilsen, 2018. Bachelor thesis (in Czech). University of West Bohemia. Faculty of Electrical Engineering. Department of Applied Electronics and Telecommunications. Supervisor: Ing. Karel Šíma

---

This thesis is focused on currently utilisable technology in the field of Internet of Things, focused on application in Smart City. Part of its content is a survey on available networking solutions suitable both for devices with access to grid power and those with limited energy resources. A selection of data transfer and processing methods is also included together with a outline of commonly measured environmental parameters and their measurement principles.

In the implementation part a atmospheric discharge detection system is being developed. The system is based on integrated lightning detection chip AS3935. It is controlled by an ARM microcontroller. Because of little detailed documentation much of the AS3935 chip properties had to be discovered experimentally. With regard to this fact the platform was connected to the RaspberryPI embedded computer. This allowed to monitor considerable amount of data in real time. After tuning the system was modified for usage with a modem allowing Internet access through LoRaWAN network.

Keywords

IoT, Smart City, IoT telecommunication, protocols, environmental parameters, lightning detection

Prohlášení

Předkládám tímto k posouzení a obhajobě bakalářskou práci, zpracovanou na závěr studia na Fakultě elektrotechnické Západočeské univerzity v Plzni.

Prohlašuji, že jsem svou závěrečnou práci vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 270 trestního zákona č. 40/2009 Sb.

Také prohlašuji, že veškerý software, použitý při řešení této bakalářské práce, je legální.

V Plzni dne 5. června 2018

Kryštof Vaněk

Podpis

Obsah

Seznam obrázků

Seznam tabulek

Seznam symbolů a zkratek

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks. IPv6 přes nízkoenergetické bezdrátové osobní sítě.
AES	Advanced Encryption Standard.
ASK	Amplitude Shift Keying. Klíčování změnou amplitudy.
BLE	Bluetooth Low Energy.
BPSK	Binary Phase Shift Keying. Binárn klíčování fázovým posuvem.
DSSS	Direct Sequence Spread Spectrum. Přímé rozprostření spektra.
GFSK	Gaussian Frequency Shift Keying. Klíčování frekvencí s gausovským filtrem
HF	High Frequency. Vysoká frekvence.
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things. Internet věcí.
IoT	Internet of Everything. Internet všeho.
IPSP	Internet Protocol Support Profile.
LF	Low Frequency. Nízká frekvence.
LPWAN	Low-Power Wide-Area Network
LR-WPAN	Low Rate Wireless Personal Area Network. Bezdrátová síť osobního dosahu s nízkou přenosovou rychlostí.
MAC	Media Access Control. Správa přístupu k médiu.

MEMS	MicroElectroMechanical Systems. Mikroelektromechanické systémy.
MPSK	M-ary Phase Shift Keying. M-stavové klíčování fázovým posuvem.
NFC	Near-Field Communication. Komunikace blízkým polem.
O-QPSK	Offset Quadrature Phase-Shift Keying. Kvadraturní klíčování fázovým posuvem s odsazením.
PHY	Physical Layer. Fyzická vrstva.
QoS	Quality of service
RFID	Radio Frequency Identification. Identifikace na rádiové frekvenci.
SHF	Super High Frequency. Super vysoká frekvence.
TCP/IP	Transmission Control Protocol/Internet Protocol
UHF	Ultra High Frequency. Ultra vysoká frekvence.

1 | Úvod

V dnešní době se pojem IoT (*IoT — Internet of Things*) stává populárním tématem. Tato disciplína se stává součástí mnoha oblastí. Jako příklady lze uvést Smart City a Průmysl 4.0. Internet věcí je ale velmi široký pojem kombinující mnoho vědních oborů, zejména pak elektrotechniku a informatiku.

Internet věcí jako pojem byl poprvé použit v rámci produktové prezentace Kevina Ashtona v roce 1999 [1; 2]. Jeho základní myšlenkou je změna původu dat, která jsou k dispozici prostřednictvím Internetu. Data produkovaná lidmi jsou omezená, stejně jako lidská pozornost, svou přesností a časem investovaným do jejich tvorby. Pokud by se podařilo připojit Internet k fyzickému světu, bylo by možné získat data o všem, a na základě toho optimalizovat veškeré procesy [1]. Proto se někdy také používá pojem Internet všeho (*IoE — Internet of everything*) [3].

Propojení fyzického světa globální informační sítí umožňuje za pomocí jednoduché, nebo i velice komplexní logiky ovlivňovat na základě získaných dat jiné fyzické objekty — vytvářet chytré aktuátory. Ty mohou řídit optimalizaci procesů, které by jinak musel ovlivňovat člověk.

Jednou z klíčových technologií Internetu věcí je RFID [4, s. 17], umožňující jednoznačnou identifikaci fyzických předmětů a tím i sledování jejich výskytu. Dalšími předpoklady je vývoj levných chytrých senzorů a mikrokontrolérů.

Přínos IoT do oblasti Smart City lze spatřit například v monitorování a automatizaci městské infrastruktury. Typicky jmenovaným příkladem je automatizovaná správa dopravy, která může být zvláště přínosná ve spojení s autonomně řízenými vozidly. Taková vozidla navíc mohou sdílet informace nejen se sítí městské infrastruktury, ale také navzájem s ostatními účastníky provozu [5]. Rovněž mohou sami tvořit část městské infrastruktury.

Podobných příkladů lze najít velké množství. Tyto příklady a případové studie sdílí společný koncept — bezdrátové senzorové sítě (IoT senzorické sítě). Tyto sítě jsou většinou zacíleny na konkrétní potřeby daného problému. Jedná se nejčastěji o měření nejběžnějších environmentálních parametrů nebo fyzikálních veličin.

Tím se z myšlenky IoT stává jeden ze stavebních kamenů Smart City, teoreticky umožňující řešit libovolný problém městské infrastruktury. Je ale nutné jednotlivé problémy důkladně analyzovat a volit k realizaci ty nejdůležitější. Zároveň je nutné pamatovat na životnost zařízení a ideálně umožnit jejich další funkční rozšíření. Tím je možné omezit negativní dopad ve formě odpadu z jednorázových chytrých zařízení s nízkou životností [7], což koresponduje s vizí Smart City jakožto nástroje ke zmenšení ekologické stopy. Dalšími cíli Smart City je posilování konkurenceschopnosti a maximalizace životní úrovně obyvatel [6].

V rámci této práce je kladen důraz na základní parametry městského životního prostředí. K realizaci měřicího systému byla zvolena detekce blesků. Ty představují ohrožení energetických a telekomunikačních sítí, stejně jako osobního i veřejného majetku. Znalost jejich výskytu tak může pomoct s redukcí negativních vlivů které přinášejí.

2 | IoT sítě pro oblast Smart City

Velkou výhodou městské zástavby je snadná dostupnost přípojení k energetické i sdělovací pevné síti. Na rozdíl od volného prostředí mimo města je tak možné využívat specializované sítě pro IoT i s velmi malým dosahem, propojené k páteřnímu zpracování skrz konvenční sdělovací prostředky. Zároveň je možné využívat sítě s větším pokrytím, které mohou obsluhovat zařízení vyžadující pohyb v rámci města, nebo taková, která nemají přístup k dedikované lokální infrastruktuře — typicky ojedinělá zařízení do domácností. Další možností propojení většího počtu senzorů přináší standardy podporující mesh topologii, umožňující kooperativní přenos dat mezi zařízeními. Tím je umožněno pokrytí velkého území bez nutnosti centrálního vysílače a velkých vysílacích výkonů. Tato topologie je také velice vhodná, pokud se jedná o oblast, která se svým tvarem silně odchyluje od kruhu, tedy například dlouhé, ale úzké pásy zařízení, kde by bylo hvězdicové pokrytí neúčinné.

2.1 Komunikace v bezprostřední blízkosti

Pro rozšíření funkce — augmentace — předmětů běžného života není nutné komunikovat na dlouhou vzdálenost. Pro předávání dat — informací — s infrastrukturou chytrých zařízení se proto používají speciální pasivní, nebo i aktivní technologie.

2.1.1 RFID

Komunikace v rámci RFID (*Radio Frequency Identification*) probíhá vždy mezi čtečkou a transpondérem — tagem [8]. Tag je malý a levný čip pro bezdrátovou komunikaci uchovávající data v něm naprogramovaná [9, s. 3]. Velikost těchto dat se pohybuje v rozsahu 16–64 kB [9, s. 6]. Hlavním přínosem RFID je elektronická identifikace fyzických objektů bez nutnosti lidské obsluhy — automatická identifikace (*Auto-ID*) — s vysokou spolehlivostí [9, s. 4].

Podle způsobu napájení lze tagy rozdělit na tři skupiny [8; 10]:

- Pasivní — pole vyslané čtečkou je usměrněno a využito jako zdroj energie pro celý čip tagu.
- Polo-aktivní — tag obsahuje baterii, která napájí interní kontrolní obvody, energie pro vysílání je získána z pole čtečky.
- Aktivní — napájení kontrolních obvodů i vysílače je zabezpečováno integrovanou baterií.

Pro komunikaci mezi čtečkou a tagem jsou využívána různá frekvenční pásma. V závislosti na použitém pásmu lze dosáhnout různých charakteristik, přičemž každá z nich je vhodná pro jistý druh aplikace. Nejčastěji využívaná pásma a jejich užití jsou popsány v tabulce 2.1.

Volba pásma rovněž ovlivňuje mechanismus přenosu informace. Pro nízké a vysoké frekvence je využívána induktivní vazba, což vyžaduje, aby byl tag v blízkosti čtečky. Pro ultra a super vysoké frekvence je využívána vazba elektromagnetického pole [9, s. 17–18].

S rostoucí frekvencí roste přenosová rychlost a je tedy možné za stejný čas načíst více tagů. Rostou ale i výrobní a provozní náklady a klesá imunita systému na vlhkost a umístění v blízkosti kovových ploch [9, s. 17–18].

RFID přináší možnost sledovat výskyt známých objektů v okolí čtečky a eliminovat tak jejich ztrátu, např. drahého, drobného lékařského vybavení [11]. Tagy také umožňují zabezpečení falšovaných produktů. Při velikosti identifikátoru — dat tagu — 64 kB, tedy 512 b, je shoda s registrovaným kusem výrobku možná s pravděpodobností $2^{-512} \approx 10^{-154}$. Po přijetí takového zboží stačí načíst identifikátor zboží a pomocí aplikace výrobce ověřit pravost v registru vyrobených kusů.

Tabulka 2.1: Nejčastější RFID pásma a jejich použití [9, s. 8; 12; 13]

Frekvenční pásmo	**Název pásma**	**Dosah**	**Užití**
125 kHz	Nízká frekvence	$< 0{,}5$ m	Globálně nelicencované; identifikace vozidel, předmětů a zvířat. Někdy nazýváno *LowRFID*
13,56 MHz	Vysoká f. HF	< 1 m	Elektronické jízdenky, bezkontaktní platby, řízení přístupu, elektronická identifikace produktů.
860–960 MHz	Ultra vysoká f. UHF	1–10 m	Silně omezené pásmo v závislosti na lokalitě; správa majetku, sledování kontejnerů a zavazadel, elektronická identifikace produktů
2,45 GHz	Super vysoká f. SHF	> 3 m	Sledování předmětů s aktivními tagy na velkou vzdálenost, automatická identifikace vozidel.

2.1.2 NFC

Near-Field Communication — komunikace blízkým polem — principiálně částečně překrývá problematiku RFID, z níž se kombinací s komunikační nadstavbou vyvinula [14; 15, s. 744]. Operuje na stejné frekvenci jako HF RFID — 13,56 MHz — na vzdálenost několika jednotek [15, s. 744; 16, s. 2261] až málo desítek centimetrů (≈ 20 cm) [14] a jedním z módů operace je identifikace NFC tagů. Na rozdíl od RFID ale neslouží výhradně k automatické identifikaci, ale umožňuje i komunikaci dvou zařízení, či emulaci jiného RFID tagu, např. identifikační karty [17].

NFC z podstaty krátkého dosahu umožňuje velmi bezpečný přenos informací, jelikož musí být komunikace iniciována cíleným přiblížením dvou zařízení do těsné blízkosti [16, s. 744–745]. Minimalizuje se tedy riziko odposlechnutí informací, neboť absolutní kontrola nad malou vzdáleností je velmi snadná. Tato metoda komunikace se skvěle hodí k lidmi vyvolané interakci se sítí strojů — čtení štítků, komunikace s chytrými obaly, které mohou zaznamenávat důležité

informace o průběhu přepravy [18], získávání a předávání malého množství informací z/do sítě [15, s. 745], případně nastavování těchto zařízení.

Velkou výhodou NFC technologie je dostupnost, jelikož touto technologií je vybavena velká část současných modelů chytrých telefonů.

2.2 Sítě malého dosahu

V případě komunikace více chytrých zařízení v lokálním měřítku — domácnosti, drobné podniky, parky,... — užití komunikačních prostředků pro kontaktní vzdálenosti již nepostačuje. Je nutné pokrýt celý půdorys lokality, tedy okruh několika desítek až stovek metrů.

2.2.1 Bluetooth Low Energy

Bluetooth Low Energy — BLE, nebo také *Bluetooth Smart* je velice energeticky nenáročná (v porovnání s klasickým Bluetooth je vysílací výkon dvakrát až stokrát menší [19, s. 4]) a levně implementovatelná verze velmi rozšířené a známé Bluetooth komunikace. BLE je určené pro zařízení s malým datovým tokem a dlouhou prodlevou mezi jednotlivými zprávami. Pro přenos dat využívá 37 kanálů o šířce pásma 2 MHz v pásmu 2,4 GHz, s časovým multiplexem a frekvenčním skákáním pro omezení interference s jinými bezdrátovými technologiemi, a 3 kanály pro zjišťování zařízení [20, s. 1]. Bylo specifikováno ve verzi Bluetooth v4.0 [21, s. 155] a je tedy podporováno všemi zařízeními, která tuto a vyšší verze standardu podporují, což je naprostá většina moderních chytrých telefonů.

V rámci BLE jsou možné dvě topologie [20, s. 2]:

- Rozhlasová (*Broadcast*), která slouží k vysílání zjišťovacích zpráv naslouchajícím zařízením — pozorovatelům (*Observers*). V této topologii je možná pouze jednostranná komunikace.
- Spojová (*Connections*), ve které se jedno nadřazené zařízení — centrála (*Central*) — spojuje s více koncovými zařízeními — periferiemi.

Spojová infrastruktura tvoří takzvané pikosítě (*Piconet*). Pokud se překrývají, jsou některá zařízení schopná přemostit spojení mezi jednotlivými pikosítěmi a vzniká tak síť mesh topologie zvaná *Scatternet*. Tato možnost byla do BLE zavedena ve verzi 4.1 a umožňuje pokrytí velkých ploch bez nutnosti vykrývání centrální bránou [21, s. 158-159].

Některá zařízení — BLE značky (*Beacon*) — nenavazují spojení ve spojové topologii, ale vysílají pouze zjišťovací zprávy. Ty obsahují krátkou zprávu pro jednoznačnou identifikaci vysílače, případně malé množství informací o jeho stavu (teplota, stav baterie,...). Takové zařízení je vhodné k jednoznačné identifikaci prostoru či objektu, na což mohou zařízení v dosahu značek reagovat zpřístupněním určitých služeb, změnou nastavení a podobně. Hlavními rozdíly oproti RFID jsou možnost měnit data obsažená ve správě značky a využití běžného spotřebitelského zařízení — mobilního telefonu — namísto specializované čtečky. Podle síly přijatého signálu je také možné odhadovat vzdálenost přijímače a značky [19, s. 4-5].

Od verze 4.2 je také podporován profil IPSP (*Internet Protocol Support Profile*), umožňující přenos komprimované IPv6 TCP/IP hlavičky v Bluetooth paketech — 6LoWPAN (*IPv6 over Low-Power Wireless Personal Area Networks*) — a propojovat tak BLE zařízení s globální sítí — Internet, nebo mezi sebou skrz centrálu. Jako bránu je možné použít opět telefon, nebo dedikovaný BLE router [21, s. 156].

Bluetooth Low Energy je díky velkému rozšíření ve spotřebitelských zařízeních ideální metodou pro interakci s ostatními smart zařízeními. Hodí se pro datové přenosy malého objemu, nastavování, identifikování a hrubou lokalizaci zařízení.

2.2.2 Sítě založené na IEEE 802.15.4

Standard IEEE 802.15.4, původně zavedený v roce 2003 definuje fyzickou a MAC vrstvu pro bezdrátové osobní sítě s nízkou přenosovou rychlostí — LR-WPAN (*Low Rate Wireless Personal Area Network*). Zařízení využívající tento standard musí být schopné operovat podle alespoň jedné ze specifikací v tabulce 2.2 [22, s. 146].

Tabulka 2.2: Režimy PHY definované IEEE 802.15.4[1] [22, s. 147]

PHY (MHz)	**Frekvenční pásmo (MHz)**	**Modulace**	**Přenosová rychlost (kb/s)**
780	779–787	O-QPSK	250
780	779–787	MPSK	250
868/915	868–868,6	BPSK	20
	902–928	BPSK	40
868/915 (volitelně)	868–868,6	ASK	250
	902–928	ASK	250
868/915 (volitelně)	868–868,6	O-QPSK	100
	902–928	O-QPSK	250
950	950–956	GFSK	100
950	950–956	BPSK	20
2450 DSSS	2400–2483,5	O-QPSK	250

Standard 802.15.4 není samostatně funkčním celkem, postrádá vyšší než druhou vrstvu OSI modelu, a nejedná se tedy o konkrétní síť. Je na něm ale možné vystavět nadstavbové protokoly, které díky specifikovaným vlastnostem fyzické vrstvy (PHY) mohou operovat ve veřejně dostupných rádiových pásmech s maximální přenosovou rychlostí až 1 Mb/s [22, s. 147], běžně pak do 250 kb /s.

[1] Tabulka 2.2 byla pro potřeby práce zjednodušena. Vynechány byly informace o symbolových a čipových rychlostech a symbolové soustavě, které pro představení standardu nejsou podstatné. Rovněž byla vynechána sekce volitelných ultra-širokopásmových variant.

Tabulka 2.3: Provozní parametry ZigBee

Lokalita	Frekvenční pásmo	Počet kanálů	Maximální přenosová rychlost
Globální	2,4 GHz	16	250 kb /s
Amerika	915 MHz	27	10 kb /s
Evropa	868 MHz	63	100 kb /s

MAC vrstva umožňuje spojování v hvězdicové, nebo peer-to-peer topologii [22, s. 8]. Dalším důležitým parametrem je možnost komprese TCP/IPv6 hlavičky a propojení se sítí Internet pomocí 6LoWPAN specifikovaná IETF RFC 6282.

ZigBee

Nadstavbu standardu IEEE 802.15.4-2011 tvoří síťová vrstva *Zigbee PRO* a aplikační vrstva *Zigbee Cluster Library*. Zigbee PRO umožňuje využití mesh síťové topologie a implementuje zabezpečovací mechanismy za užití 128-bit AES šifrování. Společně s aplikační vrstvou tvoří celý síťový protokol vhodný pro zařízení s nízkým energetickým rozpočtem, která mohou být nasazena v libovolné ZigBee síti.

ZigBee umožňuje připojení až 65 tisíc zařízení a v závislosti na lokalitě může být provozováno v režimech podle tabulky 2.3 s dosahem nad 300 m v otevřeném prostranství a 75–100 m v interiérech [23]. Stalo se velmi oblíbenou platformou pro chytré domácnosti, například Philips Hue

Další sítě založené na IEEE 802.15.4

K síti ZigBee vzniklo na základě standardu IEEE 802.15.4 několik konkurenčních protokolů, z nichž do většího povědomí pronikly Z-Wave a Thread. Srovnání základních parametrů protokolů následuje v tabulce 2.4.

Tabulka 2.4: Srovnání parametrů sítí založených na standardu IEEE 802.15.4

	Zigbee [23]	**Z-Wave** [24; 25]	**Thread** [26; 27]
Dosah	> 300 m	100 m	nezjištěno
Maximální počet uzlů	65 000	232	> 250
Maximální přenosová rychlost	250 kb /s	100 kb /s	250 kb /s
Frekvenční pásma	2,4 GHz Sub-GHz	Sub-GHz	2,4 GHz
Topologie	mesh	mesh	mesh

2.2.3 Wi-Fi

Technickou specifikaci Wi-Fi konektivity jistě není potřeba popisovat,[2] jelikož se jedná o obecně známou technologii, optimalizovanou pro co nejrychlejší přenos objemných dat spotřebitelských zařízení. Odtud také plyne její sporná vhodnost pro IoT zařízení, která zpravidla generují pouze malé datové toky. Samotné připojení do Wi-Fi vyžaduje nemalý výpočetní výkon a pro mnoho chytrých zařízení je tak připojení zcela nemožné.

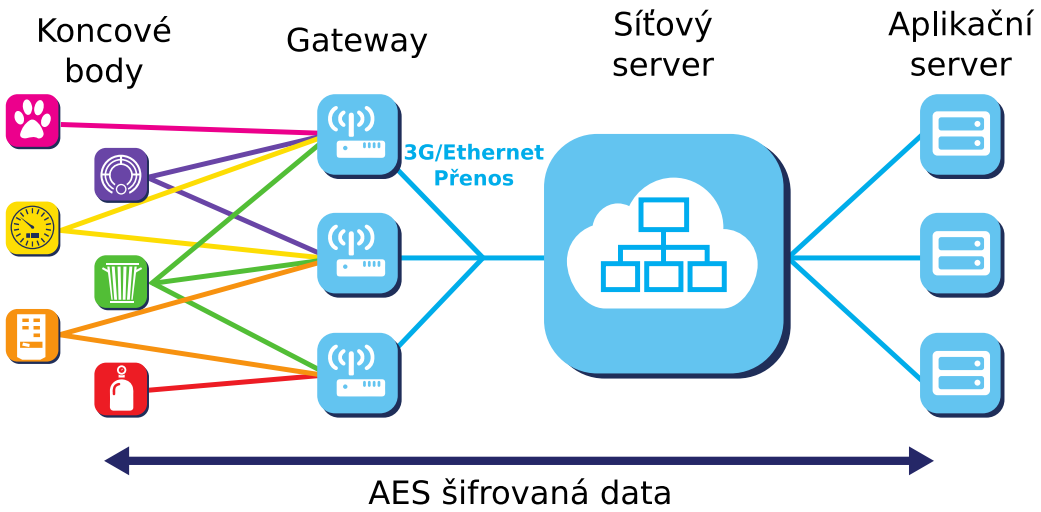
Nespornou výhodou je ale běžnost a uživatelská znalost sítě. Pokud se tedy jedná o zařízení napájená ze sítě disponující větším výpočetním výkonem — např. embedded Linuxové systémy, systém pro řízení přístupu pomocí RFID — je Wi-Fi naopak ideální volbou.

2.3 Sítě dlouhého dosahu

2.3.1 LoRaWAN

LoRa je modulace vyvinutá firmou Semtech zaměřená na přenosy malých datových rámců na velkou vzdálenost. Jedná se o modulaci přímo vyvinutou pro IoT a cílí tak hlavně na energetickou úspornost a jednoduchou implementaci.

Topologie sítě je hvězdicově rozvětvená. Základní hvězdice přístupových bran — které tvoří přemostění LoRa komunikace do zpracovacích serverů skrze Internet — dále tvoří hvězdice s LoRa zařízeními [28, s. 8]. Schéma topologie je znázorněno na obrázku **??** Pro přenos dat využívá 10 kanálů v Sub-GHz pásmech[3], z nichž 8 je určených pro komunikaci s proměnnou rychlostí od 250 b/s do 5,5 kb/s, jeden kanál s přenosovou rychlostí 11 kb/s a jeden kanál pro FSK modulaci s přenosovou rychlostí 50 kb/s [29, s. 13]. Zpráva vyslaná koncovým zařízením je zachycena a zpracována všemi bránami dané sítě, které jsou v dosahu.



Obrázek 2.1: Schéma topologie sítě LoRaWAN [29, s. 8]

Maximální velikost užitných dat MAC vrstvy je 59–250 byte v závislosti na nastavení modulace.[4] Tento limit je dán omezením fyzické vrstvy pro danou modulační rychlost [28, s. 38].

[2] Základní specifikace je předmětem standardu IEEE 802.11. Další informace jsou dostupné na webových stránkách Wi-Fi aliance `https://www.wi-fi.org`.

[3] V Evropě 868 a 433 MHz [28, s. 10].

[4] Údaj platí pro evropské pásmo 868 MHz

Hlavička MAC paketu a řídící příznaky mohou mít velikost 7–23 byte [28, s. 20]. V nejhorším případě je tak možné přenést 36 byte a v nejlepším 243 byte dlouhou zprávu aplikace koncového bodu.

LoRa modulace je založena na frekvenční modulaci s rozprostřeným spektrem chirpovou sekvencí. To umožňuje flexibilně řídit poměr mezi citlivostí přijímače a přenosovou rychlostí [30].

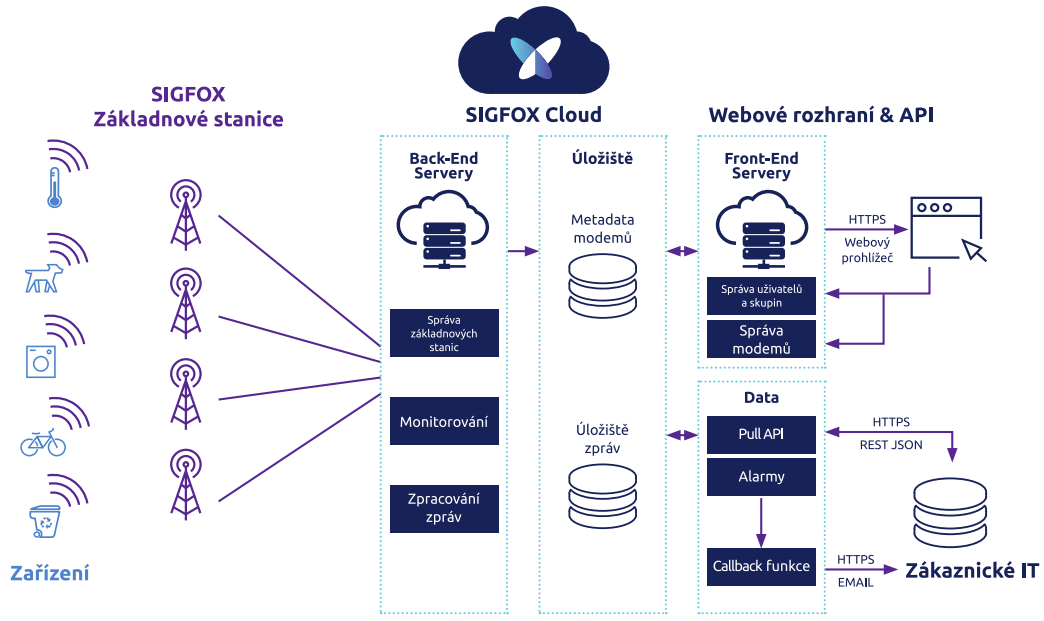
Specifikace LoRa dělí zařízení podle schopnosti přijímat data do tří tříd [28, s. 10]:

- Třída A — umožňuje příjem dat ve dvou přijímacích oknech po odvysílání zprávy.
- Třída B — umožňuje kromě příjmu dat v oknech po odvysílání příjem v časových slotech řízených z brány.
- Třída C — umožňuje přijímat data v libovolném časovém okamžiku, s výjimkou vysílacího okna.

Vzhledem k nutnosti zachytávat a zpracovávat signál rostou s narůstající třídou nároky na napájení. Třídy B a C jsou však pro zařízení nepovinné. V poslední verzi specifikace — LoraWAN 1.1 — je rovněž umožněno přecházení mezi jednotlivými sítěmi — Roaming. To do budoucna otevírá možnosti pro pohyblivá zařízení, která by se jinak dostala z dosahu své domovské sítě.

2.3.2 SigFox

Síť SigFox operuje v Evropě v pásmu 868 MHz a 915 MHz ve zbytku světa. Využívá ultra-úzkopásmovou modulaci s šířkou kanálu 100 Hz při přenosové rychlosti 100–600 bit/s podle regionu [31, s. 8]. Pro zlepšení spolehlivosti je každá zpráva vysílána třikrát, v různých časových rámcích na rozdílných frekvencích. Přístup k přenosovému kanálu je náhodný [31, s. 9]. Stejně jako u sítě LoRaWAN je topologie sítě hvězdicová [32] a zpráva je zachytávána všemi bránami v dosahu [31, s. 9], viz obrázek 2.2.



Obrázek 2.2: Schéma topologie sítě SigFox [31, s. 13]

Maximální velikost přeneseného datového rámce aplikace je stanovena na 12 byte, přičemž denně může v síti každé zařízení odeslat 140 zpráv a přijmout 4 zprávy o velikosti 8 byte za

předpokladu plného využití základnových stanic — bran. Pokud je síť využita méně, je možné přijmout i více zpráv. Přijetí zprávy je iniciováno zařízením a mezi vysílacím a přijímacím oknem, trvajícím maximálně 20 s, je prodleva 20 s [31, s. 10].

Síť má velice dobré pokrytí, které v České republice buduje společnost SimpleCell Networks a.s. [33]. Umožňuje také zcela transparentní roaming do všech pokrytých zahraničních oblastí [34]. Vzhledem k uzavřenosti sítě, existenci pouze jednoho poskytovatele a velkému omezení provozních parametrů sítě je ztížen vývoj zařízení. Společnost SigFox poskytuje síťový emulátor a rádiový analyzátor, který tento problém odstraňuje a umožňuje připravit zařízení na certifikaci [35].

2.3.3 Mobilní sítě

Podobně jako Wi-Fi tvoří běžně dostupný, výkonný protipól nízkoenergetickým sítím krátkého dosahu, jsou mobilní — celulární — sítě protipólem LPWAN (*Low-Power Wide-Area Network*) sítím jako je LoRa, či SigFox. Pro zařízení s větším výpočetním výkonem a přístupem k dobrému zdroji energie mohou být mobilní sítě vhodným řešením. V posledních verzích — 4G a v budoucnu i 5G — umožňují také přenosové rychlosti o několik řádů vyšší, než jaké nabízí sítě specializované pro drobná IoT zařízení.

Za pozornost ovšem stojí standardy, které vznikají se zaměřením na IoT zařízení, tedy s nízkými energetickými nároky, ovšem za využití základnových stanic mobilních sítí. Těmito jsou LTE-M, NB-IoT (*Narrowband IoT*) a EC-GSM-IoT s maximálními přenosovými rychlostmi 1 Mb/s, 250 kb/s a 240 kb/s.

Tyto standardy si kladou za cíl zejména sníženou cenu komunikačního hardware v porovnání s běžnými mobilními čipsety, stejně tak jako snížené nároky na energii, konkrétně desetiletý provoz zařízení z baterie o kapacitě 5 W h [36; 37].

2.4 Shrnutí a porovnání IoT sítí

Současná řešení sítí pro IoT umožňují rozmanitou škálu dosahu pokrytí, což přináší možnost volby specifického typu komunikace a tím optimalizace aplikace pro dané užití. Při zachování požadavku na energetickou úsporu s rostoucím dosahem klesá přenosová rychlost. Výjimku z tohoto pravidla tvoří IoT sítě založené na mobilních technologiích, které svou rychlostí při zachování malé energetické náročnosti vynikají.

IoT sítě dlouhého dosahu mají omezený celkový denní přenesený objem dat. Toto omezení plyne z provozu ve volných nelicencovaných pásmech [38, s. 11]. I v tomto případě platí, že se tento limit netýká sítí založených na mobilních technologiích.

Výhody modifikací mobilních sítí jsou ale limitovány nasazením jednotlivých operátorů. Neexistuje síť, která by pokrývala větší územní celek, s výjimkou nasazení LTE-M v Severní Americe [37, s. 26,27].

3 | Zpracování dat v IoT

Data získaná ze sítě chytrých senzorů je třeba odeslat k dalšímu zpracování. K tomu je nutná sada protokolů umožňující jednoznačnou identifikaci zdroje dat a jejich spolehlivé doručení. Data přenesená k dalším aplikacím, ať už centralizovaným, nebo cloudovým, mohou poskytnout konsolidované, informačně hodnotné výstupy, případně ovlivňovat parametry jiných zařízení a procesů, dostupných po síti v opačném směru.

3.1 Přenos dat mezi IoT zařízeními v globální síti

Většina sítí popsaných v kapitole 2 neumožňuje přenos TCP/IP hlavičky přímo v paketu zprávy koncového bodu. Je tedy nutné, aby brána dané síťové technologie překládala informaci o identifikátoru konkrétního zařízení tak, aby bylo možné tyto informace předat skrze TCP/IP protokol až k cílovým serverům [39, s. 45].

K tomuto účelu se využívá několik protokolů: DDS, CoAP, AMQP, MQTT, XMPP, HTTP REST [39, s. 4; 40, s. 2353]. Formát předávaných dat bývá často JSON (*JavaScript Object Notation*), případně jeho komprimované nebo zakódované varianty [39; 41, s. 45].

3.1.1 Formát JSON

Jedná se o jednoduchá formát pro předávání dat mezi aplikacemi. Je snadno čitelný lidmi, čímž umožňuje velice jednoduché ladění programů, stejně tak je ale snadno zpracovatelný algoritmicky. JSON je textové vyjádření datové struktury objektu, nebo seznamu (pole). Jednotlivé struktury mohou být vnořené, tedy například hodnota v poli může být objekt.

Data jsou klíčována názvy — řetězci, k nimž náleží hodnoty oddělené dvojtečkou. Jednotlivé vstupy jsou odděleny čárkou [42]. Například tedy pro předání informací o osobě jménem John, žijící v New Yorku, s věkem 31 let by vypadala takto [43]:

```
{ "name":"John", "age":31, "city":"New York" }
```

Obrázek 3.1: Ukázka datového formátu JSON

3.1.2 MQTT — *Message Queuing Telemetry Transport*

Transportní protokol MQTT byl původně vyvinut v roce 1999 a v roce 2013 byl standardizován neziskovým konsorciem OASIS [40, s. 2354]. V roce 2016 byl pro MQTT v.3.1.1 přijat mezinárodní standard ISO/IEC 20922 [44].

Protokol je nadstavbou protokolu TCP/IP. Klade si za cíl snadnou implementaci, úsporné datové přenosy a otevřenost. Využívá schématu publikování/odebírání mezi třemi uzly řetězce — poskytovatel (*Publisher*), zprostředkovatel (*Broker*) a odběratel (*Subscriber*) [40, s. 2345; 45, s. 1,2]. Jednotlivé zprávy předávané mezi zařízeními jsou přiřazeny tématům (*Topics*). Ty slouží pro třídění jednotlivých zpráv pomocí tematických filtrů (*Topic Filter*). Odběratel se přihlašuje zprostředkovateli k odběru zpráv daného tématu (*Subscription*), čímž je vytvořen specifický tematický filtr odběratele [40, s. 2345; 45, s. 10]. Je tak možné přímé předání zprávy bod–bod, případně zesilování zpráv bod–skupina, nebo naopak zhuštění skupina–bod.

Protokol umožňuje tři stupně ověření předání zprávy — QoS (*Quality of Service*). Tyto stupně jsou definovány číselně jako [45, s. 34; 46]:

0 — Zpráva je vyslána, ale není ověřeno její doručení. Může být tedy doručena maximálně jednou, v případě úspěchu.

1 — Po vyslání zprávy následuje časové okno, během kterého příjemce potvrdí její přijetí, čímž je komunikace zakončena. V případě, že toto ověření není během časového intervalu doručeno, je odeslání zprávy opakováno. Zpráva je tedy doručena minimálně jednou, může být ale doručena vícekrát, např. v případě kdy je zpráva při každém opakování doručena správně, ale nedaří se potvrzení zprávy.

2 — Kromě ověření doručení, shodně jako v QoS 1, je také ověřeno samotné ověření. Je tak zajištěno, že odesílatel zprávy je informován o úspěšném přijetí a nepokouší se o další opakování. Tento mechanismus umožňuje zajištění doručení zprávy právě jednou.

QoS je specifikována výhradně mezi dvěma zařízeními. Vyslání zprávy poskytovatelem s QoS 2 nutně neznamená jisté a neopakované doručení zprávy odběrateli, jelikož odběratel při svém přihlášení specifikuje vlastní QoS, se kterou chce zprávy přijímat [46].

Pro svou jednoduchost je vhodný k implementaci v zařízeních s omezeným výpočetním výkonem, tedy například přímo v koncových bodech IoT sítí, které mají možnost vysílání TCP/IP paketů.

3.1.3 AMQP — *Advanced Message Queuing Protocol*

Tento otevřený standard byl navržen pro spolehlivé předávání zpráv v podnikových sítích. Je orientovaný na spoje bod-bod, umožňuje ale i jiné konfigurace a je pomocí něj možné vytvořit i mechanismus publikování/odebírání, podobně jako je tomu u MQTT [40, s. 2355; 47, s. 1]. Je ale plně symetrický a umožňuje tak iniciovat spojení jak na straně koncového bodu, tak na straně obslužného serveru [47, s. 10; 48].

Základem standardu je transportní vrstva, která umožňuje vytváření jednosměrných spojení (*Links*) mezi jednotlivými uzly (*Nodes*) [47, s. 31]. Spoje mohou být párové a vytvářet tak obousměrné komunikační kanály. Ty jsou nadále přiřazovány do relací (*Sessions*) [47, s. 44]. Po této transportní vrstvě je nutné přenášet zprávy standardizovaného formátu, který musí být podporovaný každou aplikací implementující AMQP, [47, s. 7] čímž je dosaženo možnosti jejich univerzálního propojení [49, s.81].

Standard je velice rozsáhlý a univerzální. Umožňuje velké množství možností propojení aplikací a jejich částí. Základním předpokladem pro implementaci AMQP je komunikační kanál umožnující konzistentní datový tok, běžně TCP/IP, může se ale jednat i o datové toky v rámci operačního systému [49].

Vzhledem ke své robustnosti a univerzálnosti je tento protokol významný zejména při dalším zpracování dat a přenosu mezi jednotlivými aplikačními servery.

3.1.4 REST — *Representational State Transfer*

REST je velice obecně definovaný princip, prvotně vytvořený již v letech 1994 a 1995 [50, s. 109]. Jednotlivé informační zdroje jsou označovány jako prostředky (*Resources*) a jejich datový obsah jako reprezentace. Každému prostředku odpovídá jeden, nebo i více, identifikátorů [50, s. 88–90]. Základní kritéria jsou [50, s. 78–85]:

1. Orientace klient–server — komunikace je iniciována klientem, což vyvolává reakci serveru [50, s. 45].

2. Nestavovost — každý požadavek klienta musí obsahovat všechny informace nutné k jeho zpracování. Server neuchovává žádný kontext, veškeré informace o sezení jsou k dispozici pouze na straně klienta [50, s. 47].

3. Mezipaměť (*Cache*) — data odeslaná v odpovědi serveru musí být rozdělena na data která mohou a nemohou být uložena do klientské mezipaměti pro budoucí znovupoužití při opakovaném požadavku.

4. Rozhraní mezi všemi komponenty systému je jednotné.

5. Vrstvený systém — každá vrstva poskytuje služby pouze přilehlé vyšší vrstvě a využívá pouze služby přilehlé nižší vrstvy [50, s. 46].

Volitelnou složkou REST je možnost získání rozšíření funkcionality klienta od serveru v podobě rozšiřujícího kódu — skriptu [50, s. 84,53].

REST Představuje záměr jak by měl fungovat *World Wide Web* [50, s. 75]. Vzhledem k založení webových technologií na protokolu HTTP tak může docházet ke splývání pojmů REST a HTTP. Samotná implementace webových REST API, kdy jsou k přenosu dat využívány HTTP metody POST, PUT, GET, DELETE a jako identifikátor prostředku slouží logické URL (*Uniform Resource Locator*) [51], svádí k tvrzení, že REST je pouze plné využití HTTP. Nejedná se ale o jedinou z možností. Teoreticky by bylo možné stejný princip nasadit v libovolném prostředí splňující výše uvedené požadavky.

3.1.5 CoAP — *Constrained Application Protocol*

Protokol CoAP vznikl jako reakce na potřebu komunikace zařízení s omezenými výpočetními a síťovými prostředky [52, s. 1]. Je navržený pro jednoduché propojení s HTTP [52, s. 1], ale namísto prosté komprese paketů je realizována část REST, optimalizovaná pro omezené aplikace [52, s. 2]. V původní podobě byl, navzdory původu v HTTP, protokol navržen za použití UDP protokolu jakožto transportní vrstvy, s přidáním zabezpečení do jednotlivých zpráv. Později bylo specifikováno i užití transportních vrstev TCP a WebSockets [53, s. 1].

Hlavička zprávy protokolu CoAP obsahuje 4 byte dlouhou hlavičku, obsahující informaci o použité verzi protokolu, typu a kódu[1] zprávy, informaci o délce proměnlivé části paketu a unikátní identifikátor zprávy [52, s. 15,16].

Coap definuje 4 typy zprávy [52, s. 10–14]:

- Potvrditelná (*CON*) — umožňuje spolehlivé doručení. Její odesílání je v případě nepotvrzení příjemcem periodicky opakováno s náhodným intervalem. Pokud na straně příjemce není možné zprávu zpracovat, je možné namísto potvrzení *ACK* odpovědět zprávou Reset.

[1] Obdoba HTTP kódu, např 4.04 — Not Found [52, s. 88]

- Nepotvrditelná (*NON*) — nevyžaduje reakci, příjemce na ni ale může reagovat zprávou Reset v případě nemožnosti zpracování. Duplicita příjmu zprávy je potlačena unikátním identifikátorem.
- Potvrzení (*ACK*) — může sloužit pro návrat vyžádaných dat, případně může být odeslána prázdná. Je vyslána vždy pouze jako reakce na zprávu *CON*.
- Reset (*RST*) — kromě výše zmíněného užití může sloužit také k datově nenáročnému zjišťování zařízení v síti zasláním prázdné *CON* zprávy, na kterou musí příjemce reagovat zprávou (*RST*) [52, s. 8]. Obdržení této zprávy tedy značí možnost komunikace s uzlem.

Na rozdíl od protokolu REST je v cílovém užití CoAP — vzájemná komunikace omezených zařízení — nutná možnost oboustranně iniciovaného přenosu. Toto výrazně omezuje model klient–server. Typicky tak implementace CoAP zahrnuje v zařízení implementaci obou rolí, klientské i serverové [52, s. 10].

3.2 IoT platformy

Data získané ze sítě senzorů je potřeba dále zpracovávat. Tato surová data v sobě mohou nést cenné poznatky o prostředí, ve kterém byly pořízeny. Bylo proto vyvinuto mnoho softwarových řešení umožňující zprávu koncových bodů a dat, jejich analýzu, vyhodnocování patřičné reakce na výstupy analýz a uživatelskou prezentace těchto dat. Ve spojitosti s těmito platformami zaznívají pojmy jako BigData, Machine Learning, Deep Learning, případně zpracování pomocí umělé inteligence. Tato problematika ovšem již spadá ryze do oblasti informatiky.

V následujícím testu bude představeno několik vybraných platforem běžně známých firem a jejich otevřené, volně dostupné alternativy.

3.2.1 Microsoft Azure IoT

Jádrem služeb Microsoft Azure Iot je Azure IoT Hub, umožňující obousměrnou komunikaci mezi IoT zařízeními a cloudem. Na tuto komunikační službu dále navazuje buď jednodušší, plně samostatná služba Azure IoT Central, nebo platforma Azure IoT accelerators, která již očekává vlastní aplikační vývoj [54; 55].

3.2.2 Amazon Web Services

Služby společnosti Amazon lze rozdělit na několik dílčích bloků, ze kterých dohromady sestává platforma AWS IoT (*Amazon Web Services internet of Things*) [56]. Jádrem systému je služba AWS IoT Core umožňující přijímat a zpracovávat data koncových bodů. Zajišťuje obousměrnou komunikace a umožňuje přemostění zařízení využívajících různé komunikační protokoly [57]. Jednotlivé koncové body je možné spravovat individuálně či po filtrovaných skupinách pomocí AWS IoT Device Management [58]. Pro pokročilou analýzu dat, předzpracovaných blokem AWS IoT Core, je možné nasadit službu AWS IoT Analytics [59].

Pro vývoj koncového bodu je k dispozici Amazon FreeRTOS, operační systém pro mikrokontroléry vyvinutý specificky pro implementaci do systému AWS IoT [60]. Pokud je uživatelem požadována jednoduchá fyzická interakce se systémem, je možné využít AWS IoT Button, jednoduché tlačítko s Wi-Fi konektivitou, kterému je v systému AWS IoT přiřazena patřičná akce [61].

3.2.3 Node-RED

Systém Node-RED je založen na JavaScriptovém prostředí Node.js [62]. Vzhledem k tomu systém dědí asynchronní, neblokující povahu založenou na obsluze událostí [63]. Principiálně se jedná o webový programovací nástroj, umožňující využití předdefinovaných vstupně-výstupních funkcí, základního třídění a tvorbu vlastních logických bloků, jejichž funkci je možné definovat prostřednictvím editoru JavaScriptového kódu [64]. Systém umožňuje výměnu dat pomocí MQTT, websockets, HTTP, případně přímý přístup k TCP i UDP kanálů. Rovněž je možné data zapisovat do lokálních SQL databází, nebo souborového systému. Samotné služby, jako MQTT broker, nebo SQL/NoSQL databázový server je ale nutné poskytnout externě.

4 Environmentální parametry a jejich měření

Kvalitu životního prostředí ovlivňuje mnoho faktorů. Pokud bychom chtěli zmapovat tyto parametry po celé městské zástavbě, případně v libovolné jiné ploše, bylo by nutné realizovat velice složitou síť senzorů. Neustálé zlevňování výroby elektronických integrovaných obvodů a pokrok v bezdrátových komunikacích však realizaci těchto sítí senzorů umožnil. Veškeré následující veličiny je tedy možné díky principům IoT měřit s detailním polohovým rozlišením, závislým pouze na výši investice do infrastruktury drobných měřicích zařízení. Vzhledem k dostupnému výpočetnímu výkonu moderních mikropočítačů je také možné tyto veličiny přímo v zařízení analyzovat a odesílat již částečně nebo zcela zpracovaná data. Je ovšem nutné pamatovat, že vzhledem k nárokům na co nejlevnější realizaci zařízení nebudou tato data naprosto spolehlivá a je tedy nutné k nim přistupovat jako k orientačním, poskytujícím hrubou představu o problému dané veličiny. Pokud by z nashromážděných dat vyplynulo, že se daná veličina pohybuje mimo rozsah hodnot povolených regulací pro tuto veličinu danou, je nutné nejprve tato data ověřit měřicími metodami a institucemi k tomu oprávněnými a až na základě těchto měření realizovat opatření.

4.1 Hluk

Za hluk je možné považovat zvuk, který je obtěžující osobám jemu vystaveným. Dlouhodobá expozice hlasitým zvukovým podnětům rovněž poškozuje zdraví těchto osob. I pokud intenzita zvuku není přímo zdraví poškozující, zmenšuje vystavení hluku pohodlí osob, kvalitu spánku a pracovní výkonnost. Je tedy důležité kontrolovat hladiny zvuku prostředí ve dne i v noci a vyvarovat se těmto negativním dopadům [65, s. 100]. Nasbíraná data potom mohou posloužit k odhalení rušivých elementů městského prostředí, zmapování hlukové zatíženosti jednotlivých oblastí a následnou korekci za účelem zlepšení životního prostředí.

Konkrétní hygienické limity hluku definuje nařízení vlády č. 272/2011 Sb., přičemž limitům pro volné prostředí v okolí staveb — hluk kontrolovatelný v rámci měřicích zařízení SmartCity ve veřejném prostředí — se věnuje část III, §12.[1] Jednotlivé limity jsou stanoveny jako součet základní hladiny akustického tlaku $L_{Aeq,T} = 50\,\mathrm{dB}$, korekcí pro noční dobu $-10\,\mathrm{dB}$ a korekcí v závislosti na druhu zdroje hluku a denní doby.

K měření intenzity hluku je nutné provést měření okamžitého bodového průběhu tlaku akustického média, ve kterém se akustický vzruch šíří. Mikrofony jsou tedy senzory určené k měření malého tlaku, specializované na časově proměnný průběh tlaku v rozsahu akustického pásma 20 Hz–20 kHz a necitlivé na konstantní tlakový posun [66, s. 431]. Z tohoto faktu vyplývá citlivost mikrofonů na mechanické podněty, neboť při konstantní ploše senzoru je měřený tlak

[1] Chráněný venkovní prostor staveb definuje § 30 odst. 3 zákona č. 258/2000 Sb. o ochraně veřejného zdraví. — Zjednodušeně volný prostor 2 m od obvodového pláště budovy.

přímo úměrný síle. Jakékoliv silové působení na senzorický element mikrofonu je tedy rovněž snímáno jako akustický signál a může tak vytvářet chybu měřené hodnoty. Pro vysokou imunitu vůči vibracím pak z druhého Newtonova pohybového zákona $\vec{F} = m\vec{a}$ vyplývá požadavek na co nejmenší hmotnost kmitavého senzorového prvku. V závislosti na principu měření je možné mikrofony rozdělit na [65, s. 136; 66, s. 434–442]:

- Rezistivní (uhlíkové) — změna odporu proměnlivě stlačené vrstvy grafitového prášku způsobuje změnu protékajícího proudu.
- Kondenzátorové — rozechvění elektrod deskového kondenzátoru s nábojem způsobuje změnu jejich vzdálenosti a tím i napětí mezi nimi.
- Elektretové — varianta kondenzátorových mikrofonů bez požadavku externího náboje díky použití vložky z trvale polarizovaného materiálu (elektretu).
- Optické — měřící interferenci mezi referenčním a od snímacího závěsu odraženým laserovým paprskem.
- Piezoelektrické — přímá transformace mechanického namáhání (ohybu) na elektrický náboj,
- Magnetoelektrické (dynamické) — indukce napětí do závitů zvukem rozechvívané cívky uložené v poli permanentního magnetu.

Z těchto principů je pro měření hluku nejvhodnější mikrofon kapacitní pro svou lineární frekvenční charakteristiku a konstantní citlivost [65, s. 136]. Pro drobná zařízení je vhodné užití mikrofonů elektretových, jelikož by zdroj polarizačního napětí toto zařízení komplikoval a přinášel by rovněž vyšší nároky na napájecí systém [65, s. 147]. Díky rozvoji MEMS je možné využívat výhody kapacitních mikrofonů i pro takto malá zařízení. MEMS mikrofony jsou vyráběny buď s analogovým výstupem, nebo přímo s integrovanými obvody upravujícími a vzorkujícími signál senzorového prvku a data poskytující skrze digitální sběrnici. Takové mikrofony je potom velmi jednoduché zapojit do mikropočítačové aplikace a jsou proto pro IoT zařízení ideální variantou.

Samotný hlukoměr se sestává z měřícího mikrofonu, obvodů upravující jeho výstupní signál, váhového filtru — stanoveného normou ČSN EN 61672-1 (IEC 61672-1) —, detektoru efektivní hodnoty a výpočtu ekvivalentní hladiny hluku [65, s. 146]. Váhové filtry jsou zařazeny pro přizpůsobení výsledné charakteristiky lidskému slyšení [65, s. 146]. Norma stanovuje užití filtru $\underline{\mathrm{A}}$[2], jehož přenosová charakteristika je dána [67, s. 402]:

$$A(f) = 20\log\left[\frac{{f_4}^2 f^4}{(f^2+{f_1}^2)\sqrt{(f^2+{f_2}^2)(f^2+{f_3}^2)}(f^2+{f_4}^2)}\right] - A_{1000} \quad [\mathrm{dB}], \quad (4.1)$$

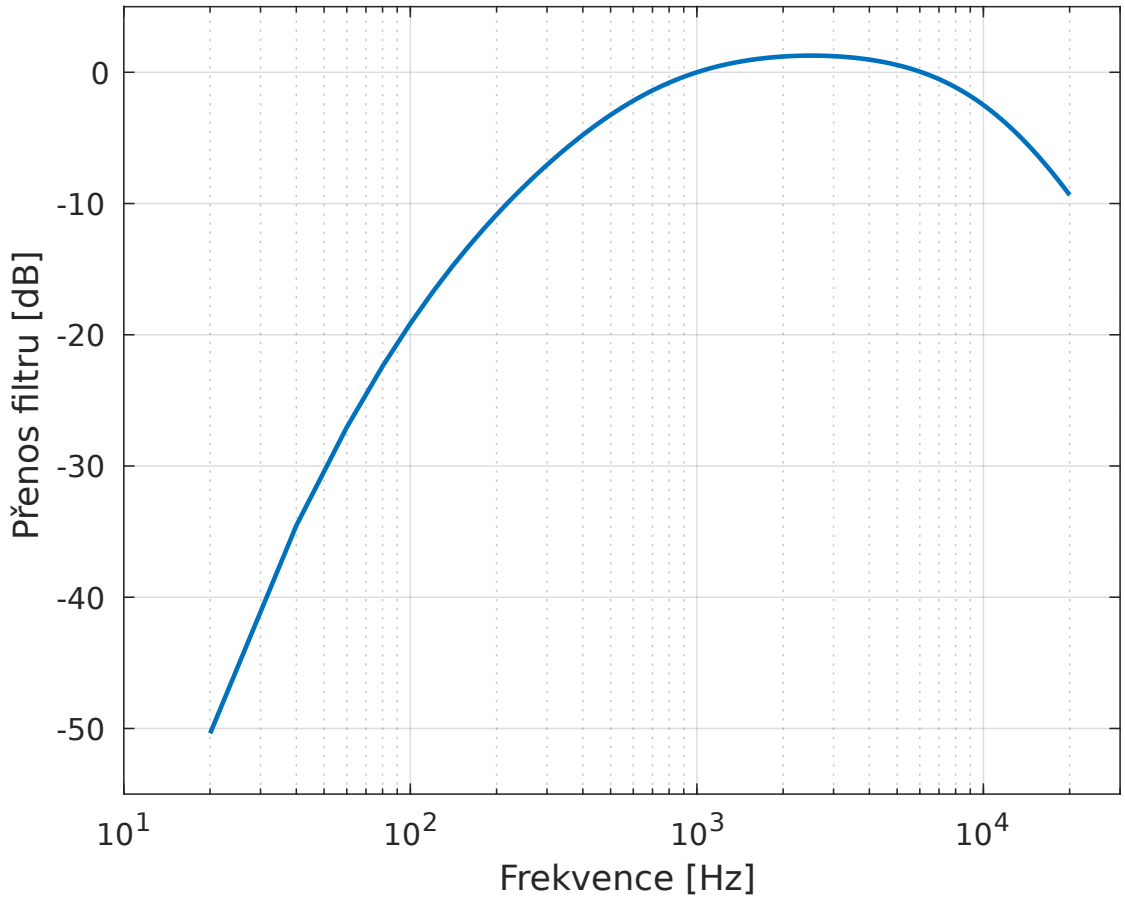
[2]Jedná se o písmenné označení jednotlivých filtrů. Dalšími druhy jsou [65, s. 146]:

- $\underline{\mathrm{B}}$ a $\underline{\mathrm{C}}$, které jsou vhodnější pro vyšší hladiny hluku,
- $\underline{\mathrm{D}}$ pro měření rázových hladin letového provozu,
- $\underline{\mathrm{E}}$ navržený s ohledem na vliv hluku na lidské zdraví,
- $\underline{\mathrm{SI}}$ určený pro měření v pásmu mluveného slova pro telekomunikace.

kde A_{1000} je konstanta normalizující přenos ke kmitočtu 1 kHz tak, že $A(1000) = 0\,\mathrm{dB}$. Číselné hodnoty jednotlivých zlomových frekvencí filtru jsou [67, s. 402]:

$$\begin{aligned} f_1 &= 20{,}60\,\mathrm{Hz}, \\ f_2 &= 107{,}7\,\mathrm{Hz}, \\ f_3 &= 737{,}9\,\mathrm{Hz}, \\ f_4 &= 12{,}194\,\mathrm{kHz}, \\ A_{1000} &= -2\,\mathrm{dB}. \end{aligned}$$

Po dosazení hodnot zlomových frekvencí a vyčíslení funkce pro jednotlivé argumenty frekvence lze získat frekvenční závislost útlumu filtru viz graf 4.1. Tento filtr obsahují všechny hlukoměry [65, s. 147].



Obrázek 4.1: Frekvenční charakteristika váhového filtru A

Pro porovnání hlukových hladin se užívá ekvivalentní hluková hladina L_{AeqT}, odpovídající střední hodnotě měřené hladiny akustického tlaku — hluku — vážené filtrem A po periodu T, dle definice

$$L_{AeqT} = 10 \log \left[\frac{1}{T} \int_0^T \left(\frac{p_A(t)}{p_0} \right)^2 dt \right], \tag{4.2}$$

kde $p_A(t)$ je akustický tlak vážený filtrem A a p_0 vztažný prahový tlak [65, s. 150].

4.2 Relativní vlhkost vzduchu

Vlhkost vzduchu společně s teplotou je důležitý parametr pro udržení komfortu osob a pro dodržení provozních parametrů mnohých technologických zařízení [66, s. 445]. Je definována jako

$$H = 100\frac{p_w}{p_s}, \tag{4.3}$$

kde p_w je parciální tlak[3] vodní páry a p_s tlak nasycené vodní páry při dané teplotě. Její hodnota vyjadřuje procentuální obsah vodní páry ve vzduchu vůči množství, které by při dané teplotě způsobilo saturaci — kondenzaci vody. Relativní vlhkost nemůže být použita nad teplotu při které za daného tlaku nastává var vody. Pro standardní atmosferický tlak je tedy tento ukazatel platný do 100 °C [66, s. 446].

Jinou možností měření vlhkosti je stanovení rosného bodu, což je teplota, pří které je relativní vlhkost za daného tlaku $H = 100\,\%$. Toto měření je ovšem omezeno teplotou bodu tuhnutí vody, kdy vlhkost na senzorovém elementu mrzne a na senzoru narůstá vrstva ledu zkreslující měření [66, s. 447].

Pro měření relativní vlhkosti je vhodný libovolný fyzikální jev závislý na koncentraci molekul vody ve vzduchu [66, s. 447]. Senzorové prvky pro měření vlhkosti mohou být kapacitní, konduktivní, optické, nebo oscilační [66, s. 445].

Kapacitní senzory jsou založeny na změně relativní permitivity dielektrického materiálu kondenzátoru. Využívají se materiály se silnou závislostí permitivity na vlhkosti (hygroskopické polymery), čímž dochází ke změně kapacity senzorového prvku [66, s. 448,449].

Konduktivní senzory mohou být dvojího typu:

- Elektrické, využívající změny vodivosti materiálu mezi elektrodami závislou na absorbované vlhkosti.
- Tepelné, zkonstruované ze dvou miniaturních termistorů připojených tenkými drátky — pro minimalizaci přenosu tepla. Jeden z termistorů je hermeticky uzavřen v suchém vzduchu a druhý je ponechán v atmosféře okolí. Oba termistory jsou zapojené do můstku a protékány proudem, který je vyhřívá na teplotu přibližně 170 °C. Vzhledem k proměnlivé tepelné vodivosti vzduchu v závislosti na relativní vlhkosti jsou tyto termistory rozdílně chlazeny a vzniká tak napěťový rozdíl na diagonále můstku. Tato metoda vyžaduje, aby byl vzduch v senzoru po dobu měření v klidu, jelikož by proudění vzduchu způsobovalo dodatečné chlazení termistoru [66, s. 452–456].

Optické senzory vynikají opakovatelností měření, jelikož mají oproti ostatním typům nižší hysterezi a hodí se proto pro kontrolu procesů velmi citlivých na vlhkost. Senzor se sestává z tenkého zrcadla se zabudovaným teplotním senzorem, které je peltierovým článkem udržované na rosném bodě, kde strmě klesá jeho odrazivost. Ta je měřena opticky fotodetektorem, na který dopadá světlo svítivé diody odražené od zrcadla. Regulační smyčka udržuje konstantní proud fotodetektorem tak, že je na ploše zrcadla rovnováha mezi výparem a kondenzací vody. Relativní vlhkost je potom možné dopočítat z teploty zrcadla a okolního tlaku [66, s. 456,457].

[3] Tlak, který by množství plynu obsaženého ve směsi vyvodilo na stěny nádoby, pokud by nebyly přítomny ostatní plyny [68].

Oscilační (piezoelektrické) senzory rovněž jako optické senzory měří relativní vlhkost vzduchu nepřímo stanovením teploty rosného bodu. Princip měření je ale mechanický. Jako senzorový element slouží tenká destička piezoelektrického krystalu, jehož rezonanční frekvence je ovlivňována hmotností vrstvy vody deponované na jeho povrchu vlivem kondenzace. Tento krystal je rovněž udržován na konstantní teplotě za pomoci peltierova článku. Kontrolní smyčka zde udržuje rezonanční frekvenci odpovídající hraně kondenzace — rosnému bodu. Hlavní obtíží konstrukce senzoru je realizace dostatečně kvalitního přenosu tepla z peltierova článku na piezoelektrický krystal.

4.3 Teplota

Společně s vlhkostí je teplota jedním ze základních parametrů prostředí určující komfort jeho obyvatel. Jedná se o jednu ze základních fyzikálních veličin a vyjadřuje část vnitřní energie těles. V rámci Smart City může sloužit zejména pro zpřesnění meteorologického modelování, případně předpověď odparu vody a tedy optimalizaci vodohospodářství.

Při měření je nutné pamatovat, že senzor teploty, který nemá stejnou teplotu jako měřený objekt, odebere, nebo předá měřenému objektu určité množství energie (tepla). Měřící prvek tedy nutně ovlivňuje měřený objekt a je nutné, aby jeho teplo nutné ke změně teploty bylo co nejmenší [66, s. 519]. Jedná se ale o relativní požadavek. Pokud bude předmětem měření stanovení teploty vzduchu v městském prostředí, bude vzhledem k množství plynu zanedbatelný senzor téměř libovolné velikosti. Jediným důsledkem senzoru s velkou tepelnou kapacitou tak může být zpoždění dat vůči reálné hodnotě, případně odfiltrování rychlých změn.

Rezistivní teploměry jsou založené na teplotní závislosti odporu elektrických vodičů. Tento jev byl pozorován již v roce 1812 a 66 bylo popsáno praktické užití platinového senzoru. Rezistivní teploměry jsou zpravidla vyráběny ve formě tenké plošné vrstvy, případně tenkého drátku materiálu. Pro svou dlouhodobou stabilitu je nejčastěji používána platina, i když je možné použít libovolný kov [66, s. 528]. Teplotní závislost rezistivity kovů je dána jako:

$$\rho(T) = \rho(T_0) \cdot \left[1 + \alpha \cdot \Delta T + \beta \cdot (\Delta T)^2\right], \tag{4.4}$$

kde T_0 je referenční teplota, $\rho(T_0)$ rezistivita při této teplotě, α a β materiálové teplotní koeficienty [69, s. 58]. Ze znalosti těchto parametrů pro daný senzor je tedy možné stanovit na základě odporu absolutní teplotu.

Dalším typem rezistivního teploměru je termistor. Na rozdíl od předchozích je vyroben z polovodiče. Ty mají přirozeně negativní teplotní koeficienty a na rozdíl od kovů tedy jejich rezistivity s rostoucí teplotou klesá. Existují i termistory s kladnými koeficienty, z hlediska přesnosti se ale upřednostňují termistory s negativními koeficienty [66, s. 532] Jelikož je závislost rezistivity těchto senzorů silně nelineární, je pro měření teploty nutné použít výpočetní model. Nejpřesnější z běžně užívaných je Steinhart-Hartův model [66, s. 533–539].

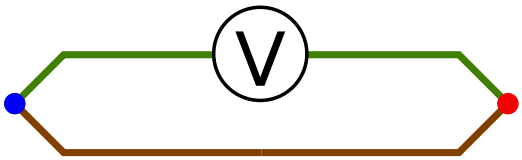
Jelikož je nutné změnu rezistivity transformovat do podoby elektrické veličiny, je nutné pro měření teploty pomocí rezistivního senzorového prvku navrhnout obvod citlivý na tuto změnu. Při tom je nutné dbát na udržení co nejmenšího protékajícího proudu senzorovým prvkem, který by v opačném případě způsoboval oteplení prvku a tím chybu měření.

Termoelektrické články využívají vzniku termoelektrického proudu v heterogenním obvodu — realizovaným po částech z jiného materiálu. Tento jev se nazývá Seebeckův jev a pokud

do obvodu zapojíme voltmetr, na jeho svorkách bude napětí přibližně:

$$U = \alpha(T_1 - T_2), \tag{4.5}$$

kde α je termoelektrický koeficient příslušného kontaktu a $T1$, $T2$ teploty jednotlivých kontaktů.



Obrázek 4.2: Propojení dvou různých materiálů kontakty s rozdílnými teplotami se zapojeným voltmetrem [66]

Podmínkou správné funkce je připojení voltmetru oběma svorkami ke stejnému materiálu, jinak by v obvodu vznikaly parazitní termoelektrické články [66, s. 550,551; 70, s. 312]. Toto zapojení je ilustrováno na obrázku 4.2. Termočlánky se podle složení dělí do několika typů označovaných písmeny. Běžnými typy jsou: T,J,E,K,R,S,B. Vzhledem k principu založeném na vzniku napětí při rozdílu teplot se jedná o relativní metodu měření. Pouze termočlánkem tedy nelze stanovit absolutní teplota měřeného objektu [66, s. 549,550].

V tomto případě je již přímo generován elektrický signál. Je ovšem nutné dbát na jeho co nejmenší zatížení, typicky tedy užít zesilovače s co největší vstupní impedancí.

Senzory s PN přechodem využívají teplotní závislosti vlastností diod a bipolárních tranzistorů. Pokud je PN přechod připojen ke zdroji konstantního proudu, stává se jeho napětí funkcí teploty přechodu. Senzory vykazují vysokou linearitu a je tak možné užití dvoubodové kalibrace strmosti charakteristiky [66, s. 556].

Optické senzory snímají záření v oblasti infračerveného spektra. Jejich hlavními výhodami jsou možnost bezkontaktního měření a rychlost [66, s. 560,561].

4.4 Tlak

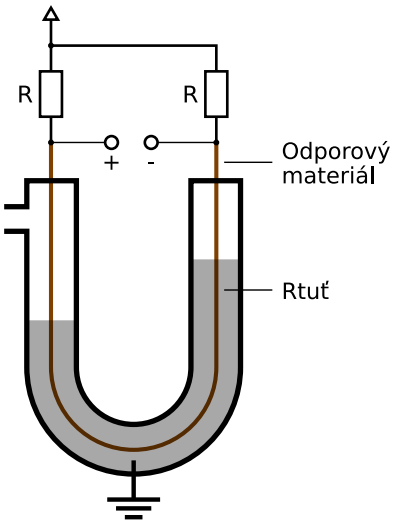
Společně s teplotou a relativní vlhkostí vzduchu tvoří tlak trojici základních meteorologických environmentálních parametrů. Tlak je jedním z určujících faktorů pro proudění vzduchu [71] a detailní znalost jeho rozložení umožňuje zlepšovat meteorologické modely. Podle vývoje tlaku v oblasti lze také očekávat srážky, případně suchá období [71].

Ve většině případů jsou senzory tlaku realizovány nepřímo, pomocí mechanické odezvy — deformace nebo posunu — hmoty senzoru [66, s. 379]. Jedná se tak o relativní měření, a pokud je požadován absolutní senzor, musí být vybaven uzavřenou referenční podtlakovou komorou [66, s. 385]. Historicky prvním zařízením pro měření tlaku byl Torricelliho rtuťový barometr. Na podobném principu lze, díky dobré vodivosti rtuti, zkonstruovat jednoduchý elektrický barometr, kde rtuťový sloupec slouží k rozvážení Wheatstonova můstku vlivem posunu zkratované oblasti odporového spojení [66, s. 378], viz obrázek 4.3.

Moderní tlakové senzory využívají ohebnou membránu, u které je měřena buď síla na ní tlakem vyvozená, nebo je sledován její pohyb. V závislosti na principu měření těchto změn lze senzory dělit na:

- Piezorezistivní — u kterých je přímo do membrány zabudována silová měrka. Celý tlakoměr je vyroben na monolitickém křemíkovém substrátu planární technologií. Tyto senzory jsou náchylné na změnu teploty, s jejímž nárůstem klesá jejich citlivost. Proto je u nich nutná teplotní kompenzace, ať už zabudovaná, nebo vnější. Další možností je udržování stabilní teploty senzoru [66, s 381–387].

- Kapacitní — které nevykazují teplotní závislost a je možné jejich výrazné přetížení. Membrána musí být konstruována aby umožnila velký pohyb elektrody proměnného kapacitoru a je tak možné do struktury zabudovat mechanické zarážky, které membránu ochrání před přetížením. V porovnání s piezorezistivními ale senzorová prvek vykazuje nelinearitu [66, s. 387,388].
- Reluktanční — konstruované s feromagnetickou membránou ovlivňující tok magnetickým obvodem [66, s. 388].
- Optické — založené na interferenci světla v dutině z polopropustnými zrcadly. Výška dutiny je ovlivňována pohybem membrány, což mění interferenční produkty měřené detektorem. Tyto senzory vynikají velkým rozsahem měřeného tlaku, nízkou teplotní závislostí a přesností [66, s. 390,391].



Obrázek 4.3: Jednoduchý elektrický rtuťový barometr [66, s. 378]

4.5 Detekce atmosferických výbojů (blesků)

Údery blesků ovlivňují bezpečí obsluhy rozvodů elektrizační soustavy, leteckou dopravu vlivem rušení rádiových spojení, mohou způsobovat lesní požáry [72], případně škody na elektrických zařízeních.

Sledování pozice výbojů může být realizováno opticky pomocí rychlých optických senzorů umístěných na geostacionárních družicích [73]. Další možností je detekce na základě signálu nízkofrekvenčního rádiového spektra produkovaného úderem blesku pozemními stanicemi [72; 74]. Tyto systémy mohou mít přesnost určení polohy menší než 1 km, detekční účinnost 70–90 % a mohou zaznamenat amplitudu proudu výboje [75]. Tyto systémy určují polohu kombinací magnetického a časového principu. Přímo ve stanici je určen směr šíření signálu na základě sady ortogonálních antén. Zachycený a zpracovaný signál je následně odeslán do centrální sítě, kde je podle pozice maxima signálu ze znalosti vzájemné polohy pozemních stanic a časového rozdílu stanovena poloha výboje [76; 77].

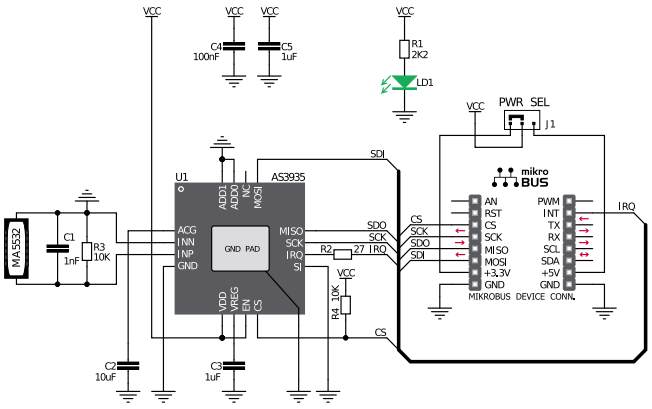
5 | Návrh systému detekce atmosferické výbojové aktivity

Vzhledem k malému rozšíření pokrytí sítí s krátkým dosahem je v současné době pro nasazení chytrých IoT zařízení v městském prostředí nutné volit sítě s dlouhým dosahem, u kterých toto pokrytí existuje. Dalšími argumenty jsou otevřenost a cena. Ze sítí představených v kapitole 2 v tomto ohledu vhodnou volbu představuje síť LoRaWAN, jelikož se jedná o velice otevřenou síť, do které je možné zapojovat zařízení bez složité autorizace — za předpokladu použití certifikovaných součástek — a existuje mnoho nezávislých sítí zajišťovaných z veřejných i soukromých prostředků, přičemž v některých je možný i provoz zdarma.

Vzhledem k jednoduchosti a dostupnosti byla pro testování detekčního prvku systému navržena testovací platforma za použití mikrokontroléru STM32F411RE na vývojové desce NUCLEO a mikropočítače RaspberryPI. Konektivita této platformy byla zajištěna technologií Wi-Fi.

5.1 Detekční prvek systému

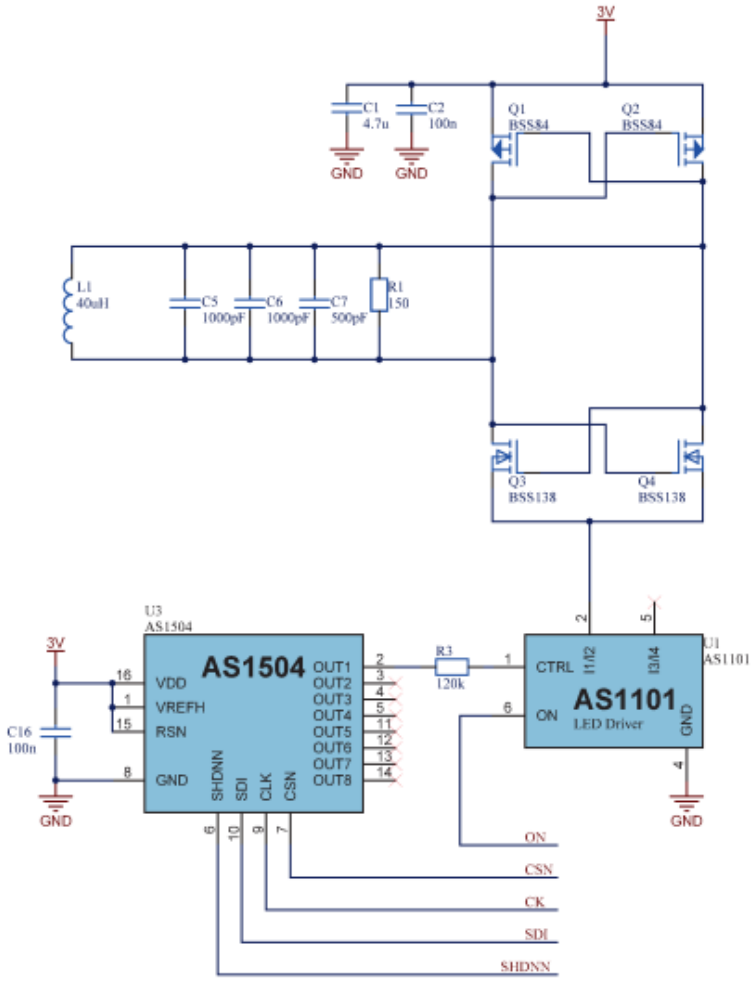
Pro řešení systému byl zadán čip AS3935 a pro prvotní testování byl použit přípravek Thunder click firmy MikroElektronika. Zapojení přípravku je znázorněno na obr. 5.1. Jedná se o modifikaci doporučeného zapojení výrobcem, doplněného o rezistory R2 a R4, které výrobce neuvádí, na princip funkce ale nemají vliv [78, s. 10]. Je povolen integrovaný napěťový regulátor, přípravek by tedy bylo možné napájet i napětím 5 V [78, s. 5]. Vzhledem k volbě napájení 3,3 V propojkou J1 není užití regulátoru nutné a bylo by tak možné ušetřit kondenzátor C3 [78, s. 9]. Jako anténa slouží obvodu paralelní rezonanční LC obvod realizovaný cívkou MA5532, kondenzátorem C1 a rezistorem R3. Obvod by měl mít rezonanční kmitočet 500 kHz a činitel jakosti $Q = 15$ [78, s. 23].



Obrázek 5.1: Schéma zapojení přípravku Thunder click [79]

5.2 Simulátor výbojové aktivity

K detekčnímu čipu AS3935 existuje evaluační souprava AS3935-DK. Ta obsahuje dvě desky, jednu s detekčním čipem, mikrokontrolérem PIC a LCD displejem, druhou se simulátorem výbojové aktivity. Podle zapojení na obrázku 5.2 je výboj simulován paralelním RLC rezonátorem shodné frekvence 500 kHz, ovšem s cívkou 40 µH. Tranzistory $Q1$ až $Q4$ tvoří H můstek řízený vlastní oscilací RLC obvodu. Budič AS1101 je řízen DA převodníkem AS1504, čímž je vytvořen 500 kHz amplitudový modulátor. Průběhy napětí převodníku bohužel nejsou známé. Tento přípravek při řešení práce nebyl k dispozici.



Obrázek 5.2: Schéma zapojení modulátoru Demo kitu AS3935 [80, s. 17]

5.3 Prvotní testování čipu AS3935

K přípravku Thunder click jsou také dostupné zdrojové soubory programu pro mikrokontrolér PIC, které jsou určené pro proprietární kompilátor mikroC firmy MikroElektronika[1]. Příklad je dostupný na adrese https://libstock.mikroe.com/projects/view/750/thunder-click-example.

Problematický je také rozsah příkladu, který umožňuje pouze ověření základní funkce a při obsluze čipu používá přímo hexadecimální adresy a hodnoty registrů. Je tedy čitelný pouze

[1]V průběhu tvorby práce výrobce doplnil příklady i pro jiné platformy a jazyky. Stále ovšem určené pro proprietární kompilátory.

za současného vyhledávání těchto hodnot v datovém listu součástky. Tyto hodnoty se kvůli struktuře dokumentu nenalézají na jednom místě a je tak nutné prostudování celého datového listu. Dalším problémem testovacího programu je absence konfigurace nastavení měřicího čipu AS3935. Z hlediska budoucího rozšiřování a implementace se tedy nejedná o vhodný zdroj, ze kterého by bylo možné vycházet při vytváření univerzální obslužné knihovny.

Nejblíže univerzálnímu použití je GNU knihovna určená pro platformu Arduino dostupná z: https://github.com/raivisr/AS3935-Arduino-Library. Vzhledem k platformě je knihovna objektově orientovaná, psaná v jazyce `C++`. Pro univerzálnost užití by byla vhodnější knihovna ve standardním C.

5.3.1 Obslužná knihovna čipu AS3935 v jazyce C

Objekt byl nahrazen strukturou, která obsahuje potřebné informace o připojeném čipu. Pomocí ukazatele na tuto strukturu je tak možné komunikovat s konkrétním čipem a v případě potřeby využívat knihovnu pro více čipů.

Důraz byl kladen zejména na neblokující povahu všech funkcí. Knihovna tedy nijak nezasahuje do přidělování výpočetního času a je možné ji použít i pro embedded operační systémy jako freeRTOS, případně ji využít jako základ pro obslužný kernel modul pro embedded linuxový systém.

Mechanismus přenosu dat pomocí ukazatele na obslužnou funkci — callback — vázanou na hardware byl převzat, jelikož umožňuje v knihovně zachovat nejvyšší možnou úroveň abstrakce nad platformou. Na rozdíl od Arduino knihovny neobsahuje struktura informace o CS a INT pinech. Obsloužení těchto signálů je ponecháno do aplikačního prostoru.

Jelikož samotný čip umožňuje komunikaci jak po sběrnici I2C, tak po SPI, jsou obě tyto možnosti v knihovně připraveny. Rozhodnutí o zvolené komunikaci je určeno podle ukazatelů funkcí, kde nulový ukazatel na I2C callback nastavuje SPI komunikaci a opačně. Řízení druhu komunikace je na čipu řízeno pinem SI (*Select Interface*), který by mohl být v aplikaci řízený softwarem a bylo by možné komunikovat s čipem střídavě po I2C a SPI. Jakkoliv je tato možnost zvláštní, nelze ji vyloučit a v rámci univerzálnosti by na ni knihovna měla být připravena. Do struktury nesoucí informace o instanci čipu byla tedy zahrnuta volba komunikačního rozhraní. V případě, že aplikace strukturu naplnila ukazateli na oba typy obslužné funkce, ale nenastavila mód komunikace, je vždy preferováno SPI.

Veškeré funkce obsažené v původní knihovně byly při přejímání postupně analyzovány a testovány. Pro lepší přehlednost byla také rozdělená makra, která v původní Arduino knihovně slučovala adresu a masku registru.[2] Operace s registry tedy probíhají pomocí sady tří hodnot — adresy, masky a bitového posunu — pro každý individuální registr, definovaných v separátním hlavičkovém souboru.

5.3.2 Zprovoznění čipu AS3935 na platformě STM32

Pro prvotní otestování funkce čipu byla knihovna testována na platformě STM32, konkrétně na vývojové desce NUCLEO-F411RE. Tato deska umožnila velice jednoduché přemostění dat přes vestavěný překladač sériového portu na USB.[3] Mikrokontrolér osazený na vývojové desce byl naprogramován tak, aby resetoval čip do továrního nastavení a periodicky vyčítal důležité registry čipu — typ přerušení, konfiguraci analogového bloku čipu, odhad vzdálenosti výboje

[2]Prostor registrů čipu AS3935 používá krátké několika-bitové registry složené do fyzických osmibitových registrů.

[3]Součást programátoru ST-Link V2-1 zabudovaného na deskách NUCLEO.

a jeho energii. Tyto informace mikrokontrolér následně vypisoval do sériového kanálu, který byl vývojovou deskou přeložen na virtuální sériový port USB (VCOM) a dále zpracován na počítači.

Po ověření základní funkce čipu byl program upraven, aby nevyčítal periodicky, ale pouze v případě změny dostupných dat — na základě signálu přerušení generovaného čipem AS3935. Tím se zabránilo opakovanému vypisování shodných stavů a zároveň bylo odstraněno riziko promeškání události mezi dvěma vyčteními čipu. Současně ale byla ztracena informace o času události. Proto byl do programu začleněn čítač reálného času (RTC) a do výpisu sériového kanálu zahrnuta informace o relativním čase. (Vzhledem k nedůležitosti absolutního času nebylo řešeno nastavení čítače na reálný čas a byl po zapnutí mikrokontroléru ponechán v nulovém nastavení. Tento čas je tedy relativní k připojení napájení systému.)

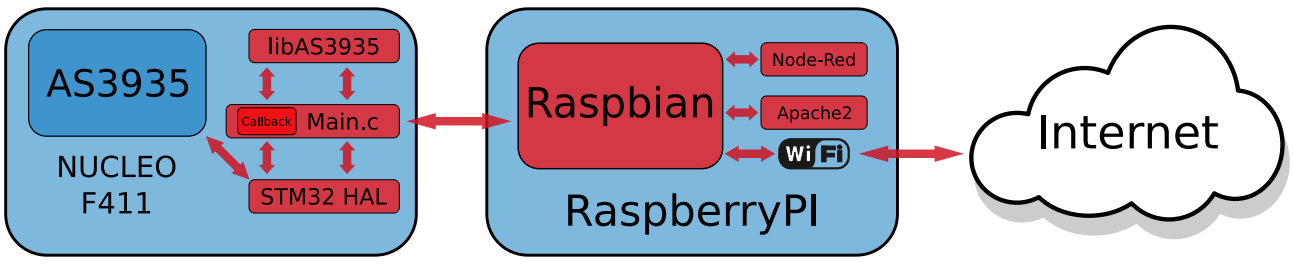
5.3.3 Dlouhodobý sběr dat

Dalším krokem vývoje bylo zaměření na dlouhodobé testování a následné hledání optimálního nastavení měřicího čipu. Vývojová konfigurace (PC–STM32–AS3935) pro dlouhodobý sběr dat není vhodná a z tohoto důvodu byl systém upraven a platforma pro dlouhodobý sběr dat byla založena na mikropočítači RaspberryPI s Linuxovým systémem Raspbian.

Na mikropočítači byl nainstalován systém Node-RED, který byl následně nakonfigurován tak, aby přijímal data ze sériového portu desky NUCLEO a zapisoval je do výstupního textového souboru, dostupného přes webový server Apache2 v základní konfiguraci. Díky využití systému NodeRed lze platformu připojit prakticky do jakéhokoliv cloudového řešení.

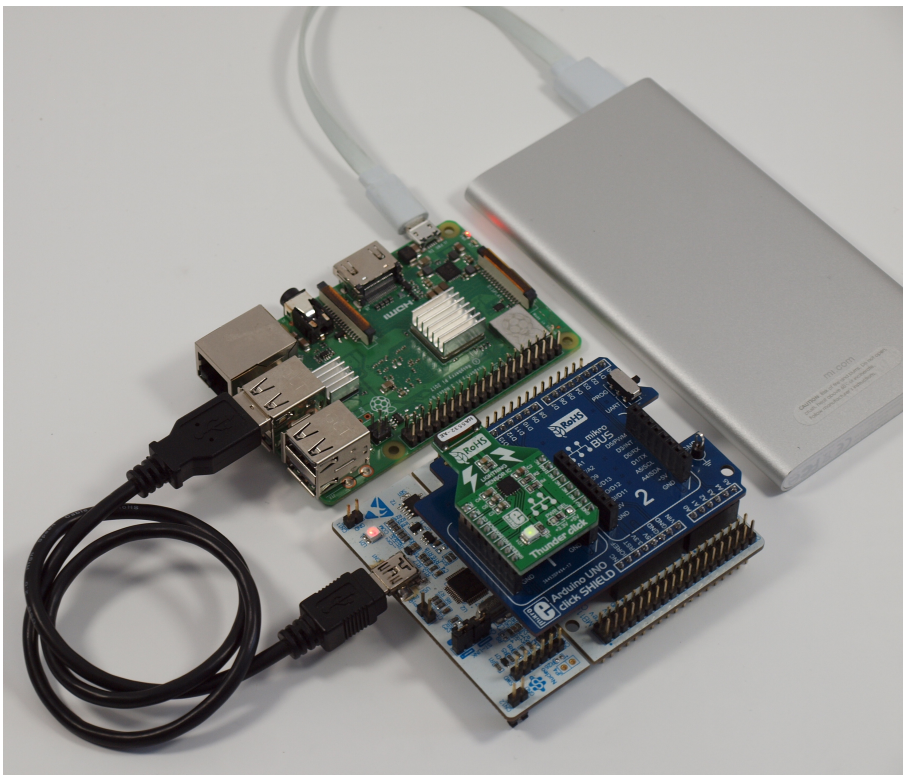
Během dlouhodobého testování je již znalost reálného času události důležitá, zejména kvůli jednoznačné identifikaci jednotlivých událostí. Proto byl v Node-RED do každé zprávy připojen řádek s informací o systémovém čase RaspberryPI. Nevýhodou tohoto řešení zůstává, že ani jedna z komponent nemá dedikovaný čítač reálného času a při každém vypnutí je tedy informace o čase ztracena. Počítač RaspberryPI získává informaci o čase z Internetu pomocí NTP serveru. Pokud ale startuje a nemá k dispozici síť, nastavení času neodpovídá realitě.[4]

Platformu je možné k síti Internet připojit skrze Ethnernet, nebo Wi-Fi připojení. Z důvodu testování, které vyžadovalo jistou míru mobility, byla platforma připojena k síti skrze Wi-Fi. Společně s bateriovým napájením tak vznikl zcela bezdrátový systém. Tato konfigurace umožnila flexibilní testování v laboratoři a možnost okamžitého pozorování výsledků měření.



Obrázek 5.3: Blokové schéma detekčního systému. Modře HW prvky, červeně SW prvky a znázornění datového toku

[4]Při výpadku proudu byl pozorován skok času cca o 15 minut zpět. RaspberryPI tedy zjevně periodicky ukládá čas do nevolatilní paměti.



Obrázek 5.4: Fotografie realizovaného detekčního systému

5.3.4 Výsledky prvotního testování

Testování na dvou hostitelských platformách přineslo zajímavé, ovšem nepříliš optimistické výsledky. Zejména se ukázala náchylnost čipu na zarušení přenášené galvanickou vazbou. Při připojení k osobnímu počítači totiž čip detekoval výrazné rušení, které nebyl schopný odfiltrovat, a jeho výstupem tedy bylo mnoho falešně hlášených výbojů.[5] Naproti tomu při připojení k mikropočítači RaspberryPI byl čip schopný okolní rušení rozpoznat a výsledkem tedy byl celkově spolehlivější systém. Shrnutí a porovnání výstupních dat je uvedeno v tabulce 5.1. Součet hlášených výbojů a rozpoznaných rušení ani v jednom z případů nesouhlasí s celkovým počtem událostí. Toto je dáno dvěma dalšími druhy událostí, které do tabulky nebyly zahrnuty. Čip AS3935 pracuje s 15minutovým statistickým oknem [78, s. 22]. Na základě těchto dat je odhadována vzdálenost čela bouřkové aktivity [78, s. 8]. Pokud se v tomto čase nevyskytne další výboj, čip upravuje statistiku a generuje přerušení bez příznaku jeho typu. Druhým typem události je manuální vyvolání vyčtení čipu tlačítkem na vývojové desce NUCLEO. Toto bylo používáno zřídka k ověření funkce řetězce, například při změně výstupního souboru dat v Node-RED.

[5] Všechny testy byly provedeny za klidného počasí bez bouřkové aktivity.

Tabulka 5.1: Porovnání dat prvotního testování na dvou hostitelských platformách

Hostitelská platforma	Celkový čas testování	Celkový počet událostí	Počet rozpoznaných rušení	Počet hlášených výbojů
Osobní počítač	22 h 55 min	545	457	52
RaspberryPI	5 d 13 h 26 min	1356	1351	0

Z dat je patrné, že čip připojený na osobní počítač byl schopný rozpoznat rušivé vlivy s úspěšností 90,5 %, kdežto při připojení na mikropočítač RaspberryPI bylo rozpoznání rušivých vlivů bezchybné. Zjevně se jedná o rušení pocházející z osobního počítače, přenášená po propojovacím USB kabelu. Vliv umístění vzhledem k osobnímu počítači lze vyloučit, jelikož při připojení přípravku na RaspberryPI a umístění do blízkosti osobního počítače, do polohy shodné s testovací polohou při připojení k počítači, nedošlo v porovnání s jiným umístěním k ovlivnění výstupních dat přípravku.

Zásadním problémem ale byla neschopnost systému detekovat bouřkovou aktivitu. Po dobu testovacího provozu proběhlo několik reálných bouřek, systém ovšem nezaznamenal žádnou výbojovou aktivitu. Ani laboratorní testování nepřineslo pozitivní výsledky. Byl proveden test detekce výboje ve vysokonapěťové laboratoři KET, kde byl použit výboj o délce 4 cm ve vzduchovém jiskřišti. Systém byl schopen detekovat jeden ze tří výbojů, ostatní maskoval jako rušení syntetické povahy. Dále byl proveden test na standardizovaný atmosferický pulz ve vysokonapěťové laboratoři KEE. Při těchto testech čip AS3935 vykazoval chování, které se ve specifikaci výrobce nedařilo dohledat. Během testu generoval přerušení s prázdným obsahem (nulový příznak a žádná data). Stejná data je možné získat při stisku tlačítka na vývojové desce NUCLEO. Patrně se tedy jedná o jev vyvolaný silným elektromagnetickým rušením vlivem výboje. Příčinou může být buď zarušení signálu na pinu mikrokontroléru desky NUCLEO připojeného k tlačítku, případně reset samotného měřícího čipu. Jelikož toto chování ale výrobce nespecifikuje, jedná se v druhém případě pouze o domněnku.

Reset mikrokontroléru lze vyloučit, jelikož nebyl pozorován výpis konfigurace testu, který je typický pro start běhu programu. Při opakování testu by bylo vhodné zakázat generování výpisu na stisk tlačítka a tím vyvrátit první ze jmenovaných možností. Při změně polohy systému do vzdálenosti od výboje dostatečné k bezporuchové funkci ovšem stále nedocházelo k očekávané detekci. Čip ale reagoval generováním přerušení s významem detekce syntetického rušení, která časově odpovídala generovaným výbojům.

Z pozorování tedy vyplývá, že detekční čip na výboje reagoval, ovšem maskoval je jako syntetická rušení. Toto chování nemusí být špatně, jelikož se skutečně o syntetické výboje jednalo.

5.4 Úpravy systému na základě výsledků prvotního testování

Negativní výsledky prvních testů vedly k opětovnému prostudování dokumentace. Pozornost byla věnována hlavně nutnosti kalibrace vnitřních oscilátorů AS3935. Oscilátory jsou vnitřně teplotně kompenzovány, vyžadují ale kalibraci při každém zapnutí čipu. Podle dokumentace je

přesnost kalibrace závislá na přesnosti nastavení rezonančního kmitočtu antény. Ten musí být nastaven s maximální chybou 3,5 % [78, s. 23].

5.4.1 Kalibrace oscilátorů čipu AS3935

Rezonanční kmitočet antény je možné zobrazit na pinu IRQ čipu AS3935. Pomocí logického analyzátoru PLA8[6] byl změřen, a i když frekvence spadala do tolerančního okna, byla upravena připojením 64pF korekční kapacity. Čip umožňuje korekci v rozsahu 0–120 pF s krokem 8 pF [78, s. 12]. Dále byla příkazem vyvolána automatická kalibrace vnitřních oscilátorů [78, s. 16,s. 23].

5.4.2 Přenastavení analogového bloku čipu AS3935

Další úpravou bylo zvýšení citlivosti analogového zesilovače a nastavení rozhodovací úrovně (registr WDTH — *Watchdog Threshold*) a filtru špiček (registr SREJ — *Spike Rejection*) na nejnižší možnou úroveň. Cílem bylo dosáhnout extrémně citlivé konfigurace.

S tímto nastavením byl čip schopný detekovat 10 výbojů v průběhu jedné bouřky. Tato detekce ale zůstala ojedinělá, neboť při dalších bouřkách systém shodně jako v minulém případě detekoval pouze rušení a to i naproti tomu, že následující bouřková aktivita byla výrazně silnější.[7]

5.4.3 Automatická kalibrace oscilátorů čipu AS3935

Manuální kalibrace přinesla první pozitivní výsledky, chování čipu ale stále neodpovídalo očekávání. Z tohoto důvodu byla pozornost dále zaměřena na automatickou kalibraci zařízení. Měření frekvence bylo realizováno čítačem mikrokontroléru za použití CAPCOM (*Capture-Compare*) jednotky. Z důvodu co nejvyšší přesnosti čítače byl nastaven takt mikrokontroléru na 100 MHz (maximální takt desky NUCLEO). Díky taktu 100 MHz čítač dosáhl časového rozlišení 10 ns. Jako zdroj hodinového signálu byl nastaven hodinový výstup programátoru ST-Link V2-1, přítomného na desce NUCLEO, který je generován na základě 8 MHz krystalu. Podle dokumentace by při výchozím dělení rezonanční frekvence měl být na výstupu čipu AS3935 kmitočet 31,25 kHz [78, s. 23]. Při této frekvenci a časovém rozlišení CAPCOM jednotky činí perioda signálu 3200 taktů čítače. Pro měření tedy postačuje 16bitový čítač, jehož přesnost bude $1/3200 = 0{,}03\,\%$, což lze považovat za dostačující.

Vzhledem ke skutečnosti, že operace nemusí být realizována v konkrétním časovém limitu, a k malému rozsahu korekční kapacity čipu AS3935 byl volen primitivní algoritmus kalibrace s postupným testováním všech kapacit. Následně byla volena korekční kapacita, k níž připadalo minimum odchylky od jmenovitého kmitočtu.

Pro sledování parametrů čipu bylo dále v programu mikrokontroléru implementováno automatické spouštění rekalibrace čipu AS3935 každou hodinu.

5.5 Výsledky po úpravách systému

V tomto nastavení systém, vzhledem k vysoké citlivosti, generoval značné množství dat, bohužel však negativních, jelikož data obsahovala pouze detekované rušení.

[6] Jedná se o klon původního Saleae Logic

[7] Během těchto bouřek došlo i k poruchám elektrizační soustavy a ke škodám na elektronických zařízeních.

Zároveň byl pozorován velký vliv umístění systému a vliv propojovacího USB kabelu mezi RaspberryPI a deskou NUCLEO.[8] Při použití dvou propojovacích kabelů různé délky při zachování pozice a nastavení systému se data liší. Ukázalo se, že užití delšího kabelu vede ke snížení počtu detekovaného rušení. Toto opět potvrzuje, že systém není dobře zkonstruován s ohledem na elektromagnetickou kompatibilitu.

Motivací ke změně polohy byla myšlenka, že by čip mohl být ovlivněn předměty v okolí. Zejména elektronikou, silovými rozvody, feromagnetickými předměty. Systém byl přemístěn do otevřenějšího prostranství, než ve kterém byl původně testován. Jednalo se o zavěšení do volného prostoru s odstupem minimálně 50cm od zdí v místě bez elektrického rozvodu, namísto původního umístění v rohu místnosti poblíž napájecí zásuvky a zařízení kancelářské povahy.

Ačkoliv očekávaným výsledkem přemístění bylo snížení počtu detekcí rušení, skutečným dopadem bylo naopak jeho zvýšení, za současného výskytu falešně detekovaných výbojů. Umístění tedy na sytém zcela jistě mělo vliv. Původní pozice však patrně nebyla zarušená, jako spíše zastíněná.

5.6 Další ladění a úpravy systému

Jelikož v předchozím testováním systém generoval značné množství dat, byl upraven zisk zesilovače zpět na výrobcem doporučenou hodnotu pro interiérové použití. Registry WDTH a SREJ byly ponechány v minimálním nastavení.

Tato změna nepřinesla zamýšlený dopad na minimalizaci rušení a falešně hlášených výbojů. Proto byly i registry WDTH a SREJ přenastaveny do výchozí hodnoty WDTH=2, SREJ=2 a během další bouřky[9] byly tyto parametry postupně laděny, dokud nebylo dosaženo detekce výbojů a zároveň potlačeno jejich falešné hlášení. Toto nastavení bylo: výchozí zesílení analogového bloku, WDTH=1, SREJ=0.

Vzhledem ke změnám v programu mikrokontroléru a postupnému narůstání objemu informací přenášeného do počítače RaspberryPI bylo přistoupeno ke změně formátu zpráv. Dosavadní formát byl zaměřen především na snadnou lidskou čitelnost a obsahoval tedy značné množství strojně nevyužitelných dat.

```
2000-01-01 00:05
Reading INT register:          0x04     Disturber detected
Reading DISTANCE register:     0x3F     (63) Out of range
Reading S_LIG_MM register:     0x00
Reading S_LIG_M register:      0x00
Reading S_LIG_L register:      0x00
```

Obrázek 5.5: Příklad výpisu první verze programu

Tento formát byl nahrazen zprávou ve formě jednoduchého jednoznakového identifikátoru separovaného rezervovaným znakem, sloužícím k rozdělením řetězce zprávy. Za tento znak byl zvolen křížek # — ASCII 32. Pomocí tohoto znaku byly zprávy rozděleny do tří skupin:

[8] Tento závěr je v rozporu s dřívějším pozorováním, kdy se ale jednalo o změnu polohy v malé vzdálenosti.
[9] Jednalo se o bouřky ve dnech 28.5.2018 a 29.5.2018, obě ve večerních hodinách.

- T: Text průběhu procesů mikrokontroléru. Tyto zprávy slouží pro ladění běhu a obsahují informace jinak nedůležité pro další zpracování. Jsou generovány během začátku programu a v průběhu automatické rekalibrace systému.
- S: Zpráva obsahující výsledky kalibrace a aktuální nastavení čipu.
- I: Data produkovaná detekčním čipem, vyčítaná mikrokontrolérem na základě přerušení.

Jako formát zprávy byl tentokrát pro jednoduché zpracování v systému Node-RED zvolen JSON, čímž došlo k výraznému ušetření přenášených dat a usnadnění zpracování zpráv. Zároveň byla zachována přímá čitelnost datového výstupu mikrokontroléru. Informace o relativním čase byla zaměněna za počet sekund od startu programu. Jako základ této hodnoty byl ponechán interní RTC mikrokontroléru, přičemž do výpočtu byly zahrnuty maximálně dny. Změna měsíce tedy způsobí resetování tohoto údaje. Energie impulzu byla převedena na jednu číselnou hodnotu.

```
I#{ "INT":0 , "DISTANCE":63 , "S_LIG":0 , "Time":67082 }
```

Obrázek 5.6: Příklad výpisu programu ve formátu JSON

5.7 Laboratorní ověření získaných parametrů

Empiricky získané nastavení bylo dále ověřeno v laboratoři za použití simulátoru výbojů EM TEST UCS 500M. Jako jiskřiště byla použita bleskojistka CPC AC240L. Parametry výboje byly: napětí 1 kV, proud 10 A, vzdálenost antény od bleskojistky 68 cm. Jako detekovaný je označen výboj, který byl čipem zaznamenán nezávisle na typu příznaku, jako identifikovaný je pak označen výboj, který byl zaznamenán s příznakem blesk. Jednotlivá měření byla prováděna skupinou 10 výbojů s periodou 5 s. V zaznamenaných datech tak bylo možné z časové znalosti jednotlivé detekce identifikovat a odfiltrovat od případného rušení. Naopak bylo také možné zjistit chybějící výboje.

Bylo provedeno několik sad testů, při kterých byl zkoumán vliv jednotlivých parametrů nastavení čipu na detekční schopnosti. Sledovány byly parametry:

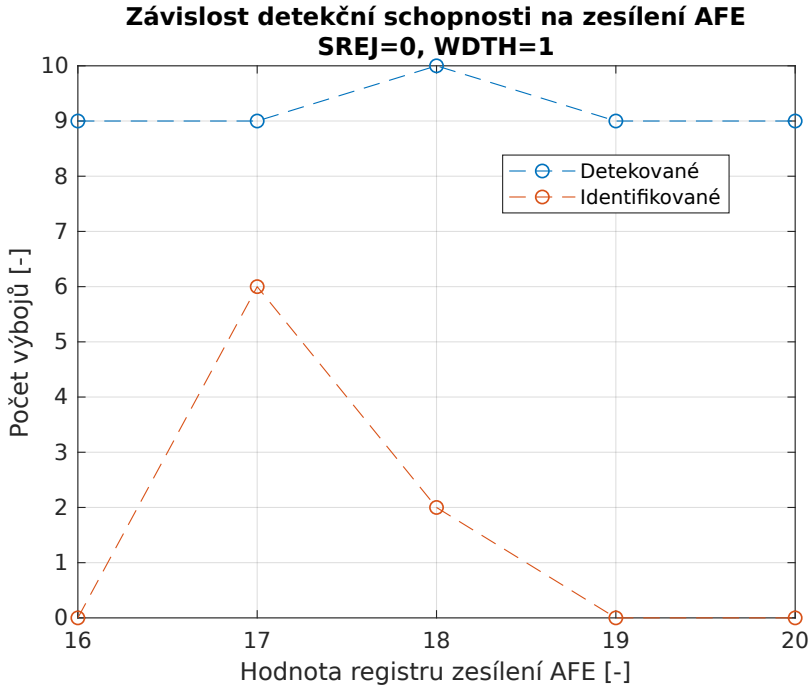
- zesílení analogového bloku — registr AFE,
- nastavení filtru špiček — registr SREJ,
- nastavení rozhodovací úrovně — registr WDTH.

Tabulka 5.2: Nastavení parametrů čipu AS3935 v průběhu jednotlivých sad měření

Sada č.	AFE	SREJ	WDTH
1	16–20	0	1
2	10–31	2 (výchozí)	2 (výchozí)
3	17	0–3	0
4	17	0–15	1

5.7.1 Jednotlivé sady testů a jejich výsledky

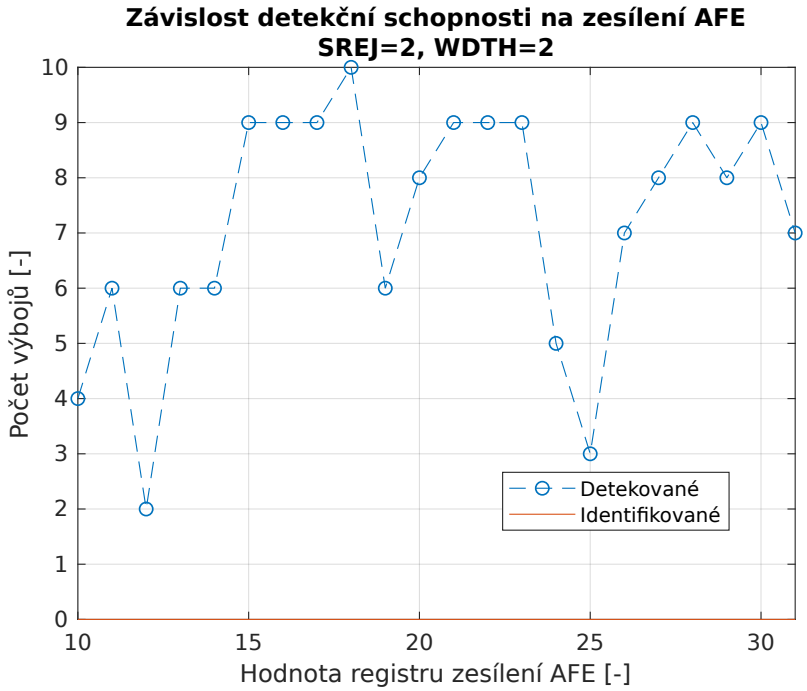
Sada č.1 byla navržena na základě pozitivních výsledků předchozího testování s podobným nastavením, s cílem zjistit optimální hodnotu registru AFE. Bylo zjištěno, že takové nastavení je AFE=17, viz graf 5.7. Výchozí hodnota pro interiérové užití, která byla během předchozího testování použita, sice vykazovala lepší detekční schopnost, hodnota AFE=17 byla ovšem lepší z hlediska identifikace výboje.



Obrázek 5.7: Výsledky první sady měření

Sada č.2 měla zjistit, zda existuje takové nastavení zesílení analogového bloku, se kterým by bylo možné dosáhnout porovnatelných výsledků se sadou č.1 za užití výchozího nastavení registrů SREJ a WDTH. Jak je patrné z grafu 5.8, takové nastavení buď neexistuje, nebo leží v hodnotách AFE< 10. Sada byla ukončena z důvodu výrazného poklesnutí detekční schopnosti.[10]

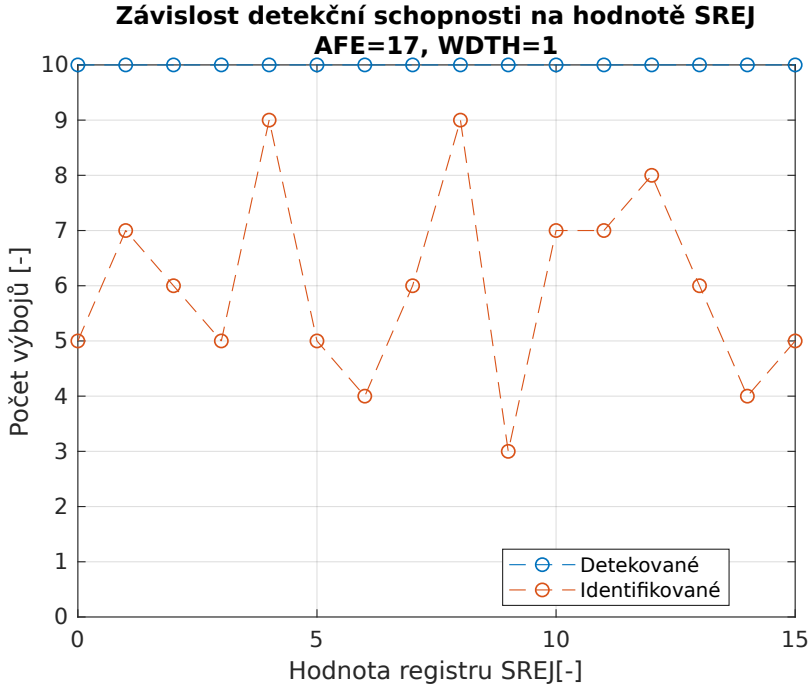
[10]Postup měření byl od vyšších hodnot AFE k nižším



Obrázek 5.8: Výsledky druhé sady měření

Sada č.3 měla ukázat, zda je možné detekovat a identifikovat výboj s nastavením WDTH=0, tedy minimálním rozhodovací úrovní. Byly detekovány všechny výboje, žádný však nebyl identifikován.

Poslední, čtvrtá, sada byla volena pro zjištění vlivu SREJ na funkci systému. Měření přineslo překvapivý výsledek. Z grafu 5.9 je patrné, že filtr špiček nemá vliv na detekční schopnost, ovlivňuje ale správnou identifikaci výboje. Z dat nelze odhadnout jakým způsobem. Jako vhodné hodnoty se jeví SREJ=4 a SREJ=8, ovšem v jejich okolí je identifikační schopnost zhoršená.

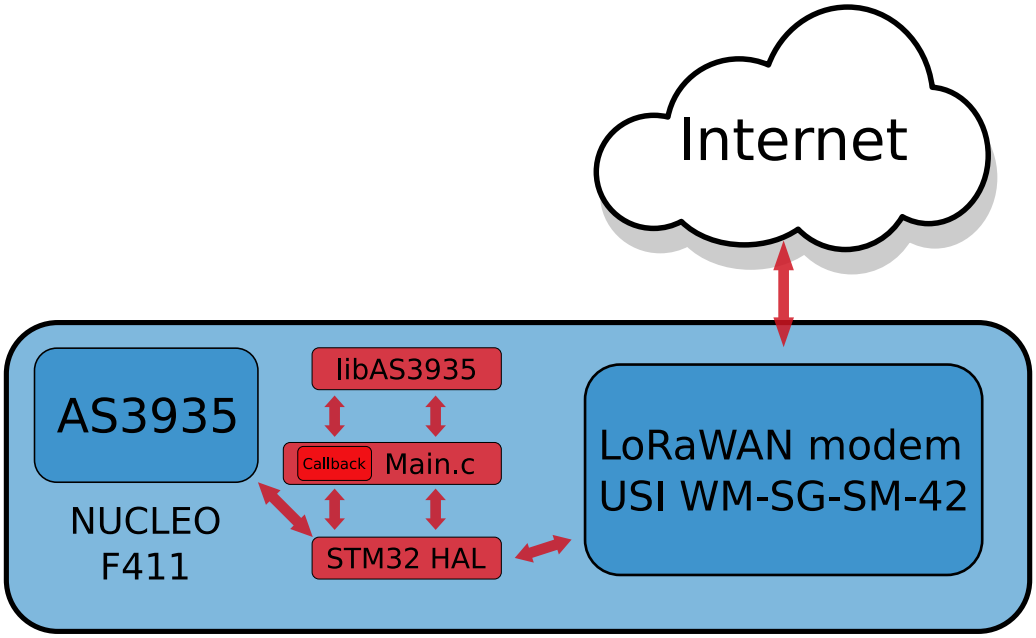


Obrázek 5.9: Výsledky čtvrté sady měření

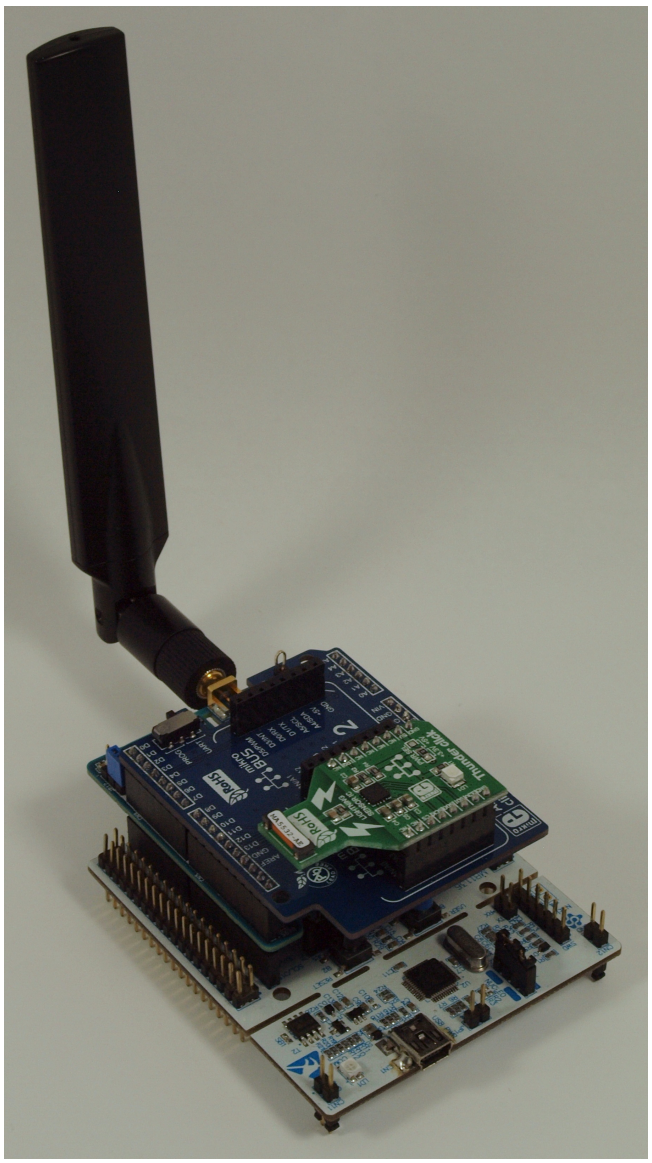
5.7.2 Implementace do sítě LoRaWAN

Jelikož se podařilo experimentálně získané nastavení detekčního čipu laboratorně ověřit a dále vylepšit, bylo možné přistoupit k úpravě systému pro IoT síť LoRaWAN. Vzhledem k malé náročnosti sítě tak bylo možné ze systému odstranit mikropočítač RaspberryPI, který představoval velkou energetickou zátěž.

Nevýhodou této změny je ztížení vzdálené rozšiřitelnosti software a nutnost dále komprimovat datový tok zařízení, vzhledem k omezení nelicencovaného pásma, ve kterém síť LoRaWAN operuje. Formát dat byl proto navržen binární, kde první byte obsahuje vzdálenost, další tři byte energii výboje. Informace o událostech označených jako rušení není přenášena. Zpráva tedy neobsahuje informaci o čase události, kterou vzhledem k absenci synchronizačního zařízení nelze získat. Informace o čase tak může být získána pouze na základě času přijetí zprávy v síti LoRaWAN. Tento údaj tedy bude zatížen chybou danou latencí zpracování a sítě.



Obrázek 5.10: Blokové schéma detekčního systému upraveného pro síť LoRaWAN. Modře HW prvky, červeně SW prvky a znázornění datového toku



Obrázek 5.11: Fotografie realizovaného detekčního systému s modemem pro síť LoRaWAN

6 | Závěr

Problematika Internetu věcí a Smart City je velice široká. Problémy a metody jejich řešení v této práci nastíněné, jsou pouze povrchovou sondou do možností této disciplíny. Existuje mnoho jiných informací, které je možné získávat a mnoho dalších metod, kterými je možné tyto informace předávat a zpracovávat. V každé části řetězce IoT je v současné době velké množství vzájemně zaměnitelných, konkurujících si řešení. Není jasné, zda tyto alternativy budou postupně zanikat, slučovat se, nebo naopak vznikat další.

S postupující penetrací elektroniky do zařízení běžného života budou dále vyvstávat otázky na užitečnost dat získatelných z těchto zařízení. Rovněž je důležité řešit problematiku ochrany osobních údajů a zabezpečení těchto zařízení proti zneužití.

Systém detekce blesků realizovaný v této práci byl úspěšně doveden do funkčního stavu a je plně integrovatelný do prostředí IoT. Metodu připojení k Internetu lze s volenými HW prostředky dobře měnit a integrovat tak systém pomocí jiných druhů konektivity, než které byly voleny v průběhu řešení této práce.

Princip detekce blesků pomocí dedikovaného integrovaného obvodu AS3935, obsahujícího bloky zpracování signálu, se z hlediska preciznosti určení polohy nemůže rovnat současným detekčním systémům. To je dáno zejména neznalostí detailního průběhu signálu a tedy nemožností jeho vzájemného porovnání s více detekčními zařízeními. Podařilo se ale nalézt takové nastavení, které při laboratorních testech vykazovalo stejnou citlivost, jako standardně použité pozemní detekční systémy.

Systém tak nad současným řešením vyniká hlavně svou velikostí a nenáročností na infrastrukturu. S použitím nezávislého napájení, například solárním panelem, by bylo možné vytvořit základní detekční síť i v odlehlých oblastech. K tomu by bylo ideální volit komunikaci s mesh topologií. V současném stádiu vývoje systém postrádá nezávislou detailní informaci o čase. Pro realizaci této detekční sítě by bylo nutné tuto informaci dodat. Vhodným řešením by mohlo být například použití časové informace ze satelitních navigačních systémů.

Vzhledem k faktu, že systém byl v této práci řešen jako evaluační platforma, složená z vývojových desek, objevovaly se problémy s elektromagnetickou kompatibilitou celku. Další pokračování ve vývoji zařízení by tedy znamenalo vytvoření specializované desky plošných spojů, navržené s ohledem na velkou citlivost detekčního čipu na elektromagnetické rušení.

Literatura

1. ASHTON, K. That 'Internet of Things' Thing. *RFID journal* [online]. 2009 [cit. 2018-06-02]. Dostupné z: http://www.rfidjournal.com/articles/view?4986.
2. MANEY, K. *Kevin Ashton, Father of the Internet of Things & Network Trailblazer* [online]. 2014 [cit. 2018-06-02]. Dostupné z: https://newsroom.cisco.com/feature-content?articleId=1558161.
3. *Internet of Everything* [online] [cit. 2018-06-02]. Dostupné z: https://newsroom.cisco.com/ioe.
4. GREENGARD, S. *The internet of things*. The MIT Press Essential Knowledge series. Cambridge: The MIT Press, 2015. ISBN 978-0-262-52773-6.
5. *On The Road To Autonomous Driving* [online] [cit. 2018-06-02]. Dostupné z: https://www.intel.com/content/dam/www/public/us/en/images/iot/autonomous-driving-infographic.png.
6. *SMART Cities* [online] [cit. 2018-06-02]. Dostupné z: http://www.iprpraha.cz/clanek/308/smart-cities.
7. HIGGINBOTHAM, S. The Internet of Trash: IoT Has a Looming E-Waste Problem. *IEEE Spectrum* [online]. 2018 [cit. 2018-06-02]. Dostupné z: https://www.spectrum.ieee.org/telecom/internet/the-internet-of-trash-iot-has-a-looming-ewaste-problem.
8. *How does an RFID system work?* [online] [cit. 2018-03-15]. Dostupné z: http://www.rfidjournal.com/faq/show?58.
9. KHATTAB, A.; JEDDI, Z.; AMINI, E.; BAYOUMI, M. *RFID Security: A Lightweight Paradigm*. Cham: Springer International Publishing AG, 2017. Analog Circuits and Signal Processing. ISBN 978-3-319-47545-5. Dostupné také z: https://link.springer.com/book/10.1007/978-3-319-47545-5#authorsandaffiliationsbook.
10. POOLE, I. *RFID Tags, Tagging, & Smart Labels* [online] [cit. 2018-03-15]. Dostupné z: http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/tags-tagging-transponders-smart-labels.php.
11. COOPER, E. *Greenville Hospital Deploys Integrated RFID Solution for Operating Room Asset Tracking* [online]. 2009 [cit. 2018-03-13]. Dostupné z: http://cdn2.hubspot.net/hub/42741/file-1935806028-pdf/Case_Studies/ThingMagic_GreenvilleHospital_CaseStudy_8_09.pdf?t=1517599378970. Případová studie. ThinkMagic.
12. POOLE, I. *RFID Frequencies and Frequency Bands*. Dostupné také z: http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/low-high-frequency-bands-frequencies.php.
13. *What is the difference between low-, high-, and ultra-high frequencies?* [online] [cit. 2018-03-15]. Dostupné z: http://www.rfidjournal.com/faq/show?60.

14. LÓPEZ-DE-IPIÑA, D.; VAZQUEZ, J.-I.; JAMARDO, I. Touch Computing: Simplifying Human to Environment Interaction through NFC Technology [online]. 2007 [cit. 2018-03-16]. Dostupné z: https://www.researchgate.net/publication/237663429_Touch_Computing_Simplifying_Human_to_Environment_Interaction_through_NFC_Technology.

15. BRAVO, J.; HERVÁS, R.; CHAVIRA, G.; NAVA, S. W.; VILLARREAL, V. From implicit to touching interaction: RFID and NFC approaches. In: *2008 Conference on Human System Interactions* [online]. 2008, s. 743–748 [cit. 2018-03-16]. Dostupné z: http://ieeexplore.ieee.org/document/4581534/.

16. COSKUN, V.; OZDENIZCI, B.; OK, K. A Survey on Near Field Communication (NFC) Technology. *Wireless Personal Communications* [online]. Roč. 71, s. 2259–2294 [cit. 2018-03-16]. Dostupné z: https://link.springer.com/article/10.1007/s11277-012-0935-5.

17. *What It Does* [online] [cit. 2018-03-15]. Dostupné z: https://nfc-forum.org/what-is-nfc/what-it-does/.

18. *NFC Everywhere: Crack open the benefits! NFC serves up protection and experiences for wine & spirits* [online]. 2017 [cit. 2018-03-13]. Dostupné z: https://blog.nxp.com/internet-of-things-2/nfc-everywhere-crack-open-the-benefits-nfc-serves-up-protection-and-experiences-for-wine-spirits.

19. JEON, K. E.; SHE, J.; SOONSAWAD, P.; NG, P. C. BLE Beacons for Internet of Things Applications: Survey, Challenges and Opportunities. *IEEE Internet of Things Journal* [online]. 2018 [cit. 2018-03-19]. Dostupné z: http://ieeexplore.ieee.org/document/8242361/.

20. ROSSEY, J.; MOERMAN, I.; DEMEESTER, P.; HOEBEKE, J. Wi-Fi helping out Bluetooth Smart for an improved home automation user experience. In: *2016 Symposium on Communications and Vehicular Technologies (SCVT)* [online]. 2016 [cit. 2018-03-19]. ISBN 978-1-5090-4361-3. Dostupné z: http://ieeexplore.ieee.org/document/7797663/.

21. SHAHID, R.; PRASANT, M.; ZHITAO, H.; THIEMO, V. Bluetooth smart: An enabling technology for the Internet of Things. In: *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* [online]. 2015, s. 155–162 [cit. 2018-03-19]. ISBN 978-1-4673-7701-0. Dostupné z: http://ieeexplore.ieee.org/document/7347955/.

22. IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)* [online]. 2011 [cit. 2018-04-02]. Dostupné z: http://ieeexplore.ieee.org/document/6012487/.

23. *Zigbee is the only complete IoT solution, from the mesh network to the universal language that allows smart objects to work together.* [online] [cit. 2018-04-05]. Dostupné z: http://www.zigbee.org/zigbee-for-developers/zigbee-3-0/.

24. *Z-Wave FAQ*. 2018. Dostupné také z: http://www.z-wave.com/faq.

25. *Z-Wave - About*. 2018. Dostupné také z: http://www.z-wave.com/about.

26. *What is Thread?* 2018. Dostupné také z: https://www.threadgroup.org/What-is-Thread.

27. THREAD GROUP, INC. *Thread Specification: 1.1.1* [online]. 2017 [cit. 2018-04-21]. Dostupné z: https://www.threadgroup.org/ThreadSpec.

28. LORA ALLIANCE, INC. *LoRaWAN™ 1.1 Specification* [online]. 2017 [cit. 2018-04-21]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf.

29. LORA ALLIANCE, INC. *What is LoRaWAN™: A technical overview of LoRa® and LoRaWAN™* [online]. 2015 [cit. 2018-04-21]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf.

30. LORA ALLIANCE, INC. *LoRaWAN ™ 101: A Technical Introduction* [online] [cit. 2018-04-21]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/lorawan-technical-intro.pdf.

31. SIGFOX S.A. *Sigfox: Technical Overview*. 2017. Dostupné také z: https://storage.sbg1.cloud.ovh.net/v1/AUTH_669d7dfced0b44518cb186841d7cbd75/dev_medias/build_technicalOverview.pdf.

32. *Sigfox Technology Overview* [online] [cit. 2018-04-29]. Dostupné z: https://www.sigfox.com/en/sigfox-iot-technology-overview.

33. *SigFox Coverage* [online] [cit. 2018-04-29]. Dostupné z: https://www.sigfox.com/en/coverage.

34. *FAQ* [online] [cit. 2018-06-04]. Dostupné z: https://simplecell.eu/faq/#toggle-id-37.

35. *SDR Dongle* [online] [cit. 2018-04-29]. Dostupné z: https://build.sigfox.com/sdr-dongle.

36. FLORE, D. *3GPP Standards for the Internet-of-Things* [online]. 2016 [cit. 2018-05-08]. Dostupné z: http://www.3gpp.org/images/presentations/3GPP_Standards_for_IoT.pdf.

37. SCHALKWYK, T. van. *3GPP LPWA Standards: LTE-M, NB-IoT & EC-GSM* [online]. 2017 [cit. 2018-05-08]. Dostupné z: https://m2mconnectivity.com.au/downloads/LPWAN%20Downloads/%28Cellular%29SierraWireless_M2MConnectivity%282017%29_watermarked.pdf.

38. LOY, M.; KARINGATTIL, R.; WILLIAMS, L. *ISM-Band and Short Range Device Regulatory Compliance Overview* [online]. 2005 [cit. 2018-05-13]. Dostupné z: http://www.ti.com/lit/an/swra048/swra048.pdf.

39. SINHA, S. R.; PARK, Y. *Building an Effective IoT Ecosystem for Your Business* [online]. Cham: Springer International Publishing AG, 2017 [cit. 2018-05-06]. ISBN 978-3-319-57391-5. Dostupné z: https://link.springer.com/book/10.1007/978-3-319-57391-5#toc.

40. AL-FUQAHA, A.; GUIZANI, M.; MOHAMMADI, M.; ALEDHARI, M.; AYYASH, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials* [online]. 2015, roč. 17, č. 4, s. 2347–2376 [cit. 2018-05-06]. ISSN 1553-877X. Dostupné z: https://ieeexplore.ieee.org/document/7123563/.

41. LYSOGOR, I. I.; VOSKOV, L. S.; EFREMOV, S. G. Survey of data exchange formats for heterogeneous LPWAN-satellite IoT networks. In: *2018 Moscow Workshop on Electronic and Networking Technologies (MWENT)* [online]. 2018, s. 1–5 [cit. 2018-05-06]. Dostupné z DOI: 10.1109/MWENT.2018.8337257.

42. *Introducing JSON* [online] [cit. 2018-05-06]. Dostupné z: https://json.org.

43. *JSON - Introduction* [online] [cit. 2018-05-06]. Dostupné z: https://www.w3schools.com/js/js_json_intro.asp.

44. OASIS OPEN. *OASIS MQTT Internet of Things Standard Now Approved by ISO/IEC JTC1* [online]. 2016 [cit. 2018-05-08]. Dostupné z: https://www.oasis-open.org/news/pr/oasis-mqtt-internet-of-things-standard-now-approved-by-iso-iec-jtc1.

45. OASIS OPEN. *MQTT Version 3.1.1* [online]. 2015 [cit. 2018-05-08]. Dostupné z: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf.

46. HIVEMQ. *MQTT Essentials Part 6: Quality of Service 0, 1 & 2* [online] [cit. 2018-05-08]. Dostupné z: https://www.hivemq.com/blog/mqtt-essentials-part-6-mqtt-quality-of-service-levels.

47. OASIS OPEN. *OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0* [online]. 2012 [cit. 2018-05-08]. Dostupné z: https://docs.oasis-open.org/amqp/core/v1.0/amqp-core-complete-v1.0.pdf.

48. VASTERS, C. *From MQTT to AMQP and back* [online]. 2017 [cit. 2018-05-08]. Dostupné z: http://vasters.com/blog/From-MQTT-to-AMQP-and-back/.

49. VASTERS, C. *The AMQP 1.0 Protocol - 2/6 - Core Elements* [online]. 2015 [cit. 2018-05-08]. Dostupné z: https://www.youtube.com/watch?v=b6C-BoOALng.

50. FIELDING, R. T. *Architectural Styles and the Design of Network-based Software Architectures* [online]. 2000 [cit. 2018-05-28]. Dostupné z: https://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf. Disertační práce. University of California.

51. IBM. *Representational State Transfer (REST) services*. Dostupné také z: https://www.ibm.com/support/knowledgecenter/en/SSZLC2_8.0.0/com.ibm.commerce.webservices.doc/concepts/cwvrest.htm.

52. INTERNET ENGINEERING TASK FORCE (IETF). *RFC 7252 - The Constrained Application Protocol (CoAP)* [online] [cit. 2018-05-28]. Dostupné z: https://tools.ietf.org/html/rfc7252.

53. INTERNET ENGINEERING TASK FORCE (IETF). *RFC 8323 - CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets* [online]. 2018 [cit. 2018-05-28]. Dostupné z: https://tools.ietf.org/html/rfc8323.

54. *Compare Azure IoT options* [online]. 2017 [cit. 2018-06-03]. Dostupné z: https://docs.microsoft.com/en-us/azure/iot-accelerators/iot-accelerators-options.

55. *What is SaaS?* [online] [cit. 2018-06-03]. Dostupné z: https://azure.microsoft.com/en-us/overview/what-is-saas/.

56. *AWS IoT* [online] [cit. 2018-06-01]. Dostupné z: https://aws.amazon.com/iot/.

57. *AWS IoT Core* [online] [cit. 2018-06-01]. Dostupné z: https://aws.amazon.com/iot-core/.

58. *AWS IoT Device Management* [online] [cit. 2018-06-01]. Dostupné z: https://aws.amazon.com/iot-device-management/.

59. *AWS IoT Analytics* [online] [cit. 2018-06-01]. Dostupné z: https://aws.amazon.com/iot-analytics/.

60. *Amazon FreeRTOS* [online] [cit. 2018-06-01]. Dostupné z: https://aws.amazon.com/freertos/.

61. *AWS IoT Button* [online] [cit. 2018-06-01]. Dostupné z: https://aws.amazon.com/iotbutton/.

62. *Node-RED* [online] [cit. 2018-06-03]. Dostupné z: https://nodered.org.

63. *About Node.js®* [online] [cit. 2018-06-03]. Dostupné z: https://nodejs.org/en/about/.

64. *Writing Functions* [online] [cit. 2018-06-03]. Dostupné z: https://nodered.org/docs/writing-functions#writing-a-function.

65. BERAN, V. *Chvění a Hluk*. Plzeň: Západočeská univerzita v Plzni, 2010.

66. FRADEN, J. *Handbook of Modern Sensors: Physics, Designs, and Applications*. Fourth Edition. New York: Springer, 2010. ISBN 978-1-4419-6465-6.

67. ČESKÝ NORMALIZAČNÍ INSTITUT. *Elektroakustika - Zvukoměry - Část 1: Technické požadavky*. ČSN EN 61672-1.

68. GOOCH, J. W. (ed.). Partial pressure. In: *Encyclopedic Dictionary of Polymers* [online]. New York, NY: Springer New York, 2007, s. 696–696 [cit. 2018-04-29]. ISBN 978-0-387-30160-0. Dostupné z DOI: 10.1007/978-0-387-30160-0_8294.

69. KUČEROVÁ, E. *Elektrotechnické materiály*. Západočeská univerzita v Plzni, 2002.

70. HAASZ, V.; SEDLÁČEK, M. *Elektrická měření: Přístroje a metody*. Českké vysoké učení technické v Praze, 2005.

71. *Why is the weather different in high and low-pressure areas?* [online] [cit. 2018-06-02]. Dostupné z: https://www.americangeosciences.org/education/k5geosource/content/weather/why-is-the-weather-different-in-high-and-low-pressure-areas.

72. GAIKWAD, N. B.; KHANDARE, A.; MAYEKAR, M.; KESKAR, A. G. Design and implementation of digital system for cost effective lightning detection sensor node. In: *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2017-07, s. 1–5. Dostupné z DOI: 10.1109/ICCCNT.2017.8203933.

73. KOKOU, P.; WILLEMSEN, P.; LEKOUARA, M.; ARIOUA, M.; MORA, A.; BRAEMBUSSCHE, P. V. den; NERI, E.; AMINOU, D. M. A. Algorithmic Chain for Lightning Detection and False Event Filtering Based on the MTG Lightning Imager. *IEEE Transactions on Geoscience and Remote Sensing*. 2018, s. 1–10. ISSN 0196-2892. Dostupné z DOI: 10.1109/TGRS.2018.2808965.

74. ARANGUREN, D.; GONZÁLEZ, J.; CRUZ, A.; INAMPUÉS, J.; TORRES, H.; PÉREZ-TOBÓN, P. S. Lightning strikes on power transmission lines and lightning detection in Colombia. In: *2017 International Symposium on Lightning Protection (XIV SIPDA)*. 2017-10, s. 273–278. Dostupné z DOI: 10.1109/SIPDA.2017.8116936.

75. CORREIA, S.; LOURENÇO, Â.; RIO, J.; PRIOR, V.; MOREIRA, N. Portuguese lightning detection network, applications and developed products. In: *2016 33rd International Conference on Lightning Protection (ICLP)*. 2016-09, s. 1–7. Dostupné z DOI: 10.1109/ICLP.2016.7791457.

76. KRIDER, E. P.; NOGGLE, R. C.; PIFER, A. E.; VANCE, D. L. Lightning Direction-Finding Systems for Forest Fire Detection. *Bulletin of the American Meteorological Society*. 1980, roč. 61, č. 9, s. 980–986. Dostupné z DOI: 10.1175/1520-0477(1980)061<0980:LDFSFF>2.0.CO;2.

77. CHRISTIAN, H. J. *A Lightning Primer* [online] [cit. 2018-06-01]. Dostupné z: https://lightning.nsstc.nasa.gov/primer/primer3.html.

78. AUSTRIAMICROSYSTEMS AG. *Datasheet: AS3935 Franklin Lightning Sensor IC: Rev. 1.2* [online] [cit. 2018-04-28]. Dostupné z: https://media.digikey.com/pdf/Data%20Sheets/Austriamicrosystems%20PDFs/AS3935.pdf.

79. *Thunder click manual* [online] [cit. 2018-06-02]. Dostupné z: https://download.mikroe.com/documents/add-on-boards/click/thunder/thunder-click-manual-v100.pdf.

80. AUSTRIAMICROSYSTEMS AG. *AS3935 Demo Kit Manual* [online] [cit. 2018-05-31]. Dostupné z: https://ams.com/documents/20143/36005/AS3935_UG000280_1-00.pdf/529d2181-b746-34ff-20d6-5acbe217086e.