

# **Bezdrátové snímače napájené technikou Energy Harvesting**

Bc. Jiří Němec

---

Diplomová práce  
2014



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2013/2014

## **ZADÁNÍ DIPLOMOVÉ PRÁCE** (PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jiří Němec**  
Osobní číslo: **A12349**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Bezdrátové snímače napájené technikou Energy harvesting**

Téma anglicky: **Wireless Sensors Powered by Energy Harvesting**

Zásady pro vypracování:

- 1. Zpracujte literární rešerší na téma senzorů založených na technice Energy Harvesting.**
- 2. Navrhněte několik senzorů založených na této technice.**
- 3. Vytvořte prototypy navržených senzorů.**
- 4. Vytvořte programové vybavení pro použité mikropočítače.**
- 5. Ověřte a zhodnoťte funkci vytvořených senzorů.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **CATSOU LIS, John. Designing Embedded Hardware. Sebastopol: O'Reilly Media, 2005. ISBN 978-0-596-00755-3.**
2. **KEATING, Michael. Low power methodology manual: for system-on-chip design. Editor Shashank Priya, D Inman. New York, NY: Springer, c2009, xvi, 300 p. ISBN 9780387718194-.**
3. **MANN, Burkhard. C pro mikrokontroléry: ANSI-C, kompilátory C, spojovací programy - linkery, práce s ATMEL AVR a MSC-51, příklady programování v jazyce C, nástroje pro programování, tipy a triky. Praha: BEN, 2003. ISBN 80-730-0077-6.**
4. **PINKER, Jiří. Mikroprocesory a mikropočítače. Praha: BEN - technická literatura, 2004. ISBN 80-730-0110-1.**
5. **STEPHEN BEEBY, Neil White. Energy harvesting technologies. Editor Shashank Priya, D Inman. New York: Artech House, c2009, xx, 517 s. ISBN 978-0-387-76463-4.**
6. **STEPHEN BEEBY, Neil White. Energy harvesting for autonomous systems. Editor Shashank Priya, D Inman. Norwood, Mass: Artech House, c2009, xx, 517 s. ISBN 978-159-6937-192.**

Vedoucí diplomové práce:

**Ing. Jan Dolinay, Ph.D.**

Ústav automatizace a řídicí techniky

Datum zadání diplomové práce:

**7. února 2014**

Termín odevzdání diplomové práce:

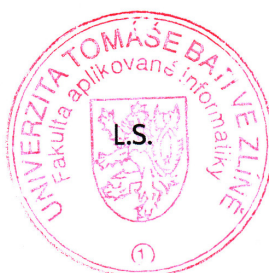
**27. května 2014**

Ve Zlíně dne 7. února 2014



prof. Ing. Vladimír Vašek, CSc.

*děkan*



doc. RNDr. Vojtěch Křesálek, CSc.

*ředitel ústavu*

### **Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### **Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- Že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

## ABSTRAKT

Práce je zaměřena na problematiku napájení bezdrátových snímačů technikou Energy Harvesting. V teoretické části popisuje energetické zdroje používané v oblasti Energy Harvesting a elektronické komponenty potřebné k jejich využití. V praktické části se zabývá tvorbou prototypu platformy bezdrátového snímače napájeného touto technikou a dále vybírá a hodnotí snímače fyzikálních veličin vhodné pro tuto platformu.

*Klíčová slova: Energy Harvesting, bezdrátový , snímač, senzor, kondenzátor, superkondenzátor, ultrakapacitor, fotovoltaický*

## ABSTRACT

The thesis focuses on powering wireless sensors using Energy Harvesting technology. The theoretical part describes the energy sources used in the Energy Harvesting and describes the necessary electronic components required for their use. The practical part deals with the creation of a prototype wireless sensor platform powered by this technique, selecting suitable sensors and testing them.

*Keywords: Energy Harvesting, wireless , sensor, capacitor, supercapacitor, ultracapacitor, photovoltaic*

Rád bych poděkoval vedoucímu práce Ing. Janu Dolinayovi, Ph.D. za cenné rady a připomínky. Dále bych rád poděkoval Ing. Tomáši Richtovi za původní inspiraci vedoucí ke vzniku této práce.

## Obsah

<b>ÚVOD</b> .....	<b>10</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>11</b>
<b>1 ENERGY HARVESTING</b> .....	<b>12</b>
1.1 BEZDRÁTOVÝ SNÍMAČ NAPÁJENÝ TECHNIKOU ENERGY HARVESTING .....	12
<b>2 ZDROJE ENERGIE</b> .....	<b>14</b>
2.1 OKOLNÍ SVĚTLO .....	14
2.1.1 Slunce .....	14
2.1.2 Princip .....	15
2.1.3 Konstrukce .....	16
2.1.4 Typy fotovoltaických článků .....	16
2.2 KINETICKÉ ZDROJE .....	17
2.2.1 Lidské tělo .....	17
2.2.2 Výrobní stroje .....	18
2.2.3 Doprava .....	18
2.2.4 Stavby .....	18
2.2.5 Elektromagnetické generátory .....	19
2.2.6 Elektrostatický generátor .....	20
2.2.7 Piezoelektrický generátor .....	21
2.3 TEPELNÉ ZDROJE .....	22
2.3.1 Termoelektrický princip .....	22
2.3.2 Pyroelektrický princip .....	23
2.4 OSTATNÍ ZDROJE .....	23
2.5 SKLADOVÁNÍ ENERGIE .....	24
2.6 ELEKTROCHEMICKÝ AKUMULÁTOR .....	24
2.6.1 Elektrochemické kondenzátory .....	25
2.7 OBVODY MANAGEMENTU NAPÁJENÍ .....	26
2.7.1 Násobič napětí .....	27
2.7.2 Zvyšující DC-DC měnič .....	27
2.7.3 MPPT (Maximum power point tracking) .....	28
<b>3 MIKROKONTROLÉR</b> .....	<b>29</b>
<b>4 KRYPTOGRAFIE</b> .....	<b>30</b>
4.1 MODERNÍ KRYPTOGRAFIE .....	30
4.2 SYMETRICKÁ KRYPTOGRAFIE .....	30
4.2.1 Proudové šifry .....	30

4.2.2	Blokové šifry .....	30
4.3	ASYMETRICKÁ KRYPTOGRAFIE .....	31
4.4	ALGORITMY NAD ELIPTICKÝMI KŘIVKAMI.....	31
<b>II</b>	<b>PRAKTICKÁ ČÁST.....</b>	<b>32</b>
<b>5</b>	<b>KOMPONENTY PLATFORMY .....</b>	<b>35</b>
5.1	ZDROJ ENERGIE.....	35
5.2	MANAGEMENT NAPÁJENÍ .....	36
5.2.1	Linear Technology LTC3108 .....	36
5.3	SKLADOVÁNÍ ENERGIE.....	40
5.4	MIKROKONTROLÉR .....	41
5.4.1	Kryptografické schopnosti mikrokontrolérů .....	44
5.5	RÁDIOVÝ PŘENOS .....	47
5.5.1	Nordic Semiconductor nRF905.....	48
5.5.2	Formát rámce .....	49
5.5.3	Použité moduly .....	49
<b>6</b>	<b>PLATFORMA BEZDRÁTOVÉHO SNÍMAČE .....</b>	<b>51</b>
6.1	PLATFORMA BEZDRÁTOVÉHO SNÍMAČE S ATMEGA644PA .....	51
6.1.1	LTC3108 .....	52
6.1.2	Atmel ATmega644PA .....	52
6.2	PLATFORMA BEZDRÁTOVÉHO SNÍMAČE S EFM32 .....	53
6.2.1	EFM32TG820F32.....	54
<b>7</b>	<b>PŘIJÍMAJÍCÍ STANICE .....</b>	<b>55</b>
7.1	PŘIJÍMAJÍCÍ STANICE S ATMEGA328P .....	55
7.2	PŘIJÍMAJÍCÍ STANICE S ATMEGA1284P .....	55
7.2.1	ATmega1284P.....	56
7.2.2	HiLink HLK-RM04.....	56
<b>8</b>	<b>SPOLEČNÉ PROGRAMOVÉ VYBAVENÍ .....</b>	<b>58</b>
8.1	ROZDÍLY MEZI PROGRAMY.....	58
8.2	PROGRAMOVÁNÍ S OHLEDEM NA ENERGII .....	58
8.3	KOMUNIKACE .....	59
8.3.1	Formát packetu .....	59
8.3.2	Šifrování packetu.....	59
8.3.3	Generování klíče.....	60
8.3.4	Distribuce klíčů.....	61
8.3.5	Možné útoky .....	61
<b>9</b>	<b>SNÍMAČE .....</b>	<b>62</b>

9.1	MAGNETICKÝ KONTAKT .....	62
9.1.1	Jazyčkový kontakt .....	62
9.1.2	Bezpečnostní varianty .....	62
9.1.3	Programová obsluha .....	63
9.2	ČLUNKOVÝ SRÁŽKOMĚR .....	64
9.2.1	Argent Data Systems 80422 .....	64
9.2.2	Programová obsluha .....	64
9.3	TEPLOMĚR DS18B20 .....	65
9.3.1	Programová obsluha .....	66
9.4	VLHKOMĚR DHT11.....	67
9.4.1	Princip činnosti.....	67
9.4.2	Programová obsluha .....	67
9.5	PASIVNÍ INFRAČERVENÝ DETEKTOR .....	68
9.5.1	Integrovaný obvod BISS0001.....	69
9.5.2	Modul detektoru HC-SR501.....	70
9.5.3	Programová obsluha .....	71
9.6	DALŠÍ UVAŽOVANÉ SNÍMAČE .....	72
9.6.1	Tříštění skla .....	72
9.6.2	Detektor kvality ovzduší.....	72
<b>10</b>	<b>OVĚŘENÍ A ZHODNOCENÍ VÝSLEDKŮ .....</b>	<b>73</b>
10.1	PLATFORMA .....	73
10.2	MAGNETICKÝ KONTAKT .....	74
10.3	ČLUNKOVÝ SRÁŽKOMĚR .....	74
10.4	TEPLOMĚR DS18B20 .....	75
10.5	TEPLOMĚR A VLHKOMĚR DHT11.....	75
10.5.1	Zkušenosti z praxe.....	75
10.6	PASIVNÍ INFRAČERVENÝ DETEKTOR .....	76
10.7	SHRNUTÍ VÝDRŽE .....	76
10.8	MOŽNÁ VYLEPŠENÍ .....	76
	<b>ZÁVĚR .....</b>	<b>78</b>
	<b>SEZNAM POUŽITÉ LITERATURY .....</b>	<b>79</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>	<b>83</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>85</b>
	<b>SEZNAM TABULEK.....</b>	<b>86</b>
	<b>SEZNAM PŘÍLOH .....</b>	<b>87</b>

## ÚVOD

Množství elektroniky na planetě se každým rokem zvyšuje, již nyní je na planetě více aktivních mobilních telefonů, než samotných lidí. Trh Internet of Things by měl dle analýz [29] do roku 2020 dosáhnout 30 až 50 miliard instalovaných kusů. Takový obrovský počet elektroniky je ale nutné nějak napájet elektrickou energií, jistě nebudou všechny umístěny poblíž elektrické zásuvky. Chytré mobilní telefony je nutné dobíjet přibližně každý den, sportovní náramky nevydrží ani týden. Pokud by vývoj pokračoval podobným směrem, budeme do několika let každý den dobíjet třeba i 10 elektrických zařízení a po dvou letech v nich měnit baterie, pokud to vůbec bude možné. To je jistě dostatečně děsivý výhled do budoucnosti.

Je tedy nutné volit jiné směry ve vývoji elektroniky. V posledních deseti letech se velmi snížila spotřeba elektrické energie klíčových elektronických komponent, to umožnilo elektronice fungovat na malou baterii poměrně dlouhou dobu, tak dlouhou, že často není limitem spotřeba energie, ale stárnutí a samovybíjení samotného zdroje energie.

Existence nízkopříkonové elektroniky se spotřebou v jednotkách  $\mu\text{A}$  umožnila využití zdrojů energie, které by byly dříve považovány za velice neperspektivní. Tuto elektroniku je možné napájet nevyužitou energií dostupnou z okolí. Jde o využití zdrojů energie jako je sluneční záření, vibrace, nebo přebytečné teplo. Tyto techniky napájení se nazývají anglickým výrazem Energy Harvesting.

Tyto zdroje energie obvykle nebývají dostupné po celou dobu běhu zařízení, energii je tedy nutné postupně akumulovat a odebírat, až jí bude potřeba použít. K napájení nízkopříkonových elektrických obvodů je vhodné využít moderní elektrochemické kondenzátory, které velmi efektivně akumulují elektrickou energii a mají velmi dlouhou životnost.

Praktickým účelem této práce je využít dostupné technologie nízkopříkonové elektroniky, elektrochemických kondenzátorů a techniky napájení Energy Harvesting a vytvořit z ní platformu pro bezdrátové snímače. V této platformě byly následně otestovány některé zvolené snímače fyzikálních veličin. Data získaná snímači jsou bezdrátově odesílány k přijímající stanici, která tyto údaje zpřístupní k využití v počítačové síti a tedy i na internetu.

Nevýhoda práce v měřítku nízkopříkonové elektroniky je nemožnost využít velké množství snímačů využívající aktivní principy snímání, které mají velké energetické nároky. Na druhou stranu může takto navržená elektronika fungovat, v ideálním případě, bez jakékoliv údržby desítky let od instalace. Životnost této elektroniky je omezena pouze životností použitých elektrických komponent. Například dvouvrstvé elektrochemické kondenzátory mají typicky udávanou životnost 100 000 cyklů, tedy při každodenním nabití a vybití se jedná o několik lidských životů, reálně však půjde o desítky let.

# I. TEORETICKÁ ČÁST

## 1 ENERGY HARVESTING

Energy Harvesting je způsob, jak využít zdroje energie z okolního prostředí, převést je v elektrickou energii, uskladnit tuto energii a následně jí napájet elektrické zařízení. Tento text se nezabývá obřími fotovoltaickými elektrárnami, které postupně nahrazují zemědělské plodiny na našich polích, či obřími větrnými elektrárnami, nýbrž využitím drobných zdrojů energie k napájení ještě menších elektrických obvodů, které monitorují fyzikální veličiny a výsledky měření odesílají bezdrátově k přijímači.

Takovéto senzory je tedy možné umístit do okolního prostředí bez nutnosti instalovat k nim kabeláž, která (dle [23]) vyjde průměrně asi na 4000 Kč za kus a rovněž bez nutnosti měnit v nich baterie. Takto napájený bezdrátový snímač, pokud je správně vytvořen a umístěn, tak může mít téměř neomezenou životnost, omezenou pouze životností jednotlivých komponent.

Využití těchto technik je umožněno převážně díky pokroku ve snižování spotřeby elektrické energie v dnešní elektronice. Moderní mikrokontroléry obsahují úsporné režimy a využívají techniky, které jim snižují spotřebu elektrické energie k řádům  $\mu W$ . Tento pokrok ve vývoji mikrokontrolérů umožňuje využívat k jejich napájení i poměrně slabé zdroje energie, které jsme ještě nedávno považovali za zoufale neperspektivní. Například se úspěšně používají v hodinkách firem Seiko a Citizen termoelektrické generátory s účinností pouhých 0,1 %.

S využitím technologie MEMS (Microelectromechanical systems), která na jeden kus křemíku umísťuje jak elektronické, tak mechanické prvky, je možné vytvořit takzvaný Smart dust. Smart dust neboli v překladu chytrý prach je složený z ohromného počtu drobných senzorů milimetrových rozměrů, které mezi sebou vytváří komunikační síť, která efektivně hospodáří s elektrickou energií a dokáže fungovat i po ztrátě většího počtu senzorů. Možností využití této technologie jsou velmi rozsáhlé. Od vojenského využití, například při sledování dění na bitevním poli, sledování opotřebení jednotlivých součástí v leteckém pumyslu HUMS (Health and usage monitoring), nebo třeba i jen sledování inventáře.

S využitím MEMS technologií je tak možné dokonce vytvořit senzory tak drobných rozměrů, že je unese i hmyz, jak dokazuje studie CSIRO a Tasmánské univerzity, která monitoruje pohyb 5000 včel a do budoucna plánují to samé například s komáry. [23][10]

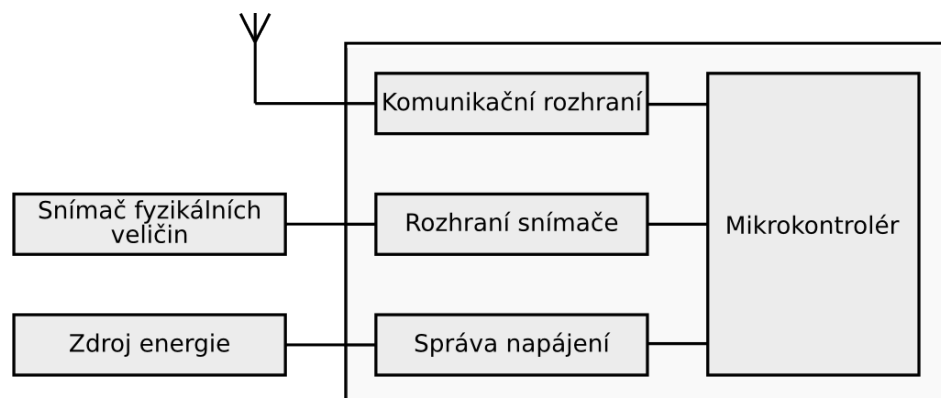
### 1.1 Bezdrátový snímač napájený technikou Energy Harvesting

Bezdrátový snímač je zavedený termín pro zařízení měřící fyzikální veličinu a odesílající ji bezdrátově k přijímači. Sensor, či český výraz snímač, je součástka používaná ke snímání, či detekci fyzikálních veličin. Takto naměřenou hodnotu je nutné zpracovat a bezdrátově odeslat k přijímači. Takové zařízení je nazýváno bezdrátový snímač, nebo



Obr. 1. Včela vybavená snímačem vyrobeným technologií MEMS [30]

těž v bezpečnostním průmyslu detektor. Energy Harvesting tento bezdrátový snímač doplňuje o způsob napájení. [23][10]



Obr. 2. Blokové schéma obecného Energy Harvesting systému

## 2 ZDROJE ENERGIE

Používané zdroje jsou schopné dodávat energii trvale, nebo nárazově, obvykle ty nárazové zdroje převládají. Často je tedy vhodné kombinovat různé zdroje energie, výběr vhodných zdrojů je nutné vybrat dle podmínek v dané aplikaci. Získaná energie se obvykle dále skladuje v elektrochemických kondenzátorech, případně v akumulátorech a počítá se tedy s nedostupností energie po celou dobu běhu, aplikace tedy počítá s dostupností například energie slunečního záření polovinu dne a v noci se přepíná do úsporných režimů s nižší spotřebou energie, případně senzor v běžeckých botách může přestat vysílat, pokud se zastaví pohyb. [23][10]

Tab. 1. Porovnání výkonové hustoty energie různých metod typu Energy Harvesting [10]

Zdroj energie	Výkonová hustota
Akustický hluk	0,003 $\mu\text{W}/\text{cm}^3$
Teplotní změna	10 $\mu\text{W}/\text{cm}^3$
RF	1 $\mu\text{W}/\text{cm}^2$ (GSM 900 MHz) 0,001 $\mu\text{W}/\text{cm}^2$ (Wi-Fi)
Okolní světlo	100 $\text{mW}/\text{cm}^2$ (přímé slunce) 100 $\mu\text{W}/\text{cm}^2$ (osvětlená místnost)
Termoelektrická energie	60 $\mu\text{W}/\text{cm}^2$ (člověk) 1-10 $\text{mW}/\text{cm}^2$ (průmysl)
Otřesy (mikrogenerátor)	4 $\mu\text{W}/\text{cm}^3$ (pohyb člověka) 800 $\mu\text{W}/\text{cm}^3$ (stroj)
Otřesy (piezoelektrický princip)	200 $\mu\text{W}/\text{cm}^3$
Proudění vzduchu	1 $\mu\text{W}/\text{cm}^3$
Stlačení tlačítka	50 $\mu\text{J.N}$
Vložka v botě	330 $\mu\text{W}/\text{cm}^3$
Ruční generátor	30 $\text{W.kg}$
Nárazy podpadku boty	7 $\text{W}/\text{cm}^2$

### 2.1 Okolní světlo

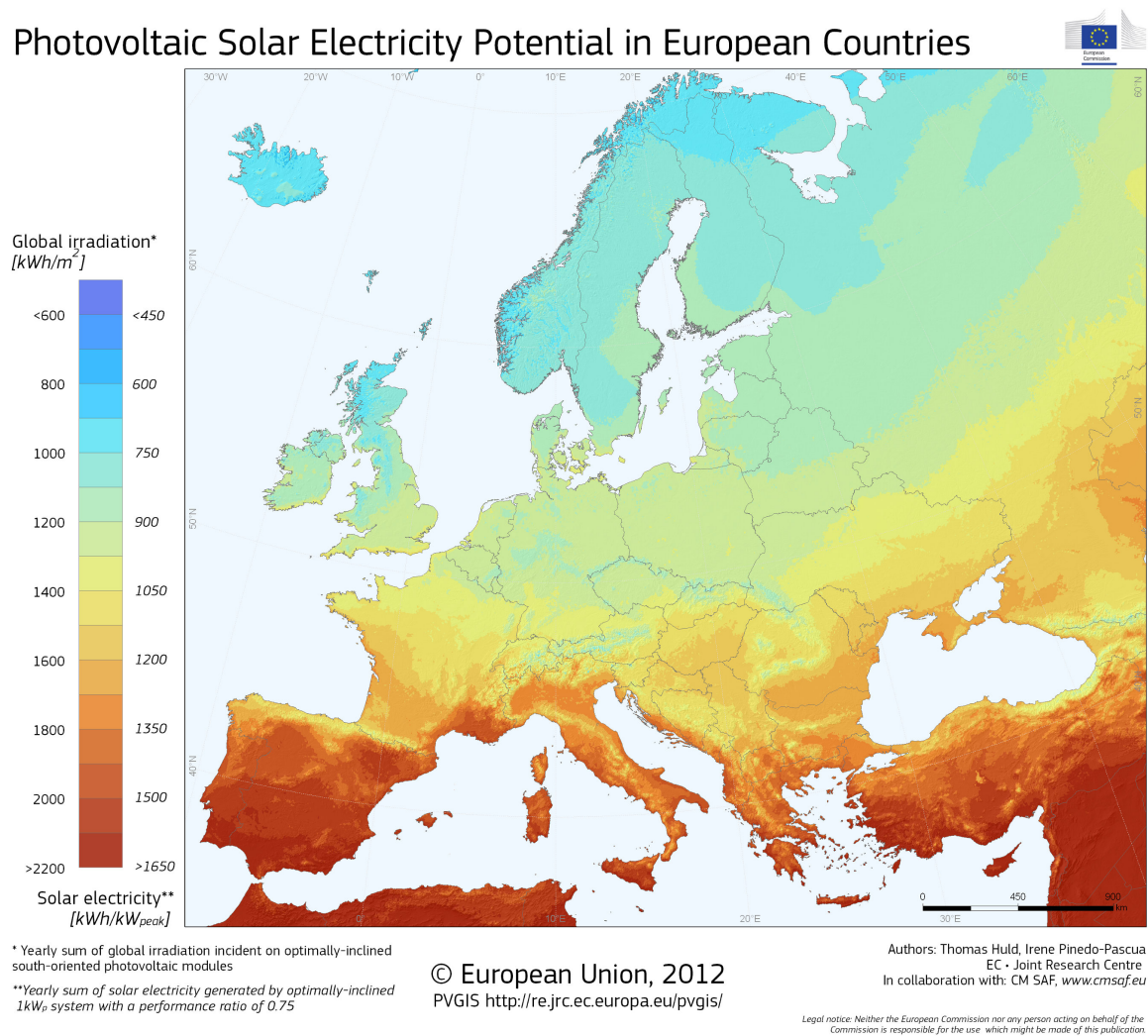
V současné době se jedná pravděpodobně o nejvíce využívanou energii pro výrobu elektrické energie typu Energy harvesting. Využívá se přímé přeměny slunečního záření na elektřinu využitím fotoelektrického jevu. Z přímého slunce je možné získat až  $100 \text{ mW}/\text{cm}^2$ , po zakrytí slunce oblaky  $10 \text{ mW}/\text{cm}^2$  a uvnitř místnosti  $100\text{-}500 \mu\text{W}/\text{cm}^2$ . [23]

#### 2.1.1 Slunce

Slunce je hvězda obíhající kolem středu galaxie Mléčná dráha, a kolem ní obíhá celá sluneční soustava a ve vzdálenosti 8,31 světelných minut i naše planeta Země. Teploty

ve středu Slunce dosahují přibližně 15 710 000 °K, ovšem na povrchu slunce jsou teploty mnohem nižší, přibližně 5 760 °K, což je teplota záření absolutně černého tělesa. Na plochu 1 m<sup>2</sup> ve střední vzdálenosti Země od Slunce dopadá průměrně 1 350 W světelné energie, což je takzvaná sluneční konstanta 1 350 W/m<sup>2</sup>. Tato hodnota se týká měření mimo atmosféru, po průchodu atmosférou se tato hodnota sníží přibližně na 1000 W/m<sup>2</sup>. Dráha Země kolem slunce je eliptická a jedná se pouze o průměrnou hodnotu pro celou planetu Zemi. [23][27]

### Photovoltaic Solar Electricity Potential in European Countries



Obr. 3. Průměrný roční úhrn slunečního záření a roční energetický potenciál na území Evropy [21]

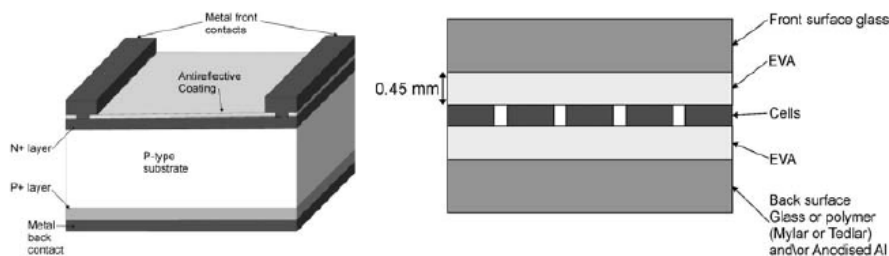
#### 2.1.2 Princip

Při vzájemném působení světla a hmoty dochází k pohlcování fotonů a uvolňování elektronů. Pokud je povrch kovu vystaven světelnému záření, dochází k uvolnění elektronů z jeho povrchu a pokud je energie záření dostatečná, tak elektron vylétne z povrchu a zanechá po sobě kladný náboj, takzvanou díru. Pokud elektron zůstane v kovu, je

přitažen k existující díře a jeho energie se při rekombinaci uvolní ve formě tepla. Jestliže místo kovu bude světelné záření dopadat na polovodičový P-N přechod, pak tento P-N přechod vytvoří bariéru, která znemožní volným elektronům z polovodiče N rekombinovat s dírami v polovodiči typu P. Ve vrstvě N se tak nahromadí volné elektrony, ve vrstvě P díry a P-N přechod znemožní jejich rekombinaci. Nahromaděním volných elektronů vznikne na P-N přechodu napětí o velikosti až 0,6 V, běžně při maximálním výkonu 0,5 V. [23][27]

### 2.1.3 Konstrukce

Křemíkový panel je velmi křehký, proto se vkládá mezi 2 vrstvy skla a případně mezi plastové vrstvy z materiálů jako EVA (Ethylene vinyl acetate).



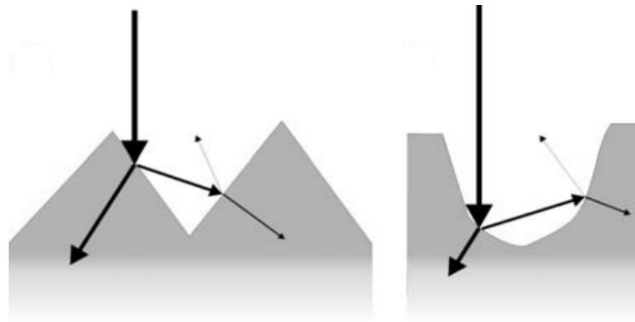
Obr. 4. Typická konstrukce fotovoltaického panelu [23]

Pokud by se vyrobil křemíkový panel tloušťky 10 mm, pak by byl schopný absorbovat 99% energie světelného paprsku délky  $1 \mu\text{m}$ ,  $35 \mu\text{m}$  tlustý panel by je schopný absorbovat pouhé 2 % stejného paprsku. 10 mm silný kus křemíku by byl drahý, proto je nutné zařídit jinými způsoby, aby se délka dráhy paprsku v panelu co nejvíce prodloužila. [23] Z těchto důvodů se na povrch při výrobě umísťují různé vrstvy ovlivňující optické vlastnosti panelů, jako třeba  $\text{TiO}_2$ ,  $\text{SiO}_2$  či  $\text{SiN}_x$  tenká antireflexní vrstva, která zabráňuje odrazům světla z povrchu. Tvar povrchu panelu je rovněž upraven, aby vytvářel světelné pasti různých velikosti, odražený paprsek se tak místo do okolí při odrazu vrací zpátky do panelu. [23]

### 2.1.4 Typy fotovoltaických článků

Výrobně nejdražší typy fotovoltaických panelů jsou **monokrystalické**, ty jsou tvořeny jedním dokonalým krystalem křemíku, který je následně rozřezán na velmi tenké vrstvy. Komerční C-Si panely dosahují účinnost 22,9 %, ovšem typicky se setkáme s 14-17 % účinnosti. [23][27][10]

Výrobně levnější jsou takzvané **polykrystalické** panely složené z většího počtu menších krystalů, což zhoršuje optické i elektrické vlastnosti, mezi jednotlivými krystaly dochází k rekombinaci a i relativně slabé přechody mezi krystaly značně kazí účinnost, poly-



Obr. 5. Světelné pasti na povrchu fotovoltaického panelu [23]

krystalické moduly mC-Si dosahují účinnosti až 15,5%, ovšem běžně dostupné moduly mají účinnost 10-14 %. [23][27][10]

Nejlevnější panely jsou z hydrogenizovaného **amorfního** křemíku (a-Si:H), tedy nejsou tvořeny velkými kusy krystalů, ale využívá se technologie rozkladu křemíku na sloučeniny, ty jsou následně nanášeny na podložky (sklo, plast či kov) a takto nanášený křemík již nemá krystalickou strukturu, nýbrž amorfní strukturu. Tato slaboučká vrstva nanášená na pevném podkladu je relativně odolná, vhodná pro aplikaci v mechanicky namáhaných podmínkách, ovšem mnohem více než u polykrytalických panelů dochází v těchto strukturách k rekombinaci a tedy účinnost je v laboratořích pouhých 12%, v běžně dostupných produktech 5-7 %. Značná výhoda oproti ostatním druhům fotovoltaických panelů je lepší účinnost práce v rozptýleném světle, tedy tento druh panelů se používá v místnostech, známé jsou například z kalkulaček. [23][27][10]

## 2.2 Kinetické zdroje

Jedná se o zdroje energie získané z pohybu, z pohybu lidské bytosti, otřesy výrobních strojů, samotného pohybu dopravních prostředků a nebo vibrací, které dopravní prostředky vyvolávají v okolí. [23]

### 2.2.1 Lidské tělo

Většina pohybů lidského těla je tvořena pohyby s velkou amplitudou a nízkou frekvencí. Kupříkladu chůze osoby s hmotností 68 kg zatěžuje patu boty 67 W energie. Na kotníku 1,7 m vysokého 76 kg vázícího chodce byla naměřena akcelerace přesahující 100 m/s<sup>2</sup> při frekvenci 1,2 Hz. [23]

Již v roce 1770 byl patentován Švýcarským hodinářem Abrahamem-Louis Perreletem mechanický mechanismus, který zajišťoval natahování hodinek pouhým pohybem majitele.

Důležitá je vysoká účinnost použitých generátorů, pokud by z nás získávaly až moc

Tab. 2. Porovnání vlastností vibračních generátorů [2]

Generátor	piezoelektrický	elektrostatický	elektromagnetický
Složitost napájecího procesu	velká	malá	velká
Obvyklá velikost	makro	integrovaný	makro
nevýhody	nízká hodnota proudu vysoký vnitřní odpor při nižších frekvencích	potřeba přídavného zdroje mechanický doraz nedostatečný výkon	nízká hodnota napětí
výhody	velký výkon široké spektrum použití		
frekvence	stovky Hz až řád kHz	řád kHz	desítky až stovky Hz

energie, mohlo by nám to způsobovat potíže při pohybu. Jeden z prototypů batohu využívající rotační generátor z pohybu nositele vygeneroval 7,37 W, ovšem nositele zatížil celými 19,1 W zátěže navíc a způsoboval mu únavu. [23]

### 2.2.2 Výrobní stroje

V průmyslu existuje ohromné množství strojů vytvářející jako vedlejší produkt činnosti vibrace, asi nejsilnější vibrace jsou tvořeny kompresory. Frekvence pohybu kompresoru 50 Hz má asi jasný původ v síťovém napětí. Akcelerace pohybu ve špičce pouhých  $0,25 \text{ m/s}^2$  a amplituda  $2,5 \text{ } \mu\text{m}$  se těžko srovnává s pohybem člověka, tato energie se ale díky pevné a relativně vysoké frekvenci již dá dobře využít. [23]

### 2.2.3 Doprava

Dopravní prostředky jako auta, vlaky, letadla a lodě vytváří ohromné množství vibrací v různých směrech. Generátor umístěný na karoserii vyrobí menší množství energie, než generátor umístěný v kole. Generátor umístěný na karoserii vyrobí více energie při jízdě v pravém pruhu dálnice D1 oproti jízdě například na německých dálnicích. Tyto pohyby nemají stálou frekvenci, ani amplitudu a elektronické obvody, které tuto energii budou využívat s tím musí počítat. [23]

### 2.2.4 Stavby

Na budovy, mosty apod. rovněž působí velké množství malých vibrací a to ze zdrojů jako zemětřesení, metra, vlaků a automobilů, nebo i samotného větru a vibrací od



Obr. 6. Bota vybavená 20 W generátorem energie [11]

Tab. 3. Energie vibrací dle umístění v automobilu

Vůz	Silnice	Umístění senzoru	Maximální akcelerace [m/s <sup>2</sup> ]	Frekvence [Hz]
Luxusní	Dálnice	Kabina	0,05	40
Luxusní	Město	Kabina	0,04	30
Malý	Dálnice	Kabina	0,04	23
Malý	Dálnice	Náprava	2	16

topení či ventilace. Této energie je opravdu málo, v budovách akcelerace dosahuje 0,1 m/s<sup>2</sup> při 10-12,5 Hz. Na 25 m dlouhý most přejetý jedním autem rychlostí 72 km/h působí ve špičkách akcelerace 0,035 m/s<sup>2</sup> při 2 Hz a 5 automobilů akceleraci zvýší až na 0,09 m/s<sup>2</sup>. [23]

### 2.2.5 Elektromagnetické generátory

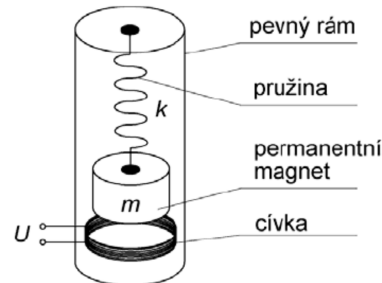
Tento typ generátorů je založen na Faradayově principu elektromagnetické indukce, tedy na vzniku elektrického napětí v uzavřeném obvodu, který je způsoben změnou magnetického indukčního toku. Využívá se tedy cívky a zdroje magnetického pole, například permanentního magnetu a jejich vzájemný pohyb vytváří na cívce elektrické napětí. Napětí  $U$  je možné určit z rovnice

$$U = -N \frac{d\phi}{dt} \quad (1)$$

kde  $\phi$  je magnetický tok,  $N$  je počet závitů cívky.

V rotační variantě tyto generátory známe v různých formách od dynama v bicyklu po obří generátory používané v jaderných elektrárnách. V Energy harvesting aplikacích se

spíše využívají jako zdroje pohybu vibrace, tedy obousměrný pohyb po jedné ose. Cívka je tedy v tomto případě připojena k oscilační hmotě a pohybuje se v magnetickém poli vytvořeném pevným magnetem. [23] [2]

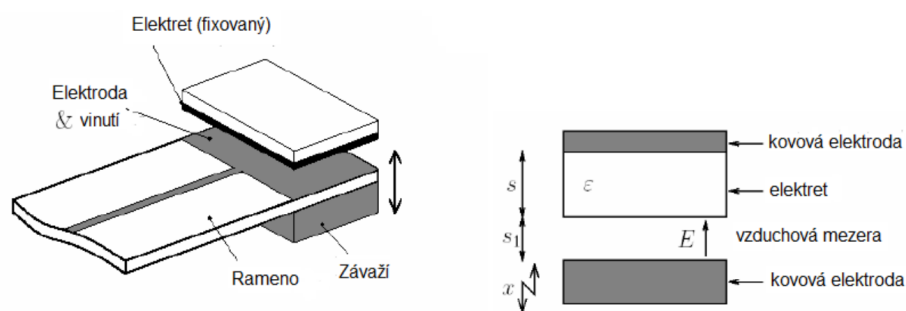


Obr. 7. Lineární elektromagnetický generátor [2]

### 2.2.6 Elektrostatický generátor

Elektrostatický generátor je založen na využití principu proměnného kondenzátoru, jehož 2 desky (elektrody) jsou od sebe izolovány vzduchem, vakuem nebo jiným izolátorem. Působením vibrací se tyto desky od sebe vzdalují a přibližují a tím se mění i jejich kapacita.

K získávání energie je nutné, aby byl tento kondenzátor již nabitý elektrickou energií. To je asi největší problém tohoto zdroje, pokud elektrostatickému generátoru úplně dojde energie, pak již není schopný se spustit. Tento problém se obvykle řeší speciální baterií oddělenou od zbytku obvodu. [23][24][2]



Obr. 8. Elektrostatický generátor [2]

Elektrostatické generátory fungují v režimech s konstantním napětím, nebo nábojem. Generátor s konstantním napětím je obvykle na začátku plně nabitý, při pohybu desek k sobě zůstává napětí dále konstantní, ovšem kapacita se snižuje a tak přebytečný náboj putuje mimo generátor do úložiště energie. Dle rovnice

$$E = \frac{1}{2}(C_{max} - C_{min})U_{max}^2 \quad (2)$$

kde  $E$  je uložená energie (jouly),  $C$  je kapacita a  $U$  napětí.

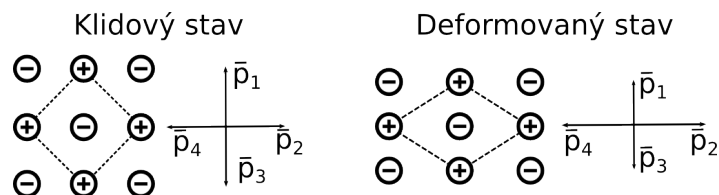
Generátory s konstantním nábojem na elektrodách jsou na začátku plně nabitě, když jsou nejbližší u sebe a proměnná kapacita je v tu chvíli na maximu. Jak se elektrody od sebe vzdalují, kapacita klesá, až je dosaženo  $C_{min}$  a od této chvíle je velikost náboje pevná a roste napětí mezi deskami. [23][24][2]

$$E = \frac{1}{2}(C_{max} - C_{min})U_{max}U_{start} \quad (3)$$

### 2.2.7 Piezoelektrický generátor

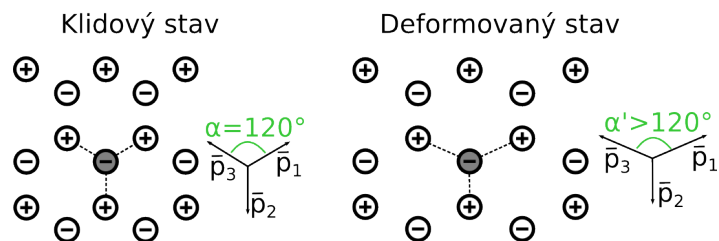
K přeměně mechanické energie na elektrickou se využívá piezoelektrických vlastností vhodných materiálů. Piezoelektrický jev je schopnost krystalu při jeho deformaci generovat elektrické napětí a opačně i deformace krystalu v závislosti na přivedeném napětí.

V piezomateriálu jsou přítomny ionty různých prvků a molekul uspořádány do krystalové mřížky, tak, že si kladné i záporné ionty navzájem prostorově odpovídají a materiál je elektricky neutrální. Pokud je takový materiál mechanicky namáhán, pak se ionty vychýlí ze svých původních pozic a na některých plochách krystalu vznikne elektrický náboj.



Obr. 9. Nepiezoelektrický krystal

Při deformaci nepiezoelektrického krystalu dochází ke zvětšování vektoru dipólu v jedné ose, ovšem ke stejnému úbytku v druhé ose. Tedy celkový součet vektorů  $\vec{p}_1$  až  $\vec{p}_4$  je 0. Zatímco suma vektorů piezoelektrického krystalu (na obrázku znázorněný  $\text{SiO}_2$ ) bude nenulová, tedy nastává polarizace, vzniká piezoelektrický jev a na elektrodách vzniká elektrické napětí. [23][24][2]



Obr. 10. Piezoelektrický krystal

## 2.3 Tepelné zdroje

Tepelná energie je téměř všude od výfuků automobilů, zahřívání elektroniky až třeba po teplo samotného jádra země ve formě Geotermální energie. V případě, že by se dala využít veškerá přebytečná tepelná energie, ušetřila by se ohromné množství fosilních paliv. Jen pro příklad na celé Zemi jsou elektrárny využívající teplo asi o výkonu 10 TW, ovšem tyto elektrárny do prostředí vypouští přibližně 15 TW energie ve formě přebytečného tepla. Další pěkný příklad je motor automobilu, který při výkonu 50 kW, vypouští ve formě tepla do prostředí dalších 35 kW. [23]

Dokonce i teplo lidského těla je možné využít. V době psaní této práce publikoval Korejský výzkumný institut KAIS Termoelektrický generátor určený pro nositelnou elektroniku, který asi z 18 °K rozdílu teplot mezi lidskou kůží a okolním prostředím na ploše 1 dm<sup>2</sup> vygeneroval až 40 mW elektrické energie.

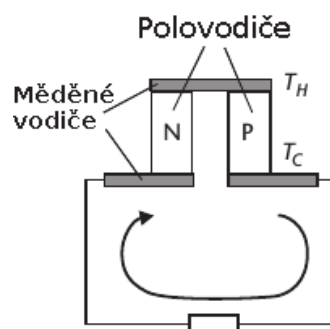
### 2.3.1 Termoelektrický princip

Rozdíl teplot (teplotní gradient) mezi dvěma rozdílnými kovy nebo polovodiči vytváří mezi těmito materiály malý elektrický potenciál. Tomuto efektu se říká Seebeckův jev. Tohoto efektu se používá k přeměně tohoto rozdílu teplot k vytvoření elektrické energie. Seebeckův jev je popsán rovnicí:

$$U = \alpha_{ab}\Delta T \quad (4)$$

kde  $U$  je napětí,  $\Delta T$  je rozdíl teplot povrchu článku a  $\alpha_{ab}$  je Seebeckův koeficient, který je pro většinu materiálů konstantní při různých teplotách.

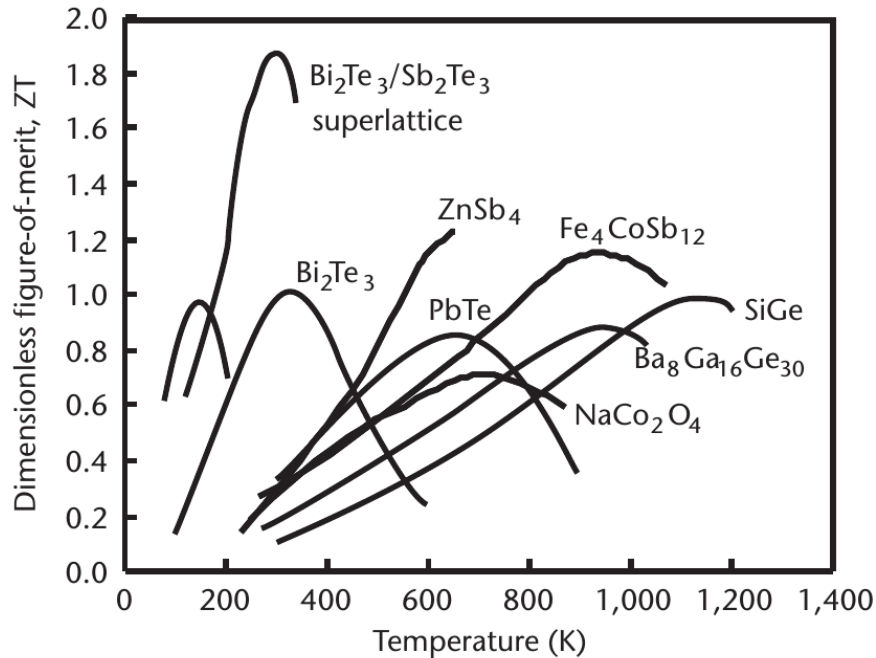
Termoelektrický generátor sestává z polovodiče typu P a polovodiče typu N, spojeného do série (měděnými) vodiči.



Obr. 11. Schéma jednoduchého termoelektrického generátoru [23]

Problémem termoelektrických generátorů je dostupnost potřebných polovodičů. Najít polovodič, který má dostatečnou elektrickou vodivost, seebeckův koeficient a zároveň vysoký rozsah pracovních teplot, je těžko řešitelná. V následujícím grafu je závislost

činitele termoelektrické jakosti ZT na teplotě. Činitel termoelektrické jakosti je závislý na Seebeckově koeficientu, elektrické a tepelné vodivosti. [23]



Obr. 12. Závislost činitele termoelektrické jakosti na teplotě vybraných materiálů [23]

Problémem těchto materiálů je tedy opravdu nízká účinnost a zároveň malé teplotní rozmezí funkce daného materiálu.

### 2.3.2 Pyroelektrický princip

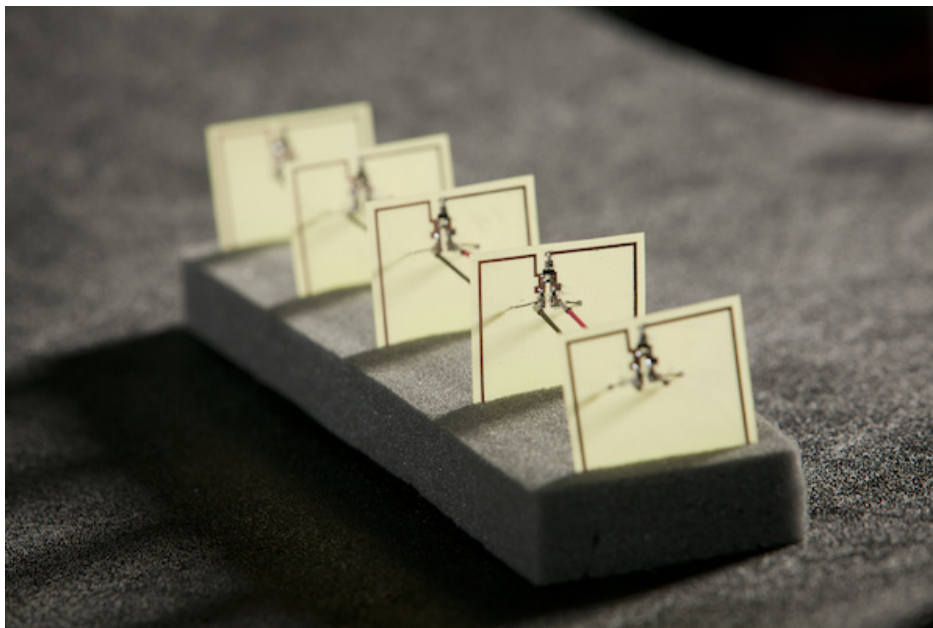
Pyroelektrický jev je schopnost některých látek při ohřívání, nebo ochlazování produkovat elektrické napětí. Tento princip je založen na periodické změně teplot. Ze změny teploty se tímto efektem vytváří i změna napětí. Nevýhodou tohoto principu je tedy potřeba zdroje tepla měnící se s průběhem času. Mezi výhody patří dostupnost materiálů zvládající vysoké teploty až 1200 °C. [23]

## 2.4 Ostatní zdroje

Existují další málo používané zdroje energie. Například z akustického hluku 160 dB byl prototyp generátoru založeného na piezoelektrickém jevu schopen vyrobit 30 mW. Pro elektroniku určenou k umístění uvnitř našeho těla je možné získat energii z cukrů obsažených v krvi.

Poměrně zajímavý zdroj energie, který v poslední době nabývá na popularitě, je rádiové vysílání. Existují drobné antény milimetrových rozměrů využívané v lékařských implantátech. Ty ovšem netěží energii z okolí, ale bývají napájeny čtecím zařízením,

podobně jako se to dělá u technologií RFID. Pak ale existují rozměnější antény určené k získání energie například z GSM vysílání jako například projekt z Duke University. Na této sadě pěti antén rozměru 40x40 mm tvořící tzv. metamateriál. Na tomto metamateriálu naladěném na 900 MHz autoři práce naměřili napětí 7,3 V, účinnost byla 36,8 %. [35]



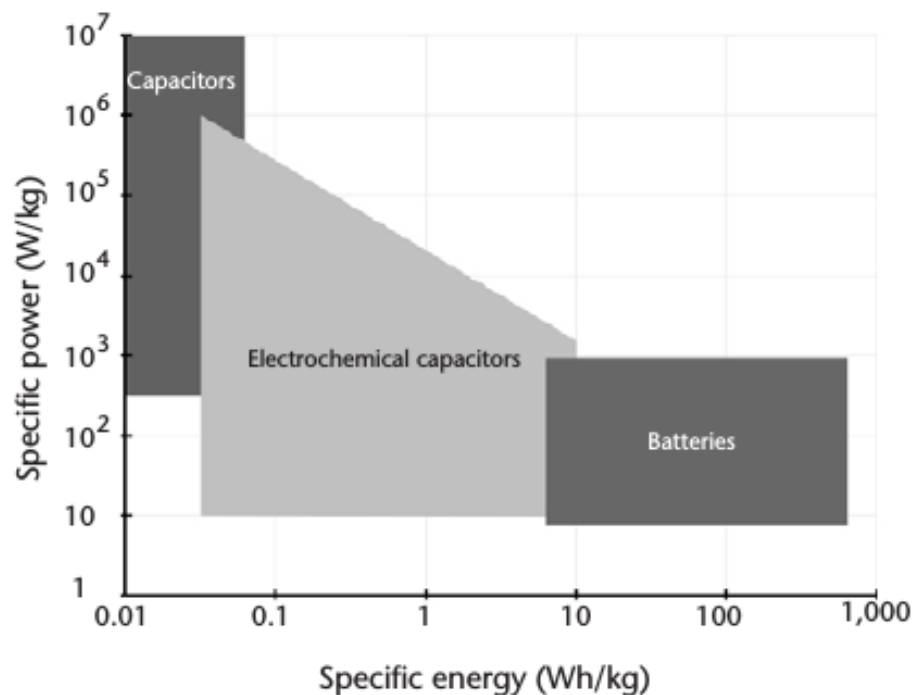
Obr. 13. Metamateriál složený z pěti antén získávající energii z rádiového vysílání [35]

## 2.5 Skladování energie

Množství získávané energie je obvykle příliš moc, nebo málo pro předpokládanou zátěž. Je jí tedy nutné uchovávat v zařízení, které poté tuto energii vydá ve chvíli, kdy je potřeba. Používají se elektrochemické akumulátory využívající chemických reakcí a různých druhů kondenzátorů, které energii ve většině případů nepřeměňují, ale uchovávají ve formě elektrostatického náboje.

## 2.6 Elektrochemický akumulátor

Elektrochemické akumulátory využívají přeměny, při které se jejich chemická energie elektrochemickými reakcemi přeměňuje na energii elektrickou. Tyto změny jsou vratné. Elektrickou energii je tedy možné přeměnit opět na energii chemickou. Schopnost akumulátoru dodat výkon je omezena vnitřním odporem, který se zvyšuje se stářím baterie. Celkově je životnost omezena faktory jako věk, provozní teplota a velikost nabíjecích a vybíjecích proudů.



Obr. 14. Porovnání jednotlivých druhů zařízení určených k uchování elektrické energie [23]

### 2.6.1 Elektrochemické kondenzátory

Elektrochemické kondenzátory též označovaný jako superkondenzátory, ultrakondenzátory případně dle konstrukce dvouvrstvé kondenzátory jsou elektrotechnické součástky schopné uchovat velké množství elektrické energie ve formě elektrického náboje. Na rozdíl od baterií mají velmi nízký vnitřní odpor, jsou tedy schopny se velmi rychle a téměř bez ztrát energie nabít i velmi rychle energii předat potřebnému elektrickému obvodu. V poslední době kapacity elektrochemických kondenzátorů dosáhly až tak vysokých hodnot, že už se tyto začínají používat třeba i v záložních zdrojích datacenter k pokrytí velkých výkyvů energie. Ovšem i tak se používají v kombinaci s elektrocentrálami a akumulátory, jelikož kapacita je sice vysoká oproti běžným kondenzátorům, tedy až tisíce Faradů, ovšem při srovnání například s lithiovým akumulátorem je hustota uložené energie stále téměř o řád nižší.

**Elektrochemické dvouvrstvé kondenzátory (EDLC)** Tento typ využívá principu elektrochemické dvojvrstvy. Dvouvrstva má tloušťku řádově 10<sup>-10</sup> m, skládá se ze dvou opačně nabitých elektrod, na jejichž povrch jsou vázány ionty opačného náboje. Elektrody jsou hliníkové fólie s vrstvou aktivního uhlíku a plochou přibližně 2000 m<sup>2</sup>/g, od sebe jsou odděleny polypropylénovým separátorem a prostor mezi nimi vyplňuje elektrolyt.

Tab. 4. Srovnání nejpožívanějších typů průmyslových baterií [15]

Typ Článku	Ni-Cd	Ni-MH	Li-ion	Olověný AGM
Hustota energie (Wh/kg)	45-80	60-120	90-120	30-50
Počet cyklů (při 80% vybití)	1500	300-500	>1500	400-500
Projektovaná životnost [roky]	5+	3-4	10+	10+
Doba nabíjení [h]	1-2	2-4	0,5-4	8-16
Samovybíjení/měsíc (při cca 20 °C) [%]	20	30	5-10	5
Nominální napětí článku [V]	1,2	1,2	3,7	2
Proudová zatížitelnost [C]				
špička	20	5	25	5
optimální	1	0,5	5	0,5
Provozní teploty (pro vybíjení) [°C]	-40-60	-20-60	-20-60	-20-60
Požadavky na servis [dnů]	30-60	60-90	180	180
Přibližné náklady [Kč/Wh]	8,25	16,25	8,25	2,75

Tento typ tedy nevyužívá žádných chemických reakcí, čím je zajištěna dlouhá životnost a možnost velmi rychlého nabíjení a vybíjení.

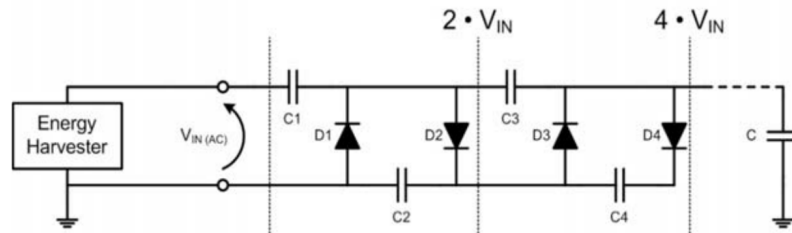
**Pseudokondenzátory** jsou založeny na změně složení povrchu elektrody, tedy na chemických reakcích. Jedna elektroda je z uhlíkového materiálu, druhá obsahuje obvykle Oxid rutheničitý  $RuO_2$ . Oxid rutheničitý je schopen přijímat a následně vydávat vodíkové ionty. V tomto typu elektrochemického kondenzátoru dochází kromě přenosu náboje mezi elektrolytem a elektrodou i k chemickým reakcím. Oproti elektrochemickým dvouvrstvým kondenzátorům má tento typ větší kapacitu. Na druhou stranu v něm probíhající chemické reakce způsobují pomalejší nabíjení a vybíjení a dochází ke stárnutí elektrod a má tedy nižší životnost. [23][16]

## 2.7 Obvody managementu napájení

Uvedené zdroje energií tuto energii dodávají obvykle nárazově, v různě nízkých či vysokých napětích. Energie je ve formě, která není použitelná pro další elektrické obvody bezdrátového senzoru (zátěž). Z toho důvodu je potřeba využít elektrický obvod, který zařídí potřebné úpravy. Takový obvod managementu napájení (PMIC power management Integrated circuit) se skládá z DC/DC měniče s optimalizovaným rozhraním k vnějšímu zdroji okolní energie (úprava vstupní impedance), obvodu managementu baterie, výstupního regulátoru a pokud je potřeba, pak i jednotky studeného startu. [23][10]

### 2.7.1 Násobič napětí

K vytvoření násobiče pro střídavý proud se používá často Villardův nebo Dicksonův kaskádní násobič. Jedná se o kombinaci diod a kondenzátorů. Těmto konstrukcím se říká nábojová pumpa a umožňují velice jednoduše kaskádově zvyšovat napětí pouhým přidáváním dalších stupňů.



Obr. 15. Villardův násobič [23]

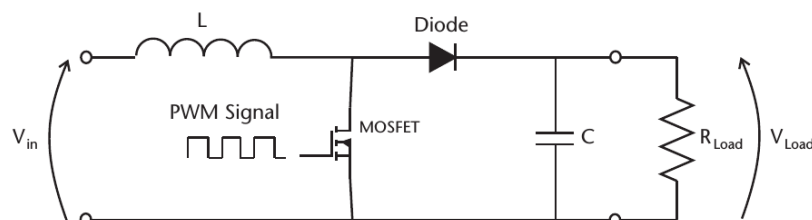
Princip funkce:

1. negativní půlvlna: je nabit kondenzátor  $C_1$
2. kladná půlvlna: je nabíjen kondenzátor  $C_2$  jednak z přímo ze zdroje, ale skrz diodu  $D_2$  i z kondenzátoru  $C_1$ , tedy na kondenzátoru  $C_2$  je v tuto chvíli dvojnásobné napětí oproti vstupnímu napětí  $V_{IN}$
3. kladná půlvlna: napětí na  $C_1$  je klesne na 0 V, což umožňuje nabití  $C_3$  diodou  $D_3$  na dvojnásobek  $V_{IN}$ .
4. záporná půlvlna: napětí na  $C_1, C_2$  je na dvojnásobku  $V_{IN}$ , stejně jako v 2. kroku, ale  $C_3$  a  $C_4$  je již nabíjí ze součtu napětí na  $C_1$  a  $C_2$ , tedy na čtyřnásobek  $V_{IN}$ .

[32] [23]

### 2.7.2 Zvyšující DC-DC měnič

Ke změně velikosti stejnosměrného napětí, případně usměrněného střídavého napětí se využívají měniče, vyžadujícího ke své funkci řídicího prvku a cívky.



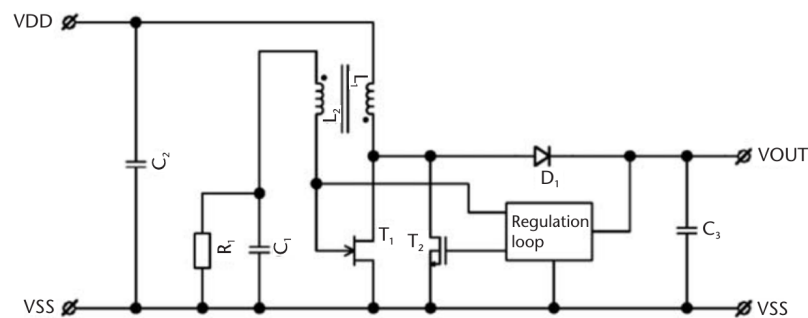
Obr. 16. DC-DC měnič [23]

Princip: Dokud je MOSFET tranzistor v sepnutém stavu, tak prochází proud cívkou a ta akumuluje energii. Jakmile je tranzistor rozpojen řídicím obvodem, tak energie naakumulovaná v cívce působí jako další zdroj, jehož napětí se přičte ke vstupnímu napětí  $V_{IN}$  a kondenzátor se přes diodu nabíjí na toto vyšší napětí. Jakmile se tranzistor opět sepne, kondenzátor pokračuje v předávání energie do zátěže, zatímco se cívka opět nabíjí. [32] [23]

### 2.7.3 MPPT (Maximum power point tracking)

K efektivnímu využití energie z fotovoltaických panelů a termoelektrických generátorů se používají obvody typu MPPT, které trvale vyhodnocují stav zdroje energie a tomu přizpůsobují parametry čerpání této energie. Jejich princip vychází ze zvyšujícího DC-DC měniče.

MPPT je vysokofrekvenční DC/DC měnič. Stejnoseměrný vstup ze zdroje energie jako fotovoltaický panel, mění na vysokofrekvenční AC a poté mění zpět na DC s velikostí napětí a proudu, které vyhovuje zdroji i zátěži. MPPT obvykle pracují na frekvencích přibližně v rozmezí 20-80 kHz. Hlavní výhody plynoucí z využití takto vysokých frekvencí je možnost využít vysoce účinných transformátorů při zachování jejich malých rozměrů a malých rozměrů i ostatních komponent. Využití těchto frekvencí na druhou stranu může způsobovat problémy s rušením okolní elektroniky. [23] [31]



Obr. 17. Nízkonapěťový DC-DC měnič určený pro fotovoltaický panel [23]

### 3 MIKROKONTROLÉR

Mikroprocesor je složitý logický obvod schopný vykonávat daný program. Jedná se pouze o aritmeticko-logickou jednotku. K vykonávání programu je potřeba být vybaven nějakým druhem pamětí, ten může být k mikroprocesoru připojen ve formě externí součástky, jako se to běžně dělá s operační pamětí v počítačích.

Pro potřeby bezdrátových snímačů je vhodné využít jednočipový mikropočítač, v anglické literatuře nazývaný “microcontroller” a zkratkami MCU,  $\mu C$ . Tento integrovaný obvod v jednom pouzdře obsahuje operační paměť (RAM), paměť k uložení programu a dat (FLASH) a je rovněž vybaven různými rozhraními pro komunikaci s okolím a periferiemi jako čítače, časovače, nebo třeba digitálně-analogové převodníky. [18] [21]

## 4 KRYPTOGRAFIE

Kryptografie je nauka o transformacích otevřeného textu na šifrovaný a naopak. Tedy způsoby jak utajit smysl zprávy, aby byly čitelné pouze se speciální znalostí.

### 4.1 Moderní kryptografie

Historie kryptografie sahá daleko do minulosti, první známé šifry spadají do období 500 let před naším letopočtem. Klasická kryptografie využívala šifer, které bylo možné efektivně luštit s použitím jednoduchých pomůcek. Nejnáročnější operace potřebná pro prolomení takové šifry kryptoanalytikem bylo zjistit typ šifry, délku klíče a až poté určení samotného klíče.

Roku 1948 Claude Elwood Shannon ve svém díle *A Mathematical Theory of Communication* mimo vytvoření základu teorie informace i navíc definoval, že: “Síla algoritmu spočívá na pilířích matematické složitosti a ne na tajnostech kolem něj.” [25]

### 4.2 Symetrická kryptografie

V symetrickém typu kryptografie se obě strany dohodnou na stejném tajném klíči (sdílené tajemství), stejný klíč je tedy využíván k šifrování i dešifrování zprávy. [25]

#### 4.2.1 Proudové šifry

Zpracovávají otevřený text po jednotlivých znacích, obvykle je z klíče generován takzvaný keystream. Jedná se o pseudonáhodnou sekvenci znaků. Otevřený text je kombinován operací XOR s keystreamem a tím vzniká šifrovaný text. K dešifrování opět stačí vygenerovat stejný keystream a ten operací XOR zkombinovat šifrovaný text, vznikne tím opět otevřený text. Takto funguje například algoritmus RC4. [25]

#### 4.2.2 Blokované šifry

Zpracovávají otevřený text po blocích dané délky, konec textu je do dané délky doplněn vhodným způsobem většinou takzvanou vycpávkou. Oproti proudovým šifrám díky pevné délce bloku je tak možné měnit pořadí znaků.

Historicky a bohužel velice často i dnes používaná šifra je DES. Jedná se o šifru pracující s bloky dat o velikosti 64 bitů, tedy 8 bajtů. Délka klíče je 56 bitů, bývá uváděn jako 64bitů, ovšem posledních 8 bitů se využívá jako kontrolní součet, nebo jsou prostě ignorovány. Samotný algoritmus je složen z řady substitucí tzv. S-boxy a permutací P-boxy. Jelikož je 56bitový klíč na dnešní dobu opravdu slabý, ale spousta obvodů je stále vybavena hardwarovými jednotkami akcelerující výpočet DES, byl vytvořen

TripleDES, což je vlastně pouze zavolání DES algoritmu 3x po sobě na stejná data vždy s jiným klíčem. Klíč se tak ztrojnásobil a má délku  $3 \times 56 = 168$  bitů.

Aktuálně nejpoužívanější algoritmus je AES, existuje ve variantách AES-128, AES-192 a AES-256, číslo značí délku bloku v bitech, AES-128 tedy pracuje s 16 bytovými bloky. [25]

### 4.3 Asymetrická kryptografie

Narozdíl od symetrické kryptografie nevyužívá pouze jeden klíč, ale používá klíčový pár. Jeden klíč je soukromý a tedy bezpečně uchován pouze u majitele a druhý klíč je veřejný, který může vidět kdokoliv, ovšem je nutné zajistit, aby nebyl během šíření nahrazen cizím klíčem, což zajišťují různé mechanismy využívající například Certifikační Autority. Klíče mezi sebou mají jistý matematický druh závislosti. Co jde jedním libovolným klíčem zašifrovat, to jde druhým klíčem z daného páru dešifrovat. Takto je možné zašifrovat data veřejným klíčem a mít zároveň jistotu, že je dešifruje pouze držitel privátního klíče a nikdo jiný. Případně lze digitálně podepsat dokument soukromým klíčem a na druhé straně tento dokument ověřit veřejným klíčem. Tento princip používají algoritmy RSA a DSA.

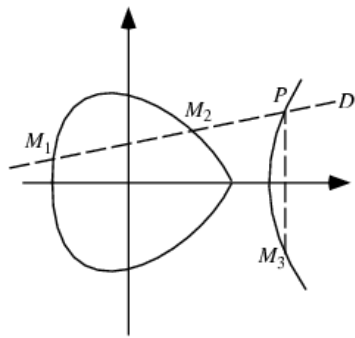
K šíření klíče dvěma stranám, které se v životě nepotkaly se používá Asymetrického algoritmu Diffie-Hellman. Opět se jedná o vytvoření soukromých klíčů na obou stranách, a využití dvou veřejných klíčů. Ty ovšem tentokrát mají trochu jiný druh závislosti. Privátní klíče jsou použity jako exponenty v jednoduchém vzorci používající oba veřejné klíče, oběma stranám jsou známy oba veřejné klíče a výsledek výpočtu zahrnující tajný klíč, z toho je spočítán nový klíč, který je znám pouze těmto dvěma stranám.

Asymetrická kryptografie je opravdu náročná na hardwarové nároky a proto se běžně používá hlavně při bezpečné distribuci symetrického klíče používaného k šifrování větších objemů dat. Velký problém je rovněž minimální délka klíče, zatímco u symetrických šifer stačí a ještě dlouho bude stačit 128bitové klíče, u asi nejrozšířenější asymetrické šifry RSA se dnes mluví o minimálně 8192 b klíči. [25]

### 4.4 Algoritmy nad Eliptickými křivkami

Jedním z řešení délky klíčů algoritmů jako RSA je ECC (Elliptic Curve Cryptography). Jedná se vlastně o geometrické výpočty nad křivkami dané rovnicí  $y^2 = x^3 + ax + b$ , podobně jako se v RSA provádí násobení prvočísel, v obrázku 18 se například proloží bod M1 a M2 přímkou a vznikne bod P. Z bodu P není zpětně možné získat body M1 nebo M2. Samozřejmě pro kryptografii není možné využívat výpočty v reálných číslech, používají se konečná tělesa typu  $F_q$ , kde  $q$  je prvočíslo, případně  $F_{2^m}$ , kde  $m$  je celé číslo. Provádí se tedy celočíselné výpočty řešené tabulkami operací.

Do eliptických křivek je upraven algoritmus určený pro digitální podpisy DSA na



Obr. 18. Eliptické křivky [36]

ECDSA, existuje varianta Diffie-Hellman - ECDH a k běžnému šifrování se používá ECIES. [37][19][28]

Tab. 5. Srovnání srovnatelných délek klíčů v kryptografii [37]

Symetrická kryptografie	RSA a Diffie-Hellman Key	Eliptické křivky
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

## II. PRAKTICKÁ ČÁST

Cílem praktické části práce bylo vytvořit ve formě prototypů platformu pro bezdrátové snímače napájené technikou Energy Harvesting a následně v ní některé snímače vyzkoušet.

Platforma se skládá ze dvou stran, které spolu přímo komunikují. Strana vybavená snímači, napájená metodou Energy Harvesting, a na druhé straně přijímací stanice, trvale napájená a vybavena rozhraním, které přijaté údaje předává dále do počítačové sítě.

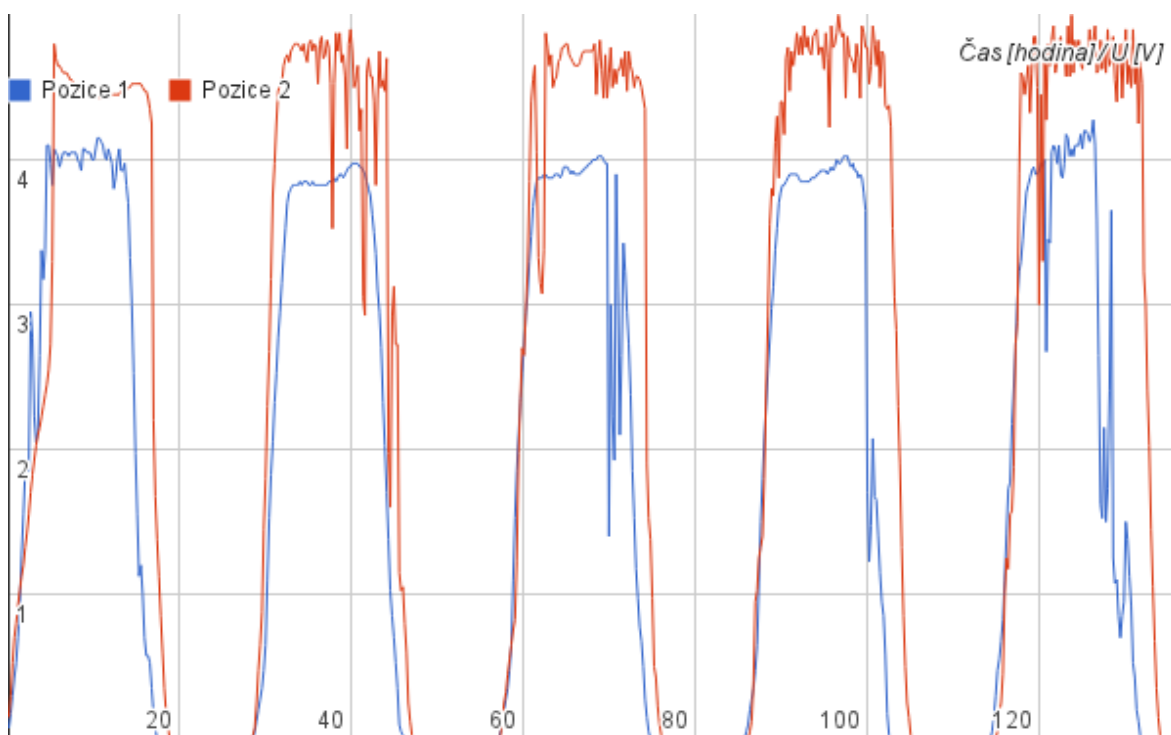
## 5 KOMPONENTY PLATFORMY

### 5.1 Zdroj energie

Plánované umístění bezdrátových snímačů je venku, ne nutně na přímém slunci. Z důvodu nepřítomnosti zdroje vibrací či dostatečného tepelného přechodu, bylo pro účely této práce jako zdroj energie zvoleno sluneční záření. Dle tabulky 1 v teoretické části je fotovoltaický panel schopný dodávat  $100 \text{ mW/cm}^2$ .

První pokusy vedly k využití fotovoltaického panelu získaného z nefunkční elektroniky. Jednalo se o polykrystalický panel (druh panelu byl orientačně určen dle typického vzhledu), přesněji panel o napětí 5V. Jednalo se tedy o 10 sériově zapojených 0,5 V článků.

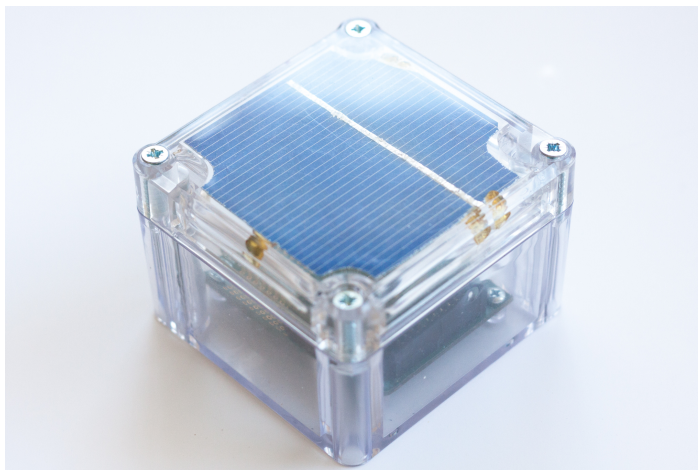
Pro určení světelných podmínek byl postaven velmi jednoduchý záznamník napětí realizovaný modulem Arduino Pro Mini. K měření napětí byl použit vestavěný AD převodník a jako úložiště dat byla použita vnitřní eeprom paměť. Počet měření byl tedy omezen kapacitou eeprom paměti. K měřením docházelo každých 6 sekund, po zaplnění 128 B paměti byl proveden výpočet mediánu a uložena hodnota do eeprom. Tento záznamník byl vodotěsně uzavřen do sklenice a umístěn na střechu domu na dvě testovací pozice na severní a jižní straně. Ovšem v obou případech směřující k jihu. Z výsledků mých měření je vidět velká strmost náběhu a sestupu naměřeného napětí.



Obr. 19. Záznam napětí na fotovoltaickém panelu v čase

Další pokusy již probíhaly s jediným fotovoltaickým článkem parametrů 4 W, 0,5 V rozměrů 6x6 palců, tedy 157x157 mm a tloušťky panelu pouhých 0,3 mm určené k za-

budování do vlastního pole fotovoltaických panelů. Dle vzhledu se může jednat o monokrystalický panel, to ovšem prodejce nespécifikoval. Jedná se o pouhý fotovoltaický článek, bez ochranné vrstvy. Jsou to vlastně dva velmi tenké kusy skla s ještě tenčím polovodičem umístěným uprostřed. Pro použití ve vybrané krabici byl tento článek zmenšen na rozměry přibližně 70x70 mm.



Obr. 20. Platforma bezdrátového snímače v krabici s fotovoltaickým článkem

## 5.2 Management napájení

Jako zdroj energie byl vybrán jeden fotovoltaický článek. Jedná se tedy o zdroj energie dostupný v našich podmínkách pouze ve dne. Tuto energii bylo třeba řádně využít, přeměnit do podoby použitelné zátěží a využít i poslední sluneční paprsek.

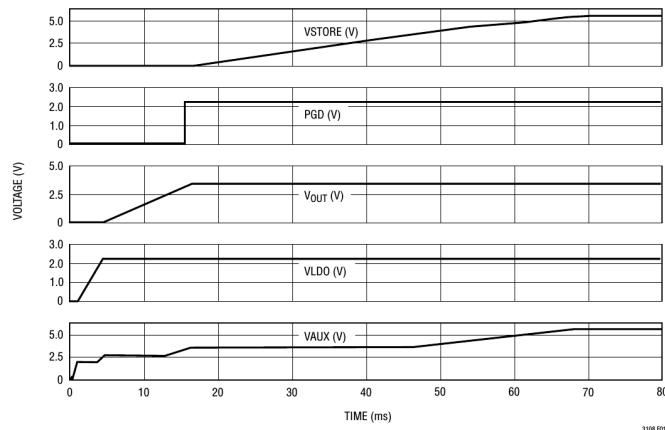
První pokusy vedly k využití DC/DC měničů, obvod firmy Mikrochip MCP1640 je dle datasheetu schopný fungovat již od 0,35 V. Bohužel v reálném nasazení tento obvod zapojený za fotovoltaický článek fungoval v horších světelných podmínkách velice špatně. Další pokusy probíhaly s integrovaným obvodem od firmy Linear Technology s označením LTC3108. Rozdíl od předchozího pokusu je, že se jedná o kompletní obvod managementu napájení určený přesně k využití v oblasti Energy Harvesting.

### 5.2.1 Linear Technology LTC3108

LTC3108 je integrovaný obvod zajišťující kompletní Energy Harvesting Power Management. Obsahuje DC/DC měnič schopný fungovat od napětí pouhých 20 mV a je tedy ideální pro použití v kombinaci s termoelektrickými nebo fotovoltaickými články, tedy se zdroji energie se stejnosměrným výstupem o nízkém napětí. Největší omezení tohoto obvodu je schopnost dodávat pouze opravdu malý proud, typicky 4,5 mA, maximálně 7 mA. Obvody připojené jako zátěž tedy často musí počítat k pokrytí krátkodobých větších odběrů i s energií uloženou v kondenzátorech.



LTC3108 zajišťuje kompletní napájení bezdrátového senzoru, výstupní napětí na výstupu  $V_{OUT}$  je možné volit z možností 2,35 V, 3,3 V, 4,1 V a 5 V. Dále obsahuje výstup  $V_{LDO}$  s konstantním napětím 2,2 V určený k napájení mikrokontroléru. Na tomto výstupu se objeví napětí vždy jako první, dříve než na  $V_{OUT}$ , tedy procesor je funkční z celého senzoru vždy jako první aby mohl ostatní obvody přepnout do úsporných režimů a nastavit do stavu, ve kterých mají minimální odběr.

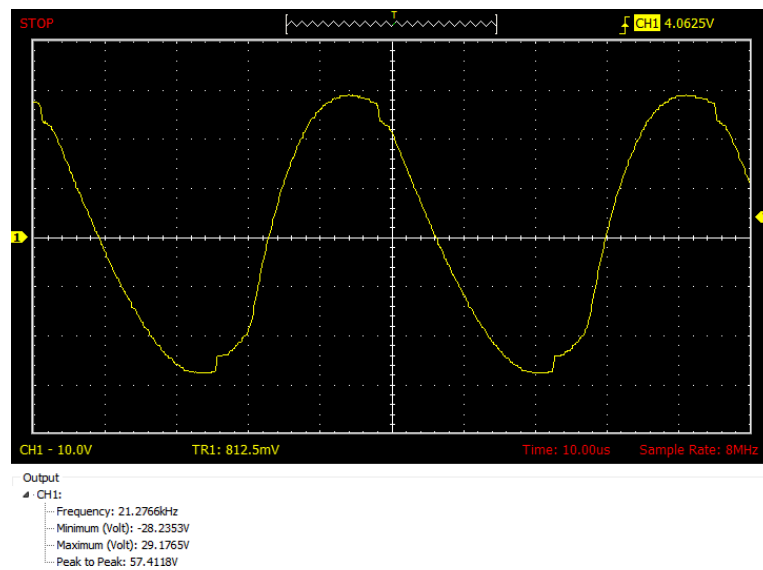


Obr. 23. Napěťové úrovně výstupů LTC3108 po zapnutí [14]

Dále obsahuje výstup  $V_{OUT2}$ , na kterém je stejné napětí jako na  $V_{OUT}$ , ale tento výstup je možné zapínat a vypínat vstupem  $V_{OUT2\_EN}$ . Tento výstup  $V_{OUT2}$  je tedy plně pod kontrolou mikrokontroléru.

Jakmile obvod téměř dosáhne potřebného napětí na  $V_{OUT}$ , přesněji je pouhých 7,5 % pod stanoveným napětím, objeví se na digitálním výstupu PGOOD logická 1, tedy je mikrokontroléru indikováno dostatečné napětí, pokud napětí poklesne o více než 9 %, tedy pod 81 % stanoveného napětí, pak PGOOD indikuje nízké napětí logickou nulou. Přebytkovou energii je možné ukládat do velkých elektrochemických kondenzátorů, případně výrobce uvádí i možnost skladovat energii v akumulátorech připojených k  $V_{STORE}$  a využívat ve chvíli, kdy je vyprodukované energie nedostatek, popř. k pokrytí špičkových odběrů. Maximální napětí na  $V_{STORE}$  dosahuje 5 V, ale maximální dodaný proud je v jednotkách mA. Je tedy určený spíše pro odolnější NiCd a NiMh akumulátory, kterým přebíjení tak nízkým proudem nijak neublíží. LTC3108 neobsahuje žádnou detekci konce nabíjení, která se používá při dobíjení například Li-Ion článků. Využit k napájení akumulátor bez dalšího managementu napájení akumulátoru tedy nepovažuji za příliš vhodné.

**Princip funkce** LTC3108 ke své funkci DC/DC měniče využívá zvenku připojený drobný transformátor a několik kondenzátorů. Následující odhad způsobu fungování samotné části DC/DC měniče byl určen dle blokového schéma, popisu v datasheetu



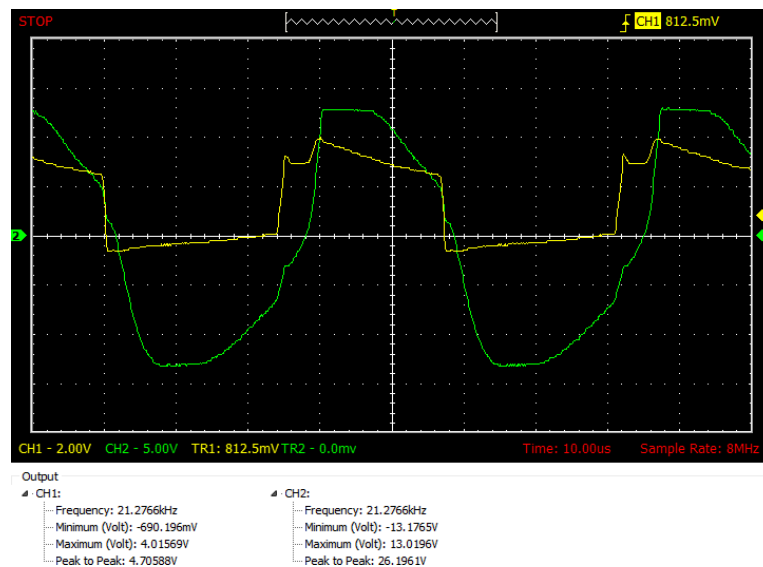
Obr. 24. Měření napětí na výstupu ze sekundárního vinutí.

[14] a výsledků měření osciloskopem (Hantek 6022BE).

Sekundární cívka, kondenzátor C2 připojený na C2 a vnitřní rezistor spolu tvoří rezonanční RLC obvod. Ten svou funkcí vytváří spínací frekvenci, která je v tomto případě ovlivňována i vlivem primárního vinutí.

Spínací frekvence z RLC je přivedena na tranzistor typu MOSFET, který dle ní uzemňuje primární vinutí transformátoru. Pokud je vinutí uzemněno, pak se primární vinutí začne nabíjet a akumuluje se v něm energie. V tu chvíli je na sekundárním vinutí záporné napětí, které ovšem diody dále nepropustí. Jakmile je MOSFET rozpojen, začne se vybíjet energie v primárním vedení a na sekundárním vedení se objeví kladné napětí patřičně zesíleno poměrem mezi počtem závitů primárního a sekundárního vedení. Během provedených měření se toto napětí ukázalo jako poměrně vysoké, na sekundárním vinutí bylo naměřeno střídavé napětí špička-špička 57,4 V. Tato hodnota přibližně odpovídá stonásobnému zesílení napětí na fotovoltaickém článku.

MOSFET v kombinaci s transformátorem kondenzátorem a frekvencí udávanou rezonančním RLC obvodem tedy tvoří DC/DC měnič násobící vstupní napětí poměrem počtu závitů primárního vinutí vůči počtu závitů na sekundárním vinutí transformátoru. Výstup tohoto měniče je přiveden kondenzátorem na vstup C1, za tímto vstupem je uvnitř obvodu soustava diod, které mění toto střídavé napětí na stejnosměrné o velikosti přibližně 2,5 V jak je vidět na kanálu 1 obrázku 25 a provádí násobení tohoto napětí. Výsledek usměrnění a násobení je přiveden na VAUX, jehož napětí dosahuje maximálně 5,25 V a z něj je napájen zbytek obvodu. Po snížení napětí VAUX stabilizátory jsou tyto napětí přivedena na výstupy  $V_{OUT}$ ,  $V_{OUT2}$  a  $V_{LDO}$  k napájení dalších obvodů, tedy zátěže.



Obr. 25. Měření napětí na vstupech CH1 (žlutý) - C1 a CH2 (zelený) - C2

### 5.3 Skladování energie

K uchování energie bylo na výběr dle obvodu LTC3108 využít elektrochemické kondenzátory, nebo NiMh/NiCd baterie. Účelem této práce byla tvorba bezúdržbového zařízení, z toho důvodu byly tedy zvoleny elektrochemické dvouvrstvé kondenzátory, které mají obvykle udávanou životnost 100 000 cyklů, tedy i při každodenním vybití by to mohlo vystačit na 3 lidské životy.

Bylo nutné sehnat velké elektrochemické kondenzátory s nízkou hodnotou ESR, tedy nízkým vnitřním odporem. Bohužel nabídka evropských prodejců elektronických součástek jako Farnell, nebo české GM Electronic byla velmi omezená a větší kapacity jako například 4 F od nich není možné koupit ani dnes.

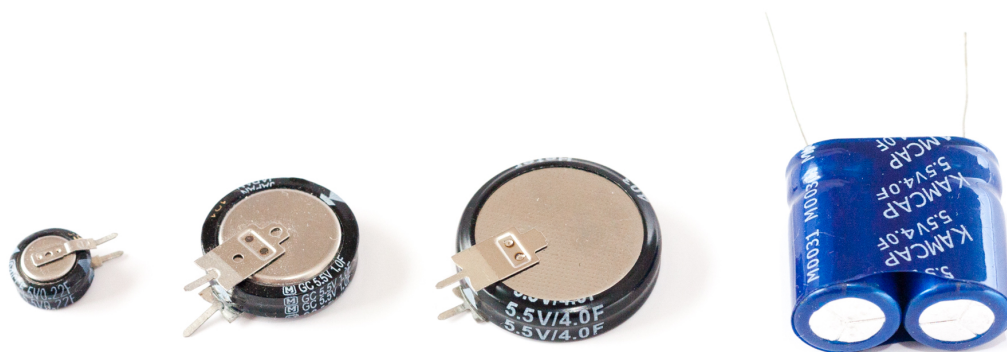
Přes ebay byly získány elektrochemické dvouvrstvé kondenzátory od firmy Panasonic. Tyto kondenzátory jsou primárně určené k zálohování paměti v elektronice, pokud se vybití hlavní zdroj energie. Jedná se o:

- 0,22 F Panasonic EECSOHD224V 5,5 V, vnitřní odpor < 30  $\Omega$
- 1 F Panasonic EECS5R5V105 5,5 V, vnitřní odpor < 30  $\Omega$

Od jiných firem byly získány dva modely s udanou kapacitou 4 F

- 4 F Heter SC5R5405Z-V 5,5 V, < 16  $\Omega$
- 4 F KAMCAP SP-Z 5,5 V

Kamcap jako jediný není knoflíkové konstrukce. Jedná se o sériově zapojenou dvojici kondenzátorů. Z rovnic používaných k výpočtům sériového zapojení kondenzátorů vyplývá, že se jedná o dvojici 8 F kondenzátorů s napětím a minimálně 2,75 V.



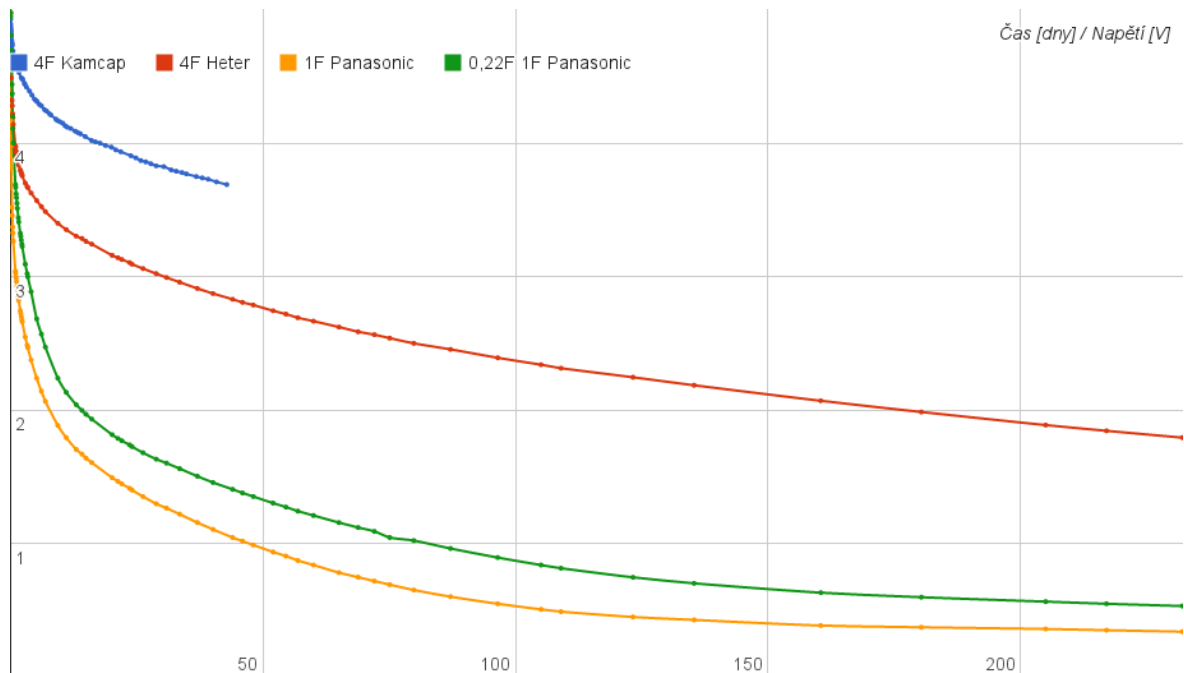
Obr. 26. Kondenzátory: zleva Panasonic 0,22 F, Panasonic 1 F, Heter 4 F a KAMCAP 4 F

Jelikož původ některých kondenzátorů nebyl zrovna důvěryhodný, otestoval jsem na nich s využitím dlouhodobého měření jejich schopnost udržet náboj dlouhou dobu. To ovlivňuje jejich vnitřní odpor. Kondenzátory zůstaly nezapojené, pouze v průběhu času byl vždy připojen voltmetr a byla zapsána naměřená hodnota. První 3 kondenzátory byly měřeny ve stejnou chvíli, v době psaní práce již měření trvalo více, jak 200 dní. 4 F KAMCAP byl získán teprve nedávno, proto jsou dostupná data přibližně z jednoho měsíce. Ovšem i tak je vidět jasný trend a prokazuje své kvality. K měření byl využíván multimetr VICTOR 81D SN:993576617 s udávanou chybou měření 0,5 %.

Z naměřeného grafu jde vyčíst výborné vlastnosti všech kondenzátorů, pokles napětí způsobený samovybíjením je velmi malý. Z měření se prokázalo, že volba většího kondenzátoru není chyba, mé původní obavy se týkaly většího vnitřního odporu u větších kapacit, což se naštěstí vyvrátilo. Jediný problém, který může způsobit větší kapacita je tak delší doba prvotního nabíjení. To může být řešitelné prvním nabitím například programátorem při instalaci. Ovšem ani to není zcela nutné, obvod LTC3108 v první řadě začne napájet zátěž a až z přebytku energie nabíjí úložiště energie, tedy v tomto případě kondenzátor. Jediný problém, který by mohl nastat je, že těsně po instalaci nebude odkud brát větší špičkové odběry proudu, které nepokryjí drobné kondenzátory a bylo by je nutné pokrývat z tohoto elektrochemického kondenzátoru.

#### 5.4 Mikrokontrolér

Při výběru mikrokontroléru bylo sice důležité volit dle spotřeby elektrické energie, ovšem důležité se ukázaly být i jiné parametry jako např. dostupnost vývojových



Obr. 27. Samovybíjení zvolených kondenzátorů

prostředí, programátorů, komunitní podpora a zkušenosti autora práce.

Moderní mikrokontroléry využívají k úspoře energie různé techniky. Dle [12] je možné nejnázne snížit spotřebu elektrické energie pouhým snížením pracovního napětí a frekvence. Spotřeba energie v integrovaných obvodech roste lineárně se stoupající frekvencí a s rostoucím napětím exponenciálně. Další způsoby úspory energie spočívají ve vypnutí celých částí MCU.

Mikrokontroléry obvykle mají několik režimů s velmi rozdílnou spotřebou energie. Režim plného běhu, ve kterém fungují veškeré periferie. Režim idle ve kterém fungují všechny periferie, ale aritmeticko-logická jednotka, čili procesor je zastaven a je probuzen po vykonání činnosti některé z periferií. Dále se používají různé režimy ve kterých jsou vypnuté další periferie, poslední nejúspornější má obvyklou spotřebu v nA a reaguje pouze na jediný vstup, který vyvolá restart celého MCU.

K porovnání spotřeby byla vytvořena tabulka několika vybraných modelů mikrokontrolérů s jejich odběrem v minimálním a v maximálním použitelném energetickém stavu. Druhý sloupec tabulky obsahuje spotřebu ve stavu, při kterém MCU běží oscilátor a MCU reaguje na externí přerušení, další sloupce označují spotřebu v běžném běhu, při kterém běží.

Ukončit volbu pouze dle minimální spotřeby z této tabulky by byla chyba. Například co se týče spotřeby při srovnání naprosto excelují mikrokontroléry MSP430, jsou výborně vybaveny periferiemi, mají oproti běžné praxi i řady MCU vybavené operačními zesilovači vhodné pro zpracování signálu. Problematické se ovšem ukázalo použití dostupných modelů v kombinaci s šifrováním. K uchování klíčů a provozu daných šifrova-

Tab. 6. Tabulka spotřeby procesorů

Spotřeba 2.2V [uA]	ext přerušeni + čas	normální běh	normální běh
Název	1MHz	1MHz	8MHz
ATmega644PA	3,5	150	1700
ATmega164PA	4,2	300	1500
EFM32ZG108	0,86	115	945
EFM32TG822F32	0,9	210	1256
EFM32G210F128	1	220	1488
MSP430F2013	0,5	220	2000
STM32L162	1,5	310	2300

cích algoritmů mají tyto mikrokontroléry často příliš malou operační paměť. Modely s dostatečnými parametry pamětí, vybavené potřebnými periferiemi, jsou na druhou stranu až moc drahé v porovnání s konkurencí.

Mnohem lépe, co se týče výkonu a kapacit dostupných modelů, na tom je řada MCU STM32L1 od firmy STMicroelectronics. Jedná se o 32bitové mikrokontroléry postavené na jádru ARM Cortex<sup>™</sup>-M3, tedy mají vysoký výkon, pokročilou sadu instrukcí, periferie dokonce obsahují AES jednotku k urychlení šifrování tímto algoritmem.

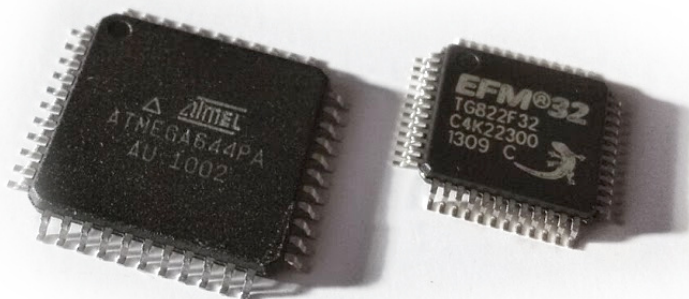
Výhodu značného výkonu ARM jádra v MCU STM32L1 mají rovněž produkty méně známé norské firmy Energy Micro, nyní již patřící pod Silicon Labs. Produkty řady EFM32 jsou od začátku navrženy pro extrémně nízkou spotřebu. Jádro je podobně jako u STM32 32bitový ARM, ovšem tyto MCU mají speciálně navržené periferie schopné fungovat v úspornějších režimech se sníženou spotřebou než jak je tomu u konkurence. Kupříkladu Low Energy UART je sériové rozhraní, je omezeno sice frekvencí do 9600 kbit/s, ale dokáže fungovat i v Deep Sleep režimu, ve kterém je zastaven hlavní oscilátor a spotřeba celého MCU dosahuje pouhé 0,9  $\mu$ A.

Řada MCU megaAVR firmy Atmel Corporation, jehož jednotlivé MCU jsou označeny ATmega, využívají osmibitovou instrukční sadu AVR. Tyto MCU sice nedisponují vysokým výkonem, ale jejich parametry jsou dostatečné pro vykonávání širokého počtu činností. Mezi výhody patří například i schopnost spínat proudy 40 mA jedním výstupem, zatímco konkurence obvykle nezvládá více jak 6 mA. Při srovnání s konkurencí ve spotřebě elektrické energie jsou na tom tyto obvody sice nejhůře, ale ten rozdíl není až tak markantní a drží se ve stejných řádech. Tyto MCU jsou velmi oblíbené v poslední době i díky projektu Arduino.

Projekt Arduino využívající převážně MCU řady megaAVR a v posledních letech získává přízeň u velkého počtu lidí, dokonce i lidí bez předchozích zkušeností s elektronikou. Jedná se o platformu, ze které je možné bez zkušeností a speciálního vybavení jako páječka, či programátor velice rychle sestavit a naprogramovat prototyp řešící daný

problém. Výhody jsou velmi vysoká rozšířenost a dostupnost softwarových knihoven a ukázek k obsluze velkého počtu komponent. To přináší velké výhody při testování většího počtu různých snímačů a bezdrátových modulů.

Ke konečnému využití MCU Atmel ATmega padlo rozhodnutí hlavně z důvodů letité zkušenosti s těmito obvody, dobré komunitní dostupnosti knihoven a příkladů. Výhody konkurenčních MCU nebyly dostatečný důvod k pořízení vybavení pro jinou rodinu MCU a učení se pro ně programovat. K vytvoření prvního prototypu bezdrátového snímače byl vzhledem k potřebným kapacitám při šifrování zvolen Atmel ATmega644PA.



Obr. 28. Atmel ATmega644PA a EFM32TG822F32

#### 5.4.1 Kryptografické schopnosti mikrokontrolérů

S volbou mikrokontroléru souvisí i volba použitých algoritmů k šifrování datových přenosů.

**Asymetrická kryptografie** je i ve světě výkonných počítačů pomalá a používá se tedy převážně k zajištění výměny klíčů a vytváření digitálních podpisů. Ovšem podepisují se pouze krátké otisky zpráv vytvořenými hashovacími algoritmy, jelikož jsou tyto algoritmy opravdu pomalé. Pokud by se tato práce týkala sensorových sítí, ve kterých se dynamicky přidávají a odebírají jednotlivé uzly, bylo by nutné využít asymetrickou kryptografii. To ovšem není tento případ.

**RSA, DSA** Vzhledem k nutnosti používat opravdu dlouhé klíče, které by samy o sobě zabraly většinu paměti RAM vybraných MCU, byly RSA a DSA vyřazeny. Rovněž potřebný výkon je velký, existují optimalizace umožňující využít například 1024bitové varianty RSA v sensorových sítích. Tyto optimalizace velmi snižují bezpečnost a časy

jednotlivých operací se dle [37] měří i na poměrně výkonných MCU s jádrem ARM v řádu minut.

**Eliptické křivky** Pro svět bezdrátových snímačů je mnohem výhodnější asymetrická kryptografie postavená nad eliptickými křivkami. Používané klíče jsou poměrně krátké a algoritmy jsou tedy rychlejší. K testům byla využita knihovna nano-ecc a měřen výkon ECDH a použitá křivka byla secp192r1. Jedná se o variantu Diffieho-Hellmanova protokolu využívaného k bezpečnému vytvoření a předání klíče mezi dvěma stranami po nezabezpečeném kanálu. 8bitová ATmega zvládla vykonat potřebné operace, tedy vygenerovat privátní a veřejný klíč a vygenerovat sdílený klíč za 3,9s, 32bitový ARM to samé zvládl za 570ms a s využitím 32bitové knihovny micro-ecc za 105ms. Bohužel malá paměť 16bitového procesoru MSP430 ho z této disciplíny vyřadila. [37]

**Symetrická kryptografie** využívá k šifrování i dešifrování stejný klíč. Výkon těchto algoritmů bývá v porovnání s asymetrickou kryptografií velice vysoký a minimální délka klíčů je velmi krátká.

**RC4** je jednoduchá proudová šifra. Proudové šifry generují takzvaný keystream, tedy řetězec, který je během šifrování obvykle operací XOR zkombinován s šifrovaným obsahem a dešifrování probíhá stejně, tedy je vygenerován stejný keystream a operace XOR zajistí dekódování.

Na začátku šifrování se u RC4 inicializuje keystream, ovšem i to je poměrně rychlé, v assembleru na 8bitové architektury AVR stačí k této operaci přibližně 6700 cyklů procesoru. Od té doby stačí přibližně 40 cyklů procesoru k vygenerování keystreamu pro další byte. Tento algoritmus je tedy velmi rychlý a je tak stále používán například i na webu, například HTTPS spojení na seznam.cz v době psaní práce využívá RC4.

Bohužel je tento velice rychlý algoritmus v dnešní době nedoporučován, začátek keystreamu je možné úspěšně napadnout statistickou analýzou [4]. Řešení tohoto problému je rozšíření inicializace keystreamu o zahazení prvních 512 vygenerovaných bytů. Tato varianta se nazývá RC4-drop512.

Implementace RC4 je z programátorského hlediska velice jednoduchá. K testům byla použita implementace z projektu AVR-Crypto-Lib ve variantě ARCFOUR pro všechny 3 MCU a výkonnostní rozdíl mezi nimi je naprosto minimální. Jelikož tento algoritmus využívá operace nad osmibitovými hodnotami a schopnost pracovat s většími bloky dat u 16 a 32bit procesoru tedy není výhodou.

**ChaCha20** Jako druhou zkoušenou proudovou šifrou byla zvolena ChaCha20. V kryptografických diskuzích je tento algoritmus doporučován jako náhrada RC4. Jejím au-

torem je Daniel J. Bernstein.

Chacha20 vychází z algoritmu Salsa20. Používaný klíč je délky 256 b a dalších 64 b se používá k přenosu nonce, tedy hodnoty, která se při každém přenosu změní. Klíč je tedy pokaždé jiný. Aritmetika tohoto algoritmu je postavená nad operacemi s 32bitovými čísly, tedy na 8bitových MCU je výkon značně degradován. Použitá implementace ChaCha20 je získána z projektu Codecrypt od českého vývojáře Mirka Kratochvila. Jedná se o variantu psanou objektově v C++ a neobsahuje assemblerové optimalizace pro konkrétní MCU. Výkon je oproti silně optimalizovanému RC4 v případě osmibitového AVR dokonce 25x nižší, na 32bitovém ARM je výkon 3x nižší a paměťová náročnost znemožnila testy na mě dostupném MSP430.

ChaCha20 je nutné pouze inicializovat klíčem a je možné využívat již první vygenerované byty keystreamu, není nutné zahazovat třeba prvních 512 B jako u RC4. Tím se snižuje výkonnostní rozdíl, zvláště u tak krátkých zpráv, jaké přenáší bezdrátové senzory.

**AES** Jedná se o velmi rozšířenou blokovou šifru. Blokované šifry šifrují po celých blocích kupříkladu 128 b, dochází nejen k náhradě, tedy substituci jednotlivých znaků, ale i ke změně pořadí. Není tak běžně možné šifrovat libovolnou délku zprávy, ale musí být vždy doplněna na určitou délku.

K měření byla zvolena 128 bitová varianta AES. Během hledání různých variant, pro 8bitovou ATmega se ukázala jako nejlepší AESLib od Davyho Landmana, ovšem podrobnější zkoumání prokázalo, že se jedná o upravenou knihovnu AVR-Crypto-Lib. Některé části AES algoritmu byly přepsány do assembleru, což oproti implementaci v samotném jazyku C zvýšilo rychlost přibližně desetinásobně. Bohužel pro MSP430 nebyla nalezena takto optimalizovaná varianta, k testování tedy bylo využito referenční řešení v jazyku C přímo od Texas Instruments a na výsledcích se tato pomalost projevila. Stejně řešení bylo použité i na 32bitovém ARM procesoru, tentokrát se již projevil rozdíl mezi 16 a 32bitovým procesorem, jelikož ten stejný kód je v absolutním počtu cyklů procesoru asi 3x rychlejší na 32bitovém systému oproti 16 bitovému.

Velká výhoda AES je hardwarová podpora, existují mikrokontroléry, které obsahují hw podporu, testovaný MCU bohužel tuto podporu neměl, ale například EFM32 zvládají jeden 128 b AES blok šifrovat pouze 53 cykly.

**DES** Z historických důvodů byly provedeny testy i na 3DES. Používá se na starším hardware, který je vybaven hardwarovou podporou tohoto algoritmu. Ani jeden ze 3 testovaných MCU tuto podporu již neměl a výsledky jsou tedy velice špatné. Jedná se o opravdu starý a pomalý algoritmus a vzhledem ke krátké délce klíče v době návrhu je nyní dokonce volaný vždy třikrát.

**Zhodnocení** Bylo zajímavé porovnat mezi sebou jednotlivé šifrovací algoritmy na různých drobných mikrokontrolérech, které jsou limitovány nejen výkonem, ale i pamětí a dostupnou energií.

Z pokusů vyplynulo, že asymetrická kryptografie je pro účely této práce až moc pomalá a tedy energeticky náročná. Bylo by ji nutné využít v případě použití sensorových sítí. V tomto případě by se již muselo počítat s výkonnými MCU s jádrem ARM a rovněž by již bylo nutné mít více dostupné energie.

Algoritmy symetrické kryptografie prokázaly vysoký výkon a vysoké stupně optimalizace v případě použití některých MCU.

Tab. 7. Porovnání rychlosti vykonávání šifrovacích algoritmů na daných MCU

[cykly procesoru na byte]	AVR 8bit	MSP430 16bit	ARM 32bit
RC4	38	39	56
ChaCha20	984	-	151
AES-128 šifrování	191	1 038	396
AES-128 dešifrování	222	1 577	544
3DES šifrování	110 849	138 679	44 911
3DES dešifrování	1 739	34 675	708

Snaha vyhledat nejrychlejší volně dostupné implementace těchto algoritmů dostupné na internetu prokázala výhody velikosti komunity uživatelů daného MCU. Kupříkladu 8bitový AVR zvládl šifrovat optimalizovanou knihovnou AES-128 menším počtem cyklů, než výkonný 32bitový ARM od Texas Instruments a pro MSP430 byly dostupné pouze referenční knihovny od výrobce.

Blokové algoritmy jako AES jsou jistě velmi vhodné při šifrování velkých bloků dat, bohužel v případě této práce a použitého rádiového modulu je možné najednou odeslat pouze 32 B a součástí musí být i adresa v nešifrované podobě. Vzhledem k principu blokových algoritmů, využívající i transpozici, tedy změnu pozice jednotlivých šifrovaných znaků, by tedy bylo možné využít u AES 128 b délku klíče a zpráva by tak byla omezena na pouhých 16 B.

Bylo zvoleno využití symetrických proudových šifer, které nemění pořadí šifrovaných bitů a mohou tedy šifrovat i pouhé jednotlivé bity. Algoritmus RC4 je velice rychlý, ale bohužel už na něj existují útoky, které by sice nedělaly problém v tomto použití, ale i tak by bylo nutné zahazovat prvních 512 B keystreamu. Z tohoto důvodu byl k šifrování zvolen algoritmus ChaCha20.

## 5.5 Rádiový přenos

K přenosu naměřené informace k přijímající stanici byl potřeba rádiový modul fungující v bezlicenčním frekvenčním pásmu, tedy v pásmu, které je možné využívat bez

individuálního oprávnění a není potřeba žádná homologace. Český telekomunikační úřad tyto pásma nazývá rádiové kmitočty vymezené všeobecným oprávněním. Jedná se o frekvence využívané bezdrátovými počítačovými sítěmi jako například Wi-Fi 2,4 GHz a 5 GHz. Různé domovní zvonky, bezdrátové myši a meteostanice používají spíše frekvence kolem 433 a 868 MHz. Dle prováděných pokusů s moduly používající pásmo 2,4 GHz, bylo toto pásmo poměrně silně zarušeno a dosah byl tak velmi krátký, přitom byl použit maximální možný výkon. K použití v této práci tedy bylo zvoleno pásmo 433 MHz, které má vzhledem k nízké frekvenci i nejdelší dosah.

433 MHz pásmo je omezeno ČTU dle všeobecného oprávnění č. VO-R/10/04.2012-7 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu. V pásmu 433,050–434,790 MHz je možné při výkonu do 1 mW e.r.p. vysílat neomezeně. Pokud se tento výkon překročí, maximálně však do 10 mW e.r.p., je možné vysílat z 1 hodiny pouze 10% času, tedy je možné v kuse vysílat 6 minut a poté je nutné 54 minut nevysílat. Ve vyvinuté platformě není dostupný zdroj energie, který by pokryl výkon potřebný i pouze ke sledování tohoto vysílání.

První pokusy s rádiovými moduly vedly k využití modulu RFM22 od firmy HOPE Microelectronics Co.,Ltd, dále byl zkoušen na 2,4 GHz fungující nRF24L01 od Nordic Semiconductor a nakonec byl vzhledem k možnostem úspory energie zvolen modul s obvodem nRF905, rovněž od Nordic Semiconductor.

### 5.5.1 Nordic Semiconductor nRF905

nRF905 je rádiový integrovaný obvod, transceiver tedy schopný vysílat i přijímat rádiové vysílání v pásmech 433, 868 a 915 MHz.

K mikrokontroléru se obvod nRF905 připojuje rozhraním SPI a několika GPIO piny, kterými se ovládá a kterými signalizuje stavy jako připravená data ke čtení, přijatá adresa a to umožňuje snížit spotřebu, jelikož pak není nutné využívat sběrnici SPI ke zjišťování stavu. Mikrokontrolér si tak pouze nastaví přerušování při změně na daných pinech a může se dále věnovat jiné činnosti, případně se uspat a tím se šetří energie. Za cenu využití většího počtu vodičů se tedy snižuje spotřeba celého řešení.

Obvod nRF905 obsahuje vnitřní stabilizátor, funguje tak v rozmezí 1,9 - 3,6 V. K úspoře energie se tento obvod umí přepnout do několika režimů s různou spotřebou. V kompletním vypnutém stavu ve kterém je odstavena i SPI komunikace má obvod typickou spotřebu 2,5  $\mu\text{A}$ , po probuzení do standby, tedy pohotovostního režimu, se spotřeba zvýší na 12,5  $\mu\text{A}$  a v té se během probíhající SPI komunikace spotřeba zvýší na 20  $\mu\text{A}$ . Během vysílání a příjmu je spotřeba v naprosto jiných řádech, jak dokazuje tabulka 8. Proto je nutné minimalizovat dobu strávenou v těchto režimech na absolutní minimum a právě k tomu jsou určeny režimy ShockBurst™. Tyto režimy zařídí některé operace, například se obvod automaticky přepne do úsporného režimu po dokončení

vysílání, ale také umožňuje periodicky vysílat stejnou zprávu dokud je nastaven daný vstup TRX\_CE na logickou nulu. Toto chování je využito na straně přijímače k vysílání potvrzování příjmu packetů. Potvrzení je odesíláno v desítkách stejných vysílání periodicky po delší dobu v dohodnutém intervalu a na bezdrátovém snímači tak může být zapnut příjem pouze na dobu příjmu jediného vysílání. Pokud se některá operace zdrží, například je daná frekvence rušena, nebo se pouze vlivem rozdílných teplot rozejdou hodiny mezi vysílačem a přijímačem, pak opakované vysílání zajistí lepší šance na příjem potvrzení v minimálním možném čase.

Tab. 8. Spotřeba energie v režimech vysílání a příjmu

Režim	Spotřeba [mA]
Vysílání -10dBm	9
Vysílání -2dBm	14
Vysílání -6dBm	20
Vysílání 10dBm	30
Příjem	12,5
Příjem se sníženou citlivostí	10,5

### 5.5.2 Formát rámce

Obvod nRF905 používá k přenosu dat GFSK modulaci, tedy trochu upravené FSK, což využívá kmitočtové klíčování, při kterém dochází ke změnám frekvence. Logická 0 má tedy jinou frekvenci oproti logické 1. GFSK k této modulaci přidává Gaussovský filtr a změna frekvence tak nenastane okamžitě, ale dochází k postupné změně.

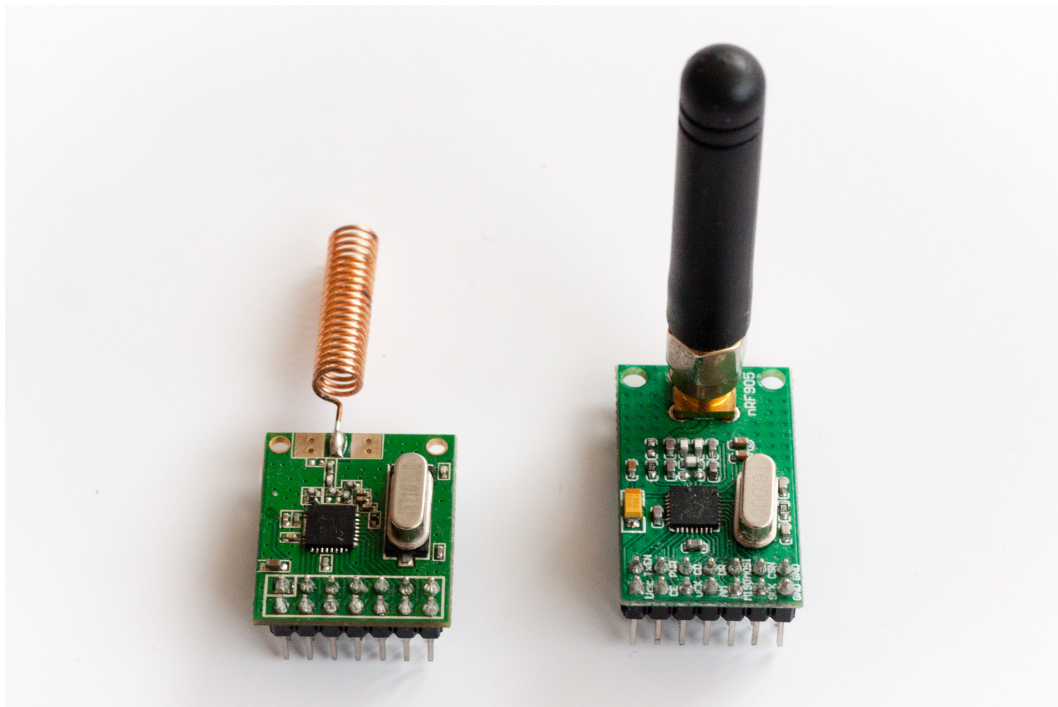
Rámec obsahuje:

1. preambuli 10 bitů logických 1
2. adresu 8-32 bitů
3. payload, neboli obsah až 256 bitů (32 bajtů)
4. volitelný kontrolní součet CRC 16 bitů

[34]

### 5.5.3 Použité moduly

Použité moduly vychází z ukázkového zapojení uvedené v datasheetu nRF905. Na obrázku 29 je použitá dvojice modulů. Použit byl ten vlevo s napevno připájenou anténou, typové značení je XL905-D01. Tento modul má osazenu anténu naladěnou na frekvenční rozsah 433.05-434.79MHz. Modul je sice možné přepnout do frekvencí



Obr. 29. Moduly rádiového obvodu nRF905

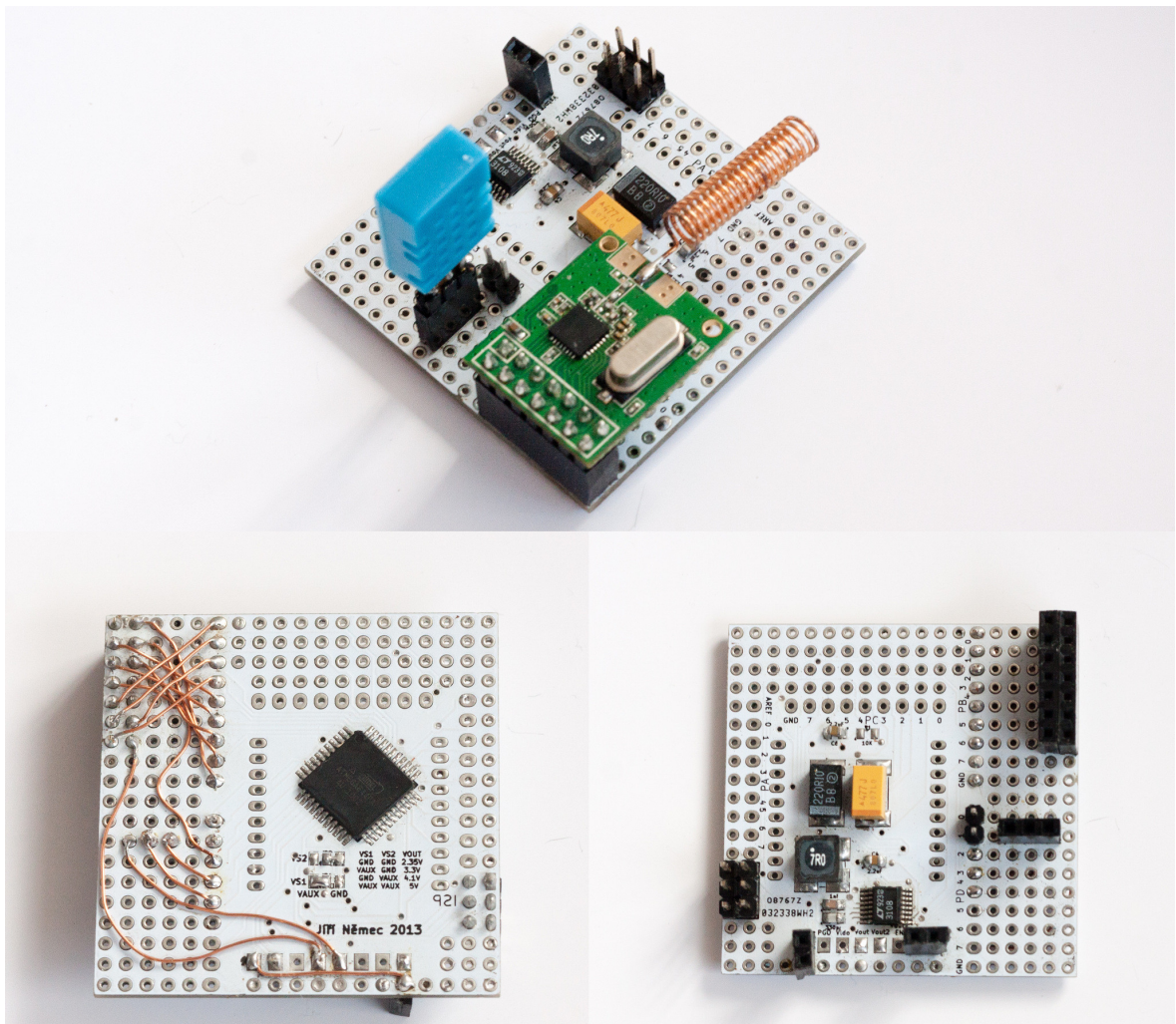
kolem 868 MHz, ovšem dosah se poté velmi sníží. Udávaný rozsah pracovních napětí je 1,9-3,6 V, tedy stejný jako samotný chip nRF905, zatímco modul na fotografii vpravo má udávaný rozsah 2,7-3,6 V.

## 6 PLATFORMA BEZDRÁTOVÉHO SNÍMAČE

Pro účely této práce byly vytvořeny 2 desky plošných spojů s mikrokontrolérem a obvodem správy napájení obvodu energií z okolí, tedy Energy Harvesting Power Management. Součástí DPS je i prototypovací oblast určená k pokusům s připojenými snímači a kolem této oblasti jsou vyvedeny jednotlivé vývody mikrokontroléru. K otestování většího počtu snímačů nakonec stačil jediný plošný spoj této platformy a jednotlivé snímače k němu byly pouze dočasně připojeny.

### 6.1 Platforma bezdrátového snímače s ATmega644PA

Napájení a Energy Harvesting obsluhuje LTC3108, jako procesor je použit Atmel ATmega644PA.



Obr. 30. Platforma bezdrátového snímače s MCU ATmega644PA

V okolí těchto dvou integrovaných obvodů jsou součástky potřebné k jejich fungování, tedy převážně kondenzátory a transformátor. Zbytek prostoru plošného spoje rozměru 50x50 mm je vyplněn prototypovací oblastí, tedy pájecími body do kterých je možné

připojovat různé součástky jako snímače fyzikálních veličin, rádiový modul. Prototypovací oblast umožňuje testovat tyto součástky bez nutnosti pokaždé navrhovat nový plošný spoj. K propojení komponent v prototypovací oblasti byl využit samopájecí drát průměru 0,4 mm. Jedná se o drát potažený izolací ve formě nátěru.

K návrhu plošného spoje byl zvolen svobodný software určený k návrhu schémat a plošných spojů KiCad. Tento software je dostupný zdarma a o jeho kvalitách snad vypovídá, že mezi autory tohoto softwarového projektu patří i vědci z Evropské organizace pro jaderný výzkum (CERN). Tento plošný spoj je autorův první, který využívá pouze SMD součástky. Vzhledem k používaným rozměrům, v případě rozstupů 0,65 mm mezi vývody obvodu LTC3108, ho již nebylo možné vyrobit v domácích podmínkách a samotnou výrobu plošného spoje bylo nutné předat specializované firmě, v tomto případě Elecrow. Další plošné spoje byly vyráběny ve firmě PragoBoard s.r.o..

### 6.1.1 LTC3108

O přísun energie se stará již dříve popsany LTC3108. Schéma zapojení vychází z příkladů v datasheetu k LTC3108 a i rozmístění součástek vychází z těchto doporučení. Transformátor byl použit doporučený model firmy Würth s poměrem počtu vinutí 1:100. Na desce plošných spojů je možné spojením pájkou vybrat všechny 4 varianty výstupního napájecího napětí.

### 6.1.2 Atmel ATmega644PA

Jako mikrokontrolér zajišťující zpracování naměřených hodnot a komunikaci s rádiovým obvodem byl zvolen Atmel ATmega644PA. Ten je napájen napětím 2,2 V z výstupu  $V_{LDO}$  LTC3108. Jedna z výhod tohoto druhu napájení je dostupnost napájení jako první, tedy tento MCU je zapnutý jako první a zapíná rádiový obvod a snímače až pokud je dostupné napájení pro ně na  $V_{OUT}$ , což je indikováno výstupem PGOOD, připojeném k GPIO vstupu PA6. Konstrukci plošného spoje zjednodušilo použití vestavěných oscilátorů, při startu se v programu volí nastavení předděličky na vnitřní 8 MHz oscilátor, možné frekvence tak jsou 1, 2, 4 nebo 8 MHz. Vzhledem k nízkému napájecímu napětí je 8 MHz již za maximální frekvencí a dle specifikací by ani vyšší frekvence nefungovaly, maximální doporučená frekvence je tak 4 MHz a v programech byla použita frekvence 2 MHz. Využití externího oscilátoru by bylo nutné hlavně z důvodů zvýšení přesnosti.

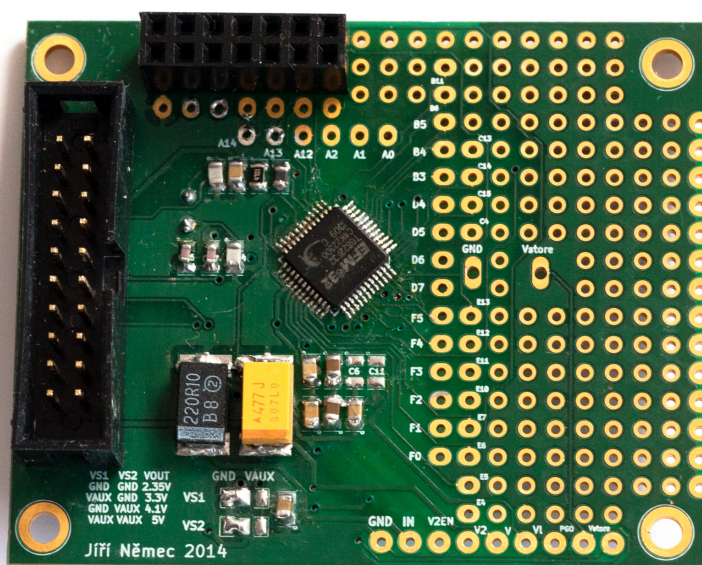
Parametry:

- 64 KB Flash
- 2 KB EEPROM
- 4 KB RAM

- Rozsah pracovních napětí: 1,8 - 5,5 V
- Maximální frekvence 20 MHz

## 6.2 Platforma bezdrátového snímače s EFM32

Mikrokontroléry firmy Energy Micro EFM32 mají velmi chytře navrženy periferie. Ty dokáží pracovat často i v úsporném režimu při opravdu nízké spotřebě v řádu stovek nA. Samotný odběr energie ve srovnatelných režimech je podobný u všech zkoušených mikrokontrolérů, rozdíl u EFM32 je schopnost provádět činnosti v úspornějších režimech, než to dělají ostatní mikrokontroléry.

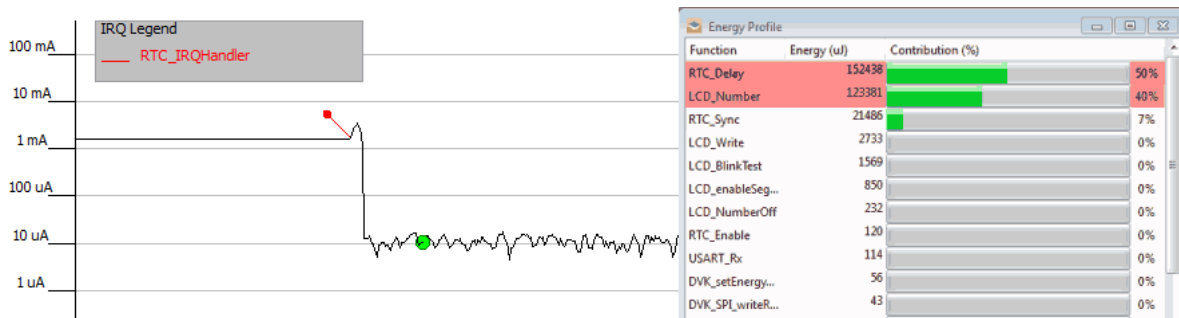


Obr. 31. Platforma bezdrátového snímače s MCU EFM32

Bohužel nebyl dostatek času na práci s tímto MCU. Podařilo se oživit až druhý plošný spoj a v ten moment se projevil problém použitého programátoru, sice měl dle specifikací fungovat již od 1,5 V, bohužel se ale s 2,2 V logikou nedokázal spojit. Byl objednan jiný programátor, ten již tímto problémem netrpěl, bohužel byl doručen až 12.5.2014, tedy v době dokončování samotného textu a tedy již nebyl čas do odevzdání práce cokoliv naprogramovat a otestovat.

Pokusy s tímto výborným MCU tedy skončily u základního rozchození komunikace, tedy odeslání zprávy přijímači.

Za zmínku stojí možnosti ladění dodaným softwarem, součástí Simplicity studia dostupného zdarma je Silicon Labs energyAware Profiler, který za použití debuggeru připojeného k EFM32 monitoruje spotřebu elektrické energie v čase a ukazuje i spotřebu volaných funkcí. [28]



Obr. 32. Silicon Labs energyAware Profiler [28]

### 6.2.1 EFM32TG820F32

Jedná se o mikrokontrolér architektury ARM Cortex-M3 firmy Energy Micro z řady Tiny Gecko. Řada Tiny Gecko se z mého pohledu liší hlavně přítomností vestavěných operačních zesilovačů, vysokým výkonem Cortex-M3 a nízkou spotřebou.

Vybrané parametry:

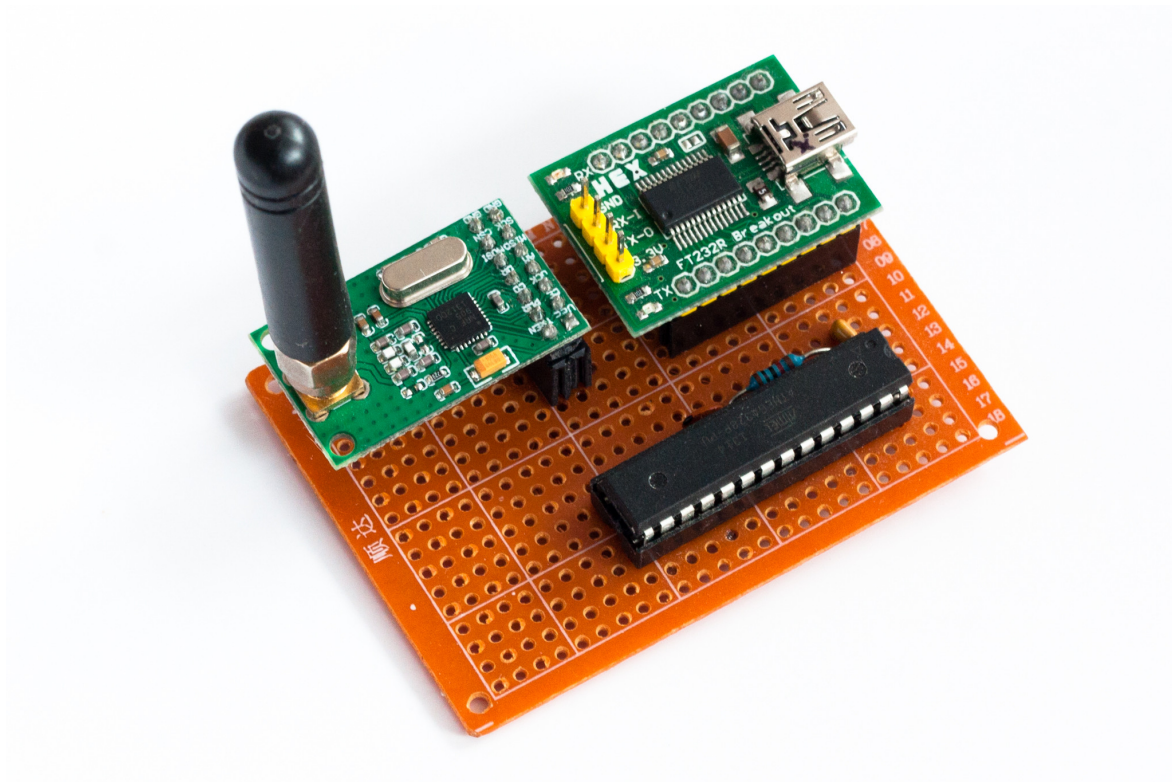
- Maximální frekvence 32MHz
- 32KB Flash
- 4 KB RAM
- Rozsah pracovních napětí 1,85 - 3,8 V
- Spotřeba 20 nA v Shutoff režimu
- 3 Operační zesilovače
- 2 univerzální porty pro sériovou komunikaci UART/SPI/IrDA/I2S
- Nízkoenergetický sériový UART port
- 8 DMA kontrolérů
- 8 PRS periferních reflexních systémů, které umožňují komunikaci mezi perifériemi bez využití procesoru
- AES jednotka

## 7 PŘIJÍMAJÍCÍ STANICE

K příjmu dat přenášených z bezdrátových snímačů byl prvně vytvořen prototyp na univerzální desce s obvodem ATmega328P a FTDI převodníkem na USB a následně plošný spoj s ATmega1284P a HiLink HLK-RM04 zajišťující komunikaci s počítačovou sítí.

### 7.1 Příjímající stanice s ATmega328P

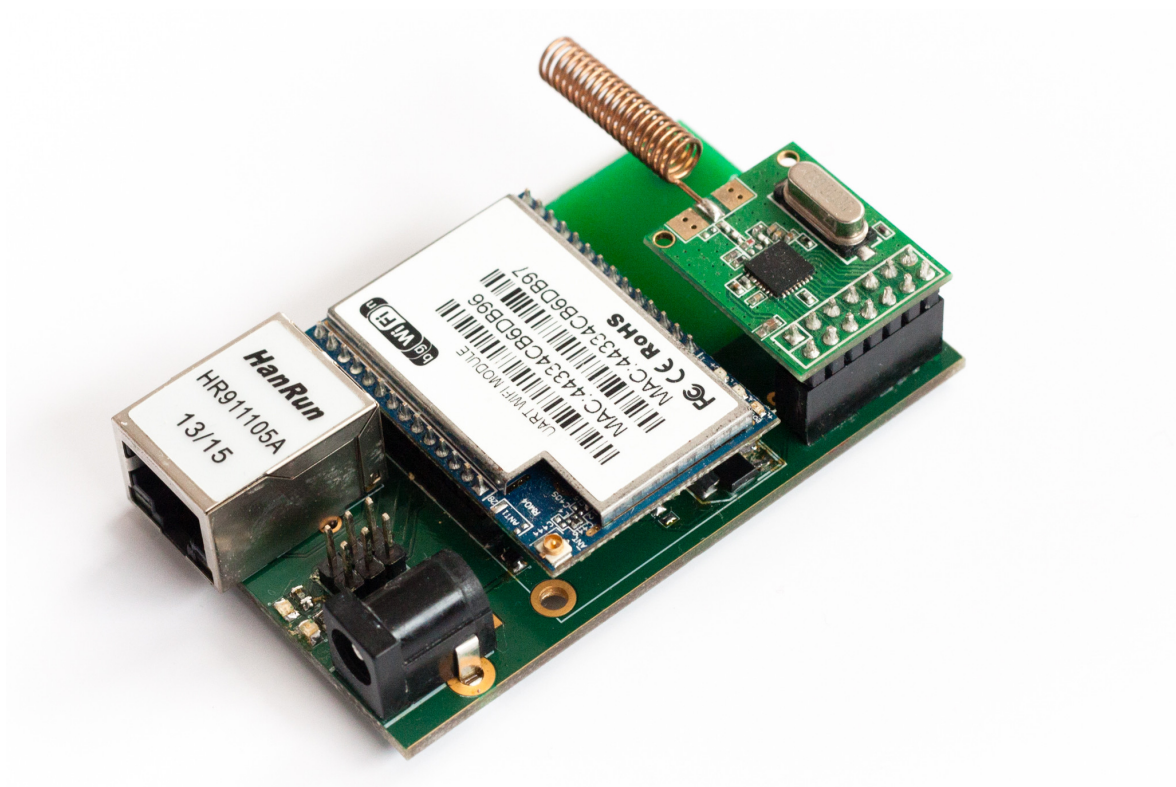
K prvním pokusům s komunikací byl vytvořen na univerzálním plošném spoji obvod zahrnující modul s nRF905, modul s FDTI RS232RS zajišťující překlad komunikace ze sériového rozhraní UART na USB a MCU ATmega328P.



Obr. 33. První prototyp přijímací stanice na univerzálním plošném spoji

### 7.2 Příjímající stanice s ATmega1284P

Tato přijímající stanice již vznikala v době, kdy byl zvolen rádiový modul nRF905, obsahuje tak místo pro připojení tohoto modulu, komunikaci s ním zajišťuje mikrokontrolér Atmel ATmega1284P. Přenos informací z mikrokontroléru ATmega1284P do počítačové sítě zajišťuje modul HLK-RM04 od firmy HiLink, jehož primární určení je převodník ze sériové linky standardu UART na Wi-Fi, či Ethernet.



Obr. 34. Přijímací stanice s MCU ATmega1284P a převodníkem HLK-RM04

### 7.2.1 ATmega1284P

O předávání informací z rádiového modulu nRF905 k převodníku sériového rozhraní na počítačovou síť HLK-RM04 se stará ATmega1284P. Hlavní činností je monitorovat stav přijatého vysílání na rádiovém modulu, na toto vysílání odpovídat a přijatou informaci předávat dále. Dále zajišťuje generování a předávání klíčů, kterými je rádiové vysílání šifrováno.

Parametry:

- 128 KB Flash
- 4 KB EEPROM
- 16 KB RAM
- Rozsah pracovních napětí: 1,8 - 5,5 V
- Maximální frekvence 20 MHz

### 7.2.2 HiLink HLK-RM04

O přenášení přijatých informací z integrovaného obvodu ATmega1284P se stará modul HiLink HLK-RM04.

Parametry:

- 4 MB Flash
- 16 MB RAM
- Procesor Ralink RT5350F 360 MHz
- 2 rozhraní UART
- WiFi standardy IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
- 2 Ethernetové rozhraní
- Rozměry: 40x30x9 mm

Tento modul je tedy velmi malý router malých rozměrů se sériovým rozhraním určený k osazení do plošného spoje. Vestavěný software umožňuje webovou konfiguraci síťových parametrů a konfiguraci dvojice sériových rozhraní. Konfiguraci je možné provést nástrojem od výrobce po samotném sériovém rozhraní AT příkazy. Jediná funkce vestavěného software je ovšem pouze přenos komunikace mezi sériovým rozhraním a síťovým spojením na nastaveném TCP portu. Je tedy nutné navázat spojení z dalšího počítače a provádět zpracování samotných dat až v něm.

Nízká cena a tím daná velká rozšířenost vedla i ke vzniku komunitního alternativního software OpenWrt pro modul HLK-RM04. Toto zařízení je sice velmi omezené co se týče hardwarových parametrů, v případě potřeby je možné odstranit například webovou konfiguraci a uvolněný paměťový prostor využít k programům potřebným pro zpracování přijatých hodnot. Tyto naměřené údaje je tak možné dále odesílat například http protokolem na servery umístěné na internetu.

## 8 SPOLEČNÉ PROGRAMOVÉ VYBAVENÍ

Všechny varianty snímačů na této platformě sdílejí stejné části programů, které zajišťují komunikaci a úsporu energie. K vývoji byl primárně použit programovací jazyk C++, ovšem byly využity i knihovny psané v jazyku C, které bylo nutné v některých případech upravit, například doplnit o vlastní energeticky úsporné varianty pauz.

Ke kompilaci zdrojových kódů byl použit GNU toolchain. Jedná se o sadu otevřených nástrojů jako kompilátor, linker (sestavovací program). Pro procesory AVR byla použita varianta AVR-GCC, pro ARM varianta GNU Tools for ARM Embedded Processors, též označována typově arm-none-eabi, označující, že výsledný program běží přímo na daném MCU a není využíván žádný operační systém a jeho knihovny a rozhraní.

Vývojové prostředí bylo použito KDevelop, ovšem využíváno bylo spíše pouze jako editor, například soubory Makefile používané k sestavení programem make byly psány ručně a nikoliv generovány.

### 8.1 Rozdíly mezi programy

Jednotlivé programy určené pro různé snímače se od sebe liší pouze souborem main.cpp a případně potřebnou knihovnou obsluhující daný snímač. Společný kód je ve formě knihovny. Tento jednoduchý způsob se ukázal velice účinný například na platformě Arduino.

V souboru main.cpp je umístěna obsluha hlavní nekonečné smyčky, která je vždy vyvinuta dle zvoleného snímače. Není problém využít kombinaci více různých snímačů připojených k jednomu kusu platformy bezdrátového snímače, ovšem v této práci byl vždy připojen pouze jeden snímač najednou.

Běžná programová obsluha snímače spočívá v inicializaci MCU, vypnutí nepotřebných komponent, počkání dokud není dostupný dostatek energie a jakmile je, tak následuje zapnutí a inicializace komponent. V následující nekonečné smyčce dále dochází k měření, odeslání hodnoty, spánku a to vše s kontrolou přítomnosti dostatku energie.

### 8.2 Programování s ohledem na energii

Programování aplikací s nízkou spotřebou má jistá specifika, software tak nebyl vytvářen pouze s ohledem na rychlost a nízké paměťové nároky, ale i s ohledem na malou spotřebu energie a hlavně na eliminaci velkých proudových odběrů. Bylo tak nutné například mezi vysílání packetu a příjem potvrzení o doručení tohoto packetu přidat pauzu, během které dochází k nabití kondenzátorů.

Rovněž běžná kontrola stavu digitálního vstupu musí být doplněna pauzou, během které dochází k přepnutí do úsporného režimu. Případně je rovnou možné využít v MCU přerušeni vyvolané změnou digitálního vstupu. Během ladění obslužného softwaru tak

bylo nutné využívat i osciloskop.

K řízení spotřeby energie bylo pro obvody ATmega vytvořeno několik funkcí. Funkce `void cpu_powersave_init ( const uint8_t except )` provádí inicializaci čítačů, vypíná nepotřebné periferie a digitální vstupy a výstupy nastavuje do stavu, ve kterém mají minimální spotřebu.

Funkce `void sleep_us ( const uint16_t us )` uspí mikrokontrolér na krátký čas zadaný v mikrosekundách do režimu idle, tedy do režimu, ve kterém je zastaven pouze mikroprocesor, ale všechny periferie dále pracují.

Pro nejdelší spánek je určena funkce `void powerdown_s ( const uint16_t s, bool reset )`, která uspí celý mikrokontrolér do stavu Power down, ve kterém zůstane běžet pouze watchdog, který ho probouzí. Ve výchozím stavu je doba spánku watchdogu nastavena na 1 sekundu, ale tento interval je možné modifikovat úpravou registrů.

### 8.3 Komunikace

Přenos naměřených hodnot probíhá ze strany senzorů ke straně přijímače, následně je vyslán potvrzovací packet od přijímače k senzoru. Časový rozestup mezi příjmem a odesláním potvrzení je pevně dán, jedná se o 50 ms. Jakékoliv ztráty vysílání jsou detekovány číslem nonce, které se zvyšuje při každém potvrzeném vysílání a slouží rovněž jako část klíče při šifrování packetu.

S komunikací, která by byla zahájena ze strany přijímače, se v této práci nepočítá, jelikož setrvání ve stavu příjmu je velmi energeticky náročné. Existují speciální obvody, které sledují danou frekvenci i s dostatečně nízkou spotřebou v řádu  $\mu\text{A}$ , ale obvykle se jedná o speciální řešení určené pouze k probuzení obvodu.

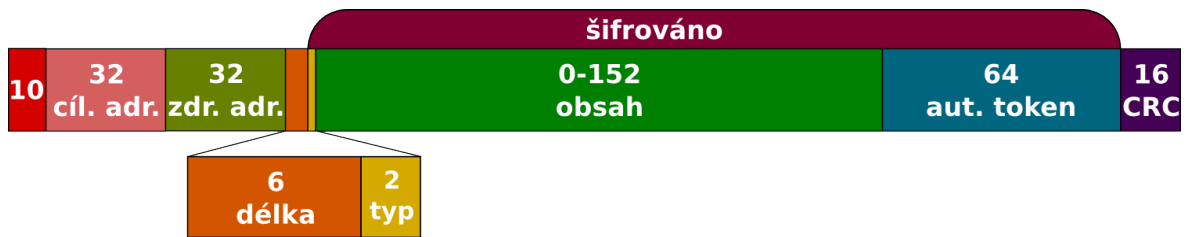
#### 8.3.1 Formát packetu

K identifikaci jednotlivých bezdrátových snímačů, byla zvolena 32 b délka adres, tedy všechny 4 B. Do payloadu, neboli obsahu nRF905 rámce je přidávána i 32 b adresa odesílatele, aby bylo možné na straně přijímače získat adresu, na kterou se posílá potvrzení. Dále je přidána 6 bitová délka packetu, tedy délka payload části rámce v bytech, maximální hodnota pak dosahuje  $2^6$  tedy 32. Zbylé 2 bity z předchozího bajtu je využito k předání informace o typu komunikace. Následuje samotný obsah, maximální délky 19 bytů a poté autentizační token zprávy.

Celkem je tedy přenášeno obvodem nRF905:

#### 8.3.2 Šifrování packetu

K šifrování je využit proudový algoritmus ChaCha20, šifruje se vše od dvoubitového typu packetu až po konec autentizačního tokenu. Autentizační token je rovněž počítán



Obr. 35. Formát přenášeného rámce

Tab. 9. Formát přenášeného rámce

Délka [bit]	Délka [Bajty]	Význam
10	1,25	preambule
32	4	cílová adresa
32	4	zdrojová adresa
6	0,75	délka
2	0,25	typ packetu
0-152	0-19	obsahu (19 bytů)
64	8	autentizační token (8 bytů)
16	2	kontrolní součet

algoritmem ChaCha20, na použitý klíč k šifrování celého packetu se operací XOR aplikuje obsah packetu. Obvykle se například u HMAC používá zřetězení klíče a obsahu a výpočet hash funkce, ale jelikož je maximální délka packetu stejná jako délka klíče, byla zvolena kombinace operací XOR. Z takto vzniklého nového klíče kombinací samotného klíče a obsahu je poté vygenerován keystream délky 8 bytů a ten je následně použit jako autentizační token.

### 8.3.3 Generování klíče

Jako zdroj náhodnosti na straně přijímající stanice byl zvolen rozdíl mezi dvěma oscilátory používanými MCU ATmega1284P. První z nich je vnitřní 128 kHz oscilátor používaný pro obvod watchdog, druhý je externí oscilátor s frekvencí v mém případě 12 MHz, kterým je řízen zbytek MCU.

Watchdog je obvod, který v běžném nastavení provede restart procesoru pokud mu přeteče vnitřní čítač, tedy pokud vznikne chyba programu a dojde k zacyklení a neprovede se příkaz nulující čítač watchdogu, celý mikrokontrolér se restartuje. Tento čítač je řízen v případě AVR procesorů inkrementován vestavěným 128 kHz oscilátorem. Režimu watchdog je možné přepnout do režimu, ve kterém místo restartování dochází pouze k vyvolání přerušení. V obsluze tohoto přerušení je přečten stav jednoho čítače řízeného hlavním 12 MHz oscilátorem a je využit poslední bit této hodnoty. Před využitím této hodnoty jako klíče je jako filtr využit Jon Von Neumanův debias algoritmus, který propustí pouze měnící se hodnoty. V případě stále se opakujících stejných

hodnot tak nedojde k použití slabého klíče.

#### 8.3.4 Distribuce klíčů

Klíče jsou generovány na přijímající stanici a distribuovány do bezdrátových senzorů během přenosu potvrzovacích packetů.

Při prvním zapnutí bezdrátového senzoru je k přenosu použit takzvaný tovární klíč, ten je společný pro všechny snímače a přijímače a je přímo součástí programu, uložen je ve FLASH paměti. Tato paměť určená k uchování programu a může být při programování zamknuta. Po zamčení ji již není možné přecíst programátorem, uložení klíče je tedy relativně bezpečné. U továrního klíče se jako nonce používá adresa přijímače. Ta je bohužel neměnná, tedy tovární klíč je bohužel použit vícekrát, i když pouze v době instalace nového snímače.

Jakmile je na straně přijímače vygenerován klíč, je tento klíč uložen do vnitřní EEPROM paměti přijímače a poté je distribuován v potvrzovacích packetech.

Jedná se o klíče délky 256 b, tedy 32 B ty jsou tedy delší, než přenášená informace, přenos tedy musí být rozdělen do 2 potvrzovacích packetů. Jakmile bezdrátový snímač přijme celý klíč, přepne se na něj a následující packety již šifruje tímto klíčem, pokud by došlo ke smazání klíčů v přijímači, nastal by problém, sice řešitelný, ale z pohledu bezpečnosti by toto řešení mohlo umožnit útok, proto se prvně vše ukládá do EEPROM a až poté vysílá.

Přijímající stanice udržuje dvojici klíčů, jakmile jeden klíč zestárne, je vygenerován nový klíč a ten se začne distribuovat k bezdrátovému snímači.

#### 8.3.5 Možné útoky

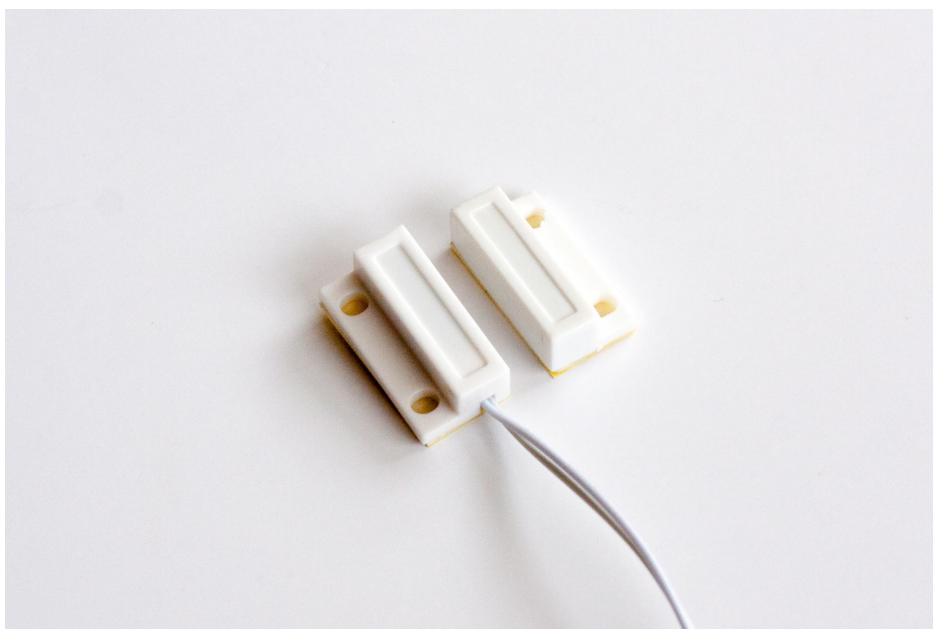
Množství přenášených informací je opravdu malé, obvykle 1-2 B samotné informace, ovšem počet pokusů na útok na klíč je rovněž omezen. Každý přenášený packet po vygenerování vlastních klíčů využívá jiné nonce, tedy klíče jsou pokaždé jiné. Jediný problém je tedy tovární klíč, tedy klíč, kterým se šifruje prvních několik packetů po připojení snímače. Pokud by tedy na tento klíč někdo vedl útok hrubou silou, bylo by potřeba vzhledem k 64 b délce autentizačního klíče  $3,4 \cdot 10^{38}$  pokusů.

## 9 SNÍMAČE

Snímače byly voleny s ohledem na nízkou spotřebu vzhledem k běhu, na navržené platformě bezdrátového snímače s mikrokontrolérem ATmega644PA. Byly testovány zástupci snímačů často používaných v bezpečnostních aplikacích v souladu se zaměřením oboru studia a rovněž snímače využívané v meteorologii.

### 9.1 Magnetický kontakt

K detekci otevření stavebních otvorů jako okna, dveře, vrata, rolety se využívají magnetické kontakty. Ty jsou složeny z permanentního magnetu na jedné straně a jazýčkového kontaktu na straně druhé. Pokud se magnet vzdálí od jazýčkového kontaktu, pak se tento jazýčkový kontakt rozeprve a přestane vést elektrický proud.



Obr. 36. Magnetický kontakt

#### 9.1.1 Jazýčkový kontakt

Jedná se o součástku obvykle složenou ze dvou magneticky měkkých kontaktů umístěných velmi blízko sebe, jedná se o vzdálenosti v setinách milimetrů. To celé je hermeticky uzavřeno v inertním plynu, případně vakuu a zataveno ve skleněné kapsli. Při umístění jazýčkového kontaktu rovnoběžně s magnetickými siločárami dostatečně silného permanentního magnetu se na koncích kontaktů vytvoří opačná magnetická polarita a kontakty prohnou a sepnou. [13][17]

#### 9.1.2 Bezpečnostní varianty

Magnetické kontakty se liší dle úrovně odolnosti proti překonání, ty nejjednodušší je

možné překonat přiblížením dostatečně silného magnetu. Vyrábí se ale i kontakty se zvýšenou odolností proti překonání pomocí cizího magnetu, ty sestávají z více než jednoho jazýčkového kontaktu. Jedna z variant je použití dvojice jazýčkových kontaktů, jeden v magnetickém poli permanentního magnetu a druhý umístěný mimo toto pole, určený k hlášení sabotáže. Pokud útočník přiblíží silný magnet k takovému magnetickému kontaktu, pak jsou sepnuty oba kontakty najednou a je vyhlášen sabotážní poplach. [13][17]

Magnetické detektory se vyrábí ve variantách:

- s jedním jazýčkovým kontaktem
- s více jazýčkovými kontakty
- s funkcí spínací, nebo rozpínací
- s vestavěným ochranným obvodem
- s nebo bez vestavěné ochranné smyčky
- s takzvanou předmagnetizací

### 9.1.3 Programová obsluha

Ke čtení stavu magnetického kontaktu používaného v bezpečnostních aplikacích je nutné periodicky zkoušet vodivost jazýčkového kontaktu. Periody mohou být relativně dlouhé i v řádu sekund. Hodnota elektrického odporu při sepnutí je velmi nízká, není tedy nutné používat specifickou úroveň napětí, stačí tedy napětí 2,2 V používané mikrokontrolérem.

Ke čtení je možné přistupovat dvěma způsoby:

1. Trvale napájet jednu stranu kontaktu a číst druhou mikrokontrolérem reagujícím pouze na nástupnou/sestupnou hranu.
2. Periodicky probouzet mikrokontrolér v dostatečně bezpečném intervalu na velmi krátký čas, během kterého se na krátký čas zapne napájení do magnetického kontaktu a provede měření.

První varianta je velmi úsporná z pohledu mikrokontroléru, teoreticky je poté možné vypnout i oscilátor a spotřeba mikrokontroléru se poté přiblíží k řádům nA. Ovšem spotřeba samotného magnetického kontaktu a přívodního vedení může být velmi vysoká a hlavně v rozepnutém stavu jinak vysoká oproti sepnutému stavu.

Ve druhé variantě má mikrokontrolér větší spotřebu, jelikož je ho nutné často probouzet, střídá tedy úsporný režim, ve kterém běží oscilátor a čítač potřebný k probuzení

po daném intervalu a režim při kterém na krátkou chvíli začne napájet magnetický kontakt, změří výstup a odpojí napájení. Měření je velmi rychlé, intervaly měření mohou být poměrně dlouhé, až v řádu sekund, tato varianta je tedy velmi úsporná.

Tato aplikace vyžaduje přenášet informace o změně stavů otevřeno/zavřeno. Přenos musí být potvrzen a pokud dojde ke ztrátě vysílání, vysílání se musí zopakovat.

## 9.2 Člunkový srážkoměr

Jedná se o přístroj používaný k měření množství částic vody dopadajících z vody na dané území a čase, tedy k měření denních srážkových úhrnů.

Člunkový srážkoměr přivádí vodu na dělený překlápěcí člunek, jakmile se jedna polovina člunku naplní na příslušný objem vody, tak se člunek překlápí, voda se z prvního dílu člunku vylije a začne se plnit druhá polovina člunku.

### 9.2.1 Argent Data Systems 80422

Součástí sady meteorologických snímačů Argent Data Systems 80422, která se u nás prodává jako sada náhradních dílů k meteostanicím WH1080 a WH1090 je i člunkový srážkoměr.

Ten sestává z plastových výlisků přesných rozměrů. Vrchní část je ve tvaru nálevky a svádí dopadající vodu na člunek, přesněji polovinu člunku. Součástí konstrukce člunku je permanentní magnet a ten se ve chvíli kdy dochází k překlopení člunku přiblíží k jazýčkovému kontaktu a tím ho na krátkou dobu po dobu překlopení sepne. Jedno překlopení dle datasheetu značí 0,2794 mm. Jedná se podobně jako u magnetického kontaktu o využití jazýčkového relé.

### 9.2.2 Programová obsluha

Jazýčkový kontakt je sepnut pouze na dobu překlápění člunku, tedy opravdu velmi dlouhý interval rozpojeného kontaktu je vystřídán velmi krátkým intervalem sepnutí kontaktu kdy dochází k překlápění. Rovněž samotné překlápění trvá proměnný časový interval.

Použité zapojení obsahuje k jazýčkovému kontaktu sérově zapojený 10 k $\Omega$  rezistor omezující proud v době sepnutí přibližně na 220  $\mu$ A při 2,2 V, v rozpojeném stavu byl naměřen odpor 40 M $\Omega$ , tedy proud při napájení obvodu 2,2 V je dle Ohmova zákona pouhých 55 nA. Zvolená strategie měření tedy spočívá ve velmi dlouhém intervalu spánku mikrokontroléru, který je nastaven reagovat na zdroj externího přerušení. Jakmile je kontakt spojen, mikrokontrolér je probuzen, odpojí se napájení a dojde k odeslání naměřených dat. Po dostatečně dlouhém ochranném intervalu je opět připojeno napájení a mikrokontrolér převeden do režimu spánku.



Obr. 37. Člunkový srážkoměr

Tato aplikace nevysílá pravidelně a intervaly mezi nově naměřenými hodnotami mohou být velmi dlouhé. Vysílání tedy musí být potvrzeno a pokud není, tak dochází k opakování vysílání.

### 9.3 Teploměr DS18B20

DS18B20 firmy Dallas Semiconductor je digitální teploměr ve formě integrovaného obvodu, který je již při výrobě kalibrován a naměřené výsledky přenáší po sběrnici 1-Wire. 1-Wire je sběrnice umožňující po pouhém jednom datovém vodiči a jednom vodiči s uzemněním přenášet jak napájení, tak naměřená data rychlostí 16 kb/s na velké vzdálenosti. Limity vzdáleností jsou až 500 m a počty snímačů připojených na jednom datovém vodiči dosahují stovek. K rozeznání jednotlivých 1-Wire snímačů každý kus obsahuje unikátní 64bitové adresy, ty bývají laserem vypáleny na pouzdro součástky.

Parametry:

- Měřený rozsah -55-125 °C
- Chyba měření  $\pm 0,5$  % v rozsahu -10-85 °C
- Rozlišení až 0,0625 °C
- Spotřeba během měření maximálně 1,5 mA



Obr. 38. Digitální teploměr DS18B20

- Spotřeba v režimu spánku 7,8 nA
- Rozsah pracovního napětí 3-5,5 V

### 9.3.1 Programová obsluha

Při zapnutí je nutné vyhledat adresu připojeného teploměru, následně se stačí posílat požadavek na měření, počkat zadaný interval dle datasheetu v rozsahu 93,75 ms pro 9 b rozlišení až 750 ms pro nejvyšší 12 b rozlišení výsledků měření a tento výsledek přečíst ve formě 16 b hodnoty.

Pro měření a hlavně záznam teploty je důležité dostat výsledek měření v čase měření, výpadek několika měření z mého pohledu nepovažuji za velký problém, ovšem pokud by přišlo opravdu staré měření po vysokém počtu pokusů, mohl by to být problém ve statistikách. Zvolené řešení tedy měří teplotu každou minutu, následně provede jeden pokus o odeslání výsledků a poté se na zbytek minuty uspí.

Teoreticky je možné ještě zvolit strategii spočívající v odesílání pouze změny teplot, ovšem poté je nutné potvrdit přijetí. Tato strategie je výhodná v případě malého počtu změn přenášených hodnot za dlouhou dobu, do procesu zaokrouhlení naměřených hodnot by bylo nutné zakomponovat i hysterezi, jinak této metodě hrozí značný nárůst přenosů a tedy i spotřeby energetické energie v zarušeném prostředí ve chvílích, kdy je teplota na rozmezí 2 hodnot. Praktické pokusy s následujícím DHT11 mě ovšem

dovedly ke zvolení první strategie.

#### 9.4 Vlhkoměr DHT11

Jedná se o velmi dostupný modul měřící relativní vlhkost v rozsahu 20-95 % a teplotu v rozsahu 0-50 °C. Rozsah naměřených teplot je relativně malý, tento snímač je tedy určený k využití v interiéru. Ke komunikaci sice používá sběrnici 1-Wire, ovšem tento obvod nemá při výrobě pro každé zařízení přiřazenu unikátní adresu, komunikace je tak sice zjednodušena, ale na druhou stranu není možné na jeden datový vodič připojit více kusů DHT11.

Parametry:

- Měřený rozsah relativní vlhkosti: 20-90 % rozlišení 1%, chyba měření  $\pm 5$  %
- Měřený rozsah teploty 0-50 °C, rozlišení 1 °C, chyba měření  $\pm 2$  °C
- Spotřeba během měření maximálně 2,5 mA
- Spotřeba v režimu spánku 100  $\mu$ A
- Dosah: až 20m
- Rozsah pracovního napětí 3-5,5 V

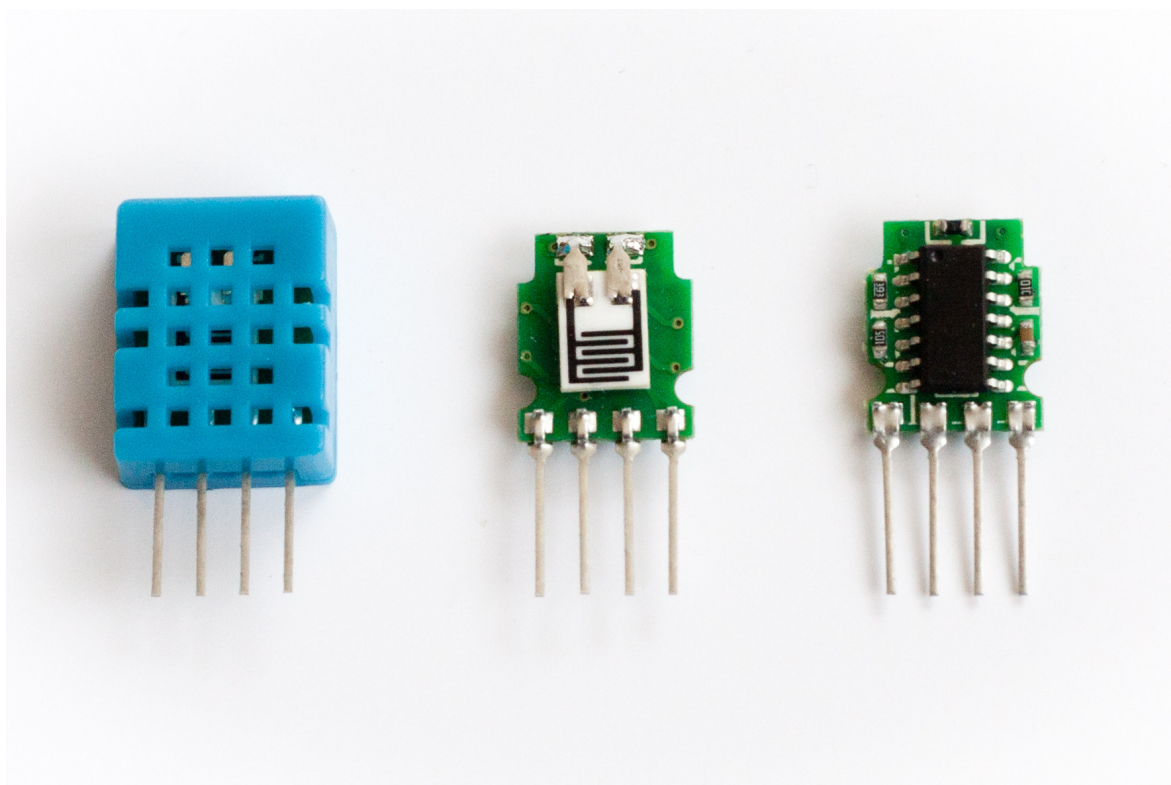
##### 9.4.1 Princip činnosti

DHT11 je odporový vlhkoměr, využívá se změny elektrolytické vodivosti na destičce s elektrodami. Velikost odporu je závislá nejen na vlhkosti, ale i na teplotě, proto je součástí i teploměr využívající termistor.

##### 9.4.2 Programová obsluha

Při zapnutí není nutné vyhledávat adresu připojeného vlhkoměru s teploměrem, stačí tedy posílat požadavek na měření, počkat na dokončení měření asi 180  $\mu$ s, přečíst výsledky měření a odpojit obvod od napájení na zbytek minuty.

Pro měření a hlavně záznamu vlhkosti je stejně jako u teploty důležité dostat výsledek měření v čase měření, zvolené řešení tedy měří teplotu každou minutu a poté provede jeden pokus o odeslání výsledků a poté se na zbytek minuty uspí. Ovšem existuje alternativní strategie zmíněná již u DS18B20 vhodná pouze do míst s minimálními změnami.



Obr. 39. Teploměr a vlhkoměr DHT11

## 9.5 Pasivní infračervený detektor

Využívá se k detekci pohybu v dané oblasti. K snímání využívá pyroelektrického snímače, který přijímá dopadající záření v infračerveném pásmu a přeměňuje ho v elektrický signál.

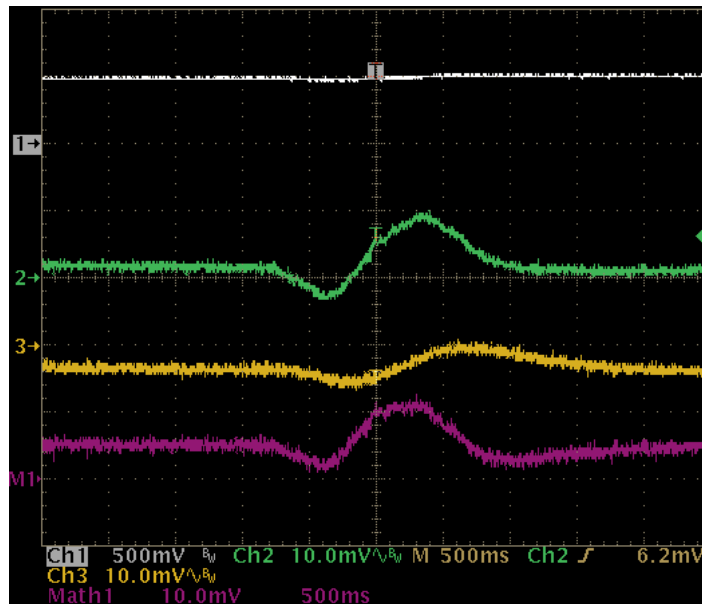
Před tímto snímačem, který měří pouze jednu hodnotu, je umístěn optický systém. Obvykle se jedná o sestavu Fresnelových čoček, která zajišťuje, aby pohybující se objekt vytvářel měnící se hodnotu. Pro lepší představu si stačí místo optiky představit pouhou sérii překážek tvořenou například plotem, při pohybu je tak chvíli objekt schován a chvíli je plně viditelný. Takové chování způsobí na pyroelektrickém snímači rozdíly naměřeného signálu. Fresnelovy čočky různě složitých konstrukcí řeší problémy takzvaných mrtvých zón a vyrábí se v různých tvarových variantách dle zamýšleného umístění detektoru, například čočky určené k umístění na chodbách, nebo čočky se sníženou citlivostí pro oblasti ve kterých se pohybují domácí mazlíčci. [13][17]

Za pyroelektrickým snímačem je umístěn elektrický obvod sledující rozdíly v měřeních a pokud je rozdíl dostatečný, pak je detekován pohyb. Tyto obvody obsahují několik zesilovačů, jelikož je naměřená hodnota velmi malá, rozdíl dle datasheetu k PIR325 je pouhý 20 mV.

Výsledky měření tedy není možné číst pouhým analogově-digitálním převodníkem obsaženým například v obvodu ATmega, signál je nutné správně napěťově posunout a zesílit.



Obr. 40. Znázornění funkce optického systému v PIR [20]



Obr. 41. Průběhy z PIR snímače během pohybu [20]

Spotřeba operačních zesilovačů jakožto samostatných součástek začíná u desítek  $\mu\text{A}$ , musí se nějakým způsobem ovládat a často je nutné pro ně vytvářet záporné napětí, které poté způsobuje rušení. Pro udržení spotřeby elektrické energie je tedy vhodné využít speciální integrované obvody.

### 9.5.1 Integrovaný obvod BISS0001

Jedná se o obvod určený ke zpracování signálu z pyroelektrického snímače s velmi malou spotřebou.

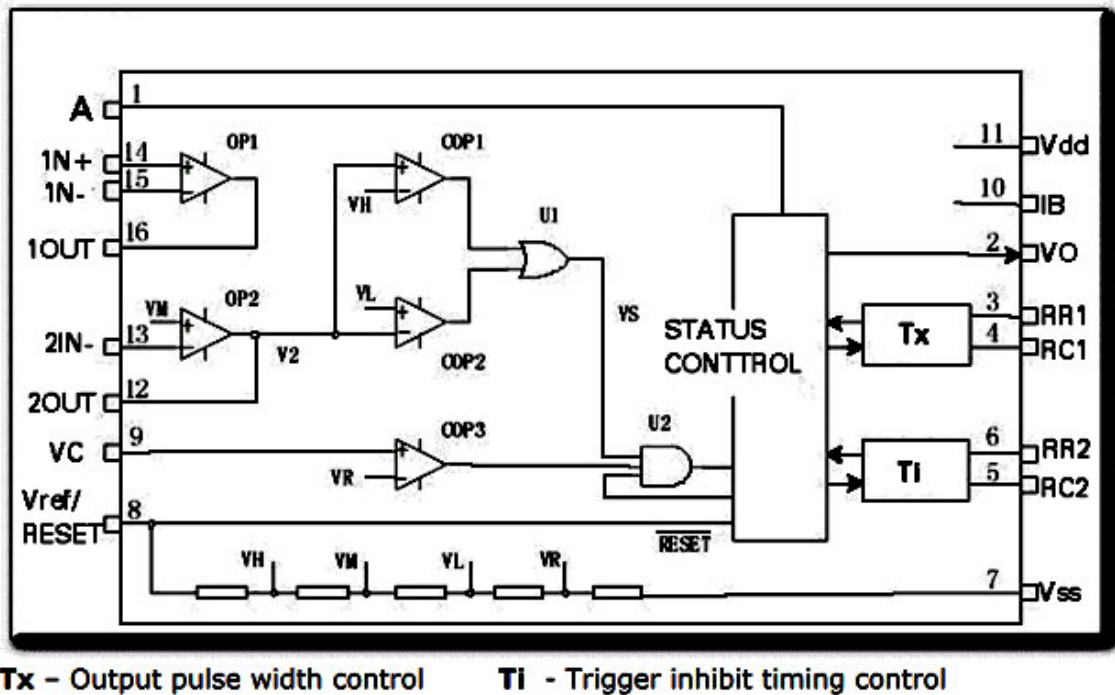
Parametry:

- Rozsah napětí 3-5V
- Spotřeba při napájení 3V  $50 \mu\text{A}$
- Spotřeba při napájení 5V  $100 \mu\text{A}$

Jak je vidět z parametrů, spotřeba tohoto obvodu je opravdu nízká, zvláště pokud je napájen nízkým napětím. Problém je, že se jedná o celý detektor, který musí být

konstantně napájen bez sebemenších výkyvů v napájení, není možné jako u předchozích snímačů provést měření jednou za čas a poté detektor vypnout, tak se i z pouhých 50  $\mu\text{A}$  spotřeby stává problém.

### Internal Block Diagram



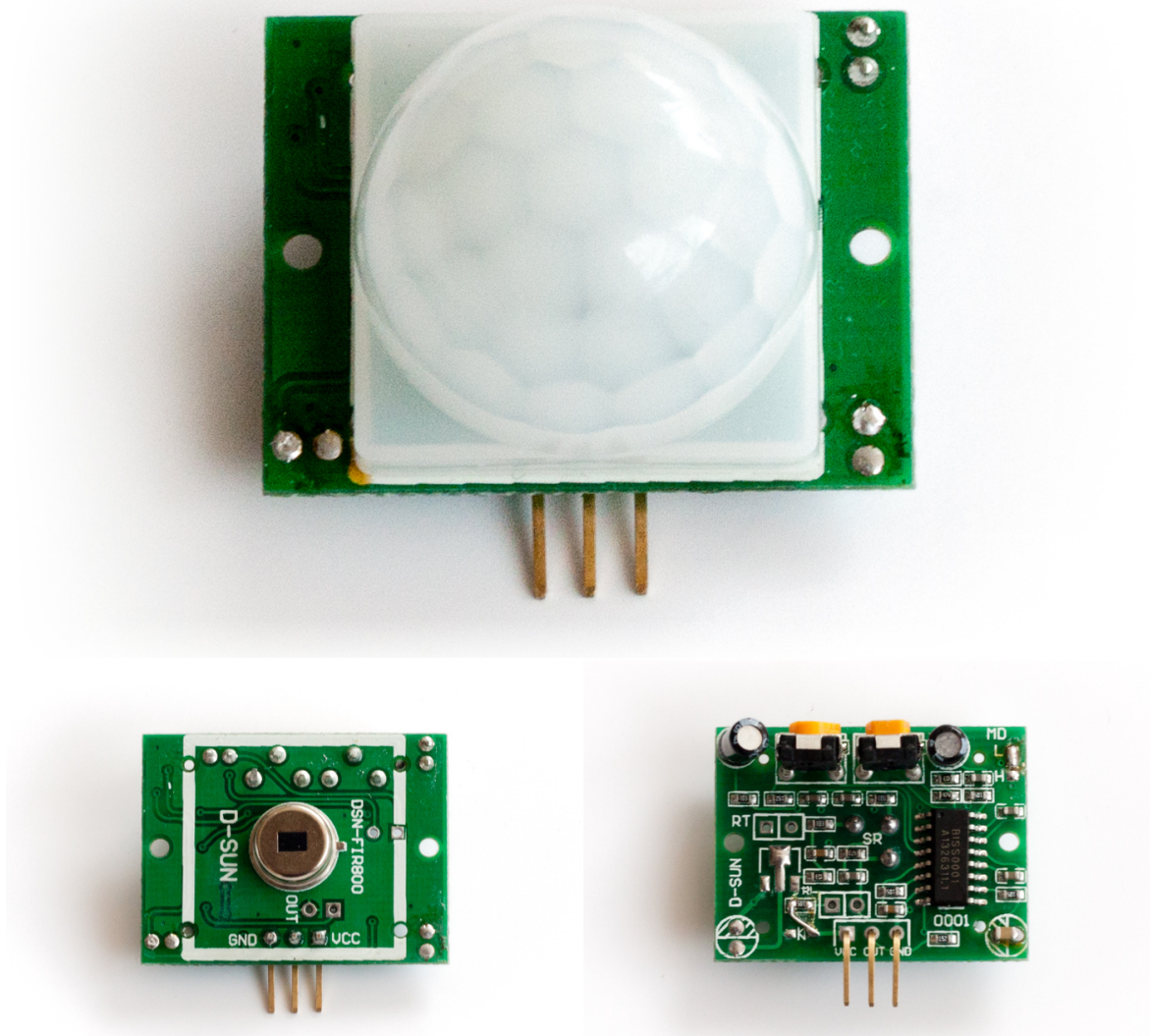
Obr. 42. Blokový diagram BISS0001 [26]

#### 9.5.2 Modul detektoru HC-SR501

Po otestování několika jiných variant byl zvolen modul detektoru HC-SR501. Tento modul byl od výroby vybaven lineárním stabilizátorem TPS7133, který mu umožňoval fungovat v rozmezí napájecího napětí 4,5-20 V, výstup tohoto stabilizátoru je 3,3 V, které jsou dostupné z napájecího obvodu LTC3108 na plošném spoji snímače. Lineární stabilizátor umístěný na HC-SR501 byl odstraněn a tím byla snížena spotřeba elektrické energie.

Parametry

- Úhel 140°
- Dosah nastavitelný v rozmezí 3-7 m
- Spotřeba proudu pod 60  $\mu\text{A}$
- Rozsah pracovních teplot -20-80 °C



Obr. 43. Modul detektoru pohybu HC-SR501

### 9.5.3 Programová obsluha

Detektor s obvodem BISS0001 má digitální výstup, jakmile je detekován pohyb přijde na tento vstup logická 1, tedy chování je podobné jako u snímačů založených na jazýčkových kontaktech, jen není nutné detekovat zákmity. Strategie čtení je tedy nastavit mikrokontrolér do režimu spánku, aby reagoval na externí přerušení a to jakmile je detekováno, tak odeslat výsledky. Poklesy napětí během vysílání mohou vyvolat falešnou detekci, proto se během vysílání odpojí napájení a po odvysílání se opět napájení připojí.

Tato aplikace vyžaduje přenášet informace o detekci pohybu. Přenos musí být potvrzen a pokud dojde ke ztrátě vysílání, vysílání se musí zopakovat.

## 9.6 Další uvažované snímače

Výběr snímačů byl velmi omezen na ty s pasivním principem snímání vzhledem k potřebné nízké spotřebě energie. Některé snímače a detektory byly za účelem dalších testů pořízeny fyzicky, ale nakonec nebyly z různých důvodů vybrány.

### 9.6.1 Tříštění skla

K detekci tříštění skla se v posledních letech již téměř výhradně využívají detektory monitorující okolní zvuky mikrofonom a detekující typický zvuk rozbití skla.

K účelu ukázky vlastních technologií vydal Texas Instruments Application Report SLAA351 a SLAA389, kde se píše o využití MCU MSP430 k detekci tříštění skla. Jako snímač je v tomto případě využit mikrofón. Spotřeba takového řešení má být v úspornější variantě softwaru 50  $\mu\text{A}$ . K pokusům byl pořízen od firmy Olimex vývojový kit pod označením MSP430-GBD. Provedené pokusy bohužel prokázaly velmi špatnou funkci. Na zvuk tříštění skla tento vývojový kit reagoval při až moc velkém přiblížení zdroje zvuku a na druhou stranu falešné poplachy spouštěl velmi náhodně, někdy stačilo v místnosti pouze s něčím klepnout, nebo pouze spustit hudbu. Přitom k testům byla použita varianta softwaru, která měla mít zlepšenu ochranu proti falešným poplachům. Od pokusů s detektorem tříštění skla tedy bylo upuštěno, není možné v rozsahu této práce přidat i spolehlivě fungující detektor tříštění skla.

Jiný pasivní způsob detekce tříštění skla je využití fólie složené ze 2 vodivých vrstev a mezi nimi izolační vrstva. Tuto fólii je možné přilepit na sklo a detekovat stejně jako magnetický snímač, pouze je možné navýšit intervaly mezi detekcí.

Dále je možné využít detektorů postavených na piezoelementu, ten vytváří energii, teoreticky je tedy možné využít k detekci komparátor vestavěný v MCU.

Oba zmíněné způsoby se ovšem již nyní téměř nepoužívají, spolehlivé detektory tříštění skla využívající zvuk je v nových instalacích nahradily a je tedy velmi složité získat i na pouhé pokusy snímače využívající jiné principy.

### 9.6.2 Detektor kvality ovzduší

Jako zástupce detektoru plynů proběhly pokusy s MQ 135 od firmy Futurlec. Bohužel ten ke své funkci zahřívá žhavicí vlákno, datasheet uvádí dobu zahřívání dokonce 24 hodin a udávaný výkon je 800 mW. Podobné parametry má většina autorem studovaných finančně dostupných detektorů plynů, tedy jejich použití by bylo velmi komplikované a k detekci plynů v ovzduší je tedy nutné volit jiné fyzikální principy.

## 10 OVĚŘENÍ A ZHODNOCENÍ VÝSLEDKŮ

Hlavním cílem praktické části bylo vytvořit prototypy, které budou fungovat celý den i noc. Pro tuto práci je tedy jako kritérium úspěchu zvolena doba nabíjení a doba vybíjení kondenzátoru. Testy byly zaměřeny na dobu potřebnou k nabíjení kondenzátoru z energie fotovoltaického článku, tedy stav ve dne. Dále byla testována doba vybíjení kondenzátoru s odpojeným fotovoltaickým článkem, tedy situace simulující noc. Testy délky vybíjení probíhaly u všech zvolených snímačů.

K testům použitý kondenzátor Heter již možná nemá původní kapacitu 4 F (vzhledem k zacházení během vývoje), ale na všechna měření byl použit stejný referenční kus. Nebyl tedy nakonec použit kvalitnější kondenzátor od firmy Kamcap, jelikož by bylo nutné provést některá měření znovu.

Některé snímače by byly schopné fungovat i při nižším napětím, ale měření byla provedena při zvoleném výstupním napětí na  $V_{OUT}$  obvodu LTC3108 3,3V, tedy konec měření nastal při poklesu napětí pod tuto hodnotu.

Testy snímačů vždy probíhaly při připojení jednoho snímače do platformy s ATmega644PA, odpojení fotovoltaického článku a dobití kondenzátoru na napětí 5V. Celková doba běhu byla určena ze záznamů na přijímající stanici. Byl vždy použit program určený speciálně pouze pro ten jeden snímač. V případech, pokud snímač neodesílá data periodicky byl tento program upraven, aby docházelo k periodickému vysílání po 10 minutách.

### 10.1 Platforma

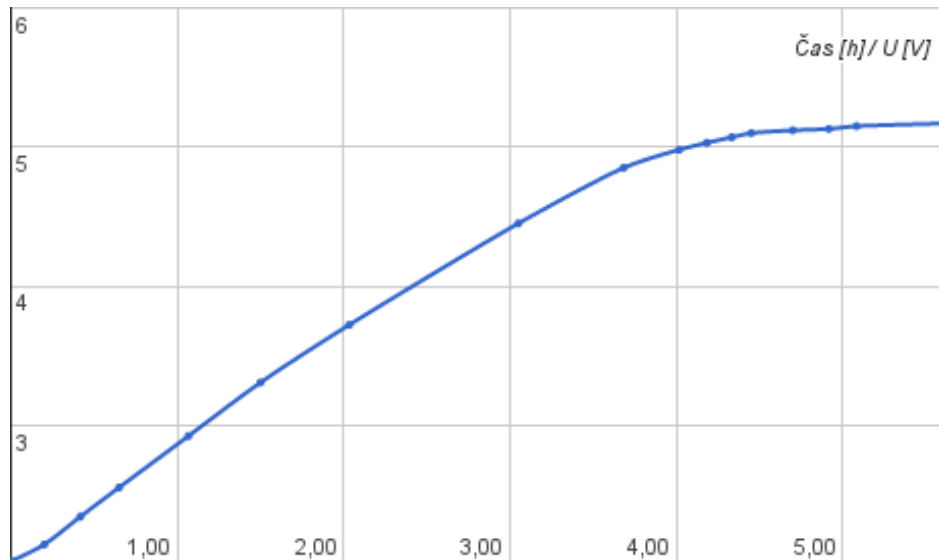
K otestování navržených snímačů byla použita platforma složená z obvodu s MCU ATmega644PA s elektrochemickým kondenzátorem Heter udávané kapacity 4 F. Dále byl použit přijímač s MCU ATmega1284P a modulem HiLink HLK-RM04 zajišťující komunikaci s počítačovou sítí.

Doba nabíjení z fotovoltaického článku byla měřena 13.5.2014 od 8:30. Fotovoltaický článek rozměrů přibližně 70x70 mm byl umístěn v místnosti za oknem, které mířilo jižním směrem a panel byl v horizontální poloze. Během doby měření se měnilo počasí a dokonce chvíli přšelo, přesto fotovoltaický článek celou dobu dodával dostatek energie a kondenzátor se dle grafu nabíjel až do 5 V téměř lineárně.

Doba nabíjení při plném provozu z 2 V do 5V je tedy dle pokusu přibližně 5 hodin. Za hodinu se napětí zvýšilo přibližně o 0,8 V. Minimální napětí 2 V nebylo zvoleno, jedná se o stav, při kterém je již obvodem LTC3108 odpojeno napájení  $V_{LDO}$  pro MCU. Jedná se tedy o minimální napětí na kondenzátoru v tomto obvodu a k dosažení nižší hodnoty by již bylo nutné silně zasáhnout do obvodu například zkratováním.

V místě měření na Vysočině bude v roce 2014 nejkratší den 14. prosinec, východ slunce

nastane v 7:44 a západ v 15:59. Nejkratší den má tedy 8 hodin a 15 minut, to je více jak potřebných 5 hodin k nabití, tedy platforma obstála a stihla se během dne nabít a to i za zhoršených světelných podmínek.



Obr. 44. Nabíjení kondenzátoru z fotovoltaického článku, závislost napětí na čase

Samotná tato platforma dokáže z 4 F kondenzátoru nabitého na 5 V do jeho na 3,3 V odeslat a přijmout potvrzení v počtu přibližně 5000. Čas běhu samotné platformy, při odesílání dat každých 10 minut, je 42 hodin.

Platforma se tedy dokázala během dne nabít a spotřeba energie je dostatečně nízká, aby 4 F kondenzátor dokázal napájet obvod i v době nedostupnosti zdroje energie, tedy v noci.

## 10.2 Magnetický kontakt

Tento typ snímače je velmi vhodný pro využití při napájení v použité platformě. Celá platforma s tímto připojeným snímačem, nastavená k odesílání prázdné hodnoty po 10 minutách z důvodů monitorování stavu, fungovala do vybití kondenzátoru 28 hodin.

## 10.3 Člunkový srážkoměr

Tento druh snímače je ideální pro provoz na vyvinuté platformě, jelikož se jedná o původně zamýšlené využití. Spotřeba energie při měření je velmi malá a rovněž počet vysílání během jednoho dne je velmi nízký, bylo by tak možné zvolit i menší kapacity kondenzátoru. Při testování docházelo k vynucenému odesílání stavu každých 10 minut, čistě z důvodů ověření funkčnosti, přesto do vybití kondenzátorů platforma s tímto snímačem komunikovala 42 hodin.

## 10.4 Teploměr DS18B20

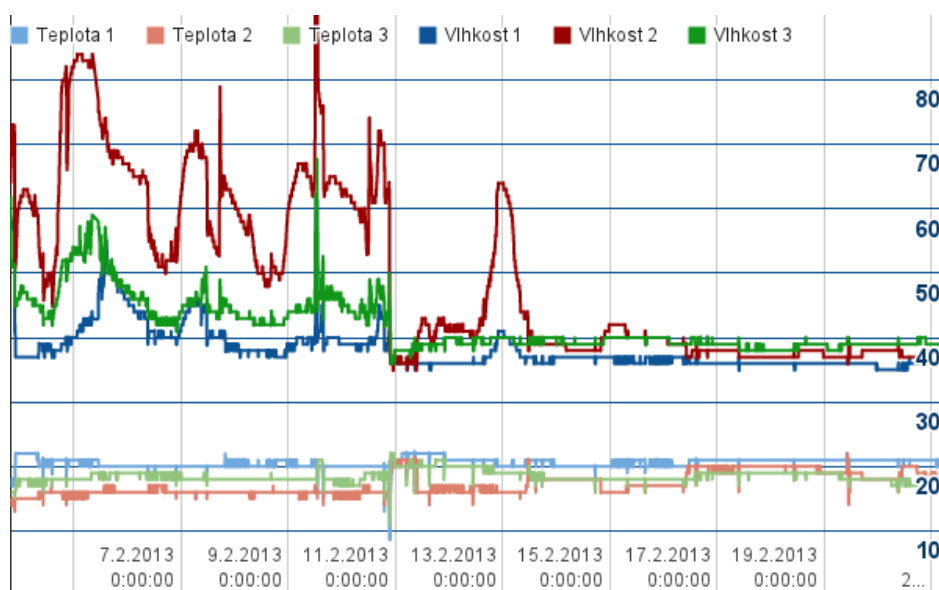
DS18B20 vyžaduje ke své funkci dle datasheetu napájení minimálně 3 V. Napájen byl tedy 3,3 V a na jedno nabití kondenzátoru na 5 V do poklesu na 3,3 V při měření a odeslání výsledku měření každou minutu vydržel takto fungovat 25 hodin a 30 minut. Tento druh snímače má sice spotřebu během měření 1,5 mA a samotné měření může trvat téměř sekundu, ale poté může být snímač dlouho vypnutý. Průměrná spotřeba je tedy velmi nízká a jedná se tedy o vhodný snímač pro napájení technikou Energy Harvesting. Mezi výhody patří i velký dosah sběrnice 1-Wire, tedy samotný snímač může být umístěn na místě s nedostatkem okolních zdrojů energie a stačí k němu natáhnout pouze dvojici vodičů.

## 10.5 Teploměr a vlhkoměr DHT11

Tento druh snímače je určený spíše pro měření vnitřních prostor, vzhledem k udávanému rozsahu měření. Trochu lépe je na tom v tomto ohledu varianta DHT22, která má ale větší spotřebu energie. Spotřeba energie je u tohoto snímače velmi malá a měření je dostatečně rychlé.

DHT11 vyžaduje ke své funkci dle datasheetu napětí minimálně 3 V. K měření a odesílání docházelo každou minutu, v takovém provozu byla výdrž celé platformy 23 hodin a 40 minut.

### 10.5.1 Zkušenosti z praxe



Obr. 45. Graf časového záznamu vlhkosti a teploty v novostavbě

Snímače DHT11 mnou byly dlouhodobě využívány v novostavbě k záznamu vlhkosti. Okamžitý přenos naměřených dat do počítačové sítě, v mém případě na službu Disk

od společnosti Google, umožnil okamžité vyhodnocení výsledků měření a případné okomentování, která činnost způsobila veliké nárůsty vlhkosti.

Pouhou změnou chování obyvatel spočívající v častějším větrání a změnou umístění sušáku na prádlo bylo dosaženo snížení relativní vlhkosti, která se ve špičkách původně dostávala i nad 80 %. Relativní vlhkost se tak snížila k hodnotám blízcím se 40 %, tím se vyřešily i problémy s plísněmi.

## 10.6 Pasivní infračervený detektor

Samotný obvod má dle datasheetu spotřebu  $50 \mu\text{A}$ , další součástky na modulu k této spotřebě dle měření přidávají dalších  $10 \mu\text{A}$ , tedy trvale je při napájení  $3,3 \text{ V}$  spotřeba  $60 \mu\text{A}$ . Během zapínání a detekce pohybu se spotřeba zvyšuje krátkodobě na  $300 \mu\text{A}$ . K měření těchto hodnot byl použit Victor 81D S/N 993576617, udávaná chyba měření  $\pm 1\%$ .

Spotřeba tohoto obvodu je sice v desítkách  $\mu\text{A}$ , to by se mohlo zdát málo oproti ostatním snímačům se spotřebou v  $\text{mA}$ , ale rozdíl je v nutnosti tento proud dodávat trvale. Další problém je potřeba napájení s minimálním rušením, jeden z testovaných detektorů byl velmi citlivý na sebemenší rušení a způsobovalo to velmi často falešné detekce. Naštěstí modul s obvodem BISS0001 fungoval správně i s poměrně nízkou spotřebou  $50 \mu\text{A}$ .

Na  $4 \text{ F}$  kondenzátor nabitý na  $5 \text{ V}$  do poklesu k  $3,3 \text{ V}$  byl celý bezdrátový senzor schopný fungovat 18 hodin, docházelo k pravidelnému vysílání po 1,5 minutách a pokaždé byl modul vypnut a znovu zapnut, během této doby tak došlo k 750 přijetí vysílání, což by odpovídalo přibližně stejnému počtu detekcí pohybu za těchto 18 hodin. 18 hodin je v porovnání s předchozími snímači méně, ale jedná se o dostatečnou hodnotu, aby snímač pokryl ze  $4 \text{ F}$  kondenzátoru na této platformě napájení nočního provozu, tedy nejdelsí noci roku 2014 v místě měření na Vysočině trvajících 15 hodin a 45 minut.

## 10.7 Shrnutí výdrže

Všechny zvolené varianty byly během testů schopné fungovat z nabitého kondenzátoru dostatečně dlouhou dobu a rovněž nabíjení z fotovoltaického článku bylo dostatečně rychlé pro zajištění 24/7 provozu.

## 10.8 Možná vylepšení

Použitá platforma byla složena z komponent dostupných v době konstrukce, se kterými má autor zkušenosti. Spotřebu energie by bylo možné snížit využitím kombinace mikrokontroléru a rádiového rozhraní ve formě System on Chip. Firma Energy Micro takové řešení slíbila představit, bohužel tato rodina produktů nebyla dostupná ani

Tab. 10. Výdrž při běhu pouze z nabitého kondenzátoru

Konfigurace platformy	Čas běhu [h]
Samotná platforma	42
Magnetický kontakt	28
Člunkový srážkoměr	42
Teploměr DS18B20	25,5
Teploměr a vlhkoměr DHT11	23,6
Pasivní infračervený detektor HC-SR501	15,7

v době psaní práce. Podobné řešení již existuje u více firem, například nRF9E5 od firmy Nordic Semiconductor kombinuje použitý nRF905 a velmi omezený osmibitový MCU. Tato řešení nejsou příliš rozšířena na trhu ve formě hotových modulů, jedná se obvykle o drahé vývojové kity. Vzhledem k technice napájení Energy Harvesting by bylo nakonec stejně nutné navrhnout plošný spoj osobou s dostatkem zkušeností s návrhem rádiových obvodů.

Výběr snímačů by bylo vhodné rozšířit i například o snímače analyzující plyny, běžně dostupná řešení využívají žhavicí element, který má moc vysokou spotřebu energie a samotné měření trvá velice dlouho.

Navrhnout spolehlivě fungující detektor tříštění skla by bylo zajímavé téma pro člověka se zkušenostmi se zpracováním signálů.

## ZÁVĚR

Práce se věnovala napájení bezdrátových snímačů technikou Energy Harvesting a to po stránce teoretické, tak i praktické, vytvořením prototypů ve formě desek elektrických plošných spojů.

Hlavní náplní teoretické části práce je rešerše na téma bezdrátových snímačů napájených metodou Energy Harvesting.

V praktické části byl vytvořen prototyp platformy ve formě plošného spoje bezdrátového snímače napájeného fotovoltaiickým článkem a uchovávacím energií ve dvouvrstvém elektrochemickém kondenzátoru. Dále byla vytvořena deska plošného spoje přijímače předávající naměřené hodnoty do počítačové sítě.

Na této platformě byly vyzkoušeny vybrané snímače fyzikálních veličin, které jsou schopny fungovat s minimální spotřebou. Byl vyzkoušen pasivní infračervený detektor pohybu a magnetické kontakty používané v bezpečnostním průmyslu a dále člunkový srážkoměr, teploměr a vlhkoměr, vhodné spíše k monitorování stavu počasí.

Pro každý snímač byl zvolen jiný druh programové obsluhy pro zajištění naprosto minimální spotřeby elektrické energie. Byly tak využity různé úsporné režimy mikrokontroléru a různé způsoby jak se z nich probudit.

K přenosu naměřené informace mezi bezdrátovým snímačem a přijímačem byl navržen vlastní formát přenášené zprávy, jehož součástí je i šifrování zprávy. Byl vybrán dostatečně bezpečný šifrovací algoritmus vhodný pro použití při nedostatku elektrické energie a byl vytvořen způsob distribuce klíčů využívající jediný symetrický šifrovací algoritmus.

Zvolené snímače fungovaly velmi dobře a jejich spotřeba byla ve všech případech dostatečně nízká k překlenutí doby nepřítomnosti zdroje energie během noci.

## SEZNAM POUŽITÉ LITERATURY

- [1] Atmel Corporation. *Datasheet ATmega164PA, ATmega324PA, ATmega644PA, ATmega1284P* [online] 2009 [cit. 2014-05-20]. Dostupné z: <http://www.atmel.com/Images/8152s.pdf>
- [2] BŘEZINA, Martin. *Studie získávání elektrické energie v leteckých aplikacích*. Brno, 2011. Bakalářská práce. Vysoké učení technické v Brně, Fakulta strojního inženýrství. Vedoucí práce Ing. Zdeněk Hadaš, Ph.D.
- [3] CATSOULIS, John. *Designing embedded hardware*. 2nd ed. Sebastopol: O'Reilly, 2005, xvi, 377 s. ISBN 05-960-0755-8.
- [4] (ED)., Kenneth G. Paterson). *Advances in cryptology - EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011 : proceedings*. Berlin: Springer, 2011. ISBN 9783642204647.
- [5] Energy Micro. *Datasheet EFM32TG822* [online] 2013 [cit. 2014-05-20]. Dostupné z: <http://www.silabs.com/Support Documents/TechnicalDocs/EFM32TG822.pdf>
- [6] Superkondenzátory. DVOŘÁK, Petr. *TZB-info - stavebnictví, úspory energií, technická zařízení budov* [online]. 2010 [cit. 2014-05-20]. Dostupné z: <http://oze.tzb-info.cz/teorie-obnovitelna-energie/6710-superkondenzatory>
- [7] Guidelines for Reliable Long Line 1-Wire Networks. *Analog, linear, and mixed-signal devices from Maxim* [online]. 2008 [cit. 2014-05-20]. Dostupné z: <http://www.maximintegrated.com/app-notes/index.mvp/id/148>
- [8] HADÁČEK, Martin. *Generování náhodných čísel na mikrokontrolérech AVR*. Brno, 2010. Bakalářská práce. České vysoké učení technické v Praze, Fakulta elektrotechnická, Katedra počítačů. Vedoucí práce Ing. Josef Hlaváč.
- [9] HAWKES, Allen, Alexander KATKO a Steven CUMMER. *A microwave metamaterial with integrated power harvesting functionality* [online]. 2013 [cit. 2014-05-20]. Dostupné z: <http://dx.doi.org/10.1063/1.4824473>
- [10] HUSÁK, Miroslav. Mikroelektronické zdroje energie z okolí – Energy harvesting. *DPS - Elektronika od A do Z*. 2013, roč. 2013, č. 2.
- [11] *InStepNanoPower* [online]. 2013 [cit. 2014-05-20]. Dostupné z: <http://www.instepnanopower.com/>
- [12] KEATING, Michael. *Low power methodology manual: for system-on-chip design*. New York, NY: Springer, c2007, xvi, 300 p. ISBN 9780387718194-.

- [13] KOLEKTIV, Luděk Lukáš a. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VerBuM, 2011, 279 s. ISBN 978-808-7500-057.
- [14] Linear Technology Corporation. *Datasheet LTC3108* [online] 2010 [cit. 2014-05-20]. Dostupné z: <http://cds.linear.com/docs/en/datasheet/3108fc.pdf>
- [15] Lithiové - Lithium Ion baterie. *FgFORTE s.r.o.* [online]. 2010 [cit. 2014-05-20]. Dostupné z: <http://www.fg-forte.cz/>
- [16] LOVECKÁ, Monika. *Návrh systému pro akumulaci elektrické energie zejména z obnovitelných zdrojů v podmínkách malých a středních instalací (rodinné domy, malé a střední bytové domy, provozovny, atp.)*. Plzeň, 2012. Diplomová práce. Západočeská univerzita v Plzni, Fakulta elektrotechnická. Vedoucí práce prof. Ing. Jan Škropil, CSc.
- [17] MALÁN, Martin. *Návrh elektronického zabezpečovacího systému pro ostrahu obytného objektu*. Plzeň, 2012. Bakalářská práce. Západočeská univerzita v Plzni, Fakulta elektrotechnická. Vedoucí práce Ing. Roman Hamar, Ph.D.
- [18] MANN, Burkhard. *C pro mikrokontroléry: ANSI-C, kompilátory C, spojovací programy - linkery, práce s ATMEL AVR a MSC-51, příklady programování v jazyce C, nástroje pro programování, tipy a triky*. Vyd. 1. Praha: BEN, 2003, 279 s. ISBN 80-730-0077-6.
- [19] MORÁVEK, P. a D. KOMOSNÝ. Asymetrická kryptografie v bezdrátových senzorových sítích. [online]. [cit. 2013-11-14]. Dostupné z: <http://access.feld.cvut.cz/view.php?cislocclanku=2009110005>
- [20] PIR detektor: skvělý sluha, ale zlý pán. MICHALEC, Libor. *HW.cz Vše o elektronice a programování* [online]. 2013 [cit. 2014-05-20]. Dostupné z: <http://www.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html>
- [21] PINKER, Jiří. *Mikroprocesory a mikropočítače*. 1. vyd. Praha: BEN - technická literatura, 2004, 159 s. ISBN 80-730-0110-1.
- [22] *Photovoltaic Geographical Information System (PVGIS)* [online]. 2012 [cit. 2014-05-20]. Dostupné z: <http://re.jrc.ec.europa.eu/pvgis/>
- [23] STEPHEN BEEBY, Neil White. *Energy harvesting for autonomous systems*. Norwood, Mass: Artech House, 2010. ISBN 978-159-6937-192.
- [24] STEPHEN BEEBY, Neil White. *Energy harvesting technologies*. 2nd ed. Editor Shashank Priya, D Inman. New York: Springer, c2009, xx, 517 s. ISBN 978-0-387-76463-4.

- [25] ŠENKERŮ, Roman. *Přednášky Kryptologie*. 2013. vyd. Zlín, 2013.
- [26] Shenzhen Sunstar Electronic Technology Co., Ltd. *Data-sheet BSS0001* [online] 2006 [cit. 2014-05-20]. Dostupné z: <https://learn.adafruit.com/system/assets/assets/000/010/133/original/BISS0001.pdf>
- [27] ŠIMONÍK, Pavel. *Autonomnost solárních systémů*. Zlín, 2010. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce doc. Mgr. Milan Adámek, Ph.D.
- [28] EnergyAware Profiler: Online Help. *Silicon Labs* [online]. 2014 [cit. 2014-05-20]. Dostupné z: <http://www.silabs.com/products/mcu/lowpower/pages/online-help-energyaware-profiler.aspx>
- [29] The Internet of Things. *Silicon Labs* [online]. 2014 [cit. 2014-05-20]. Dostupné z: <http://www.silabs.com/products/pages/internet-of-things.aspx>
- [30] Bee sensors take flight to help farmers. DE SOUZA, Paulo. *Commonwealth Scientific and Industrial Research Organisation* [online]. 2014 [cit. 2014-05-20]. Dostupné z: <http://www.csiro.au/en/Portals/Media/Bee-sensors-take-flight-to-help-farmers.aspx>
- [31] STRAKA, Michal. *Typový projekt elektroinstalace pro rodinný dům využívající fotovoltaický systém*. Brno, 2010. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav elektroenergetiky. Vedoucí práce Ing. Roman Hamar, Ph.D.
- [32] *Studijní materiály elektro: pro učební obor elektrikář – slaboproud* [online]. 2014 [cit. 2014-05-20]. Dostupné z: <http://www.mbest.cz/>
- [33] TEXAS INSTRUMENTS INCORPORATED. *TI LaunchPad* [online]. 2014 [cit. 2014-05-20]. Dostupné z: <http://www.ti.com/ww/en/launchpad/launchpad.html>
- [34] Using a RTLSDR dongle to validate NRF905 configuration. *Embedded Systems and Microcontrollers Portal* [online]. 2014 [cit. 2014-05-20]. Dostupné z: <http://www.embeddedrelated.com/showarticle/548.php>
- [35] Wireless Device Converts "Lost" Energy into Electric Power. *Engineering news from Duke Engineering* [online]. 2013 [cit. 2014-05-20]. Dostupné z: <http://www.pratt.duke.edu/news/wireless-device-converts-lost-energy-electric-power>
- [36] Elliptic Curve. *Wolfram MathWorld* [online]. 2014 [cit. 2014-05-20]. Dostupné z: <http://mathworld.wolfram.com/EllipticCurve.html>

- [37] ŽELEZNÝ, Jiří. *Asymetrická kryptografie pro bezdrátové sensorové sítě*. Brno, 2012. Bakalářská práce. Masarykova Univerzita. Vedoucí práce Mgr. Jiří Kůr.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

AC	Alternating current (střídavý proud)
AES	Advanced Encryption Standard
ARM	Advanced RISC Machine ( 32bitová architektura mikrokontrolérů )
AVR	označení osmibitové architektury mikrokontrolérů firmy Atmel
DC	Direct current (stejnoseměrný proud)
DES	Data Encryption Standard
DSA	Digital Signing Algorithm
EEPROM	Elektricky mazatelná, programovatelná paměť
ECDH	Elliptic curve Diffie–Hellman
ECDSA	The Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
e.r.p.	efektivní vyzářený výkon (effective radiated power)
UART	Universal Asynchronous Receiver-Transmitter
MCU	Jednočipový počítač (Microcontroller)
MEMS	Microelectromechanical systems
MPPT	Maximum power point tracking
RAM	Paměť s náhodným přístupem (Random-access memory)
RSA	asymetrická šifra, zkratka složená ze jmen Rivest, Shamir, Adleman
SMD	Surface mount device (součástka pro povrchovou montáž)

## SEZNAM OBRÁZKŮ

Obr. 1. Včela vybavená snímačem vyrobeným technologií MEMS [30].....	13
Obr. 2. Blokové schéma obecného Energy Harvesting systému .....	13
Obr. 3. Průměrný roční úhrn slunečního záření a roční energetický potenciál na území Evropy [21].....	15
Obr. 4. Typická konstrukce fotovoltaického panelu [23] .....	16
Obr. 5. Světelné pasti na povrchu fotovoltaického panelu [23] .....	17
Obr. 6. Bota vybavená 20 W generátorem energie [11] .....	19
Obr. 7. Lineární elektromagnetický generátor [2] .....	20
Obr. 8. Elektrostatický generátor [2] .....	20
Obr. 9. Nepiezoelektrický krystal.....	21
Obr. 10. Piezoelektrický krystal .....	21
Obr. 11. Schéma jednoduchého termoelektrického generátoru [23] .....	22
Obr. 12. Závislost činitele termoelektrické jakosti na teplotě vybraných materiálů [23] .....	23
Obr. 13. Metamateriál složený z pětice antén získávající energii z rádiového vysílání [35] .....	24
Obr. 14. Porovnání jednotlivých druhů zařízení určených k uchování elektrické energie [23] .....	25
Obr. 15. Villardův násobič [23] .....	27
Obr. 16. DC-DC měnič [23] .....	27
Obr. 17. Nízkonapěťový DC-DC měnič určený pro fotovoltaický panel [23].....	28
Obr. 18. Eliptické křivky [36].....	32
Obr. 19. Záznam napětí na fotovoltaickém panelu v čase.....	35
Obr. 20. Platforma bezdrátového snímače v krabici s fotovoltaickým článkem .....	36
Obr. 21. Ukázkové schéma zapojení LTC3108 [14].....	37
Obr. 22. Blokové schéma LTC3108 [14] .....	37
Obr. 23. Napěťové úrovně výstupů LTC3108 po zapnutí [14] .....	38
Obr. 24. Měření napětí na výstupu ze sekundárního vinutí. ....	39
Obr. 25. Měření napětí na vstupech CH1 (žlutý) - C1 a CH2 (zelený) - C2 .....	40
Obr. 26. Kondenzátory: zleva Panasonic 0,22 F, Panasonic 1 F, Heter 4 F a KAM-CAP 4 F .....	41
Obr. 27. Samovybíjení zvolených kondenzátorů.....	42
Obr. 28. Atmel ATmega644PA a EFM32TG822F32 .....	44
Obr. 29. Moduly rádiového obvodu nRF905 .....	50
Obr. 30. Platforma bezdrátového snímače s MCU ATmega644PA .....	51
Obr. 31. Platforma bezdrátového snímače s MCU EFM32.....	53
Obr. 32. Silicon Labs energyAware Profiler [28] .....	54

---

Obr. 33. První prototyp přijímací stanice na univerzálním plošném spoji .....	55
Obr. 34. Přijímací stanice s MCU ATmega1284P a převodníkem HLK-RM04 .....	56
Obr. 35. Formát přenášeného rámce .....	60
Obr. 36. Magnetický kontakt .....	62
Obr. 37. Člunkový srážkoměr .....	65
Obr. 38. Digitální teploměr DS18B20 .....	66
Obr. 39. Teploměr a vlhkoměr DHT11 .....	68
Obr. 40. Znázornění funkce optického systému v PIR [20] .....	69
Obr. 41. Průběhy z PIR snímače během pohybu [20] .....	69
Obr. 42. Blokový diagram BISS0001 [26] .....	70
Obr. 43. Modul detektoru pohybu HC-SR501 .....	71
Obr. 44. Nabíjení kondenzátoru z fotovoltaického článku, závislost napětí na čase. ....	74
Obr. 45. Graf časového záznamu vlhkosti a teploty v novostavbě .....	75

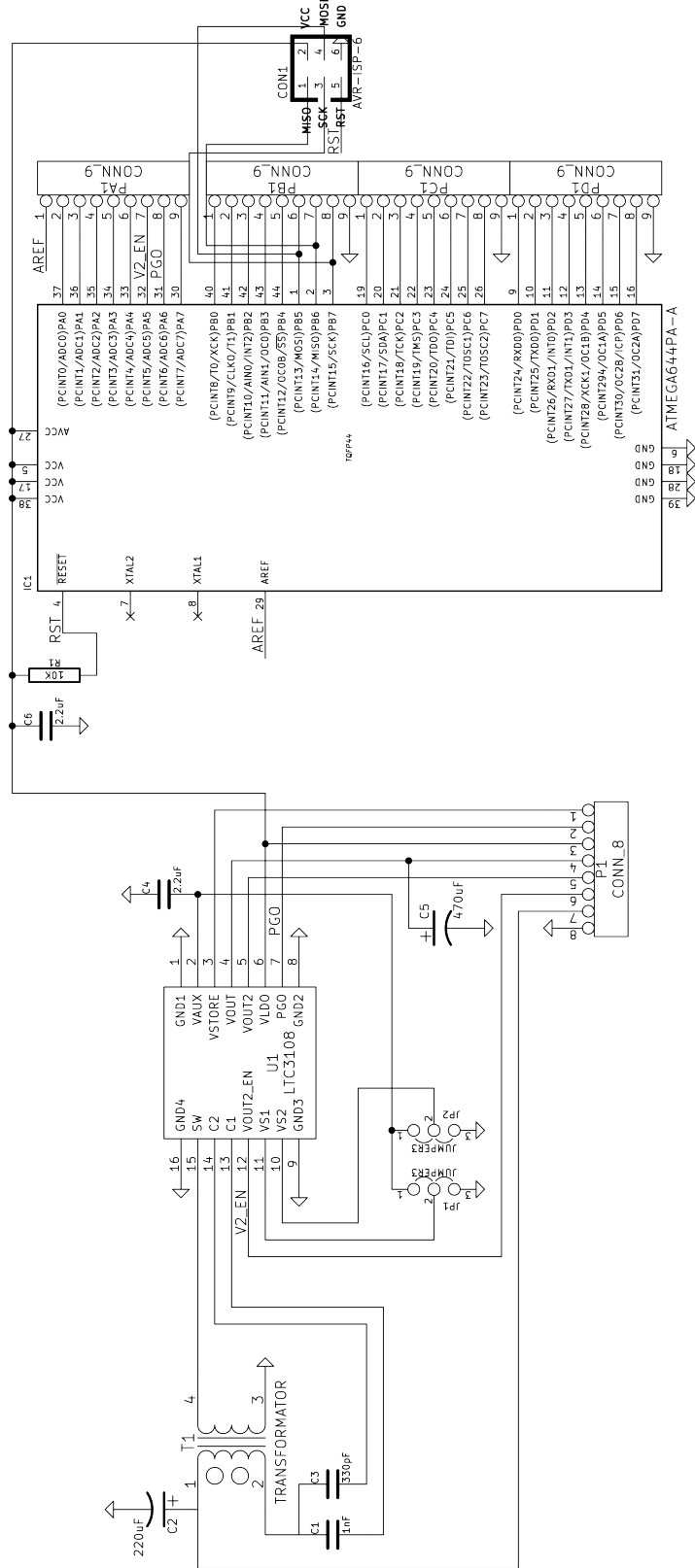
**SEZNAM TABULEK**

Tab. 1. Porovnání výkonové hustoty energie různých metod typu Energy Harvesting [10] .....	14
Tab. 2. Porovnání vlastností vibračních generátorů [2] .....	18
Tab. 3. Energie vibrací dle umístění v automobilu .....	19
Tab. 4. Srovnání nejpožívanějších typů průmyslových baterií [15] .....	26
Tab. 5. Srovnání srovnatelných délek klíčů v kryptografii [37] .....	32
Tab. 6. Tabulka spotřeby procesorů .....	43
Tab. 7. Porovnání rychlosti vykonávání šifrovacích algoritmů na daných MCU ...	47
Tab. 8. Spotřeba energie v režimech vysílání a příjmu .....	49
Tab. 9. Formát přenášeného rámce .....	60
Tab. 10. Výdrž při běhu pouze z nabitého kondenzátoru .....	77

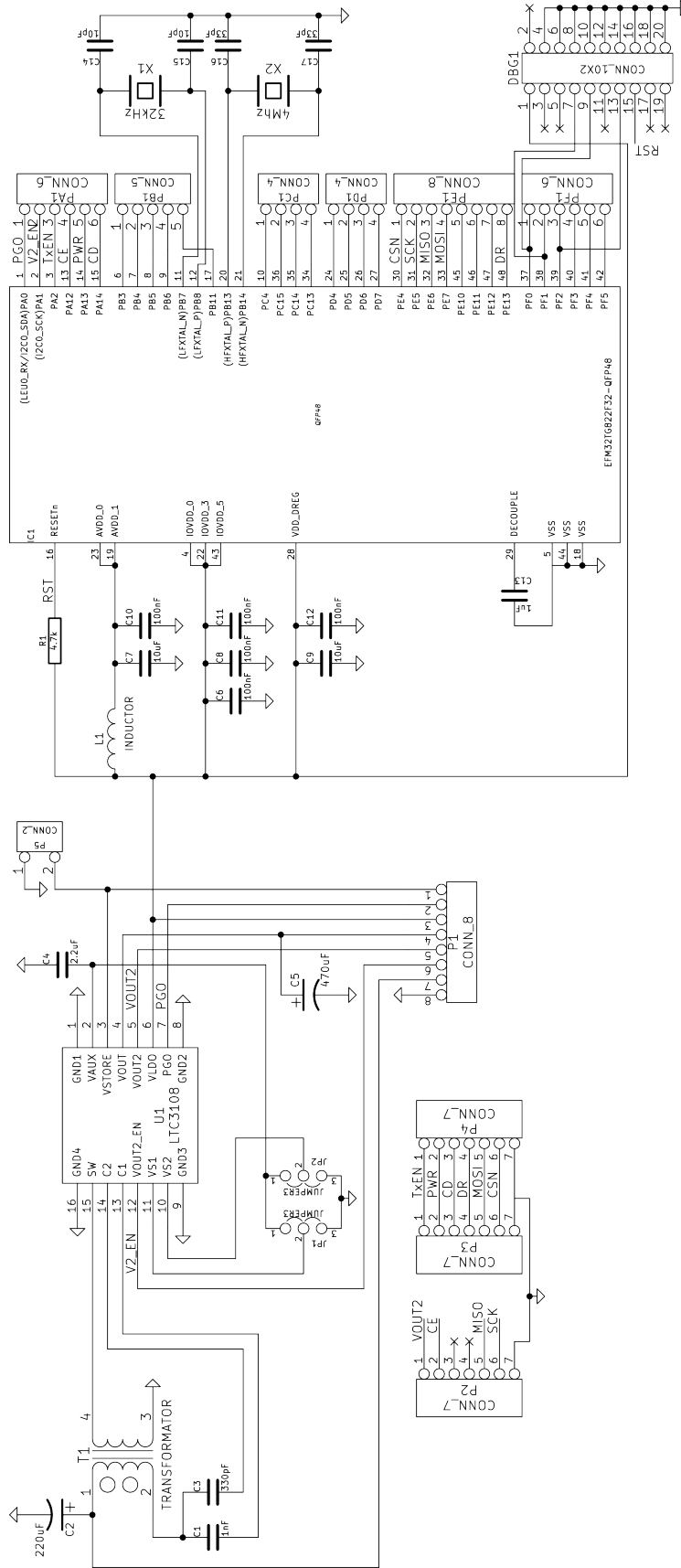
## SEZNAM PŘÍLOH

- P I. Schéma platformy snímače s ATmega644PA
- P II. Schéma platformy snímače s EFM32
- P III. Schéma přijímače
- P IV. Obsah přiloženého CD

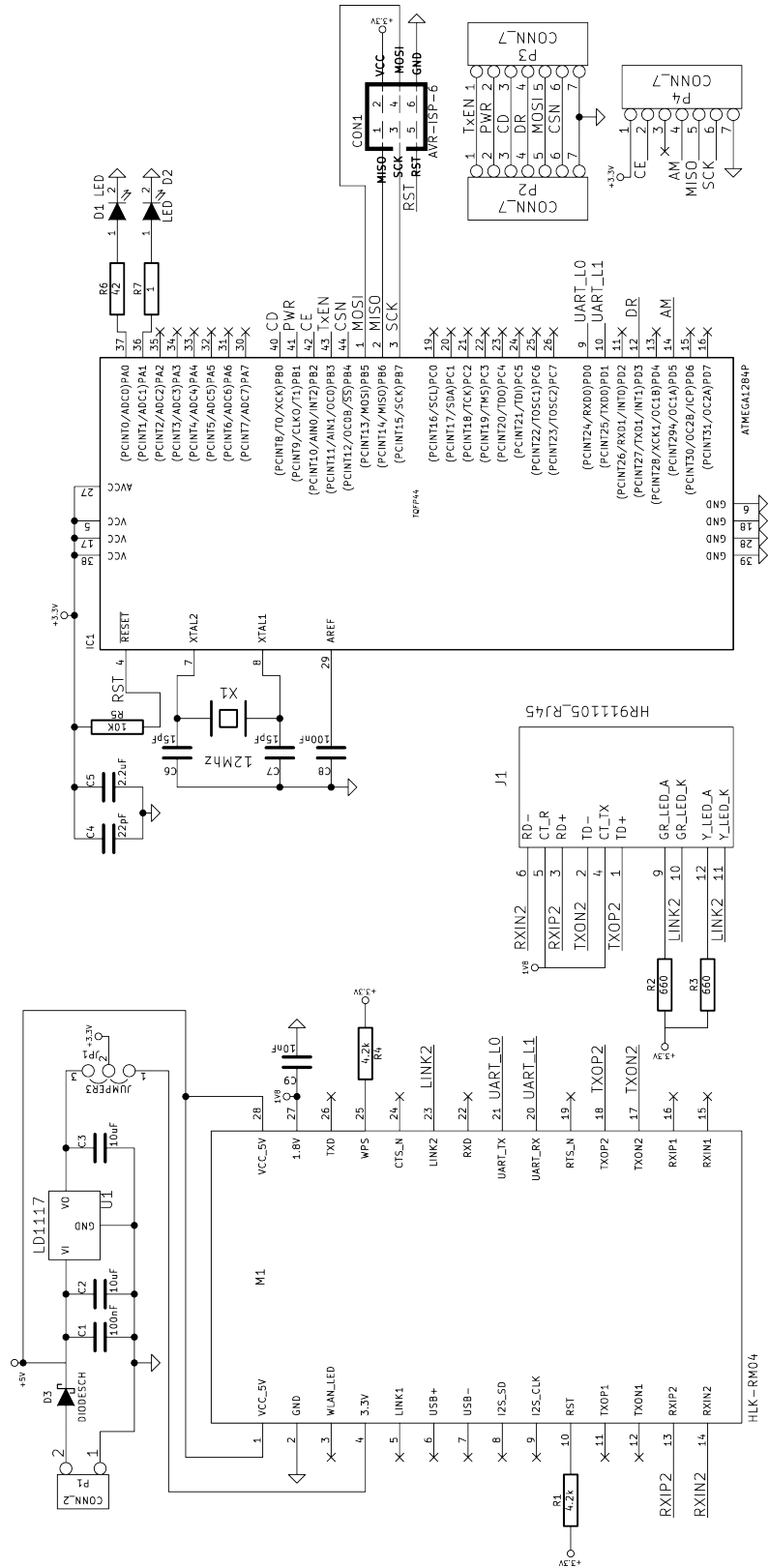
# PŘÍLOHA P I. SCHÉMA PLATFORMY SNÍMAČE S ATMEGA644PA



# PŘÍLOHA P II. SCHÉMA PLATFORMY SNÍMAČE S EFM32



# PŘÍLOHA P III. SCHÉMA PŘIJÍMAČE



## **PŘÍLOHA P IV. OBSAH PŘILOŽENÉHO CD**

Text této práce v elektronické podobě, zdrojové kódy a schémata plošných spojů, včetně gerber souborů použitých k jejich výrobě, je možno nalézt na přiloženém CD.