Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Konstrukce pokročilé IoT meteostanice se sondami

Bc. Lukáš Kovář

© 2021 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Lukáš Kovář

Systémové inženýrství a informatika
Informatika

Název práce

Konstrukce pokročilé IoT meteostanice se sondami

Název anglicky

Construction of an advanced IoT weather station with probes

Cíle práce

Diplomová práce je tematicky zaměřena na měření a přenos fyzikálních veličin bezdrátovou metodou a jejich vyhodnocení. Hlavním cílem práce je navržení funkčních prototypů IoT meteostanice a přidružených sond.
Dílčí cíle práce jsou následující:
- analýza vhodné architektury navrženého systému
- návrh přenosového protokolu
- jednoduchá předpověď počasí z naměřených dat
- implementace astronomických algoritmů (východ/západ Slunce, fáze Měsíce)
- zhodnocení ekonomické stránky a porovnání s konkurenty

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýze odborných informačních zdrojů. Teoretická část analyzuje současný stav technologií a poznání, rovněž se zabývá produkty konkurence. Praktická část práce je zaměřena na realizaci a konstrukci senzorové stanice a přidružených sond. Na základě získaných teoretických poznatků a výsledků praktické části práce budou formulovány závěry této práce.

Doporučený rozsah práce

60-80 stran

Klíčová slova

bezdrátová senzorová stanice, meteostanice, sonda, atmosférický tlak, teplota, vlhkost, osvětlení, konstrukce, astronomie, Slunce, Měsíc

---

Doporučené zdroje informací

Coombs, Clyde, and Happy Holden. Printed Circuits Handbook, Seventh Edition. New York, N.Y: McGraw-Hill Education, 2016. ISBN 978-0071833950

GU, Changyi. Building Embedded Systems [online]. Berkeley, CA: Apress, 2016. DOI: 10.1007/978-1-4842-1919-5. ISBN 978-1-4842-1918-8.

Horowitz, Paul. The art of electronics. New York, NY: Cambridge University Press, 2015. ISBN 978-0521809269

KLABZUBA, Jiří. Aplikovaná meteorologie a klimatologie. Praha: Česká zemědělská univerzita, 2001. Edice: 1. ISBN 978-80-213-0726-1

Ott, Henry W. Electromagnetic compatibility engineering. Hoboken, N.J: John Wiley & Sons, 2009. ISBN 978-0470189306

SMITH, Peter. Practical astronomy with your calculator or spreadsheet. Cambridge: Cambridge University Press, 2017. ISBN 978-1108436076

Walker, Jearl, Robert Resnick, and David Halliday. Halliday & Resnick fundamentals of physics. Hoboken, NJ: Wiley, 2014. ISBN 978-1118230718

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Ing. Alexandr Vasilenko, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 29. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 21. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 19. 03. 2021

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Konstrukce pokročilé IoT meteostanice se sondami" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2021 _____

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu práce Ing. Alexandru Vasilenkovi, Ph.D. za užitečné připomínky k práci, své rodině za podporu při realizaci mých nápadů a všem, kteří vydrží u čtení této práce až do konce.

Konstrukce pokročilé IoT meteostanice se sondami

Abstrakt

Práce si klade za cíl popis konstrukce prototypu IoT meteostanice skládající se z bezdrátové sondy snímající neelektrické veličiny (teplota, tlak, vlhkost, osvětlení, UV index) a hlavní stanice, na kterou jsou tato data předávána. Přenos dat probíhá pomocí nově navrženého protokolu. Meteostanice umožňuje také jednoduchou předpověď počasí z naměřených dat, předpověď východu a západu Slunce a fází Měsíce. Naměřená data je možné prohlížet buď přes webové rozhraní meteostanice připojené k lokální Wi-Fi síti nebo fyzicky pomocí dotykového barevného displeje. V úvodní části práce jsou popsána teoretická východiska v oblasti meteorologie, astronomie, teoretické informace zahrnující popis vhodných architektur systému, firmwaru, přenos dat paketovým rádiem a šifrování dat. V praktické části jsou využity informace z části teoretické a na jejich základě je vybrána vhodná architektura systému, vytvořen nový komunikační protokol obsahující šifrovací nádstavbu, implementovány algoritmy meteorologických a astronomických předpovědí. Práce se rovněž zabývá postupem výroby hlavní stanice i sondy, ekonomickou stránkou a porovnáním s konkurencí. V diskuzi jsou zhodnoceny výsledky vlastní práce a navrženy možnosti dalšího rozvoje zařízení. V závěrečném ustanovení je zhodnocena celá práce a dosažení jejích vytyčených cílů.

Klíčová slova

bezdrátová senzorová stanice, meteostanice, sonda, atmosférický tlak, teplota, vlhkost, osvětlení, konstrukce, astronomie, Slunce, Měsíc

Construction of an advanced IoT weather station with probes

Abstract

The work aims to describe the design of a prototype IoT weather station consisting of a wireless probe sensing non-electrical quantities (temperature, pressure, humidity, lighting, UV index) and the main station to which these data are transmitted. Data transfer takes place using a newly designed protocol. The weather station also allows simple weather forecasting from measured data, Sunrise, Sunset and Moon phases calculation. The measured data can be viewed either via the web interface of the weather station connected to the local Wi-Fi network or physically using the touch color display. The introductory part of the thesis describes the theoretical basis in the field of meteorology, astronomy, theoretical information, including a description of suitable system architectures, firmware, packet radio data transmission and data encryption. In the practical part, the information from the theoretical part is used and on the basis of them a suitable system architecture is selected, a new communication protocol containing an encryption superstructure is created, algorithms of meteorological and astronomical forecasts are implemented. The work also deals with the production process of the main station and probe, the economic side and a comparison with the competition. The discussion evaluates the results of own work and suggests opportunities for further development of the device. The final provision evaluates the whole work and the achievement of its set goals.

Keywords

wireless sensor station, weather station, probe, atmospheric pressure, temperature, humidity, illumination, construction, astronomy, Sun, Moon

Obsah

Seznam obrázků

Seznam tabulek

Seznam algoritmů

1 Úvod

V dnešní době jsou meteorologické stanice součástí každé modernější domácnosti. Všechny tyto stanice se od sebe však značně liší jak nabízenými funkcemi, přesností, designem, tak cenou.

Běžné stanice dokáží měřit teplotu, vlhkost a tlak. S pomocí výpočetních algoritmů a zadání dodatečných údajů, jako jsou například zeměpisné souřadnice, kde se stanice nachází, a aktuální čas, dokáží vypočítat další informace, jako je například východ a západ Slunce, aktuální fáze Měsíce či propočítávat aktuální pozice ostatních planet sluneční soustavy. Při využití těchto algoritmů meteostanice přebírá základní funkce astrolábu.

Značná popularita meteostanic je dána také tím, že tyto přístroje dokáží z naměřených dat předpovídat i počasí v krátkém intervalu, čímž mohou podat přesnější data pro určitou lokaci než globální předpověď.

Zásadním trendem 21. století jsou zařízení, která přidáním operačního systému a připojením k internetu získávají zcela nové možnosti využití. Taková síť inteligentních zařízení vytváří internet věcí (anglicky „Internet of Things“ - IoT). Tato zařízení lze mezi sebou navzájem propojit a vyměňovat si data.

Meteostanici vybavenou IoT funkcionalitou je možné využívat v tzv. chytré domácnosti. Data naměřená meteostanicí mohou být následně využita například vytápěcím systémem pro udržení optimální teploty v domácnosti, senzor vlhkosti meteostanice může sloužit pro regulaci větrání. Předpověď východu a západu Slunce poslouží pro ovládání žaluzií či rolet.

V rámci této diplomové práce není možné obsáhnout veškerou problematiku týkající se celé elektronické konstrukce a teoretických podkladů, neboť jednotlivé části jsou značně rozsáhlé.

2 Cíl práce a metodika

Diplomová práce je tematicky zaměřena na měření a přenos fyzikálních veličin bezdrátovou metodou a jejich vyhodnocení.

Hlavním cílem práce je navržení funkčních prototypů IoT meteostanice a přidružených sond.

Mezi dílčí cíle práce patří analýza vhodné architektury navrženého systému, návrh přenosového protokolu, jednoduchá předpověď počasí z naměřených dat, implementace astronomických algoritmů pro východ a západ Slunce a předpověď fází Měsíce. Jedním z dílčích cílů práce je také zhodnocení ekonomické stránky a porovnání s konkurenty.

Práce se v teoretické části zaměřuje na popis a postup výpočtu jednotlivých meteorologických a astronomických algoritmů a dále se věnuje teoretickým aspektům, které se týkají samotné stavby zařízení. Pozornost je věnována jak oblasti hardwaru, tak firmwaru, přenosu dat bezdrátovou metodou nebo oblasti kryptografie.

Praktická část je zaměřena na realizaci a konstrukci senzorové stanice a přidružených sond.

Informace obsažené v této diplomové práci jsou čerpány primárně z odborné literatury a publikací; jako sekundární zdroje jsou v práci využity odborné webové stránky.

Na základě získaných teoretických poznatků a výsledků praktické části budou formulovány závěry této práce.

3 Teoretická východiska

3.1 Definice IoT

IoT (Internet of Things, česky „Internet věcí“) popisuje síť malých zařízení - „věcí“, které jsou vybaveny senzory, softwarem a dalšími technologiemi za účelem připojení a výměny dat s jinými zařízeními a systémy přes internet. (Rouse, 2016)

Definice internetu věcí se vyvinula v důsledku sbližování celé řady technologií - analytiky reálného času, strojového učení, senzorů umístěných ve zboží a vestavěných systémů. (Rouse, 2016)

Na spotřebitelském trhu se pod pojmem IoT většinou skrývají produkty vztahující se ke konceptu „inteligentního domu“, včetně zařízení a spotřebičů (jedná se například o svítidla, termostaty, domácí bezpečnostní systémy, kamery, chytré meteostanice a další zařízení), které podporují jeden nebo více ekosystémů, do nichž jsou schopny se připojit a je možné je dálkově ovládat například pomocí notebooku či chytrého telefonu.

Zařízení internetu věcí je možné seskupovat a vytvářet tak datové sítě pokrývající celá města. Pokud tato zařízení ovládají veřejné prostředky (mosty, semafory, dohledové kamery, turnikety atp.), hovoříme o tzv. chytrých městech (smart cities). (Lai et al., 2020)

Rychlý nástup internetu věcí předznamenává jisté nebezpečí týkající se zabezpečení a ochrany soukromí. Vzhledem k tomu, že řada senzorů je teoreticky zranitelných, bylo zapotřebí vydat nové mezinárodní standardy týkající se této oblasti. (Lai et al., 2020)

3.2 Meteostanice

Meteorologická stanice je soubor přístrojů a senzorů, které měří atmosférické a případně půdní podmínky. Běžně měřenými proměnnými jsou například osvětlení, teplota, relativní vlhkost, déšť a vítr. (Bayer et al., 2017)

Existuje velké množství různých druhů meteostanic, od modelů používaných v domácnostech až po profesionální meteostanice, které jsou využívány například pro přesné měření v zemědělství či pro měření vstupních dat pro výpočetní modely předpovědí počasí.

Obrázek 1: Příklady meteostanic
Vlevo: Domácí meteostanice SENCOR SWS 230; Zdroj: mall.cz
Vpravo: Profesionální meteostanice ČZU; Zdroj: (Kořínek, 2010)

3.3 Meteorologie

Meteorologie je vědou na pomezí fyziky a chemie zabývající se zemskou atmosférou, zejména složením, strukturou a pohybem atmosféry. Hlavním cílem meteorologie je kompletní pochopení a předpověď atmosférických jevů (Ametsoc, 2012).

3.3.1 Základní pojmy

- Teplota
  - Teplota je meteorologický prvek udávající tepelný stav ovzduší, tj. schopnost vzduchu přijímat nebo předávat tepelnou energii. (Meteocentrum, 2020)
  - Pro měření teploty se využívá několik stupnic, pravděpodobně nejznámější je stupnice Celsiova, která je standardizována 0°C pro bod tání a 100°C pro bod varu. Celsiova stupnice se standardně využívá v oblastech, kde platí metrický systém (Britannica, 2014).
- Atmosférický tlak

  - Atmosférický tlak, také nazývaný jako barometrický tlak, je síla, kterou působí atmosféra Země na jednotkovou plochu v daném místě. Atmosférický tlak je proměnlivý, v daném místě kolísá okolo určité hodnoty, nejvyšších hodnot dosahuje při hladině moře a s rostoucí výškou klesá.

- Vlhkost
  - Vlhkost udává, jaké množství vody v plynném stavu (vodní páry) obsahuje dané množství vzduchu.

- Rosný bod
  - Rosný bod je teplota, při které je vzduch maximálně nasycen vodními parami (relativní vlhkost vzduchu dosáhne 100%).

- Intenzita osvětlení
  - Intenzita osvětlení je veličina definovaná jako světelný tok dopadající na jednotku plochy. Nejčastěji využívanou jednotkou je Lux (lx), který je definován světelným tokem 1 lumenu (lm) dopadajícího na plochu $1m^2$.

- UV index
  - Byl představen v roce 1992 v Kanadě v důsledku sílících obav ohledně zvyšování průniku UV radiace skrze ozónové díry a byl standardizován Světovou meteorologickou organizací a Světovou zdravotnickou organizací v roce 1994 (Fioletov et al., 2010).
  - Je navržen jako lineární škála, přímo úměrná intenzitě UV záření, které způsobuje popálení lidské kůže.

3.3.2 Počasí

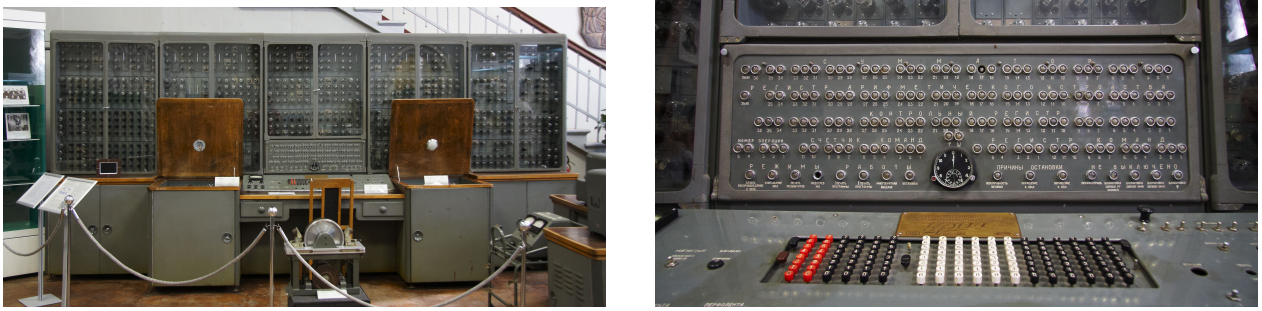
Počasí je okamžitý stav atmosféry (teplota, vlhkost) na určitém místě v určitém čase (Ametsoc, 2015).

Počasí je možné předpovídat pomocí numerických modelů či algoritmů, od velmi jednoduchých (používaných v domácích meteostanicích, jako je například algoritmus Zambretti) až po mimořádně přesné a náročné numerické modely, jakými je například model ALADIN.

3.3.2.1 Numerická předpověď počasí

Jako první v historii se o výpočet předpovědi ručně pokusil Lewis Fry Richardson mezi léty 1916 až 1922 (Brožková, 2010). První skutečný výpočet pro předpověď počasí byl proveden na počítači ENIAC (5. března 1950), přičemž byl použit model navržený meteorologem J. Charneym, který byl spolunaprogramován Johnem F. Neumannem (Brožková, 2010)(Černikovský – Brožková, 2019)(Hill, 2012, str. 216). Tímto krokem byl položen základ numerické předpovědi počasí.

V ČR (resp. tehdejším Československu) se teoretické základy a stavby modelů počaly rozvíjet již v 50. - 60. letech 20. století ve spolupráci s MFF UK[1] a ÚFA AV[2] (Černikovský – Brožková, 2019). V 60. letech probíhaly pravidelně výpočty na tehdy dostupné výpočetní technice (URAL1 [na obrázku č.2], URAL2, LEO360); v 80. letech se jednalo o stroje ROBOTRON EC1055, EC1057.



Obrázek 2: Ural-1
Vlevo: celkový pohled na mainframe; Zdroj: (Panther, 2009b)
Vpravo: indikátory, ovládací konzole; Zdroj: (Panther, 2009a)

3.3.2.2 Algoritmus Zambretti

Algoritmus Zambretti je jednoduchý algoritmus pro předpověď počasí. Tento algoritmus od společnosti Negretti and Zambra byl prvotně implementován v prognostickém zařízení pro předpověď počasí na počátku 20. století.

Algoritmus zvažuje absolutní hodnotu tlaku, trend tlaku, roční období a směr větru (ačkoliv směr větru a roční období mají malý vliv na změnu výstupu). Algoritmus funguje na principu výpočtu čísla Z, které je následně interpretovatelné z tabulkové hodnoty. (Scott, 2010)

[1]Matematicko-fyzikální fakulta Univerzity Karlovy
[2]Ústav fyziky atmosféry Akademie věd České republiky

Postup výpočtu (Scott, 2010):

Algoritmus 1 Zambretti: Výpočet atmosférického tlaku sníženého na hladinu moře

Z naměřeného tlaku „P“, teploty ve stupních Celsia „T“ a nadmořské výšky v metrech „h“ vypočítáme atmosférický tlak snížený na hladinu moře „P_0“:

$$P_0 = P\left(1 - \frac{0.0065 \cdot h}{T + 0.0065 \cdot h + 273.15}\right)^{-5.257} \tag{1}$$

Algoritmus 2 Zambretti: Výpočet trendu tlaku

Vypočítáme trend tlaku:

- Pokud je trend tlaku klesající, vypočítáme číslo Z následovně:

$$Z = 130 - \frac{P_0}{81} \tag{2}$$

- Pokud je trend tlaku setrvalý (neměnný), vypočítáme číslo Z následovně:

$$Z = 147 - \frac{5 \cdot P_0}{376} \tag{3}$$

- Pokud je trend tlaku rostoucí, vypočítáme číslo Z následovně:

$$Z = 179 - \frac{2 \cdot P_0}{129} \tag{4}$$

Algoritmus 3 Zambretti: Korekce směru větru

Upravíme číslo Z dle směru větru:

- Pro severní vítr změníme Z následovně:

$$Z = Z + 1 \tag{5}$$

- Pro jižní vítr změníme Z následovně:

$$Z = Z - 2 \tag{6}$$

Algoritmus 4 Zambretti: Korekce ročního období

Upravíme číslo Z dle aktuálního ročního období:

- Pokud je zima, změníme číslo Z následovně:

$$Z = Z - 1 \tag{7}$$

- Pokud je léto, změníme číslo Z následovně:

$$Z = Z + 1 \tag{8}$$

- Vyhledáme předpověď dle tabulky č.1 (Algoritmus Zambretti)

Tabulka 1: Tabulkové hodnoty algoritmu Zambretti

Predikční číslo (Z)	**Text předpovědi počasí**
1	stabilní klidné počasí
2	hezké počasí
3	hezké počasí, počátky destabilizace
4	vcelku dobré, později deštivo
5	deštivé počasí, začíná se zhoršovat
6	neklidné počasí, později déšť
7	přeháňky, později dojde ke zhoršení
8	přeháňky, později podstatné zhoršení
9	značně neklidné počasí, déšť
10	stabilní klidné počasí (1)
11	hezké počasí (2)
12	hezké počasí, možné přeháňky
13	vcelku příjemné, přeháňky pravděpodobné
14	deštivo v pestrých intervalech
15	proměnlivý déšť
16	neklid, občas déšť
17	déšť v četných intervalech
18	velmi neklidné, déšť
19	bouřky, silný déšť

Predikční číslo (Z)	Text předpovědi počasí
20	stabilní klidné počasí (1)
21	hezké počasí (2)
22	zlepšování počasí (vyjasňování)
23	vcelku příjemné, zlepšování
24	vcelku příjemné, pravděpodobně přeháňky
25	brzké přeháňky, zlepšování
26	proměnlivé počasí („aprílové počasí“)
27	spíše neklidné, později vyjasnění
28	neklidné, pravděpodobně zlepšení
29	neklidné, krátké záblesky hezkého počasí
30	velmi neklidné, občas hezké počasí
31	bouřlivo, pravděpodobné zlepšování
32	bouřlivo, silný déšť

Zdroj tabulky: (Scott, 2010)

3.4 Astronomie

Astronomie je exaktní věda, která se zabývá studiem hvězd a ostatních vesmírných těles, kvantitativním zkoumáním vesmíru a fyzikálními zákony, které jej řídí: pohyby jednotlivých objektů, strukturami, formováním a vývojem různých nebeských objektů. (Unsöld – Baschek, 2002)

3.4.1 Juliánské datum

Juliánské datum, často též nazývané jako juliánský den, označuje počet dní, které uběhly od 1. ledna 4713 před naším letopočtem (Techopedia, 2021).

Juliánské datum se běžně používá v informatice a astronomii k výpočtu rozdílu mezi počátečním a konečným datem (Techopedia, 2021; Britannica, 2021).

Výpočet juliánského dne probíhá následovně (Subsystems, 2017):

Algoritmus 5 Výpočet juliánského dne

1. Datum je zadáváno jako Y = rok, M = měsíc, D = den
2. Pokud je měsíc leden nebo únor, odečíst 1 od roku a přidat 12 k měsíci
3. Následně je zapotřebí provést následující výpočty:
   (a) A = Y / 100 a následně zapsat celočíselnou část
   (b) B = A / 4 a následně zapsat celočíselnou část
   (c) C = 2 - A + B
   (d) E = 365.25 * (Y + 4716) a zapsat celočíselnou část
   (e) F = 30.6001 * (M + 1) a zapsat celočíselnou část
   (f) JD = C + D + E + F - 1524.5

3.4.2 Lunární fáze (fáze Měsíce)

Fáze Měsíce vznikají díky tomu, že se mění vzájemná poloha Slunce, Země a Měsíce a pozorovatel pak vidí různě velkou část osvětlené měsíční polokoule. (Gabzdyl, 2020)

Fáze Měsíce jsou následující (Almanac, 2021):

Fáze	Viditelnost¨	Ilustrace	
		severní polokoule	jižní polokoule
Nov	Neviditelný		
Dorůstající srpek	Pozdní ráno až po setmění		
První čtvrt	Odpoledne až brzký večer		
Dorůstající měsíc	Pozdní odpoledne až většina noci		
Úplněk	Celá noc		
Couvající měsíc	Většina noci a brzké ráno		
Poslední čtvrt	Pozdní noc a ráno		
Ubývající srpek	Před rozedněním až odpoledne		

Tabulka 2: Fáze Měsíce
Zdroj: (Almanac, 2021)
Zdroj ilustrací: (Almanac, 2007)

3.4.2.1 Předpověď lunárních fází

Předpovídat fáze Měsíce je možné několika způsoby. Mezi ty jednodušší patří tzv. naivní způsob.

Nov (tedy doba, kdy není povrch přivrácené strany měsíce osvětlen žádným slunečním světlem) se opakuje v poměrně pravidelných intervalech mezi 29.27 až 29.83 dny, přičemž dlouhodobý průměr činí 29.53059 dnů (29 dní, 12 hodin, 44 minut a 3 sekundy) (Espenak, 2019). Tento cyklus se nazývá synodický měsíc nebo také lunace. (Espenak, 2019)

Nejjednodušším způsobem, jak vypočítat aktuální fázi Měsíce je tedy porovnat ji s dobou, kdy byl nov a poté vypočítat, kolik měsíčních cyklů uběhlo. Toho je možné docílit tak, že je zjištěn počet dní od známého novu a poté jej vydělit dobou lunace. (Subsystems, 2017)

Dne 1.6.2000 ve 12:24:01 byl měsíc v novu. Vypočtená hodnota juliánského dne z tohoto data činí 2451549.5 (vůči této referenční hodnotě se bude počítat aktuální fáze Měsíce).

Příklad výpočtu fáze Měsíce pro den 1.3.2017 (Subsystems, 2017):

Algoritmus 6 Naivní výpočet fáze Měsíce pro den 1.3.2017

1. Vyjádření data jako Y = 2017, M = 3, D = 1
2. Jelikož je měsíc březen (M = 3), není zapotřebí upravovat hodnoty
3. Provedení následujících výpočtů
   (a) A = Y / 100 a zapsat celočíselnou část, tedy **A = 20**
   (b) B = A / 4 a zapsat celočíselnou část, tedy **B = 5**
   (c) C = 2 - A + B, tedy **C = -13**
   (d) E = 365.25 * (Y + 4716) a zapsat celočíselnou část, tedy **E=2459228**
   (e) F = 30.6001 * (M + 1) a zapsat celočíselnou část, tedy **F = 122**
   (f) JD = C + D + E + F - 1424.5, tedy **JD = 2457813.5**

Nyní, když je vypočítán aktuální juliánský den, je možné vypočítat, kolik dní uběhlo od zvoleného novu.
dnů od novu = 2457813.5 - 2451549.5 = 6264 dní
Tato doba se následně vydělí dobou lunace, díky čemuž je zjištěno, kolik novů uběhlo od stanoveného data:
počet novů = 6264 / 29.53 = 212.123 cyklů
Nyní je zapotřebí vynásobit necelou část čísla dobou lunace:
dní od cyklu = 0.123 * 29.53 = 3.63 dní od novu
Tuto dobu je poté možné porovnat se samotnou dobou lunace a případně interpretovat dle tabulky č.2 (Fáze Měsíce).

Výpočty uvedené v algoritmu č.6 (Naivní výpočet fáze Měsíce pro den 1.3.2017) jsou velmi zjednodušené a ne zcela přesné, nicméně pro odhadnutí přibližné fáze Měsíce jsou dostatečné.

3.4.3 Předpověď východu a západu Slunce

Předpověď východu a západu Slunce je podstatně náročnější než předpověď lunárních fází, které byly popsány v předcházející kapitole. Při výpočtu východu a západu Slunce je zapotřebí brát v úvahu zjednodušený model celé sluneční soustavy, přičemž existuje celá řada algoritmů schopných vypočítat požadované informace. Některé algoritmy jsou jednodušší (slouží pouze pro orientaci), některé jsou velmi složité (počítají s korekcí rozptylu světla v atmosféře planety a dalšími parametry). (Saifee, 2016)

Dle (Strous, 2020) je poloha Slunce na obloze při pohledu z planety (například ze Země) určena čtyřmi pravidly:

- Časem.
- Pohybem planety okolo Slunce, ke kterému nedochází při konstantní rychlosti kvůli excentricitě oběžné dráhy planety.
- Úhlem mezi osou otáčení planety a rovinou oběžné dráhy planety, který se nerovná 90°. To způsobuje roční období.
- Umístěním/polohou pozorovatele na planetě, která určuje, do jaké výšky na obloze se Slunce může dostat.

Pro potřeby této práce byla vybrána rovnice východu Slunce - „Sunrise equation“. Ta je vhodná pro poměrně přesné určení východu a západu Slunce, avšak pro zcela přesné astronomické výpočty není příliš vhodná. Dalším zajímavým způsobem výpočtu může být algoritmus východu/západu publikovaný v (Williams, 1990).

Postup výpočtu rovnice východu/západu Slunce je následující (Strous, 2020), zjednodušená verze z tohoto zdroje je rovněž na wikipedii pod heslem „Sunrise equation“:

Algoritmus 7 Sunrise equation: Výpočet aktuálního juliánského dne

$$n = J_{datum} - 2451545.0 + 0.0008 \tag{9}$$

kde:
n je počet dní od poledne 1. ledna 2000
J_{datum} je aktuální juliánské datum
2451545.0 je ekvivalentem juliánského roku pro 1.1.2000, poledne
0.0008 je zlomek juliánského dne pro započtení přestupných sekund a terestrického (dynamického) času

Algoritmus 8 Sunrise equation: Výpočet středního slunečního času

$$J^* = n - \frac{l_w}{360^\circ} \tag{10}$$

kde:
J^* je aproximace středního slunečního času při n vyjádřená jako juliánský den s denním zlomkem
l_w je zeměpisná délka pozorovatele na Zemi (západ je záporný, východ je kladný)

Algoritmus 9 Sunrise equation: Výpočet střední sluneční anomálie

$$M = (357.5291 + 0.98560028 \times J^*) \ mod \ 360 \tag{11}$$

Algoritmus 10 Sunrise equation: Výpočet rovnice středu

$$C = 1.9148 \sin(M) + 0.0200 \sin(2M) + 0.0003 \sin(3M) \tag{12}$$

kde
1.9148 je koeficient rovnice středu pro planetu, na které se nachází pozorovatel (v tomto případě se jedná o Zemi)

Algoritmus 11 Sunrise equation: Výpočet ekliptické zeměpisné délky

$$\lambda = (M + C + 180 + 102.9372) \ mod \ 360 \tag{13}$$

kde
102.9372 je hodnota argumentu šířky pericentra

Algoritmus 12 Sunrise equation: Výpočet slunečního tranzitu

$$J_{tranzit} = 2451545.0 + J^* + 0.0053 \sin(M) - 0.0069 \sin(2\lambda) \tag{14}$$

kde:
$J_{tranzit}$ je juliánské datum pro místní skutečný sluneční tranzit (nebo sluneční poledne)
2451545.0 je ekvivalentem referenčního juliánského roku (1.1.2000)
$0.0053 \sin(M) - 0.0069 \sin(2\lambda)$ - jedná se o zjednodušenou verzi časové rovnice (rozdíl mezi pravým a středním slunečním časem)

Algoritmus 13 Sunrise equation: Výpočet deklinace Slunce

$$\sin\delta = \sin\lambda \times \sin 23.44^\circ \tag{15}$$

kde:
δ je deklinace Slunce
23.44° je maximální sklon rotační osy Země k Slunci

Algoritmus 14 Sunrise equation: Výpočet hodinového úhlu

Rovnice obsahuje korekce pro atmosférický lom a průměr solárního disku

$$\cos\omega_o = \frac{\sin(-0.83^\circ) - \sin\phi \times \sin\delta}{\cos\phi \times \cos\delta} \tag{16}$$

kde:
ω_o je hodinový úhel od zenitu pozorovatele
ϕ je severní zeměpisná šířka pozorovatele na Zemi (sever je kladný, jih záporný)

Algoritmus 15 Sunrise equation: Výpočet východu a západu Slunce

$$J_{vychod} = J_{tranzit} - \frac{\omega_o}{360^\circ} \tag{17}$$

$$J_{vychod} = J_{tranzit} + \frac{\omega_o}{360^\circ} \tag{18}$$

kde:
J_{vychod} - aktuální juliánské datum pro východ Slunce
J_{zapad} - aktuální juliánské datum pro západ Slunce

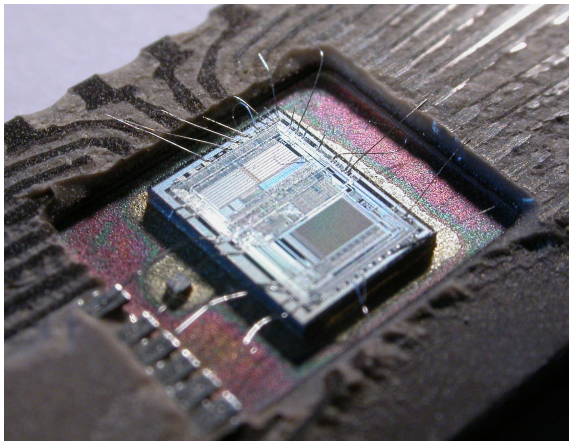
3.5 Hardware

Hardware označuje fyzické prvky počítače či výpočetního systému, skládá se z mnoha různých částí, z nichž nejdůležitější je základní deska. Ta je rovněž složena z velkého množství komponent,

které napájí a ovládají toto zařízení. (Mullins, 2014)

3.5.1 Monolitický počítač

Monolitický počítač, častěji nazývaný jako mikrokontrolér (MCU - microcontroller unit) je malý počítač, který je uzavřen v pouzdře a vytváří tak integrovaný obvod. Mikrokontrolér obsahuje jeden či více procesorových jader společně s pamětí a vstupně/výstupními periferiemi. To znamená, že obsahuje jak programovou paměť, tak operační paměť (RAM). Mikrokontroléry bývají navrženy pro vestavěné systémy, na rozdíl od mikroprocesorů, které se využívají v „běžných“ osobních počítačích. (Brain, 2000) Existuje celá řada mikrokontrolérových linií, které se liší výkonem, spotřebou a dalšími parametry. Mezi zástupce mikrokontrolérů patří ESP32 a AVR.



Obrázek 3: Intel 8742
Odhalené jádro 8 bitového mikrokontroléru Intel 8742, který obsahuje CPU pracující na frekvenci 12 MHz, 128 bajtů RAM, 2048 bajtů EEPROM a vstupně-výstupní periferie (I/O), to vše na jednom čipu. Některé z bondovaných drátů byly bohužel poškozeny v důsledku otevírání pouzdra. Zdroj: (Sameli, 2003)

3.5.1.1 ESP32

ESP32 je série velmi levných mikrokontrolérových systémů na čipu (SoC) s nízkou spotřebou, které integrují Wi-Fi a dual-mode Bluetooth. Jedná se o vlajkovou loď šanghajské společnosti Espressif Systems.

ESP32 užívá architekturu Xtensa LX6 od společnosti Tensilica, která se zabývá návrhem a prodejem intelektuálního vlastnictví k polovodičovým jádrům.

Série obsahuje jedno či dvě jádra LX6, anténové přepínače, symetrizační člen, nízkošumový

přijímací zesilovač, filtry, moduly napájení a řadu dalších modulů, které obsahují i jiné mikrokontrolérové rodiny.

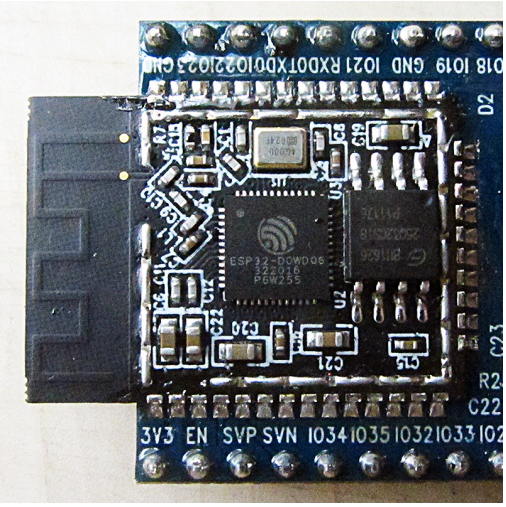
Espressif Systems vyrábí ESP32 na zakázku ve společnosti TSMC pomocí 40nm procesu. (Espressif, 2020)

Vybavení ESP32 dle datového listu (Espressif, 2020) jsou následující:

- Procesory
  - Hlavní výpočetní jednotka (CPU): Jednojádrový či dvoujádrový procesor Xtensa LX6, pracující na frekvenci 160 nebo 240 MHz a dosahující až 600 DMIPS
  - Ultra nízkopříkonový koprocesor
- Paměti
  - 520 KiB SRAM
- Bezdrátové připojení
  - Wi-Fi: 802.11 b/g/n
  - Bluetooth: v4.2 BR/EDR a BLE (fyzická vysílací/přijímací část je sdílena s Wi-Fi)
- Periférie
  - 12 bitový SAR ADC, až 18 kanálů
  - 2x 8 bitové DAC
  - 10x dotykový senzor (kapacitní snímání pomocí GPIO)
  - 4x SPI
  - 2x I^2S
  - 2x I^2C
  - 3x UART
  - SD/SDIO/CE-ATA/MMC/eMMC kontrolér
  - SDIO/SPI slave kontrolér
  - Ethernet MAC rozhraní s dedikovaným DMA a podporou PTP (IEE 1588 Precision Time Protocol)
  - CAN bus 2.0

  - Kontrolér pro ovládání infračerveného dálkového ovladače (TX/RX, až 8 kanálů)
  - Motor PWM
  - LED PWM (až 16 kanálů)
  - Hallův senzor
  - Ultra nízkopříkonový analogový předzesilovač
- Bezpečnost
  - IEEE 802.11 všechny standardní bezpečnostní prvky jsou podporovány, včetně WFA, WPA/WPA2 a WAPI
  - Secure boot
  - Šifrování flash paměti
  - 1024 bitové OTP, až 768 bit pro zákazníky
  - Kryptografická akcelerace
    * AES
    * Hash (SHA-2)
    * RSA
    * ECC
    * Generátor náhodných čísel (RNG)
- Napájení
  - Interní regulátor
  - 5μA spotřeba při hlubokém spánku
  - Probuzení pomocí přerušení na GPIO, časovač, ADC měřením, dotykem na kapacitní senzor

Obvyklé bývá, že čip ESP32 bývá osazen v pomocném modulu, který obsahuje dodatečné součástky (externí flash paměť, případně externí RAM, anténu a další). Příklad takového modulu je k vidění na obrázku č.4 (ESP32-WROOM-32).



Obrázek 4: ESP32-WROOM-32
Zdroj: (Krent, 2017)

ESP-IDF ESP-IDF (Espressif IoT Development Framework) je framework určený pro vývoj aplikací na platformě ESP32. (Espressif, 2020)

Framework obsahuje velkou řadu knihoven vytvořených přímo společností Espressif Systems, ale rovněž i velké množství knihoven třetích stran. Příkladem knihoven třetích stran je modifikovaný operační systém FreeRTOS, knihovna Mbed TLS pro implementaci TLS a SSL, lwIP pro implementaci TCP/IP.

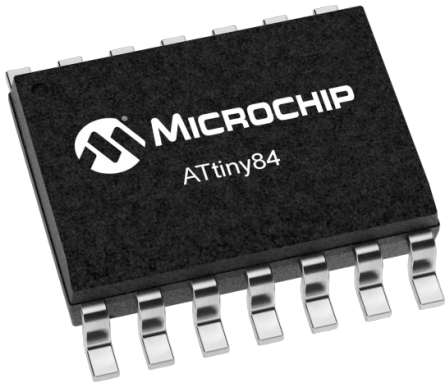
Součástí je rovněž knihovna pro vytváření DSP algoritmů a audio knihovna schopná kódovat nebo dekódovat různé audio datové proudy. Mezi podporovanými formáty jsou například FLAC, MP3, OGG, OPUS či obyčejný WAV.

Zajímavostí rovněž je, že ESP-ADF obsahuje rozhraní pro rozpoznávání hlasu.

3.5.1.2 AVR

AVR je označení pro rodinu 8-bitových RISC mikrokontrolérů. AVR je modifikovanou harvardskou architekturou, kdy je fyzicky oddělena paměť programu a dat. AVR bylo vyvinuto dvěma studenty Norského institutu technologie (NBTH), Alf-Egil Bogenem a Vegardem Wollanem, posléze byla tato technologie prodána společnosti Atmel. (Hill, 2021)

AVR je v současné době využíván pro jednodušší vestavěné systémy, které nevyžadují velký výpočetní výkon.



Obrázek 5: AVR ATTINY84
Zdroj: (Microchip, 2021)

3.5.2 Ochrany zařízení - fyzikální aspekty

V této kapitole budou teoreticky rozebrány základní fyzikální aspekty ochrany konstruovaného zařízení. Předpokládáme, že je zařízení připojeno ke stejnosměrnému zdroji napájení (DC - Direct current).

3.5.2.1 Nadproud

V elektrické distribuční soustavě je označení „nadproud“ taková situace, kdy vodičem (či vodivou trasou) prochází větší množství elektrického proudu, než na které byl původně navržen, což vede k nadměrnému zahřívání a riziku požáru či poškození připojeného zařízení. (Schneider Electric, 2012)

Možnými příčinami nadproudu bývá zkrat, nadměrná zátěž, nesprávný návrh zařízení a další.

Pro ochranu před nadproudem se využívá nadproudových ochran, což jsou například pojistky nebo jističe. (Schneider Electric, 2012)

- Pojistka
  - Pojistka je zařízení, které obsahuje tenký tavný drátek. Při překročení mezní hodnoty elektrického proudu a času dojde k přetavení tohoto drátku a tím k přerušení obvodu, který se nachází za pojistkou. (Wright, 2004, str. 2) Použitá pojistka musí být posléze vyměněna.
- Jistič

– Jistič je zařízení, které podobně jako pojistka při nadměrném elektrickém proudu odpojí elektrický obvod.(Saxena et al., 2012) Na rozdíl od běžné (tavné) pojistky je možné jistič po odstranění závady znovu uvést do výchozího stavu.

3.5.2.2 Přepětí

Přepětí je takové napětí, které svou velikostí překračuje maximální možné napětí, na které bylo zařízení navrženo.

Zdrojem přepětí je řada dějů, například:

- Poruchy vzniklé v důsledku zkratů a zemních spojení
- Přechodné děje při zapínání a vypínaní
- Děje při náhlé ztrátě zatížení

Přepětí je nežádoucím jevem a může způsobit trvalé poškození elektroniky, která je k takovémuto napětí připojena.

Crowbar circuit Crowbar circuit (doslovný překlad do češtiny „obvod páčidla“ či „páčidlový obvod“) je takový elektrický obvod, který zamezuje poškození zařízení v důsledku přepětí na zdroji.

Obvod pracuje tak, že při přepětí způsobí zkrat na vstupních terminálech zařízení, což vede k nadměrnému průchodu proudu a tím přetavení pojistky či vyhození jistícího prvku nacházejícího se na vstupu nebo před zařízením.

3.5.2.3 Podpětí

Podpětí je přesným opakem přepětí - jedná se o napětí, které je svou velikostí nižší než nejnižší možné napětí, na které bylo zařízení navrženo.

Na rozdíl od přepětí, podpětí nemusí nutně znamenat trvalé poškození elektroniky, ale může docházet ke značným chybám při výpočtech prováděných digitálními obvody, pokud je zařízení napájeno z větve, která má podpětí.

Brownout detection „Brownout“ je v mikontrolérové technice částečný úbytek napětí zdroje pod úroveň požadovanou pro spolehlivou funkčnost mikrokontroléru.(Colley, 2019) Během tohoto úbytku napětí na zdroji může dojít k chybám, jako je například poškození paměti a obsahu registrů(Lau – Cheng, 2011), z čehož plyne, že program v tomto mikrokontroléru nebude vykonán korektně.

Principem brownout detektoru je tedy zamezit mikrokontroléru ve vykonávání programu (brown out drží mikrokontrolér v permanentním módu restartu, dokud nedojde k obnovení korektní úrovně napětí).(Colley, 2019)

3.5.2.4 Obrácená polarita

Obrácenou polaritou u stejnosměrného napětí rozumíme přehození polarit + a -. Může se tak stát například nesprávným vložením baterie (jejím obrácením) do zařízení či využitím napájecího síťového zdroje, který má sice konektor totožný se vstupním konektorem zařízení, avšak piny na tomto konektoru jsou přehozeny. Nejčastěji se takto stává u tzv. „univerzálních adaptérů“, které obsahují větší množství konektorů, které je možné zapojit i obráceně.

Pokud by zařízení nebylo chráněno před obrácenou polaritou a napájení by bylo aplikováno obráceně, v drtivé většině případů by došlo k trvalému poškození polovodičových prvků zařízení.

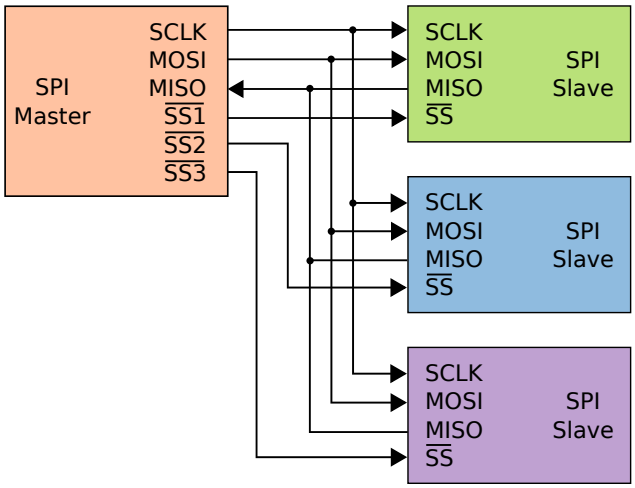
3.5.3 Sběrnice

Sběrnice je komunikační systém, který přenáší data mezi jednotlivými komponentami systému. (Doncescu, 2020) Aby bylo zařízení možno k této sběrnici připojit, je nezbytné, aby byla přesně definována pravidla, jak daná sběrnice funguje a jak se má připojené zařízení chovat. Těmto pravidlům se říká protokol sběrnice. (Doncescu, 2020) Navíc musí být definovány mechanické a elektrické specifikace. (Doncescu, 2020) Sběrnic je celá řada, v této kapitole budou rozebrány pouze ty nejběžnější, které se současně vyskytují v navrženém zařízení.

3.5.3.1 SPI

SPI (Serial Peripheral Interface) - sériové periferní rozhraní je synchronní komunikační rozhraní, které se využívá pro komunikaci na krátké vzdálenosti, hlavně ve vestavěných systémech. Rozhraní bylo vyvinuto společností Motorola v polovině 80. let 20. století a stalo se de facto standardem. Na sběrnici se nachází jedno řídící (master) a jedno nebo více podřízených (slave) zařízení. Master obsahuje generátor hodinového signálu, který je rozveden do všech připojených slave zařízení.

Hodinový signál je rozváděn vodičem označovaným jako SCK. Kromě vodiče s hodinovým signálem jsou uzly propojeny dvojicí vodičů většinou označovaných jako MISO (Master In, Slave Out) a MOSI (Master Out, Slave In), pomocí nichž se obousměrně přenášejí data. Posledním signálem je signál SS (Slave Select), který slouží k výběru slave zařízení, se kterým master aktuálně komunikuje. (Tišnovský, 2008)



Obrázek 6: SPI master se třemi zařízeními slave
Zdroj: (Burnett, 2006a)

3.5.3.2 I²C

I²C (Inter-Integrated Circuit) je multi-master, multi-slave sériová komunikační sběrnice vyvinutá v roce 1982 společností Philips Semiconductor (nyní NXP Semiconductors). (NXP Semiconductors, 2014) I²C obsahuje stejně jako SPI jeden vodič hodinového signálu (v tomto případě označovaný jako SCL), avšak na rozdíl od SPI neumožňuje obousměrný přenos dat, jelikož obsahuje pouze jeden datový vodič (označovaný jako SDA). Z toho vyplývá, že data jsou na I²C přenášena poloduplexně. Rovněž to znamená, že zařízení implementující tuto sběrnici musejí být interně složitější, jelikož musí umět automaticky přepnout mezi vstupním a výstupním módem. (Tišnovský, 2008)

I²C nemá na rozdíl od sběrnice SPI adresní vodič. Výběr zařízení tedy probíhá pomocí hardwarové adresy, která je každému zařízení zadána během výroby (u některých zařízení je možné tuto adresu měnit).

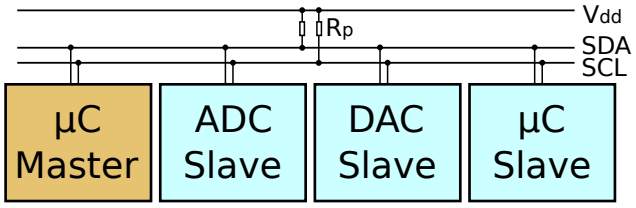
Sběrnice se využívá pro připojení nízkorychlostních periferií a je možné ji využít i na delší vzdálenosti (kvalitní kabel rozumné délky - tzn. pár metrů), jelikož maximální povolená kapacitance na sběrnici je 400pF.

Jak již bylo zmíněno výše, I²C obsahuje dva vodiče nazvané SDA a SCL, na rozdíl od sběrnice SPI jsou tyto linky připojeny k napájecí větvi pomocí pull-up rezistorů a signalizování na těchto linkách probíhá pomocí otevřeného kolektoru. (NXP Semiconductors, 2014) Typické napětí sběrnic je +5 V či +3.3 V, avšak systémy s jiným napětím jsou povoleny.

Adresy zařízení připojené k I²C bývají 7bitové, méně často se využívá 10bitové rozšíření. (TOTALPHASE, 2013)

Klasická rychlost je 100 kbit/s ve „standard mode“ a 400 kbit/s ve „fast mode“. (NXP Semiconductors, 2014)

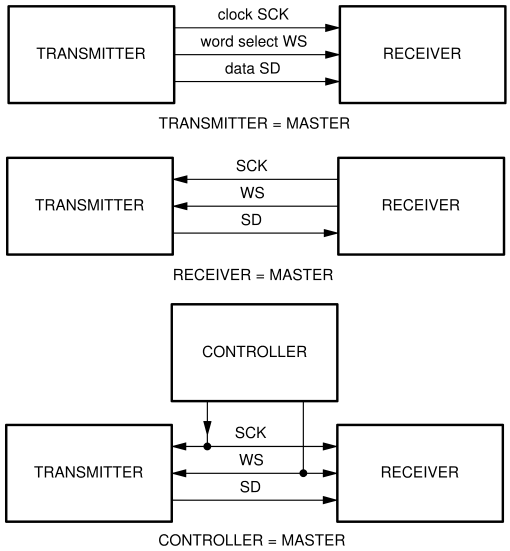
Na následujícím obrázku je znázorněna jedna řídící jednotka typu mikrokontrolér (μC master) a tři podřízená zařízení (slave), v tomto případě se jedná o analogově-digitální převodník (ADC slave), digitálně-analogový převodník (DAC slave) a další mikrokontrolér (μC Slave).



Obrázek 7: I^{2}C sběrnice
Zdroj: (Burnett, 2006b)

3.5.3.3 I^{2}S

I^{2}S (Inter-IC sound) je sběrnice užívaná pro spojování digitálních audio zařízení. Specifikace této sběrnice pochází od společnosti Philips Semiconductor (I^{2}S bus specification; únor 1986, revidováno 5. června 1996). (Cypress, 2016)(Philips Semiconductors, 1996) Sběrnice slouží primárně pro přenos zvuku z mikrokontroléru/mikroprocesoru do zvukového submodulu.



Obrázek 8: I^{2}S druhy konfigurace
Vektorováno
Zdroj: (Philips Semiconductors, 1996)

3.6 Firmware

Jako firmware označujeme počítačový program, který poskytuje nízkoúrovňové ovládání specifického hardwaru zařízení. (Mullins, 2014) Firmware může poskytovat standardizované operační rozhraní pro komplexní software zařízení (čímž umožňuje jistou hardwarovou nezávislost a multiplatformnost) nebo (u méně složitých zařízení) slouží jako kompletní operační systém zařízení, provádějící veškerou kontrolu, monitoring a manipulaci s daty.

Typické je využití firmwaru u vestavěných systémů (embedded systems), které na rozdíl od univerzálního programovatelného počítače plní jeden specifický účel (například semafory, pračky, kalkulačky, meteostanice, sondy...).

3.6.1 LVGL

LVGL (Light and Versatile Graphics Library) je knihovna, která je využívána pro tvorbu grafického uživatelského rozhraní (GUI) u vestavěných systémů. Knihovna obsahuje řadu předpřipravených prvků a vizuálních efektů (animace jednotlivých prvků, rozbalovací menu atp.). (Kiss-Vamosi, 2020)

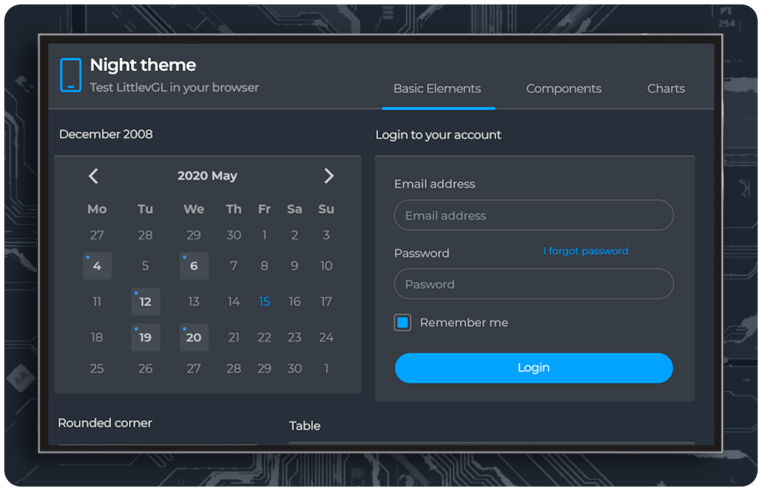
Funkce knihovny (Kiss-Vamosi, 2020):

- Výkonné stavební bloky: tlačítka, grafy, seznamy, posuvníky, obrázky atp.
- Pokročilá grafika: animace, vyhlazování hran, průhlednost, plynulé posouvání
- Využití řady vstupních zařízení: dotyková obrazovka, myš, klávesnice, enkodér, tlačítka aj.
- Podpora různých druhů displejů: monochromatické a barevné
- Hardwarově nezávislé, je možné využít s jakýmkoliv mikrokontrolérem, který splňuje minimální požadavky
- Dobrá škálovatelnost i při využití skromných prostředků (64 kB Flash, 10 kB RAM)
- Podpora velkého množství jazyků se zpracováním UTF8, obousměrné texty
- Plná přizpůsobitelnost grafických prvků pomocí stylů podobných CSS
- Operační systém, externí paměť a GPU jsou podporovány, avšak nejsou vyžadovány
- Hladké vykreslování i při využití vyrovnávací paměti pro jeden snímek

- Napsáno v jazyce C pro maximální kompatibilitu
- Bindování pro Micropython
- Simulátor pro vývoj na PC bez nutnosti připojení externího hardwaru

Požadavek	Minimálně	Doporučené
Architektura	16, 32 nebo 64 bitový mikrokontrolér či procesor	
Taktovací frekvence	> 16 MHz	> 48 MHz
Flash/ROM	> 64 kB	> 180 kB
Statická RAM	> 2 kB	> 4 kB
Zásobník (Stack)	> 2 kB	> 8 kB
Halda (Heap)	> 2 kB	> 8 kB
Buffer displeje	> 1x hor. roz. disp.	> 10x hor. roz. disp.
Kompilátor	C99 či novější	

Tabulka 3: Požadavky knihovny LVGL
Zdroj: (Kiss-Vamosi, 2020)



Obrázek 9: Ukázka obrazovky vytvořené v knihovně LVGL
Zdroj: (Kiss-Vamosi, 2020)

3.6.2 SQLite

SQLite je systém pro relační řízení báze dat (RDBMS - Relational database management system) obsažený v knihovně programovacího jazyka C.

Na rozdíl od mnoha jiných systémů pro správu databází není SQLite databázovým strojem typu klient-server. Spíše se jedná o knihovnu, která bývá vložena do konečného programu. (SQLite, 2020a)

SQLite není samostatně funkčním procesem, se kterým by mohla konečná aplikace komunikovat. Místo toho je knihovna SQLite slinkována s požadovanou aplikací a tudíž se stává nepostradatelnou součástí této aplikace. Linkování může být statické nebo dynamické podobně jako u ostatních knihoven. Aplikace, která využívá SQLite, tak činí pomocí přímého volání funkcí, které snižují latenci v přístupu k databázi, toto volání je účinnější než meziprocesová komunikace (IPC).

SQLite ukládá celou databázi (definice, tabulky a data samotná) jako jediný soubor.

Výhoda tohoto „bezserverového“ řešení je, že nevyžaduje takřka žádnou konfiguraci: není zapotřebí spouštět/konfigurovat server, není třeba administrátora, který by vytvořil nové databáze a přiřadil k nim přístupy jednotlivým uživatelům, rovněž nejsou nezbytné žádné konfigurační soubory. Pokud dojde k výpadku napájení, není zapotřebí žádné další akce po znovuzapnutí. (SQLite, 2020b)

Naopak značnou nevýhodou „bezserverového“ řešení je fakt, že není možné, aby několik procesů současně četlo a zapisovalo. Čtení je možné provádět ve vícero procesech, avšak zápis nikoliv. V případě využití serverového řešení je na démonu SQL serveru, jak si s tímto jevem poradí - k démonu se připojí několik procesů a démon vnitřně určuje, kdy databázi „zamkne“, aby mohlo dojít k zápisu požadovaných informací. V případě SQLite je zapotřebí řídit přístup procesů, které si přejí zapisovat tak, aby v jednu chvíli zapisoval pouze jeden proces (a ostatní vyčkávaly), a to takovým způsobem, aby nedošlo k poškození integrity dat díky nesprávnému vstupu do kritické sekce. Tomuto klasickému výpočetnímu problému se běžně říká „Problém čtenářů a písařů“ a je možné jej řešit mutexy (zámky) či semafory.

3.6.3 Bootstrap (framework)

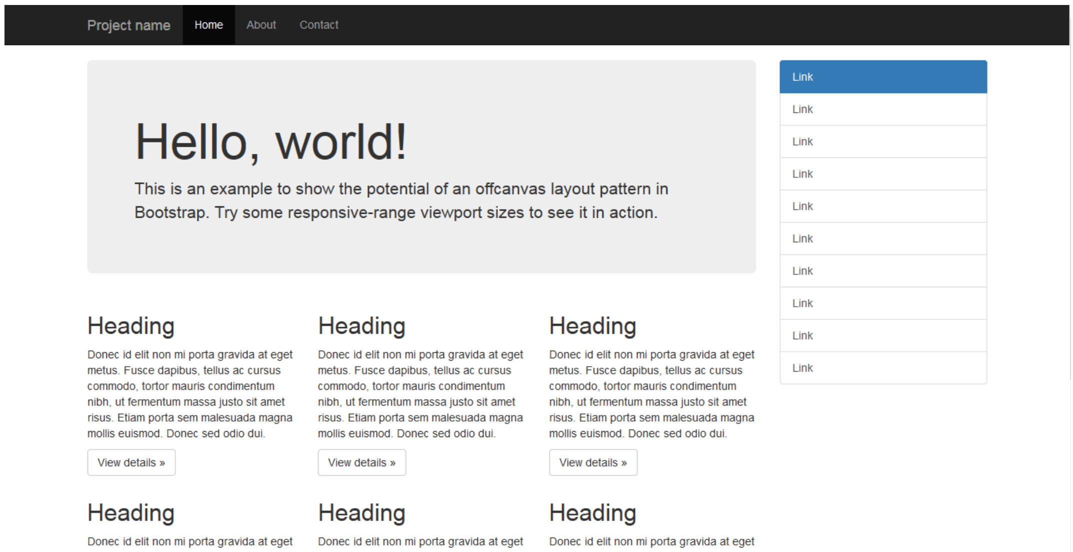
Bootstrap je open-source CSS framework, který je zamýšlen pro vytváření responzivních webových prezentací. Obsahuje CSS a (volitelně) JavaScriptové šablony pro typografii, formuláře, tlačítka, navigace a ostatní komponenty nezbytné pro vytvoření uživatelského rozhraní. (Mark Otto, 2011)

Bootstrap tedy poskytuje základní definice stylů pro všechny prvky HTML. Výsledkem je jednotný vzhled tabulek, formulářových prvků a jiných elementů napříč webovými prohlížeči.

Bootstrap využívá komponenty JavaScriptu ve formě pluginů jQuery. Tím jsou poskytnuty další prvky uživatelského rozhraní, jako jsou dialogová okna, popisy nástrojů, kolotoč (carousel) atp. Každá komponenta Bootstrapu se skládá z HTML struktury, deklarací CSS a v některých případech

doprovodného JavaScriptového kódu.

Bootstrap rovněž umožňuje jednoduše měnit rozvržení, která ovlivňují celou stránku.



Obrázek 10: Typický vzhled stránky s využitím frameworku Bootstrap
Zdroj: (Bootstrap developers, 2014)

3.7 Wi-Fi

Wi-Fi (Wireless Fidelity) je bezdrátová technologie na bázi mikrovlnného spojení. Tato technologie využívá bezlicenčního frekvenčního pásma, proto je ideální pro budování levné, ale výkonné sítě bez nutnosti pokládky kabelů. Uživatelé tak spolu mohou komunikovat, sdílet data i periferie (např. síťovou tiskárnu nebo skener), dělit se o připojení k internetu nebo spolu hrát počítačové hry, a to vše bezdrátově. Aby mezi sebou mohla komunikovat zařízení různých výrobců i různých platforem, existují mezinárodní standardy. Jejich specifikací se zabývá institut IEEE (z angl. Institute of Electrical and Electronic Engineers) - specifikace standardů bezdrátových lokálních sítí jsou publikovány pod číslem 802.11. (Joyce, 2010)

3.8 Přenos dat paketovým rádiem

Paketové rádio je digitální rádiová komunikace používaná pro přenos dat. Data jsou ve vysílači zabalena do datových paketů, které jsou posléze v přijímači dekódovány.

3.8.1 Paket

V telekomunikační technice se pod pojmem paket rozumí formátovaná data, která je možné přenést přes síť. Paket obsahuje kontrolní informace a uživatelská data (užitečný náklad - payload). Kontrolní informace poskytují data nezbytná pro korektní doručení paketu (jako je například cíl doručení, zdroj původu, detekce chybovosti - CRC a jiné). (Traore, 2021) Obvyklé bývá, že tyto dodatečné informace jsou v hlavičce či patičce paketu.

3.8.2 CRC

CRC je označení pro cyklický redudantní součet (cyclic redudancy check), což je hashovací funkce, která je používána k detekci chyb během přenosu dat. (Gad et al., 2015) Z dat, u kterých je zapotřebí zajistit integritu, je vypočítáno CRC. Po přenosu je z přijatých dat vypočteno CRC stejným způsobem a následně je tato vypočtená hodnota porovnána s tou, která dorazila společně s daty. Pokud se hodnoty liší, došlo při přenosu k poškození dat.

3.8.3 Data whitening

Data whitening je metoda kódování dat, která potlačuje delší série jedniček nebo nul v odesílaných datech, což pomáhá udržet vyrovnanější spektrum. (Christiansen, 2010).

Metoda pracuje na takovém principu, kdy je na vstupní data použita operace exkluzivní disjunkce (XOR) s pseudonáhodnou sekvencí předtím, než jsou tato data odeslána. Jakmile jsou data odeslána a na druhé straně přijata přijímačem, je na tato data aplikována operace XOR stejnou sekvencí, což má za následek rekonstrukci původních dat. (Christiansen, 2010)

3.8.4 Kódování Manchester

Kódování Manchester je technika, která umožňuje zakódovat hodinový signál a data synchronního bitového proudu, přičemž ve výsledném proudu se nevyskytují dlouhé úseky nepřetržitých jedniček nebo nul. (Maxim, 2005) Při použití této techniky se skutečná binární data neposílají jako posloupnosti logických jedniček a nul, místo toho jsou bity přeloženy do mírně odlišného formátu, který má oproti přímému kódování řadu výhod: (Mills, 2009)

- Sériový bitový tok má nulovou DC složku
- Detekci chyb je jednoduché implementovat

Obecně platí, že při přenosu sériových dat do přijímače musí být zachována nulová stejnosměrná složka. Je tomu tak proto, aby demodulátor v přijímači mohl správně interpretovat přijatá data jako jedničky a nuly, což toto kódování umožňuje.

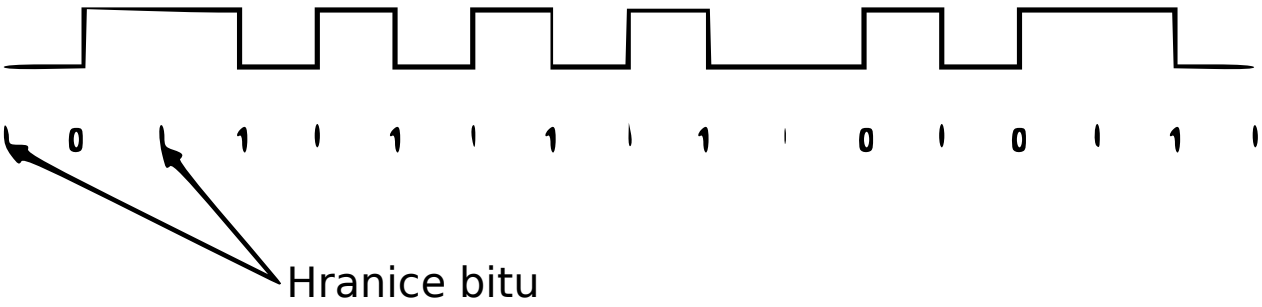
Kódování Manchester má následující pravidla: (Mills, 2009)

- Pokud jsou originální data logická 0, pak je kód Manchester: 0 do 1 (přechod nahoru ve středu původního bitu)
  - Alternativně je kód Manchester 1 do 0 při využití invertovaného kódu Manchester
- Pokud jsou originální data logická 1, pak je kód Manchester: 1 do 0 (přechod dolů ve středu původního bitu)
  - Alternativně je kód Manchester 0 do 1 při využití invertovaného kódu Manchester

Z výše uvedeného je patrné, že jsou zapotřebí dva bity pro data zakódováná kódem Manchester oproti jednomu bitu v originálním datovém proudu.

Příklad kódování Manchester: (Mills, 2009)

Mějme následující 8 bitový datový proud: „0 1 1 1 0 0 1“, který je pomocí kódu Manchester zakódován jako „01 10 10 10 10 01 01 10“. Nejméně významný bit (LSB) je uveden nejvíc vlevo. Příklad je uveden na následujícím obrázku:



Obrázek 11: Křivka kódování Manchester při vstupní sekvenci 01111001
Zdroj: (Mills, 2009), přeloženo, vektorováno

3.9 Kryptografie

Kryptografie se zabývá studiem a využitím technik pro bezpečnou komunikaci za přítomnosti třetích stran nazývaných jako „protivníci“ (adversaries). (Leeuwen, 1990)

Obecněji řečeno, kryptografie pojednává o konstrukci a analýze protokolů, které zabraňují třetím stranám nebo veřejnosti číst soukromé zprávy. (Bellare – Rogaway, 2005)

Původce šifrované zprávy sdílí techniku dekódování pouze se zamýšlenými příjemci, aby se zabránilo přístupu protivníků. Kryptografická literatura často používá jména Alice („A“) pro odesílatele, Bob („B“) pro zamýšleného příjemce a Eva („E“) pro protivníka (odvozeno z anglického originálu „eavesdropper“ - odposlouchávač). (Biggs, 2008)

Kryptografie prodělala za svou existenci enormní rozvoj - od jednoduché Caesarovy šifry používané ve starověku až po post-kvantové algoritmy šifrování, které jsou schopné čelit útoku protivníka, který disponuje kvantovým počítačem.

Kvantové počítače pro současná kryptografická schémata představují značný problém, jelikož pomocí Shorova algoritmu je poměrně snadné prolomit aktuálně používané asymetrické šifrování RSA. (Bernstein et al., 2017)

Šifrování je proces zabezpečující informace před nechtěným přístupem nebo použitím. (Jaikaran, 2016)

Šifrování využívá umění kryptografie ke změně informací, které lze číst (prostý text) na nečitelný text. (Jaikaran, 2016)

Dešifrování využívá obdobně opačné změny, kdy z šifrovaného textu je možné získat čitelný text. (Jaikaran, 2016)

Kryptografie se klasicky dělí na dvě odvětví: symetrickou kryptografii a asymetrickou kryptografii.

3.9.1 Symetrická kryptografie

Symetrická kryptografie využívá takové algoritmy, které používají stejné kryptografické klíče pro šifrování prostého textu i dešifrování šifrovaného textu. Klíče mohou být buď to identické, nebo může dojít k jednoduché transformaci mezi těmito klíči. (Sabir, 2016, str. 147) Tento požadavek, tedy aby obě strany měly přístup k tajnému klíči, je jednou z hlavních nevýhod šifrování pomocí symetrického klíče ve srovnání s šifrováním pomocí veřejného klíče (asymetrickou kryptografií). (Mullen – Mummert, str. 112)

Symetrická kryptografie bude v následujících kapitolách rozdělena na dvě podmnožiny, konkrétně se jedná o podkapitoly 3.9.3 (Blokové šifry) a 3.9.4 (Proudové šifry).

3.9.2 Asymetrická kryptografie

Asymetrická kryptografie je taková kryptografie, která využívá párů klíčů: veřejných klíčů (public keys), které mohou být šířeny veřejně a soukromých klíčů (private keys), které zná pouze vlastník. Generování těchto klíčů závisí na kryptografických algoritmech založených na matematických

problémech, které produkují jednosměrné funkce. Efektivní zabezpečení vyžaduje, aby byly zachovány pouze soukromé klíče, veřejný klíč může být otevřeně distribuován bez ohrožení bezpečnosti. (Stallings, 1999)

Příklad užití je následující: jakákoliv osoba může zašifrovat zprávu pomocí veřejného klíče příjemce, avšak tuto zprávu je možné dešifrovat pouze pomocí soukromého klíče příjemce.

Asymetrická kryptografie rovněž umožňuje autentizaci. Odesílatel může zkombinovat zprávu se svým soukromým klíčem a vytvořit tak ke zprávě digitální podpis. Kdokoliv s odpovídajícím veřejným klíčem odesílatele může zkombinovat stejnou zprávu s předpokládaným digitálním podpisem s ní spojeným, aby ověřil, zda byl podpis platný, tedy zda byl skutečně vytvořen vlastníkem odpovídajícího soukromého klíče (tedy původcem zprávy). (Bernstein, 2008)

Jedním z nejstarších a doposud stále využívaným systémem asymetrické kryptografie je RSA.

3.9.3 Blokové šifry

Bloková šifra je označení pro takový typ symetrické šifry, která pracuje s bloky pevně stanovené délky. Pokud je dat mnoho, jsou rozdělena na vícero bloků, přičemž poslední blok musí být zarovnán, pokud obsahuje volné místo. Při šifrování (a dešifrování) je tak každý blok transformován pomocí daného šifrovacího algoritmu.

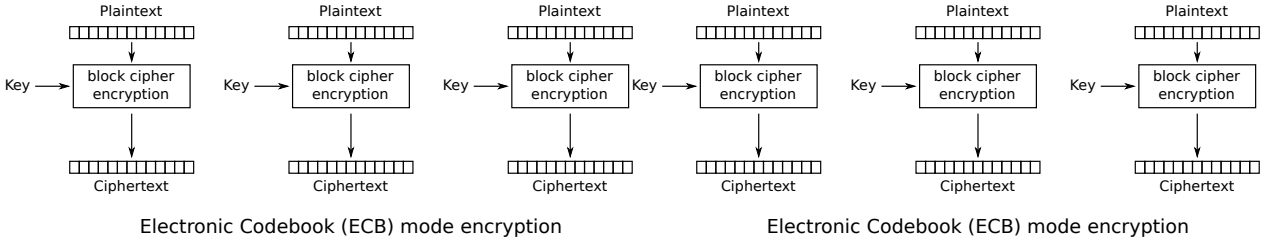
Zajímavostí je, že velká část blokových šifer je postavena na určitých konstrukčních vzorech, jedním z příkladů takovéhoto konstruktu je Feistelova síť, která byla prvně užita v šifře Lucifer (předchůdce šifry DES) vyvinuté německo-americkým kryptografem Horstem Feistelem. (Hoang – Rogaway, 2018). Dalším příkladem konstrukčního vzoru je substitučně-permutační síť, na které je postavena například šifra AES (Rijndael), Square a jiné. Dalším a podstatně méně známějším konstruktem je Lai-Masseyho schéma (Yun et al., 2010), které je využito v šifrách IDEA a IDEA NXT.

Bloková šifra klasicky umožňuje šifrovat/dešifrovat pouze jeden blok o specifické délce. U zpráv s proměnnou délkou musí být data nejprve rozdělena do samostatných šifrovacích bloků. V nejjednodušším případě, známém jako ECB (Electronic codebook), je zpráva nejprve rozdělena do samostatných bloků velikosti bloku šifry (případně rozšiřuje poslední blok o zarovnání/výplň) a poté je každý blok nezávisle šifrován a dešifrován. Avšak využití této naivní metody je obecně považováno za nebezpečné, protože stejné bloky prostého textu budou vždy generovat stejné bloky výstupu (pro stejný klíč), takže ve výstupu se objeví určité vzory a struktura vstupních dat může prosakovat. (Menezes et al., 1996)

3.9.3.1 Provozní režimy blokových šifer

Bylo definováno velké množství provozních režimů blokových šifer. Účelem šifrovacích režimů je maskovat vzory, které existují v šifrovaných datech, pokud je využito ECB.

ECB (Electronic codebook) Zpráva je v tomto případě rozdělena do bloků, přičemž každý blok je šifrován/dešifrován samostatně. Jak již bylo uvedeno výše, tento přístup není příliš vhodné využívat v praxi, jelikož může dojít ke kompromitaci dat.



Obrázek 12: Ilustrace provozního režimu ECB (šifrování/dešifrování)
Zdroj: (WhiteTimberwolf, 2013f,e)

Šifrování paralelizovatelné	✓
Dešifrování paralelizovatelné	✓
Čtení pomocí náhodného přístupu	✓

Tabulka 4: Vlastnosti ECB

CBC (Cipher block chaining) Cipher block chaining je provozní režim, který vymysleli Ehrsam, Meyer, Smith a Tuchman v roce 1976 (jedná se o patent US4074066A). (Ehrsam et al., 1976) V tomto režimu je každý blok vstupního textu XORován s předchozím šifrovaným blokem předtím, než je zašifrován. Z toho vyplývá, že každý blok šifrovaného textu závisí na všech doposud zpracovaných blocích prostého textu. Aby byla každá zpráva jedinečná, je nezbytné v prvním bloku využít inicializačního vektoru (IV).

První blok má index 1, matematický vzorec pro CBC šifrování je:

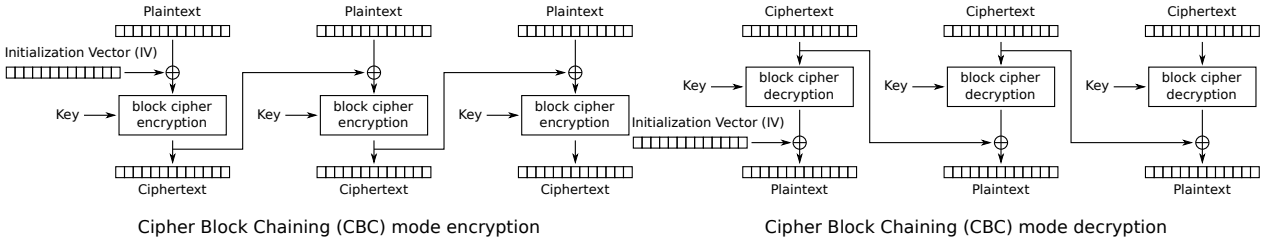
$$C_i = E_K\left(P_i \oplus C_{i-1}\right) \tag{19}$$

$$C_0 = IV \tag{20}$$

Matematický popis pro CBC dešifrování je:

$$P_i = D_K(C_i) \oplus C_{i-1} \tag{21}$$

$$C_0 = IV \tag{22}$$



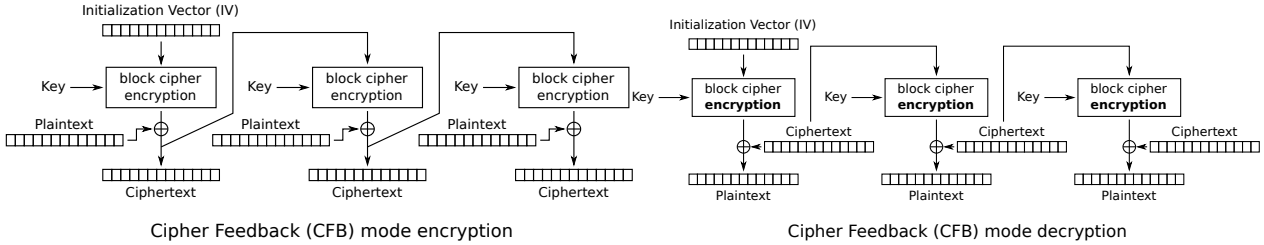
Obrázek 13: Ilustrace provozního režimu CBC (šifrování/dešifrování)
Zdroj: (WhiteTimberwolf, 2013b,a)

Šifrování paralelizovatelné	✗
Dešifrování paralelizovatelné	✓
Čtení pomocí náhodného přístupu	✓

Tabulka 5: Vlastnosti CBC

CFB (Cipher feedback) Cipher feedback je režim, který je velmi podobný CBC. CFB převádí blokovou šifru do sebesynchronizující proudové šifry.

Sebesynchronizující proudová šifra je taková šifra, u které, pokud dojde ke ztrátě části šifrovaného textu (například v důsledku chyb v přenosu), ztratí přijímací strana pouze část původní zprávy a měla by být schopna pokračovat ve správném dešifrování zbytku bloků po zpracování určitého množství vstupních dat.

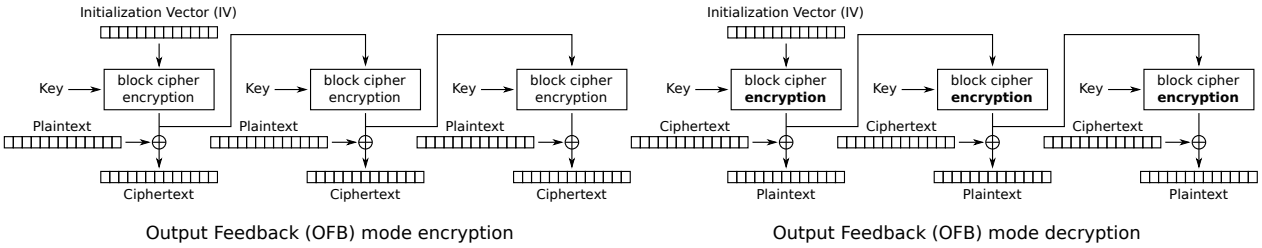


Obrázek 14: Ilustrace provozního režimu CFB (šifrování/dešifrování)
Zdroj: (WhiteTimberwolf, 2013d,c)

Šifrování paralelizovatelné	✗
Dešifrování paralelizovatelné	✓
Čtení pomocí náhodného přístupu	✓

Tabulka 6: Vlastnosti CFB

OFB (Output feedback) OFB převádí blokovou šifru do synchronní proudové šifry. Je generován výstupní blok, který je následně XORován s prostým textem tak, aby se získal zašifrovaný výsledek. Stejně tak jako v klasických proudových šifrách, záměna bitu v šifrovaném textu způsobí změnu bitu v dešifrovaném textu na totožné pozici. Tato vlastnost umožňuje využití kódů pro opravu chyb, i když jsou využity ještě před samotným šifrováním.



Obrázek 15: Ilustrace provozního režimu OFB (šifrování/dešifrování)
Zdroj: (WhiteTimberwolf, 2013h,g)

Šifrování paralelizovatelné	✗
Dešifrování paralelizovatelné	✗
Čtení pomocí náhodného přístupu	✗

Tabulka 7: Vlastnosti OFB

3.9.3.2 AES

AES, známá také svým původním jménem Rijndael, je specifikace pro šifrování elektronických dat zavedená americkým Národním institutem pro standardy a technologie (NIST). (NIST, 2001)

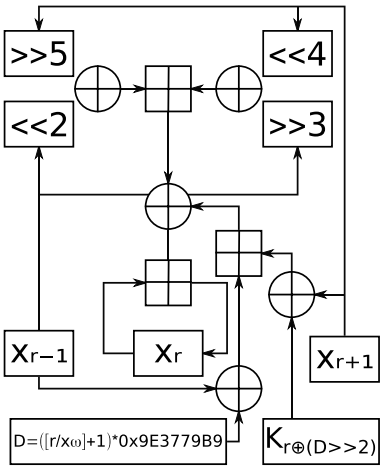
AES je podmnožinou blokové šifry Rijndael(Daemen – Rijmen, 2003) vyvinuté Vincentem Rijnmanem a Joanem Daemenem, kteří během procesu výběru AES předložili NIST návrh Rijndael. Rijndael je rodina šifer s různými velikostmi klíčů a bloků. NIST pro AES vybrala tři členy této rodiny, z nichž každý měl velikost bloku 128 bitů, ale tři různé délky klíčů: 128, 192 a 256 bitů.

Vláda USA přijala AES, který nahrazoval starší standard šifrování dat (DES) (Westlund, 2002), který byl publikován v roce 1977.

3.9.3.3 XXTEA

XXTEA je malá bloková šifra, která opravuje slabiny dřívější šifry XTEA, která sama vznikla z důvodu oprav dalších slabin v původní šifře TEA (Russell, 2004).

XXTEA využívá nevyváženou Feistelovu síť, díky své minimální velikosti je vhodná pro využití v systémech, které mají velmi omezené hardwarové parametry.



Obrázek 16: Jedno kolo / runda šifry XXTEA
Zdroj: (Mahdal, 2013)

3.9.4 Proudové šifry

Proudová šifra je takový druh symetrické šifry, u které je vstupní datový proud zkombinován s pseudonáhodným šifrovaným proudem (keystream). Výsledkem tak je výstupní šifrovaný proud. V praxi jsou obvykle proudy kombinovány pomocí operace exluzivní disjunkce (XOR). Na rozdíl od blokové šifry nejsou vstupní data rozdělena na jednotlivé bloky.

3.9.4.1 SALSA20

Salsa20 je rodina 256 bitových proudových šifer navržených v roce 2005. 20 kolová šifra Salsa20/20 je rychlejší než AES a je návrhářem doporučena pro typické kryptografické aplikace. Šifrování Salsa20/12 a Salsa20/8 se sníženým počtem kol patří mezi nejrychlejší dostupné 256 bitové proudové šifry a jsou doporučeny pro aplikace, kde je rychlost důležitější než spolehlivost. (Bernstein, 2007)

3.9.4.2 RC4

RC4 je rychlá a implementačně mimořádně jednoduchá proudová šifra původně využívaná v SSL/TSL spojení. Byla navržena Ronem Rivestem v roce 1987 pro RSA Data Security, Inc. a udržována jako obchodní tajemství, dokud v roce 1994 neunikla na veřejnost. Šifra byla použita ve Wi-Fi protokolu WEP. (Stosic, 2012)

V RC4 bylo nalezeno větší množství zranitelností a v současné době je tedy považována za nebezpečnou. (Popov, 2015)

3.10 Analýza konkurence

Podle nahraditelnosti výrobku můžeme rozlišovat čtyři úrovně konkurentů (Kotler, 1992):

1. Firma může za své hlavní konkurenty považovat firmy, které nabízejí podobné výrobky stejným zákazníkům za podobné ceny.
2. Firma se může k otázce konkurence stavět šířeji a považovat za své konkurenty výrobce podobných výrobků všech tříd.
3. Firma může vidět záležitosti ještě šířeji a považovat za konkurenty všechny firmy, které nabízejí podobnou službu.
4. Nejširší způsob nahlížení je, že za konkurenta může být považován každý, kdo soupeří o tytéž zákazníkovy peníze.

V praktické části této diplomové práce bude analyzována konkurence dle bodu 1.

4 Vlastní práce

4.1 Zvážení alternativ pro konstrukci

Před samotným zahájením vývoje zařízení byla provedena řádná rešerše a byla zvážena řada alternativ, které by měly vyhovovat požadavkům kladeným na zařízení.

Požadavky na hlavní zařízení (novou „hlavní stanici“) byly následující:

1. Ovládání dotykovým barevným displejem.
2. Schopnost přijímat, ukládat, vyhodnocovat a v některých případech i interpretovat naměřená data.
3. Schopnost připojit se do lokální sítě (buďto pomocí Ethernetu či Wi-Fi, sekundárně i technologie Bluetooth pro připojení k chytrému mobilnímu telefonu).
4. Kromě administrace pomocí dotykového displeje by rovněž bylo vhodné, pokud by zařízení obsahovalo webové rozhraní (podobně jako domácí routery či switche), pomocí kterého by bylo možné vzdáleně prohlížet aktuálně naměřená data (rovněž také výstup těchto dat - grafy) a zařízení dálkově nastavit.
5. Podpora většího množství sond (ať už se jedná o situaci, kdy je ke stanici připojeno větší množství totožných sond, nebo o situaci, kdy je ke stanici připojeno větší množství rozdílných sond [tedy sond, které snímají různé fyzikální veličiny]).
6. Volitelně (nikoliv však nezbytně nutně) by bylo vhodné, pokud by zařízení obsahovalo USB rozhraní pro připojení k osobnímu počítači (ať už z důvodu „servisovatelnosti“ či z důvodu stažení naměřených dat).
7. Rovněž by bylo příhodné, kdyby zařízení bylo schopné komunikovat s ostatními zařízeními nacházejícími se v chytré domácnosti, ať už souvisejí či nesouvisejí s počasím (hlásiče požáru, inteligentní osvětlení, chytré zásuvky...).
8. V ideálním případě by toto zařízení mohlo být využito jako centrální prvek chytré domácnosti (možnost poslouchání rádia, ovládání ostatních chytrých zařízení).
9. Vhodné by též bylo, pokud by zařízení umělo „přečíst“ naměřené hodnoty pro uživatele s vizuálním hendikepem.

10. Příhodné by rovněž bylo, kdyby bylo možno stanici napájet z palubní sítě automobilu, dodávky, karavanu atp. bez použití externích převodníků.

11. Všechny knihovny využité v konečném zařízení musí mít permisivní licenční podmínky, aby bylo možné zdrojové kódy, schémata a všechny výrobní podklady rovněž šířit pod permisivními podmínkami, nebo naopak využít všechny podklady ke komerční činnosti.

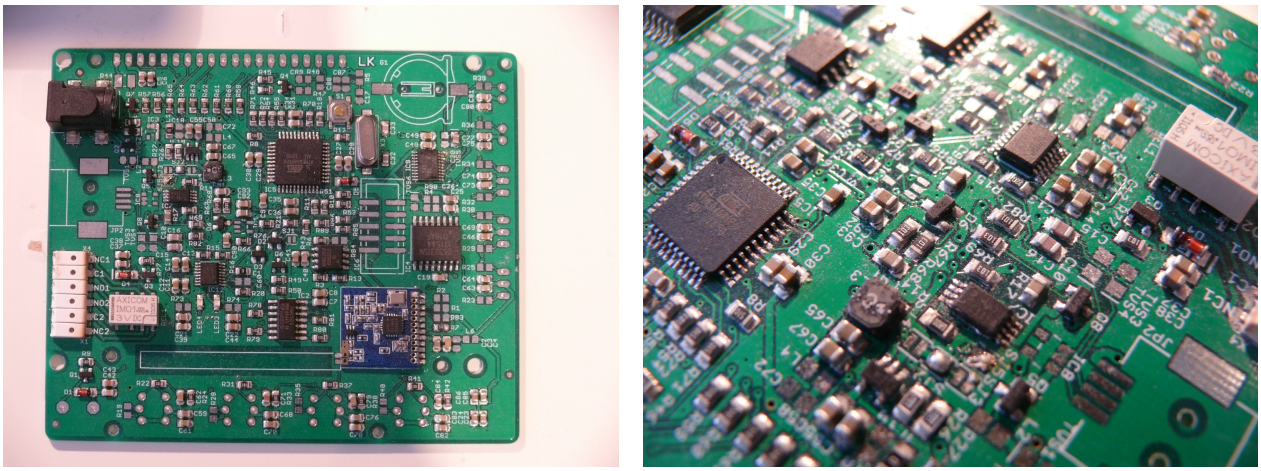
Již v bakalářské práci bylo navrženo zařízení a sonda, které některé z těchto požadavků splňují. Zařízení z bakalářské práce obsahovalo USB port pro nahrávání/stahování dat, paměť pro uložení naměřených hodnot, grafický černobílý displej o rozlišení 128x64 pixelů. Ovládání bylo realizováno čtyřmi podsvícenými tlačítky, dodatečné informace suplovaly kontrolní diody (příjem dat, připojení k PC atp.). V zařízení byl implementován obvod reálného času, aktuální datum a čas se tedy neztratily ani v případě výpadku napájení, hodiny byly zálohovány knoflíkovou baterií. Zařízení mohlo být napájeno buď to z USB portu připojeného počítače nebo z externího adaptéru, přepnutí mezi napájecími větvemi bylo realizováno automaticky proudovým multiplexorem.

Z výše uvedeného odstavce je patrné, že už toto zařízení je poměrně komplexní. Zařízení bylo postaveno na 8 bitovém mikrokontroléru ATMega644[3], taktovaném na frekvenci 8 MHz. Později byl do zařízení implementován vlastní operační systém (respektive se jednalo o preemptivní scheduler, ovladače HW, čili jádro operačního systému). Využití operačního systému bylo vhodné, jelikož zařízení muselo vykonávat vícero úloh „najednou“.

Zařízení vyvinuté v rámci bakalářské práce je vyspělé, avšak nereflektuje úplně poslední trendy v rámci IoT - tedy aby se ovládalo podobně jako smartphone a aby k datům byl přístup i z jiných zařízení, v případě správné konfigurace zařízení a sítě rovněž odkudkoliv z celého světa.

Připojení k Ethernetu či Wi-Fi by bylo teoreticky možné i s 8 bitovým mikrokontrolérem AVR (za použití externího modulu), avšak přístup do webového rozhraní by potřeboval větší množství výpočetních prostředků (obzvlášť při využití SSL/TLS) a v případě využití většího barevného displeje je již tato architektura nedostatečná. Bylo tedy zapotřebí vytvořit nové zařízení s výkonnějším hardwarem. Již vyvinuté části z bakalářské práce tak mohly být využity při tvorbě nového zařízení.

[3] 64kB Flash, 4 kB RAM, 2 kB EEPROM



Obrázek 17: Strana součástek hlavní stanice vyvinuté v rámci bakalářské práce

Fotografie byly pořízeny v průběhu osazování, ne všechny komponenty jsou osazeny, na některých komponentách jsou ještě viditelná rezidua tavidla a studené spoje

Vlevo: celkový pohled na zadní stranu (modrý obdélníček mírně vpravo dole je bezdrátový modul, anténa v obrázku neosazena)

Vpravo: detail mikrokontroléru, spínaného zdroje, proudového multiplexoru, výstupního relé (bílá komponenta vpravo) a USB kontroléru

Obrázek 18: Přední strana hlavní stanice vyvinuté v rámci bakalářské práce

Vlevo: Celkový přední pohled na nezapojené zařízení

Vpravo: Bootující zařízení s připojeným kabelem programátoru (dodává i proud) a sondami logického analyzátoru (červené spojky v horní části obrázku)

4.1.1 Výběr architektury pro nové zařízení

V předchozí kapitole byla z důvodu nedostatečného výpočetního výkonu vyloučena 8 bitová architektura AVR pro tvorbu nového zařízení.

Architektura MSP430 od společnosti Texas Instruments je vhodnější spíše do ultra-nízkopříkonové elektroniky, což v tomto případě není nezbytně nutné.

Další zvažovanou architekturou byla architektura ARM (běžně používaná v současných smartphonech a jednodeskových počítačích). Z této architektury by v úvahu přicházela „mikrokontrolérová linie“ - například STM32 od švýcarské společnosti STMicroelectronics, která by poskytovala dostatek výkonu (obzvlášť u vyšších řad, např. u řady STM32F4). Ve většině případů by bylo zapotřebí využít externí Wi-Fi modul (pokud by nebyla využita řada STM32Wx) a bylo by nezbytné znovu vyvinout velkou část softwaru.

Z ARM byla rovněž zvažována „mikroprocesorová linie / SoC“, a to především SoC od společnosti Allwinner, které bývají využívány v tabletech či jednodeskových počítačích. Jednalo se hlavně o Allwinner A13 (Cortex-A8 1 GHz, GPU Mali400), výkonnější Allwinner A20 (dvoujádro; Cortex-A7 1 GHz) a Allwinner A33 (Čtyřjádro; ARM Cortex-A7 1.5 GHz, GPU Mali400).

Výhody mikroprocesorů oproti mikrokontrolérům:

- Je na nich možné spustit „plnohodnotný“ operační systém - tedy buďto Linuxovou distribuci (eventuelně Android), nebo ideálně FreeBSD.
- Je možné využít „klasické“ vývojové postupy jako v případě vývoje pro desktop:
  - Jednoduché využití předpřipravených grafických knihoven a frameworků.
  - Webové rozhraní by bylo možné naprogramovat „klasickou cestou“ - tedy například pomocí PHP, MySQL a serveru Apache.
    - Jednoduchá obsluha MySQL démona oproti složitému zamykání/odemykání databáze při souběžném přístupu v případě využití SQLite tak, jak bylo popsáno v teoretické části (kapitola 3.6.2 [SQLite]).
- Značný výpočetní výkon.

Naopak nevýhody:

- Náročný vývoj hardware:
  - U vyšších řad je vhodnější či nezbytné využívat „meandrování“ vysokorychlostních digitálních tras na základní desce - obzvlášť u sběrnice spojující RAM modul s SoC.

Meandrování je nezbytné, aby všechny signály dorazily „ve stejný čas“. Korektní vytvoření těchto tras je časově velmi náročné.

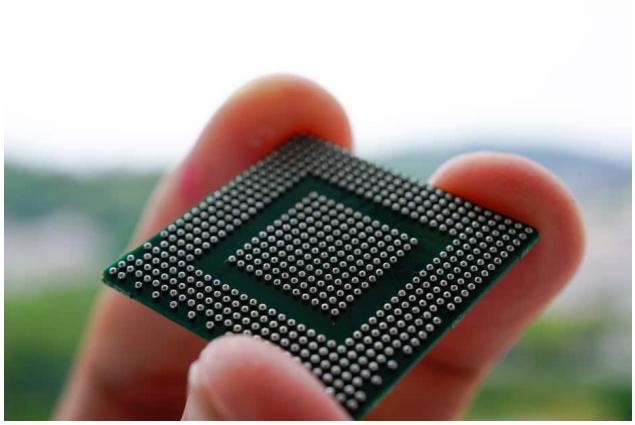
  - Nezbytné vícevrstvé DPS (vyšší cena).

- Mimořádně náročné osazování a následná kontrola v domácích a poloprofesionálních podmínkách:

  - Většina z mikroprocesorů, RAM a flash pamětí nezbytných pro tvorbu takovéhoto zařízení je dodávána v pouzdře BGA (Ball grid array). BGA má řadu výhod (např. velké množství pinů v malém pouzdře), avšak také řadu nevýhod (mezi hlavní patří mimořádně složité pájení a následná kontrola). BGA bývá v praxi osazováno osazovacím automatem a korektnost osazení bývá nejčastěji kontrolována automatizovaným rentgenem nebo endoskopem vloženým pod pouzdro.

- (Většinou) nezbytné změny/záplaty v jádře operačního systému:

  - Obvykle nízkoúrovňové ovladače hardwaru.
  - U Linuxového jádra nezbytné zveřejnění zdrojového kódu (GPL licence).



Obrázek 19: Ukázka pouzdra BGA
Zdroj: (Shashikanth, 2020)

Posledním zvažovaným druhem bylo ESP32 od společnosti Espressif. ESP32 je dvoujádrový mikrokontrolér, o němž bylo již psáno v teoretické části - kapitola č.3.5.1.1 (ESP32).

Výhody ESP32:

- Obstojný výkon.

- Wi-Fi a Bluetooth implementovány přímo na čipu.
- Velmi levné.
- Přímo určeno na IoT projekty.
- Mikrokontrolér spolu s anténou, externí flash a RAM pamětí k dispozici ve formě modulů, které je možné připájet k základní desce.
- Velké množství knihoven portováno přímo do vývojového frameworku výrobce, včetně síťových knihoven a modifikovaného operačního systému FreeRTOS.

Nevýhody ESP32:

- Autor práce nemá s danou platformou žádné zkušenosti.
  - Subjektivní názor.

Po delší úvaze bylo tedy zvoleno řešení postavené na technologii ESP32.

4.2 Pojmenování projektu

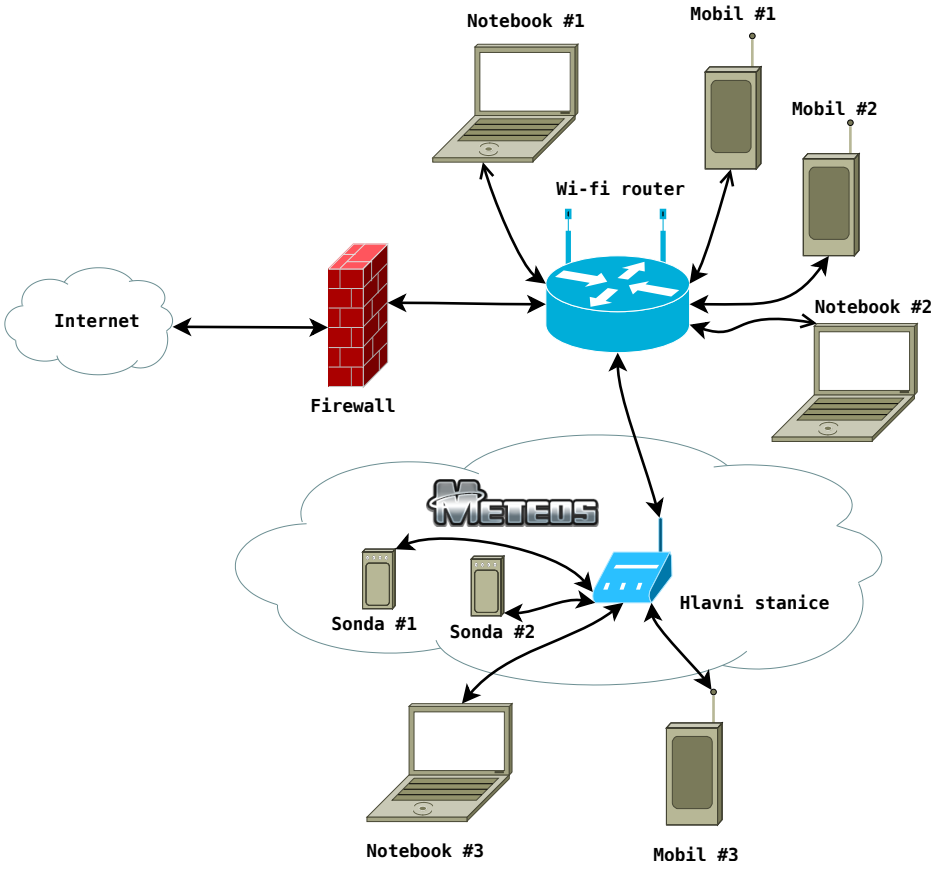
Jelikož je celý projekt mimořádně rozsáhlý, bylo zapotřebí jej pojmenovat a vytvořit logo, které by se zobrazovalo v zařízení a v administračním rozhraní.

Celý projekt je víceméně implementací **Meteo**rologického **s**ystému (zkráceně „Meteos“).

Vlevo: logo s nižším rozlišením (využívané ve webovém rozhraní)
Vpravo: logo s vysokým rozlišením (používané tam, kde je zapotřebí vysokého rozlišení)

Obrázek 20: Logo projektu

4.3 Schéma domácí sítě s využitím ekosystému Meteos



Obrázek 21: Schéma sítě s využitím ekosystému Meteos

Na obrázku č.21 je patrný návrh domácí sítě s využitím ekosystému Meteos.

K hlavní stanici se lze připojit pomocí hlavního přístupového prvku domácí sítě (Wi-Fi routeru). Avšak je rovněž možné, aby se zařízení klientů přihlásilo přímo k hlavní stanici. Ta je totiž schopna sama vytvořit další přístupový bod nové Wi-Fi sítě, pomocí kterého je možné se připojit. Dodatečné informace o síti jsou suplovány DHCP serverem, který pracuje přímo na hlavní stanici.

4.4 Hardware

V této kapitole bude rozepsán konkrétní návrh hardware jak pro novou hlavní stanici, tak pro sondy.

4.4.1 Hlavní stanice

Hlavní stanice je zařízení, které se nachází v interiéru a měří zde teplotu, tlak, vlhkost, osvětlení a UV index. Lze ji napájet širokým napájecím napětím od 6 do 36 V DC, pro napájení je tedy možné použít například běžný zdroj notebooku či jiný, dostatečně tvrdý zdroj v uvedeném rozsahu napětí. Díky širokému rozsahu vstupního napětí je možno stanici jednoduše využívat bez jakéhokoliv aktivního adaptéru například v autě či obytném voze, ať už se jedná o běžný osobní automobil, který má napětí palubní sítě 12 V, či větší automobil, jehož napětí palubní sítě je 24 V. Navržené zařízení rovněž obsahuje ochranu proti zkratu.

Zařízení je na svém vstupu mimořádně odolné - přepěťová ochrana je dimenzována na 200 V DC, které je zařízení schopné trvale ustát a přitom se nepoškodit. Pokud je napěťový impulz vyšší než 36 V, zařízení se automaticky přizpůsobí a je kratší chvíli schopné pracovat i mimo rozsah napájecího napětí. Pokud je impulz příliš silný nebo dlouhý, aktivuje se vnitřní ochrana zařízení, která jej vypne, aby se zabránilo poškození. Po odeznění tohoto děje se stanice opět po určité době sama zapne. Jelikož například v napájecí soustavě automobilu může dojít ke značnému nárůstu napětí, kdy je náhle odpojena velká zátěž od alternátoru, je tato ochrana nezbytná.

Stanice má rovněž ochranu proti nesprávné polaritě, ta je dimenzována na -40 V a je v zařízení z důvodu ochrany proti přepólování. Může k němu dojít poměrně snadno, když případný uživatel použije „univerzální napájecí adaptér“, který sice má napájecí koncovku, kterou požaduje zařízení, avšak jeho napájecí větve jsou přehozeny. V tomto případě se stanice nezapne, ale ani nepoškodí.

V zařízení je rovněž ochrana proti podpětí. Pokud napětí na svorkách zdroje klesne pod 5.5 V, zařízení se automaticky odpojí.

Všechny kabelové vstupy a výstupy jsou rovněž chráněny transily.

Na základní desce zařízení se nachází wattmetr, který měří aktuální spotřebu a je schopný rovněž varovat například při vybití baterie automobilu pod mez, kdy již nejde nastartovat.

Zařízení je postaveno na modulu mikrokontroléru ESP32, který pomocí sběrnic komunikuje s ostatními součástkami; schéma sběrnic a napájení je možné vidět na zjednodušeném schématu hlavní stanice na obrázku č.22 (Zjednodušené schéma hlavní stanice).

Stanice obsahuje USB rozhraní, které bylo v současné revizi využito k nahrávání firmwaru, do budoucna se počítá například s možností stahování naměřených dat pomocí kabelového spojení (stahování dat je rovněž možné přes webové rozhraní meteostanice).

K modulu ESP32 je připojena externí flash paměť, která slouží k uchování naměřených dat jak hlavní stanice, tak připojených sond a rovněž veškerého nastavení.

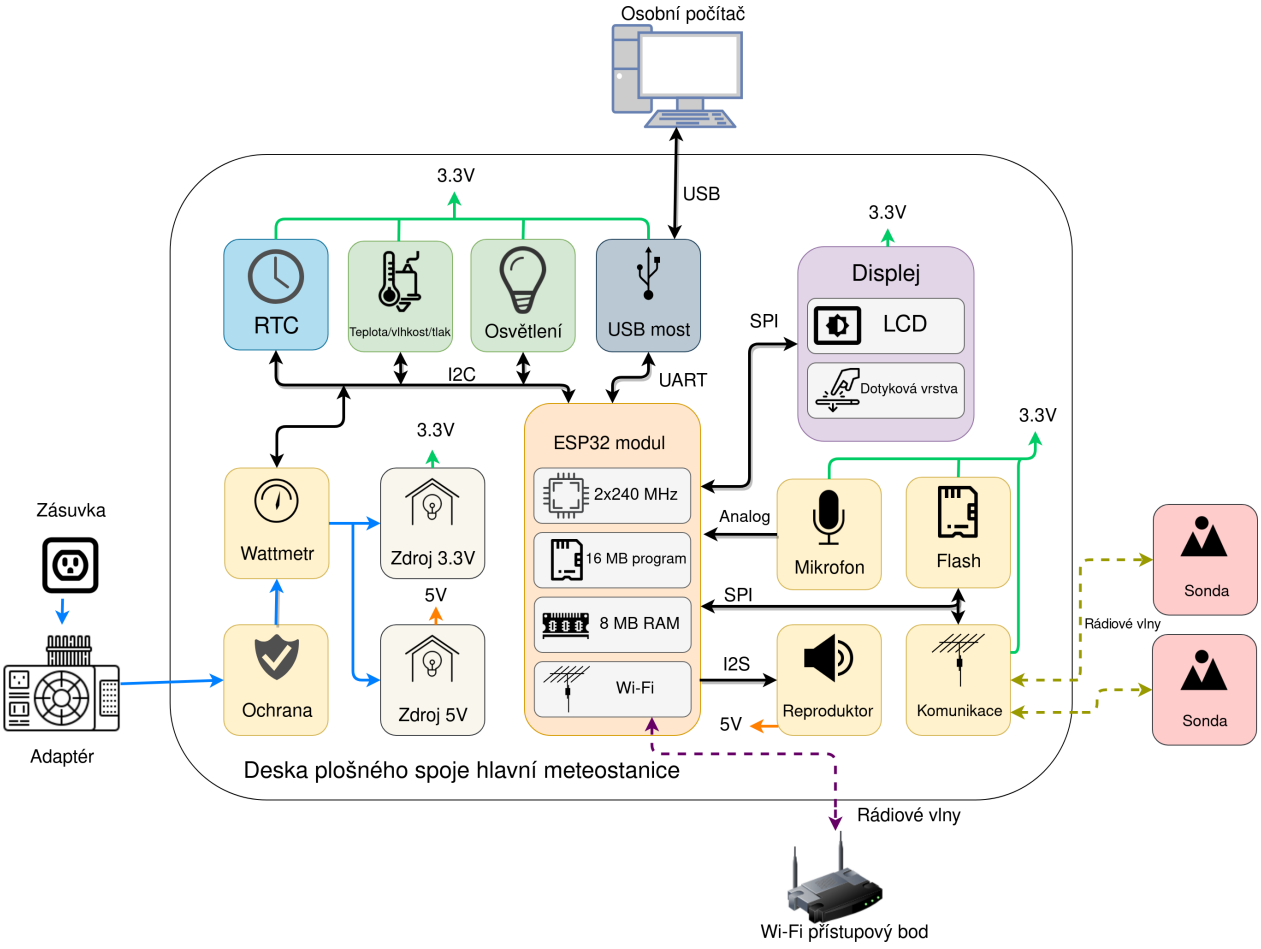
Zařízení obsahuje mikrofon, který je zamýšlen jako jednoduchý hlukoměr, díky němuž je možné

automaticky měnit hlasitost vestavěného reproduktoru. V budoucích revizích firmwaru se počítá s využitím mikrofonu k ovládání pomocí hlasu.

Stanice dále obsahuje reproduktor, který je schopný přehrávat hudbu (internetové rádio), případně přehrávat lidský hlas (vhodné při předčítání naměřených hodnot, ve firmware prozatím neimplementováno).

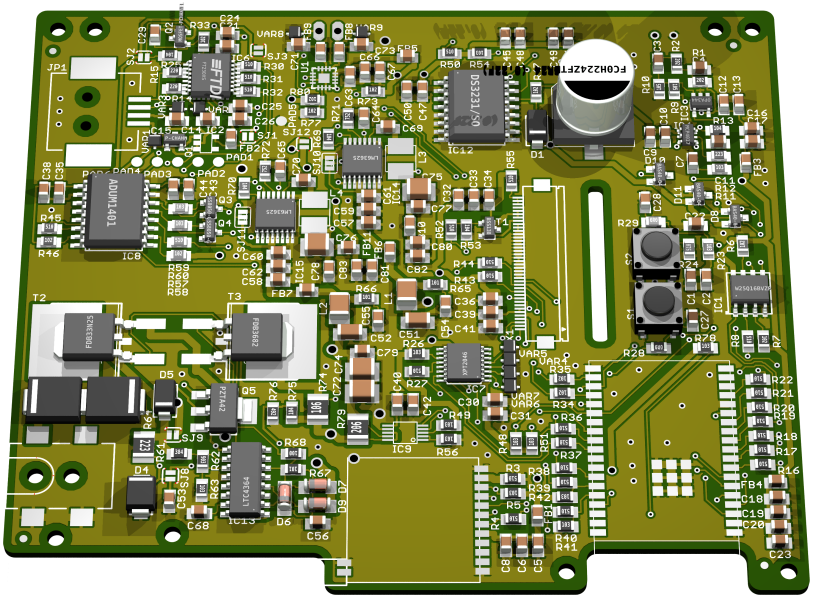
Zařízení obsahuje dotykový barevný displej s rozlišením 480x320 pixelů a dotykovou odporovou vrstvou.

Navržené zařízení obsahuje modul pro bezdrátový přenos dat mezi hlavní stanicí a přidruženými sondami.

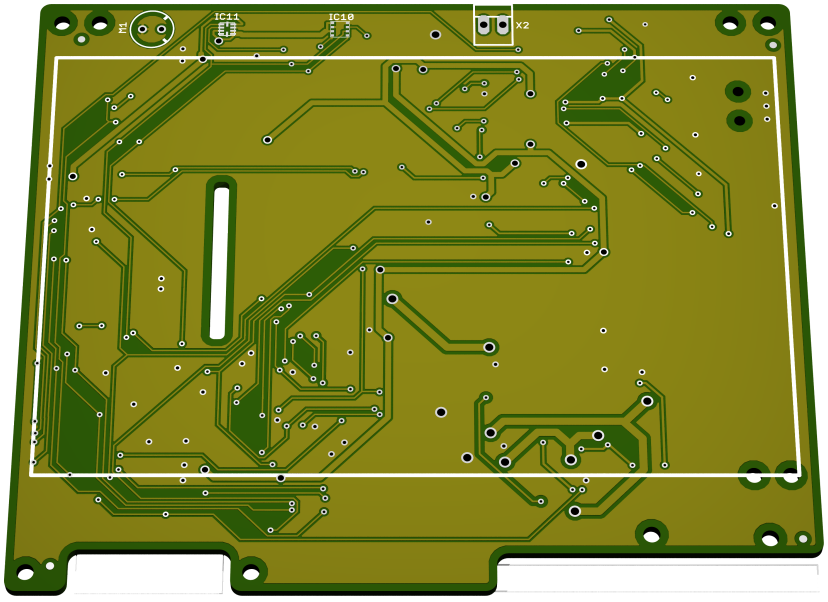


Obrázek 22: Zjednodušené schéma hlavní stanice

4.4.1.1 Render základní desky nové hlavní stanice



Obrázek 23: Render nové hlavní stanice - strana součástek



Obrázek 24: Render nové hlavní stanice - přední strana
Velká část přední strany DPS hlavní stanice obsahuje displej (velký bílý obdelník), dále jsou zde senzory (horní část), je zde rovněž viditelný výřez na plochý kabel displeje.

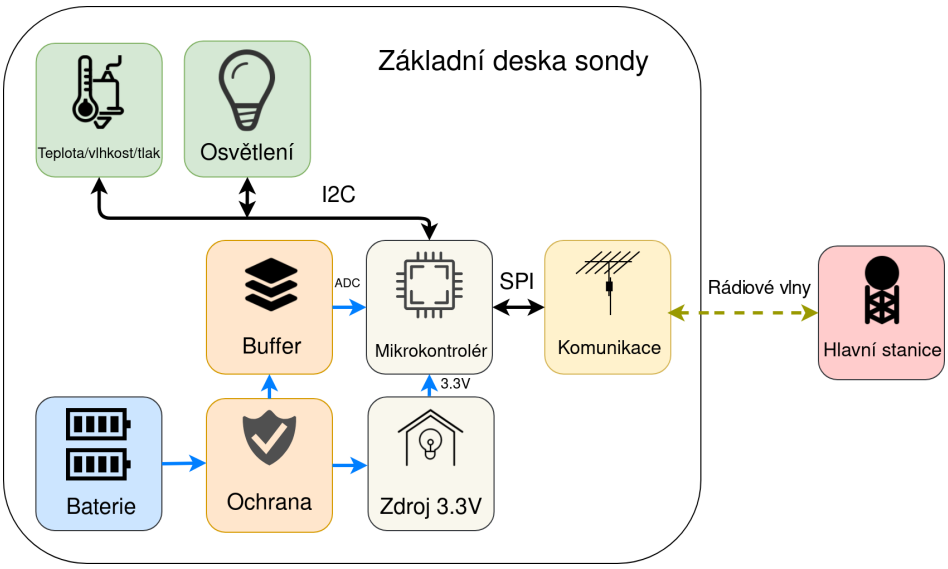
4.4.2 Sonda

Sonda je zařízení, které může být využito jak v interiéru, tak exteriéru. Slouží k měření fyzikálních veličin a k přenosu těchto naměřených dat na hlavní stanici, která se nachází v interiéru.

Sonda je napájena pomocí dvou AA monočlánků, obsahuje vyspělý spínaný zdroj, který je schopný nastartovat již od 0.5V a je schopen pracovat až do 0.3V. Baterie vybité pod tuto úroveň je možné prohlásit za kompletně vybité.

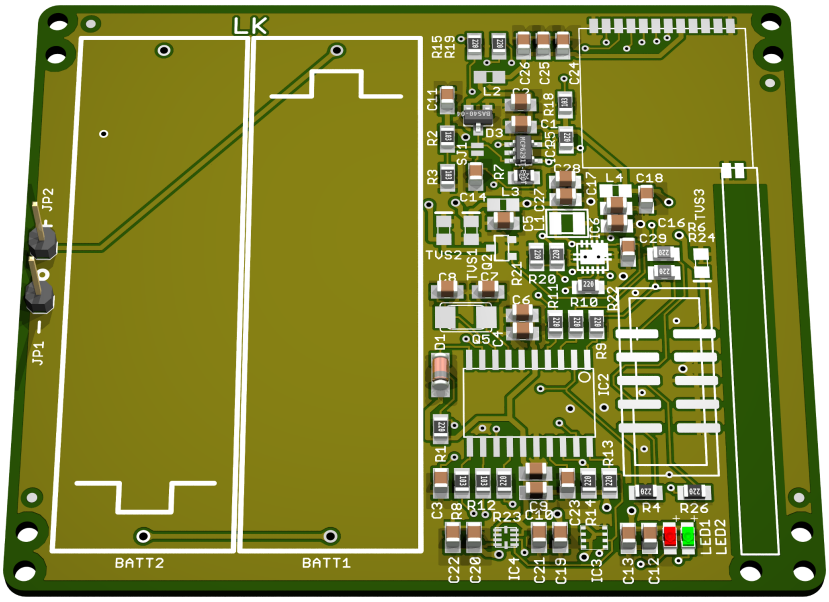
Sonda je postavena na mikrokontroléru AVR ATTINY861. Mikrokontrolér komunikuje se senzory, které jsou umístěné na stejné základní desce. Zjednodušené schéma sondy je možné prohlédnout na obrázku č.25 (Zjednodušené schéma sondy)

Zařízení je na svém vstupu chráněno transily a proti přepólování (pokud by uživatel vložil baterie do zařízení obráceně).

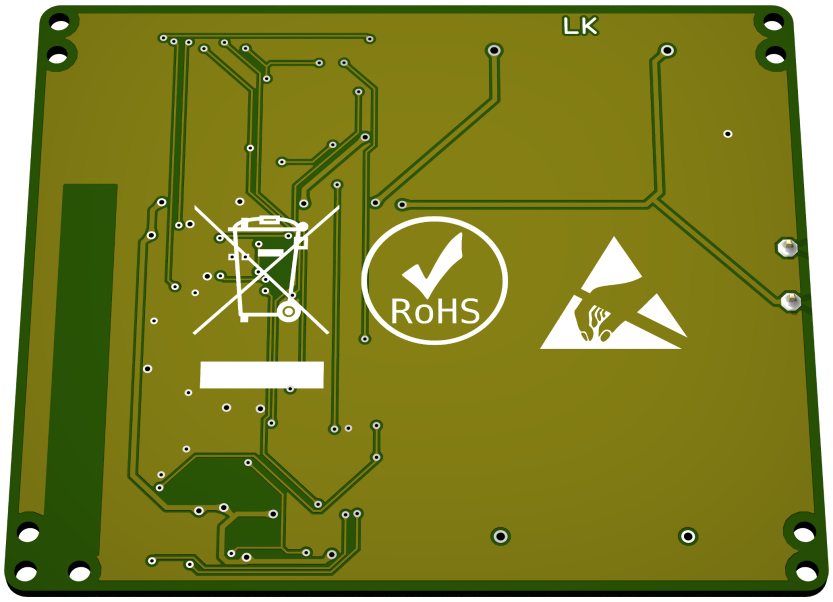


Obrázek 25: Zjednodušené schéma sondy

4.4.2.1 Render sondy



Obrázek 26: Render sondy - strana součástek



Obrázek 27: Render sondy - zadní strana

4.5 Firmware

Firmware je softwarové vybavení jak sondy, tak hlavní stanice.

4.5.1 Hlavní stanice

Firmware hlavní stanice je velmi komplexní. Obsahuje ovladače hardwaru („drivery“), knihovny síťových protokolů, kryptoknihovny, webserver, rozhraní pro přístup k databázi SQLite a další komponenty, které jsou vzájemně svázány s modifikovaným operačním systémem FreeRTOS.

Celý firmware hlavní stanice je napsán v programovacím jazyce C.

Bylo rovněž uvažováno o využití jazyka C++ z toho důvodu, že by v něm bylo možno lépe modelovat informační systém (kapitola č. 4.5.2) a využít některý z návrhových vzorů (obzvlášť vhodný by byl MVC - Model view controller) pro vytvoření uživatelského rozhraní. Jelikož je však velká část nízkoúrovňových rutin napsána v „čistém“ jazyce C, byl objektový přístup C++ nahrazen procedurálním přístupem v jazyce C tak, aby nedocházelo k míchání paradigmat a nutnosti využívat jiný kompilátor podporující C++.

Vzhledem k tomu, že vývoj firmwaru započal ještě předtím, než byl hotov hardware, na kterém měl tento firmware pracovat, byl vývoj firmwaru poměrně složitý. Jelikož je firmware poměrně velký a nahrávání do zařízení zabere dlouhou dobu, byly části, které nezbytně nesouvisí s hardwarem vytvářeny a simulovány přímo v osobním počítači. Informační systém tak byl de facto navržen přímo na desktopu (v jazyce C byl napsán velmi jednoduchý server, který zpracovával a vyřizoval požadavky a tak bylo možné tento systém otestovat). Tento přístup znamenal značné urychlení vývoje a testování, navíc bylo možné využít nástroje jako Valgrind pro hledání úniků paměti, jelikož úniky paměti jsou obzvlášť pro vestavěné systémy velmi nebezpečné.

4.5.1.1 Předpověď počasí

Ve firmwaru hlavní stanice je implementován klasický algoritmus Zambretti přesně tak, jak byl popsán v teoretické části, konkrétně v kapitole č.3.3.2.2 (Algoritmus Zambretti). Tento algoritmus byl přepsán do programovacího jazyka C, předpověď počasí je v současné době pouze textová dle tabulky č.1 (Algoritmus Zambretti).

4.5.1.2 Předpověď fází Měsíce

V kapitole č.3.4.2.1 (Předpověď lunárních fází) byl popsán naivní algoritmus pro aktuální výpočet fáze Měsíce. Tento algoritmus byl přepsán do jazyka C a na jeho základě lze nyní určit, v jaké fázi se Měsíc v konkrétní den nachází.

4.5.1.3 Předpověď východu a západu Slunce

Předpověď východu a západu Slunce je v meteostanici implementována pomocí algoritmu „Sunrise equation“, který byl podrobněji rozepsán v teoretické části, kapitole č.3.4.3 (Předpověď východu a západu Slunce). Stejně tak jako u předpovědi počasí a předpovědí fází Měsíce byl tento algoritmus přepsán do jazyka C, byl staticky slinkován s ostatními částmi programu a poté byl nahrán do zařízení.

4.5.2 Informační systém hlavní stanice

Informačním systémem rozumíme softwarové vybavení hlavní stanice, které umožňuje správu dat uložených v zařízení, vytváření grafů, správu přístupů jednotlivých uživatelů a nastavení zařízení. Informační systém je úzce svázán s firmwarem hlavní stanice a tedy i s operačním systémem, na kterém tato hlavní stanice pracuje.

Přístup k informačnímu systému je dvojí: buď to fyzickým zalogováním na hlavní stanici (pomocí dotykového displeje a zobrazené softwarové klávesnice) nebo pomocí webového rozhraní.

Velká část informačního systému je naprogramována v jazyce C, což je poměrně nezvyklé oproti ostatním informačním systémům; běžné bývá, že je webový informační systém navržen v PHP využívající (My)SQL databázi, alternativně (u velkých podnikových aplikací) jsou využity Jakarta/Java Servlety.

Oba výše uvedené přístupy jsou velmi náročné na systémové požadavky. PHP je interpretovaný jazyk, navíc jeho portování na tak omezenou platformu, kterou využívá hlavní stanice, by bylo značně náročné. Originální Java využívá virtuální stroj, který vytváří prostředí pro aplikace a umožňuje JIT kompilaci. Vytvoření nového virtuálního stroje a JIT kompilátoru na platformě využité v hlavní stanici by pro jednoho člověka bylo takřka nemožné.

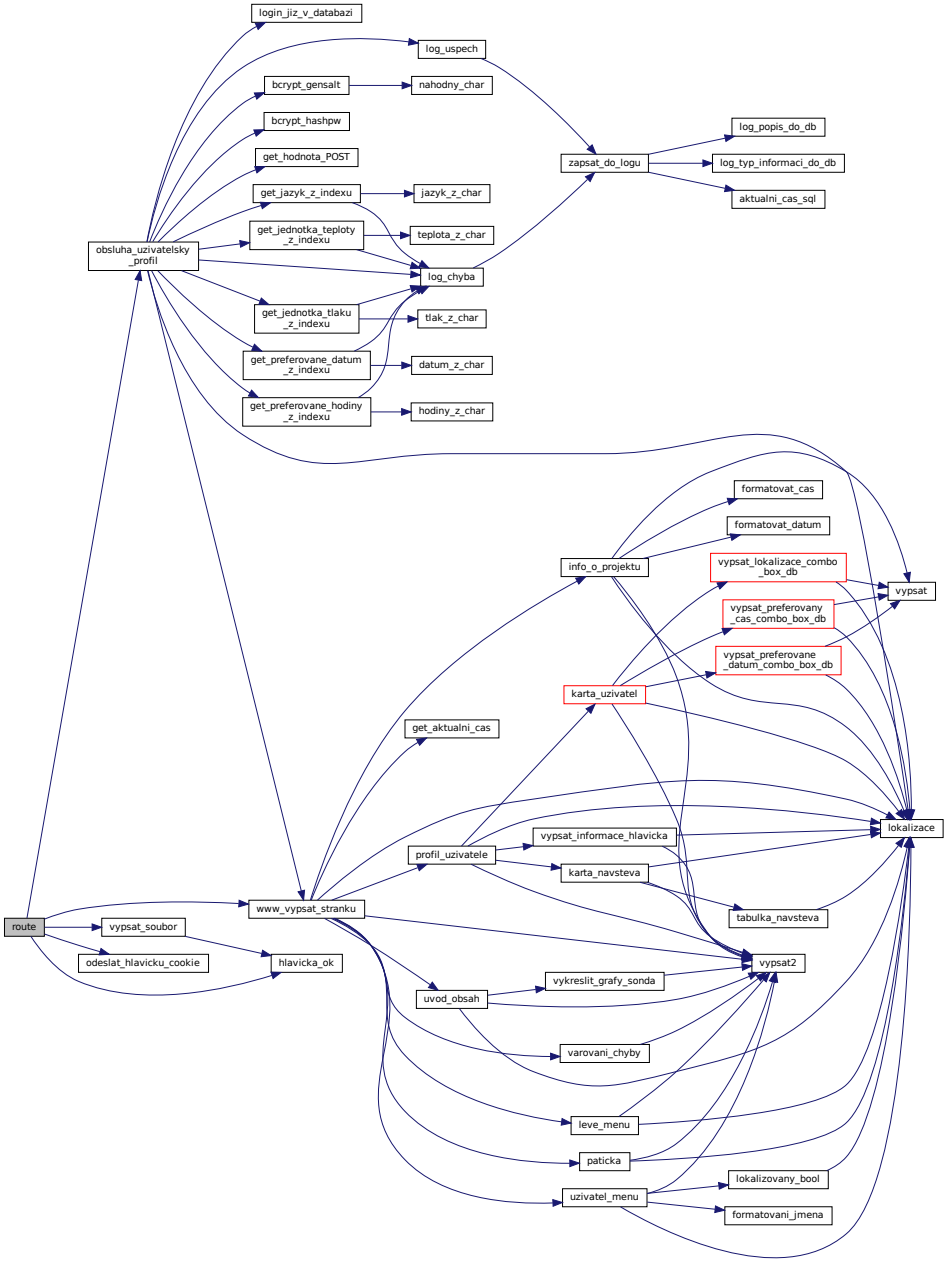
Byl tedy zvolen „old-school“ přístup, který mírně připomíná CGI[4] využívané hlavně na přelomu milénia, kdy parametry hardwaru byly velmi skromné.

Odpovědnost v informačním systému je však možné rozdělit klasicky na frontend a backend:

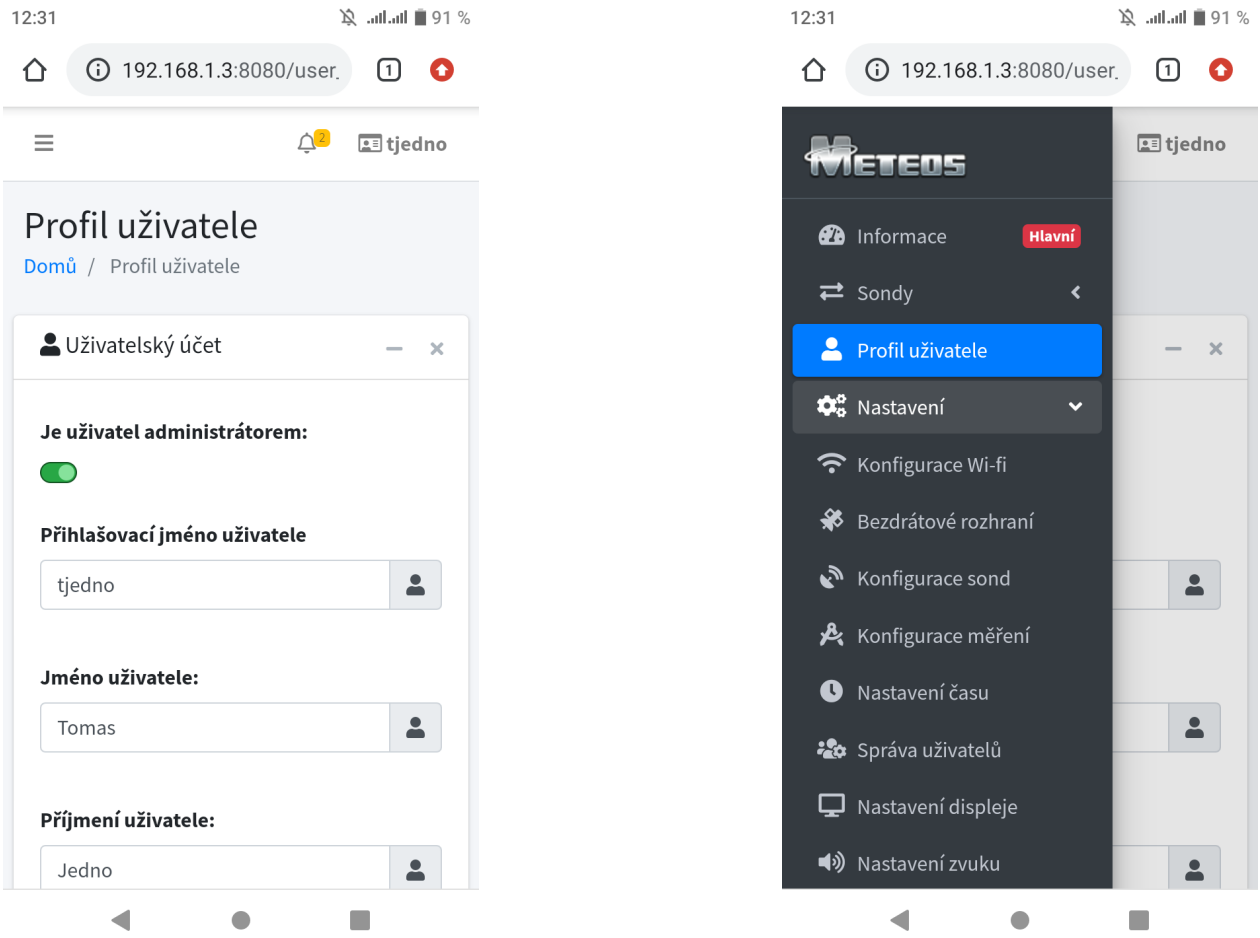
- Backend je vrstva operující nad samotnými daty, tato vrstva je celá napsána v jazyce C.
- Frontendy (prezenční vrstvy) jsou de facto dvě:
  - Webový frontend, který využívá minifikovaný framework Bootstrap (tedy HTML, CSS a JavaScript), kód pro připojeného klienta je emitován backendem.

[4]Common Gateway Interface

– „Lokální“ frontend, který uživateli zprostředkovává GUI na vestavěném dotykovém displeji (využita knihovna LVGL, v programovacím jazyce C).



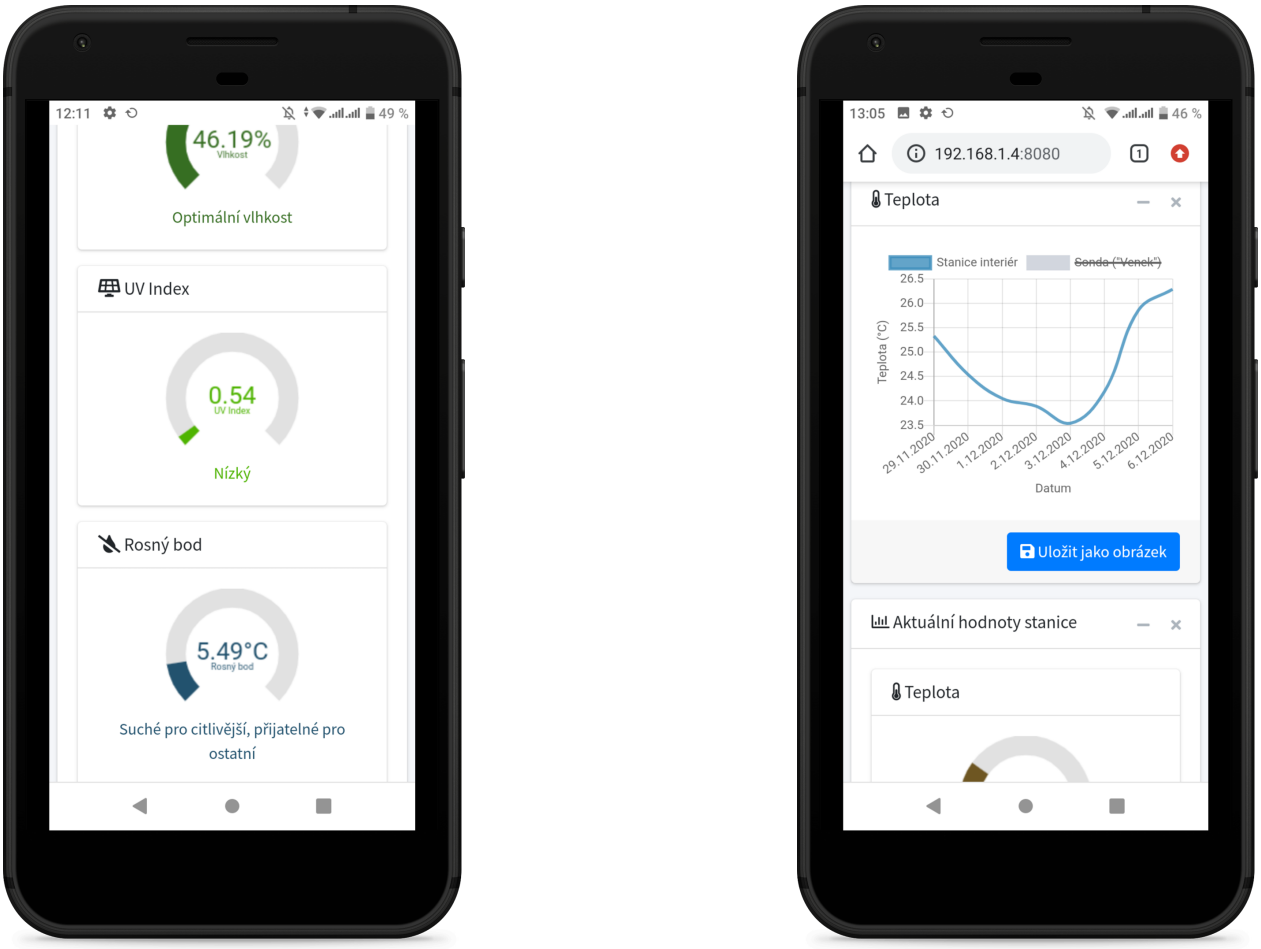
Obrázek 28: Graf volání funkcí z pohledu webserveru
Graf generován přímo ze zdrojových kódů
Zobrazena pouze část volaných funkcí ve firmwaru hlavní stanice



Obrázek 29: Ukázka editace údajů aktuálně přihlášeného uživatele (webový frontend, mobilní verze - Chrome, Android 9)

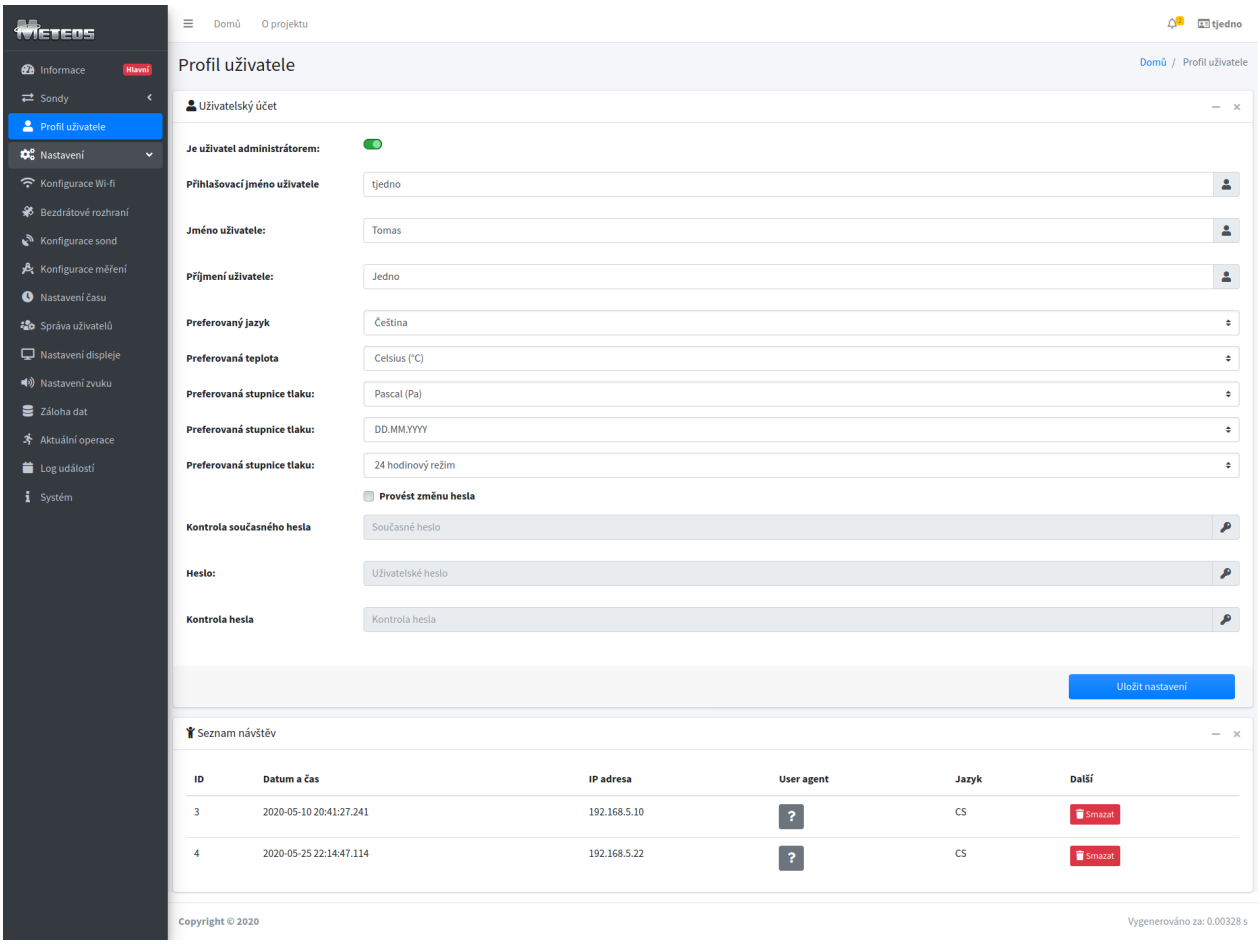
Vlevo: Menu deaktivováno
Vpravo: Menu aktivováno

Obrazovky naměřených hodnot je možné vidět na následujících obrázcích:



Vlevo: obrazovka aktuálně naměřených údajů, včetně základní interpretace
Vpravo: Graf historických dat (v tomto případě průměrné denní teploty za 8 dnů)

Obrázek 30: Ukázka obrazovek naměřených údajů



Obrázek 31: Ukázka editace údajů aktuálně přihlášeného uživatele
webový frontend, PC verze, Firefox, vyfocená celá stránka, pre-alpha verze

4.5.2.1 Ukládání dat v hlavní stanici

Veškeré ukládání dat v hlavní stanici probíhá za pomoci relační databáze SQLite, která je staticky slinkována s ostatním firmwarem a následně nahrána do zařízení. Celá databáze (tedy její data) je uložena ve flash paměti zařízení.

4.5.2.2 Přístup k informačnímu systému / autentizace uživatele

Uživatel se standardně prokazuje uživatelským jménem a heslem. Jméno uživatele a otisk hesla jsou uloženy v databázi. Při přihlášení je na heslo aplikována hashovací funkce bcrypt a poté je vypočtená hodnota zkontrolována s hodnotou uloženou v databázi. Pokud se hodnoty shodují, uživatel byl ověřen a v systému je vytvořena nová sezóna. Bcrypt by bylo vhodnější nahradit jiným hasho-

vacím schématem - scrypt nebo lépe Argon2, jelikož však má zařízení velmi omezené hardwarové prostředky, je nutné se držet funkce bcrypt s nižším faktorem ceny (cost factor).

Algoritmus 16 Aktuální implementace sezóny

```
typedef struct sezona {
    char * jmeno_uzivatele;
    char * prijmeni_uzivatele;
    char * login;
    char * token;
    char * otisk_hesla;
    int id_uzivatele_databaze; //slouzi rovnez jako primarni klic v databazi - v teto strukture
        se uchovava pro pripad, kdyby si uzivatel pral zmenit login a dalsi udaje
    role role_uzivatele;
    long aktivni_od;
    jazyk preferovany_jazyk;
    teplota_jednotky preferovana_teplota;
    tlak_jednotky preferovany_tlak;
    preferovane_hodiny hodiny_preference;
    preferovane_datum datum_preference;
} sezona;
```

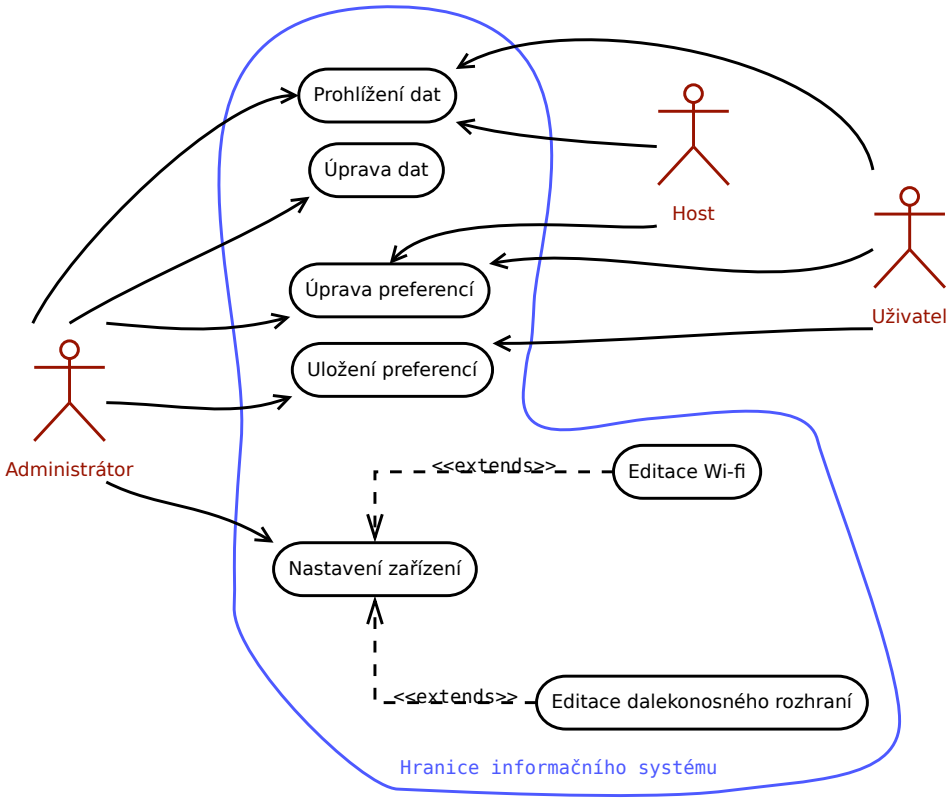
Po vytvoření sezóny se uživatel vůči informačnímu systému prokazuje pomocí autentifikačního cookie.

4.5.2.3 Role uživatele

V současné verzi existují 3 role uživatelů, které jsou následující:

- Host
  - V dané relaci má přístup pouze k naměřeným datům. Informační systém uchovává informace o aktuálně zalogovaných hostech.
    - Je tedy možné, aby v dané relaci host změnil některé své preference (primárně se jedná o preferované jednotky teploty, tlaku aj. a rovněž o preferovaný jazyk).
    - Po ukončení relace si systém nepamatuje preference hosta a host si je při dalším přihlášení musí znovu nastavit.
    - Pro zapamatování preferencí slouží účet „Uživatel“.
- Uživatel
  - Na rozdíl od hosta se uživatel přihlašuje pomocí svého uživatelského jména a hesla. Jediný rozdíl oproti hostovi je v tom, že si informační systém pamatuje, co uživatel nastavil v předcházející relaci.

- Správce (administrátor)
  - Správce/administrátor má kompletní kontrolu nad systémem.
    - Je podporováno vícero administrátorských účtů, není tedy zapotřebí jeden sdílený účet.
  - Správce je oprávněn měnit veškeré nastavení celého systému, například:
    - Preferovaná Wi-Fi síť, ke které je připojená meteostanice
    - Přidávání/odebírání a editace uživatelů
    - Přiřazování/odebírání administrátorského oprávnění
    - Konfigurace sond
    - Konfigurace hlavní stanice (četnost měření)
    - Nastavení času hlavní stanice (NTP včetně adres nových NTP serverů, případně manuální zadání času)
    - Nastavení lokality hlavní stanice (nutné pro výpočet východu a západu Slunce)
    - Nastavení displeje (režim šetření energií, kdy se po určité době displej vypne)
    - Nastavení zvuku (automatická/manuální hlasitost, případné deaktivování)
    - Záloha dat (export z interní SQLite databáze)
    - Prohlížení aktuálních operací meteostanice (přihlášení uživatelé...)
    - Aktualizace firmwaru zařízení



Obrázek 32: Diagram užití informačního systému
Zjednodušeno

4.5.3 Sonda

Firmware sondy primárně implementuje přenosový protokol, který bude podrobněji rozepsán v kapitole č.4.6 (Protokol přenosu dat mezi sondami a hlavní stanicí).

4.6 Protokol přenosu dat mezi sondami a hlavní stanicí

Tato kapitola pojednává o navrženém protokolu, který zprostředkovává komunikaci mezi sondami a hlavní stanicí.

Navržený protokol je vylepšením velmi jednoduchého protokolu, který byl navržen v bakalářské práci.

Protokol je navržen pro polo-duplexní přenos, jelikož transceivery v obou typech zařízení jsou polo-duplexní (v jednu chvíli je možné pouze vysílat nebo pouze přijímat).

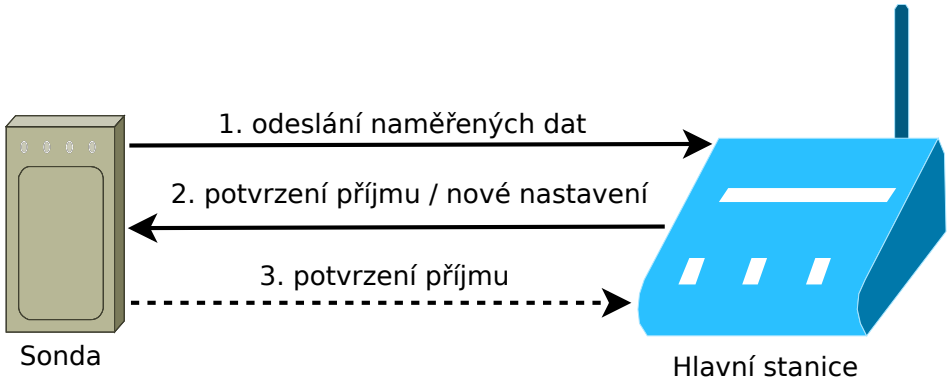
Jedním z hlavních předpokladů protokolu je, že hlavní stanice bude neustále naslouchat možným paketům, přičemž sondy budou většinu času neaktivní.

Spojení nejčastěji inicializuje sonda (která odesílá naměřená data v určitém intervalu) a posléze čeká na potvrzení příjmu nebo na nové instrukce (změna nastavení sondy). Pokud bylo odesláno nové nastavení, sonda potvrzuje příjem. Pokud sonda neobdrží potvrzení příjmu od hlavní stanice, ponechává naměřená data ve své operační paměti (přiřadí k nim časovou značku) a pokusí se je odeslat v dalším vysílacím okně.

Jelikož záleží na pořadí přijatých paketů a dochází k potvrzování doručených zpráv, jedná se o spojovanou komunikaci.

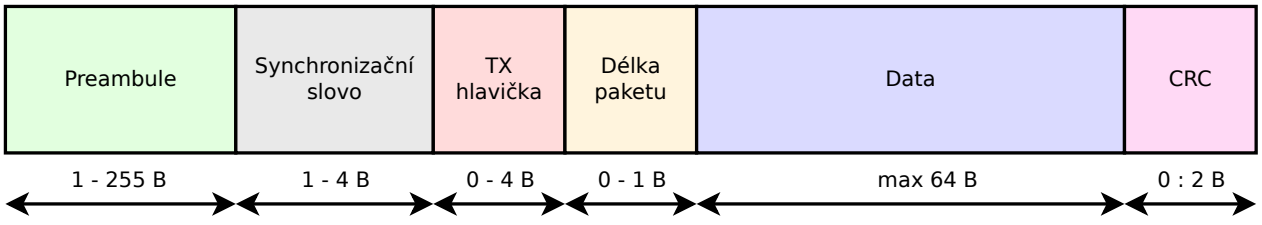
Protokol v současné verzi využívá hvězdicovou topologii.

Běžný typ operace ilustruje obrázek č.33 (Diagram protokolu při běžném užití).



Obrázek 33: Diagram protokolu při běžném užití

Na obrázku níže je uvedena hardwarová struktura paketu tak, jak ji vysílá/přijímá transceiver obou zařízení.



Obrázek 34: Struktura paketu

- První část obsahuje **preambuli a synchronizační slovo**, které slouží k detekci přijatého paketu.
- „**TX hlavička**“ obsahuje adresu přijímače. Pokud přijímač přijme paket, jehož hlavička se liší od adresy tohoto přijímače, je paket zahozen. Využito při nešifrovaném spojení.

- „**Délka paketu**“ určuje, jak velké množství dat je přenášeno.
- „**Data**“ obsahuje samotný užitečný náklad (payload) - tedy například nastavení, naměřená data, jak bude probráno v podkapitolách popisujících strukturu podpaketů. Datové podpakety jsou zabaleny do obalů, které určují, zda-li byl paket odeslán šifrovaně či nešifrovaně.
- „**CRC**“ volitelně obsahuje kontrolní součet paketu, aby byla detekována případná chyba při přenosu.

Transceiver obou zařízení obsahuje automatický detektor preambule. Preambuli je možné volit v délce 1-255 bajtů, přičemž transceiver vyhledává vzor v nastavitelné délce.

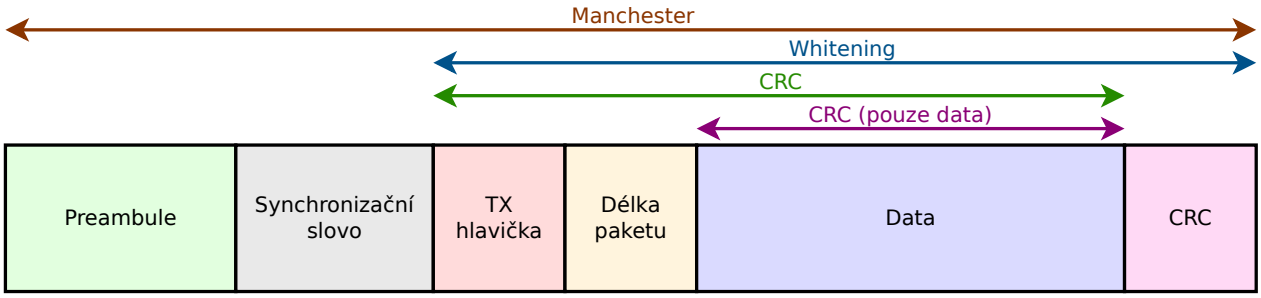
Pokud je detekována nesprávná preambule, přijímač pokračuje ve vyhledávání preambule, pokud není nalezeno synchronizační slovo. Jakmile je detekována nová preambule (správná či nesprávná), je následně vyhledáváno synchronizační slovo (sync). Pokud není sync nalezen, zařízení přejde automaticky do nového vyhledávání.

4.6.1 Délka preambule

Preambule je detekována tzv. prahem detekce preambule. Délka tohoto prahu určuje, zda-li zařízení správně zachytí paket či nikoliv; může dojít ke dvěma případům - buď to je paket zcela minut (nedetekován), nebo je nesprávně detekován signál, který není datovým paketem. V obou případech může dojít ke ztrátě požadované informace. Ve firmwaru hlavní stanice jsou naprogramovány jednotlivé délky prahu detekce v závislosti na modulační technice. V protokolu jsou tato pole z toho důvodu, že v budoucnu může dojít ke změně firmwaru a prahy bude možné volit manuálně.

4.6.2 Data whitening, kódování Manchester a CRC

Pro zvýšení spolehlivosti přenosu byly do protokolu implementovány možnosti nastavení Data whitening, kódování Manchester a CRC. Pokrytí jednotlivých úseků datového paketu ilustruje následující obrázek:



Obrázek 35: Oblasti paketu pokryté Data whitening, kódováním Manchester a CRC

Protokol umožňuje zvolit, zda-li je CRC aplikováno pouze na data, či i na TX hlavičku a délku paketu.

4.6.3 Párování sondy a hlavní stanice

Sondu/y je nejprve zapotřebí spárovat s hlavní meteostanicí. K meteostanici je v současné verzi možné v jednu chvíli připojit až 255 sond, přičemž je ovšem nezbytné brát v potaz další omezení: na daném kanálu/frekvenci může v jednu chvíli vysílat pouze jedno zařízení. Pokud by na jedné frekvenci bylo připojeno větší množství sond, která by odesílala v krátkém intervalu data, mohlo by dojít ke vzájemnému rušení.

Je zde ovšem další problém, který souvisí s nepřesností oscilátorů jednotlivých sond. Pokud je sond více a mají nastaven stejný interval odesílání, může v určité době dojít k souběhu oscilátorů, díky čemuž sondy vysílají ve stejný čas, což vede k rušení a nefunkčnosti celého systému (například jedna sonda se mírně předbíhá, druhá se mírně opožďuje). Nějakou dobu poté trvá, než se oscilátory od sebe navzájem „vzdálí“ a přenos signálu pokračuje korektně. V mezidobí tak může dojít ke ztrátě většího množství dat a nemožnosti nastavovat takto postižené sondy. Z tohoto důvodu byla do protokolu zabudována ochranná funkce, která má zajistit, aby k tomuto souběhu nedocházelo (respektive pokud k němu dojde, bude z velké části eliminován). Toho je docíleno tak, že je k intervalu vysílání sond přidána umělá odchylka, která určuje, o kolik milisekund se může vysílání zpozdit či naopak předběhnout. Sonda poté volí hodnotu odchylky náhodně (maximum je nastavená odchylka) a přičítá/odečítá ji k původnímu intervalu vysílání. Sonda poté vysílá s mírně změněným časem. Tuto funkcionalitu je samozřejmě možné vypnout.

4.6.3.1 Princip párování

Princip párování je následující:

- Hlavní stanici je zapotřebí přepnout do režimu přidávání nových sond (buď to přes webové rozhraní, nebo přes dotykový displej).
  - V režimu přidávání nových sond je na hlavní stanici zapotřebí vyplnit identifikační číslo sondy a jednorázové heslo (oba tyto údaje jsou zadány do sondy ve výrobě a koncovému uživateli jsou dodávány v papírové podobě a jsou rovněž uvedeny na zadní straně každé sondy).
  - Po zadání potřebných údajů se hlavní stanice přesune na tzv. rendez-vous frekvenci (jedná se o hlavní frekvenci, na které se setká jak hlavní stanice, tak sonda, přesná frekvence je napevno určená ve firmwaru obou zařízení). Hlavní stanice poté začne periodicky vysílat paket párování, na který očekává odpověď.
  - Poté je zapotřebí zapnout sondu (vložit do ní baterie).
    * Pokud sonda doposud nebyla párována s žádnou meteostanicí, automaticky se přesune na rendez-vous frekvenci a očekává párovací paket. Pokud sonda již byla párována, přesune se na rendez-vous frekvenci po dobu 10 vteřin (aby případně bylo možné spárovat sondu s novou hlavní stanicí). Pokud během této doby neobdrží nový párovací paket, automaticky se přesune na frekvenci, kterou sdílí s meteostanicí, se kterou byla původně spárována.

#	**Velikost (B)**	**Datový typ**	**Funkce**
1	1	uint8_t	ID paketu
2	8	uint8_t[8]	Inicializační vektor
3	4	uint32_t	Výrobní adresa stanice
5	16	uint8_t[16]	Nové heslo
∑	29 B (232 b)		

Tabulka 8: Struktura párovacího paketu

4.6.4 Paket nastavení

Paket nastavení je odeslán hlavní stanicí ihned po odeslání a následném potvrzení příjmu párovacího paketu. Paket nastavení obsahuje nastavovací parametry sondy. Paket může být rovněž odeslán v případě, pokud si uživatel přeje provést změnu dané sondy.

Pozn.: Paket nastavení je vždy šifrován.

#	Velikost (B)	Datový typ	Funkce
1	1	uint8_t	ID paketu
2	1	uint8_t	Modulační technika (enumerace)(tab č.10)
3	1	uint8_t	Dodatek modulační techniky (tab č.14)
4	1	uint8_t	Velikost preambule (v bajtech)
5	1	uint8_t	Práh detekce preambule (v nibblech)
6	1	uint8_t	Délka synchronizačního slova (v bajtech)
7	4	uint8_t[4]	Hodnoty synchronizačního slova
8	4	uint32_t	Pracovní frekvence (v Hz)
9	2	uint16_t	Odchylka frekvence (v Hz)
10	4	uint32_t	Rychlost přenosu dat (v bit/s)
11	1	uint8_t	Vysílací výkon (enumerace) (tab č.11)
12	1	uint8_t	Rozsah CRC (enumerace) (tab č.12)
13	1	uint8_t	CRC polynom (enumerace) (tab č.13)
14	4	uint32_t	Adresa hlavní stanice
15	4	uint32_t	Nová adresa sondy
16	8	uint64_t	Prodleva mezi vysíláními (v milisekundách)
17	4	uint32_t	Odchylka vysílání (v milisekundách)
∑	43 B (344 b)		

Tabulka 9: Struktura paketu nastavení

#	Hodnota$_{(2)}$	Typ modulace
1	00	OOK
2	01	FSK
3	10	GFSK

Tabulka 10: Modulační techniky

#	Hodnota$_{(2)}$	Výstupní výkon
1	000	-8 dBm
2	001	-5 dBm
3	010	-2 dBm
4	011	+1 dBm
5	100	+ 4 dBm
6	101	+7 dBm
7	110	+10 dBm
8	111	+13 dBm

Tabulka 11: Enumerace vysílacího výkonu

#	Hodnota$_{(2)}$	Typ rozsahu
1	00	Vypnuto
2	01	Zapnuto
3	10	Pouze data

Tabulka 12: Rozsah CRC

#	Hodnota$_{(2)}$	Typ polynomu
1	00	CITT
2	01	IBM16
3	10	IEC16
4	11	Baicheva

Tabulka 13: CRC polynom

#	Hodnota$_{(2)}$	Funkce
	???X	Data whitening
	??X?	Kódování Manchester
	?X??	Inverze kódování Manchester[5]
	X???	Polarita preambule kódování Manchester[6]

Pozn.: X označuje pozici bitu, 1 znamená zapnuto, 0 vypnuto

Tabulka 14: Dodatek modulačních technik

4.6.5 Paket kompenzačních koeficientů

Naměřené hodnoty senzoru teploty/tlaku/vlhkosti musejí být kompenzovány dle zadaných koeficientů, které jsou do senzoru zadány během výroby. Z důvodu výpočetní náročnosti je vhodné provádět kompenzaci na hlavní stanici a ne na sondách. Z toho důvodu je zapotřebí koeficienty přenést na hlavní stanici při párování. Struktura paketu obsahující kompenzační koeficienty je uvedena v následující tabulce:

[5]Bere se v potaz pouze, pokud je aktivováno kódování Manchester, pokud je tento bit vynulován, pár „10“ je považován za Manchester 0 a pár „01“ je považován za Manchester 1. Pokud je tento bit nastaven, je operace invertována: každá dvojice „10“ bude považována za Manchester 1 a každá dvojice „01“ bude považována za Manchester 0.

[6]Přenáší se série jedniček, pokud je bit nastaven, jinak se přenáší série nul.

#	Velikost (B)	Datový typ	Funkce	Označení
1	1	uint8_t	ID paketu	
2	2	uint16_t	Koeficienty kompenzace teploty	T1
3	2	int16_t		T2
4	2	int16_t		T3
5	2	uint16_t	Koeficienty kompenzace tlaku	P1
6	2	int16_t		P2
7	2	int16_t		P3
8	2	int16_t		P4
9	2	int16_t		P5
10	2	int16_t		P6
11	2	int16_t		P7
12	2	int16_t		P8
13	2	int16_t		P9
14	1	uint8_t	Koeficienty kompenzace vlhkosti	H1
15	2	int16_t		H2
16	1	uint8_t		H3
17	2	int16_t		H4
18	2	int16_t		H5
19	1	int8_t		H6
∑	34 B (272 bit)			

Tabulka 15: Struktura paketu kompenzačních koeficientů

4.6.6 Datový paket

Datový paket určuje strukturu naměřených dat:

#	Velikost (B)	Datový typ	Funkce
1	1	uint8_t	ID paketu
2	4	int32_t	Teplota
3	4	int32_t	Vlhkost
4	4	int32_t	Tlak
5	2	uint16_t	UV
6	2	uint16_t	IR
7	2	uint16_t	Osvětlení
8	2	int16_t	ADC baterie (10 bit hodnota)
∑	21 B (168 bit)		

Tabulka 16: Struktura datového paketu

Nameřená data jsou „surové hodnoty“, na kterých musí být provedena kompenzace na hlavní stanici (z důvodu velikosti kódu a náročnosti na výpočetní prostředky).

Mírně upravený paket slouží k odeslání hodnot z kruhového bufferu, které nebylo možné odeslat v předcházejících vysílacích oknech (hlavní stanice byla mimo dosah, došlo k rušení nebo jiné nezvyklé události). Z tabulky níže je patrné, že paket navíc obsahuje časovou značku (jedná se o počet milisekund, které uběhly od doby zachycení těchto naměřených hodnot). V paketu se naopak nevyskytuje ADC baterie, jelikož uchovávat historii hladiny baterie není naprosto nezbytné.

#	Velikost (B)	Datový typ	Funkce
1	1	uint8_t	ID paketu
2	8	uint64_t	Časová značka
2	4	int32_t	Teplota
3	4	int32_t	Vlhkost
4	4	int32_t	Tlak
5	2	uint16_t	UV
6	2	uint16_t	IR
7	2	uint16_t	Osvětlení
∑	27B (216 bit)		

Tabulka 17: Struktura datového paketu pro historická měření

4.6.7 Šifrovací nádstavba

Přenášená data je možné šifrovat pomocí šifrovací nádstavby. Byla zvolena softwarová implementace, jelikož transceiver v sondě ani v hlavní stanici hardwarové šifrování nepodporuje.

Pro volbu korektního šifrovacího algoritmu bylo zvažováno několik alternativ: XXTEA, Salsa20 a AES; v rozšířeném výběru byly rovněž zvažovány šifry RC4 a Trivium.

Jelikož obě zařízení pracují na velmi omezeném hardwaru (obzvláště sondy), byla preferována nízká hardwarová náročnost (využití RAM, velikost kódu a výpočetní náročnost - počet cyklů, které musí CPU zařízení provést, aby správně zašifrovalo daná data), druhotnou preferencí byla obstojná forma zabezpečení. Všechny následující údaje o šifrách jsou uvedeny vůči hardwaru sond.

Nejlépe ohledně velikosti dopadla (proudová) šifra RC4, jejíž naivní implementace v jazyce C zabrala pouze zhruba 250 bajtů (záleží na nastavení kompilátoru). Jelikož je RC4 jednoduchá, bylo možné ji reimplementovat přímo v jazyce symbolických adres (Assembleru), díky čemuž velikost implementace klesla na 112 bajtů. Počet cyklů pro inicializaci je v naivní implementaci zhruba 64 tisíc, u Assemblerové implementace je to cca 7 tisíc hodinových cyklů. RC4 je však v současnosti[7]

[7] Ke dni 1.3.2021

již považována za prolomenou(Popov, 2015)(Constantin, 2014) a proto s ní nebylo dále pracováno.

Trivium byla druhá nejmenší proudová šifra, jejíž velikost implementace činila zhruba dvojnásobek RC4, avšak cyklů nezbytných pro inicializaci bylo zapotřebí takřka 800 tisíc. Trivium byla navržena spíše pro hardwarovou implementaci než pro softwarovou(Canniere – Preneel) a primárně proto nebyla dále zvažována.

Poslední testovanou proudovou šifrou byla Salsa20, jejíž referenční implementace potřebuje dle studie uvedené v (Meiser et al., 2008) 4478 bajtů flash paměti a 322 bajtů RAM; pro inicializaci bylo zapotřebí 1700 cyklů, pro přípravu klíče 249 cyklů, pro přípravu IV 71 cyklů a pro samotné šifrování 90802 cyklů. Z důvodu velkého množství obsazené flash paměti byla tato šifra brána jako alternativní možný přístup.

Dle stejné studie je pro AES zapotřebí 6664 bajtů flash paměti, 329 bajtů RAM, pro inicializaci bylo zapotřebí 568 cyklů, pro přípravu klíče 6953 cyklů, přípravu IV 196 cyklů a samotné šifrování 12574 cyklů. Z důvodu enormní velikosti implementace šifry (> 80% celkové velikosti flash paměti sondy) byla AES bohužel vyřazena.

Poslední zvažovanou šifrou byla XXTEA, která byla navržena pro vestavěné systémy. Šifra poskytuje omezené zabezpečení (je náchylná k některým možným útokům), avšak je poměrně malá, její implementace je snadná a není zatížena žádnými patenty.

V následující tabulce jsou uvedeny výsledné velikosti sestavené šifry XXTEA pro sondu:

text	data	bss	dec	hex	filename
1458	3	0	1461	5b5	bin/release/sonda.elf

Tabulka 18: Datová velikost implementace XXTEA
Zdroj: vlastní zpracování, kompilováno pomocí (starší verze) avr-gcc 5.4.0 s vlajkou -Os ze zdrojového kódu uvedeného v příloze 8.1.2 (Zdrojový kód šifry XXTEA v jazyce C)

Nakonec byla zvolena šifra XXTEA, která je nakonfigurována v režimu CBC.

4.6.7.1 Struktura paketu při využití šifrovací nádstavby

Struktura datových paketů uvedená výše je zabalena do dalšího pomocného obalu, který určuje, zda-li je paket přenášen šifrovaně či nikoliv. Pokud je přenášen nešifrovaně, je na začátek užitečného nákladu přidán jeden bajt s hodnotou 0x00, který definuje, že zbytek paketu je odeslán nešifrovaně. Pokud je zapotřebí použít šifrování, je třeba odeslat hodnotu 0x01 následovanou inicializačním vektorem a šifrovaným nákladem. Konkrétní struktura šifrovaného obalu je uvedena v následující tabulce:

#	Velikost (B)	Datový typ	Účel	
1	1	uint8_t	ID paketu	
2	8	uint8_t[8]	Inicializační vektor	
3	?[8]	?[9]	Náklad	Šifrováno
4	4	uint32_t	Adresa hlavní stanice	
5	4	uint32_t	Adresa aktuální sondy	
6	4	uint32_t	Inkrement[10]	
∑	21 B (168 b)[11]			

Tabulka 19: Struktura obalovacího paketu využívající šifrovací nádstavbu

4.6.8 Struktura obalovacího paketu bez využití šifrovací nádstavby

Struktura datových paketů uvedená výše je zabalena do dalšího pomocného obalu, který hlavní stanici informuje o tom, že takto odeslaný paket není šifrovaný a rovněž o adrese aktuální sondy.

#	Velikost (B)	Datový typ	Funkce
	1	uint8_t	ID paketu
	?[12]	?[13]	Užitečný náklad
	4	uint32_t	Adresa aktuální stanice

Tabulka 20: Struktura obalovacího paketu bez využití šifrovací nádstavby

4.6.9 ID jednotlivých paketů

Každý paket má ve své hlavičce uvedeno ID, které jej odlišuje a tedy přesně definuje, jakým způsobem má tento paket být interpretován.

V tabulce níže jsou uvedeny ID jednotlivých paketů:

[8] Velikost v závislosti na daném paketu
[9] Datová struktura v závislosti na daném paketu
[10] V každém následujícím paketu je hodnota zvýšena o jedna, slouží jako velmi triviální ochrana před útokem přehrání (replay attack)
[11] Bez užitečného nákladu (payload)
[12] Velikost v závislosti na daném paketu
[13] Datová struktura v závislosti na daném paketu

#	ID paketu$_{(16)}$	Jméno paketu
1	0x00	**Nešifrovaný obal**
2	0x01	**Šifrovaný obal**
3	0x02	Párovací paket
4	0x03	Paket nastavení
5	0x04	Paket koeficientů
6	0x05	Datový paket (naměřená data)
7	0x06	Datový paket (historická měření)
8	0xFE	**Korektní příjem** (bez dat)
9	0xFF	**Chyba ve vykonání** (bez dat)

Tabulka 21: ID jednotlivých paketů

4.6.10 Síla přijatého signálu

Do protokolu je v širším významu možné zařadit i detekci síly signálu, která probíhá přímo v transceiveru a z jehož registrů je přečtena mikrokontrolérem. Protokol je navržen tak, aby v případě nízké síly přijatého signálu (a případně ztracených paketů) automaticky došlo ke zvýšení vysílacího výkonu sondy a/nebo snížení rychlosti vysílání (za cenu vyšší spotřeby energie). Síla signálu je také prezentována uživateli, který se může rozhodnout, zda-li tuto funkcionalitu například nezakázat či nepřesunout celý ekosystém (hlavní stanici a všechny sondy) na jinou frekvenci než je aktuálně používaná (například z důvodu velkého rušení ostatními přístroji operujícími na stejné/blízké frekvenci).

4.7 Postup výroby a ekonomická stránka

Tato kapitola pojednává o postupu výroby a ekonomické stránce stavby obou typů zařízení před případným uvedením na trh.

Při vývoji by bylo vhodné nejprve vytvořit hardware zařízení a až posléze na toto zařízení programovat softwarové vybavení (firmware).

V tomto případě to však z důvodu rozsahu nebylo možné a vývoj hardwaru a části firmwaru (webové rozhraní) probíhal souběžně. Firmware, u kterého bylo zapotřebí testovat přímo na zařízení, byl vytvořen až posléze.

Hardware tedy představuje hmotný produkt, který musí být sestaven, firmware (softwarové vybavení) a plány/schémata hardwaru jsou ve své podstatě nehmotným statkem.

Cena hardwaru se skládá primárně z ceny desek plošných spojů, které musejí být vyrobeny na zakázku z výrobních výkresů, z SMT šablon, které jsou rovněž vyrobeny na zakázku, dále z komponent, které je zapotřebí na tyto desky osadit, ceny osazení a případného dodatečného materiálu. Po osazení a odzkoušení je zapotřebí vyvinuté zařízení otestovat na EMC kompatibilitu tak, aby bylo možné výrobkům udělit značku CE. Díky značce CE je poté možné zařízení legálně prodávat. V širším významu do ceny hardwaru může být započtena i cena šasi / krabiček, do kterých jsou osazené desky plošných spojů vmontovány. Posledním nákladem by bylo přibalení napájecího zdroje a případných baterií. Poté je produkt nezbytné zabalit a odeslat. Vytvoření skladovacích prostor a distribuční sítě bylo v tomto případě zanedbáno, v celkové kalkulaci by pak došlo k navýšení o skladovací a logistické náklady. Stejně tak nebyla vzata v úvahu cena práce.

4.7.1 Desky plošných spojů

Jak již bylo uvedeno, desky plošných spojů musejí být vyrobeny na zakázku z vytvořených plánů (gerber soubory pro plotr, soubory excellon pro CNC vrtačku). Z důvodu nižších výrobních nákladů byly obě zařízení navrhovány na dvouvrstvé DPS, i když by bylo vhodnější využití čtyřvrstvých DPS.

Cena DPS se běžně určuje dle jejich velikosti, povrchového zpracování, výsledné barvy masky, vrstev potisku a počtu vývrtů. V ceně DPS bývá obvykle zahrnuta i kontrola vyrobitelnosti dodaných výrobních podkladů a jejich konverze pro výrobní linku (panelizace a jiné) a například také výroba filmů nezbytných pro prvovýrobu.

Jelikož je v EU až na výjimky zakázáno využívání olovnaté pájky, bylo zapotřebí vyrábět desky s ohledem na direktivu RoHS.

Velikost desky plošných spojů sondy je 77 x 65 mm.

Velikost desky hlavní stanice je 100 x 85 mm.

Desky jak sond, tak hlavní stanice jsou vyrobeny s následujícími parametry:

Specifikum	Hodnota
Počet vrstev	2
Materiál	FR4
FR4-TG	TG 130-140
Tloušťka desky	1.6 mm
Minimální šířka trasy	> 6 mil (0.1524 mm)
Minimální šířka mezery	> 6 mil (0.1524 mm)
Minimální vývrt	> 0.3 mm
Nepájivá maska	Ano, obě strany, zelená
Potisk masky	Ano, obě strany, bílá
Povrch spojů	HAL bez olova
Zpracování průchodek	Průchodky zakryté maskou
Tloušťka plátování mědi	1 oz (35 μm)

Tabulka 22: Specifikace desek plošných spojů

- Česká republika (společnost PRINTED s.r.o.)
  - Výrobní cena 10 kusů DPS hlavní stanice je 7 856,- Kč (bez DPH, bez dopravy).
  - Výrobní cena 10 kusů DPS sondy je 5 124,- Kč (bez DPH, bez dopravy)
- Čína (společnost 嘉立創 [Jia Li Chuang])
  - Výrobní cena 10 kusů DPS hlavní stanice je 6.10 $ (≈134,- Kč[14]) (bez DPH, bez cla, bez dopravy)
  - Výrobní cena 10 kusů DPS sondy je 6.10 $ (≈134,- Kč[15]) (bez DPH, bez cla, bez dopravy)

Cena výroby DPS pro výrobu prototypů je v ČR velmi vysoká, z tohoto důvodu je vhodné desky vyrobit v Číně, kde je cena výroby mimořádně nízká a vyplatí se i s dopravou, daní a vyřízením celních dokumentů. Vyrobené desky jsou přitom ve stejné, či dokonce vyšší kvalitě zpracování.

4.7.2 SMT šablony

SMT šablony jsou nezbytné pro bezproblémové osazení DPS, slouží k nanášení pájecí pasty, díky které jsou poté zapájeny jednotlivé komponenty. Prototypovou sérii je možné vyrobit i bez SMT šablon, osazení je však podstatně pracnější.

[14]Kurz dle ČNB ke dni 30.10.2020
[15]Kurz dle ČNB ke dni 30.10.2020

- Česká republika (společnost PRINTED s.r.o.)
  - Výrobní cena šablony pro hlavní stanici je 1 596,- Kč (bez DPH, bez rámu, bez dopravy)
  - Výrobní cena šablony pro sondu je 1 596,- Kč (bez DPH, bez rámu, bez dopravy)
- Čína (společnost 嘉立創 [Jia Li Chuang])
  - Výrobní cena šablony pro hlavní stanici je 7.05 $ (≈155,- Kč[16]) (bez DPH, bez rámu, bez dopravy)
  - Výrobní cena šablony pro sondu je 7.05 $ (≈155,- Kč[17]) (bez DPH, bez rámu, bez dopravy)

Opět stejně jako v případě DPS, i u SMT je vhodné zadat výrobu v Číně. Kvalita výroby SMT šablon je v Číně rovněž totožná či dokonce vyšší ve srovnání s výrobou v ČR.

4.7.3 Komponenty

Komponenty jsou prvky, které se osazují na základní desky obou typů zařízení.

Nejdraží komponenty pro obě zařízení jsou senzory, spínané zdroje a integrované obvody celkově (ochranné obvody, RTC, transceivery, mikrokontroléry), pro hlavní stanici je rovněž poměrně drahým prvkem displej s dotykovou vrstvou.

Pasivní prvky (kondenzátory, rezistory, tlumivky...) jsou v obou zařízeních zastoupeny poměrně hojně, avšak jejich cena je nízká. Některé hodnoty jednotlivých prvků jsou využity několikrát, takže není nutné nakupovat větší množství různých komponent s rozdílnou hodnotou (např. terminační rezistory, odrušovací kondenzátory).

Komponenty tvoří značnou část výrobní ceny, obzvláště u prototypové série, kde nemohou být využity úspory z rozsahu. U prototypové (vývojové) série je možné nakoupit tyto komponenty přes neoriginální distributory z Číny. Tito distributoři mohou dodávat levnější komponenty z toho důvodu, že je nakupují v ohromném množství, nebo se jedná o klony originálních součástek. Jelikož zde není žádná záruka korektní funkčnosti takovýchto komponent, je naprosto nezbytné, aby finální produkt byl sestaven pouze z komponent, které dodávají oficiální distributoři (Arrow, Mouser) či přímo výrobce dané komponenty (Texas Instruments, Maxim Integrated, originální výrobci v Číně atp.).

[16] Kurz dle ČNB ke dni 30.10.2020
[17] Kurz dle ČNB ke dni 30.10.2020

Některé komponenty používané v zařízení však na distributorských kanálech oficiálních redistributorů není možné sehnat a musejí se objednat přímo od výrobce z Číny (např. dotykový displej hlavní stanice a dotykový kontrolér snímající místo dotyku a sílu stisku).

Pasivní prvky (keramické kondenzátory, rezistory, tlumivky) je možné sehnat poměrně levně přímým kontaktem výrobců v Číně, tyto komponenty se obvykle nakupují v tisícových množstvích, jelikož mohou být využity při stavbě různých druhů zařízení.

V tabulkách níže je uvedena cenová kalkulace nákupu komponent, jsou uvedeny dvě alternativy: „Cena oficiální“ značí renomované distribuční kanály (Arrow.com, Mouser.com), „Cena Čína“ uvádí cenovou kalkulaci pro malé čínské dodavatele.

Rozdělení prvků	**Hlavní stanice**		**Sonda**	
	Cena oficiální	Cena Čína	Cena oficiální	Cena Čína
Pasivní prvky[18]	477,2	111,5	177,36	23,479
Polovodiče[19]	405,98	219,024	12,89	2,665
Integrované obvody[20]	986,141	714,77	397,85	263,4
Ostatní[21]	384,4	237,346	66,28	5,83
∑	**2 253,721**	**1 282,19**	**654,38**	**295,374**

Tabulka 23: Kalkulace komponent
Ceny v Kč bez DPH, kusová výroba, bez využití úspor z rozsahu.

4.7.4 Osazení a oživení

Jakmile jsou k dispozici desky, komponenty a šablony, může dojít k osazení a oživení prototypu. Osazení v prototypové výrobě většinou provádí člověk (nanesení pájecí pasty přes šablonu a ruční osazení komponent). V sériové výrobě jsou tyto úkony již prováděny na výrobní lince, kde nanesení pasty provádí robot a osazení provádí osazovací automat (ideální je, když i výroba desek a šablon probíhá ve stejné továrně). Zajímavostí je, že už prototypy obou navržených zařízení mají vytvořeny značky pro automatické zarovnání optické vize osazovacího automatu. Ruční osazení trvá v závislosti na manuální zručnosti osoby, která provádí osazení, v ideálním případě je možné obě zařízení sestavit během jednoho dne. Při využití strojového osazení je doba závislá na rychlosti výrobní linky, rychlé výrobní linky jsou schopny obě zařízení osadit do minuty.

[18] Rezistory, kondenzátory, induktory/tlumivky
[19] Diody - TVS, zener..., tranzistory
[20] Mikroprocesory, senzory aj.
[21] Mechanické konektory, displej a další

Po osazení přichází na řadu oživení, kdy jsou oba typy zařízení zapnuty, jsou do nich nahrány aktuální verze firmware a je otestována jejich funkčnost (u prototypové výroby opět vše provádí lidská obsluha, u sériové výroby je možné oživení a nahrání firmwaru automatizovat). Jakmile je zařízení oživeno, přichází na řadu vmontování do krabičky.

4.7.5 Krabička / šasi

U prototypové výroby, kdy není nezbytné provádět testování EMC (bližší informace jsou uvedeny v následující kapitole), není šasi nutné vyrábět. Krabičky elektrozařízení bývají nejčastěji z plastu (ABS), první prototyp šasi je možné vymodelovat a vytisknout na 3D tiskárně. V sériové výrobě není 3D tisknutý obal příliš vhodný, neboť není vizuálně tolik atraktivní a výroba je časově náročná. Pro sériovou výrobu je vhodné takto navržený model převést do vstřikolisové formy, kterou je nutné vyrobit pouze jednou a následně se vyrábí již jen plastové výlisky. Cena vstřikolisové formy je tedy jednorázový náklad. Záleží na složitosti, dané firmě, náročnosti převodu a dalších parametrech, proto je cena velmi pestrá a nelze nyní přesnou cenu vyčíslit. Výroba samotných výlisků je po zahájení velmi levná (pár korun za kus, opět je možné využít úspory z rozsahu).

4.7.6 EMC testování

Aby zařízení mohlo být v EU legálně prodáváno, potřebuje označení CE, kterému předcházejí tzv. EMC testy (testování elektromagnetické kompatibility).

EMC testy zjišťují, zda-li dané zařízení neovlivňuje jiný objekt ve své blízkosti či sebe samotné. Také se testuje, zda-li je zařízení schopné odolávat rušení, které vydávají ostatní zařízení v jeho blízkosti a jak případně reaguje na vzájemné ovlivňování.

Pravé EMC testování je velmi nákladné, jelikož probíhá v řízeném prostředí (v anechoické komoře, která musí být řádně odstíněna) a na velmi drahých měřících přístrojích, které obsluhuje vyškolený personál.

Malé EMC testy stojí obvykle vyšší desítky tisíc korun až po stovky tisíc pro testy speciálních zařízení, opět velmi záleží na firmě či testovacím ústavu, který tyto testy provádí, z tohoto důvodu není možné udat přesnou cenu pro zařízení navržené v rámci této práce.

Pokud zařízení neprojde EMC testy, musí být přepracováno. Z důvodu úspory financí je obvyklé, že na zařízení jsou provedeny předemisní testy. Zařízení je měřeno za pomoci méně přesných přístrojů a v neřízeném prostředí, kde mohou být výsledky zkresleny ostatními zařízeními v blízkosti a jinými vlivy.

U zařízení navrženého v rámci bakalářské práce byl proveden základní předemisní test vyzařování, který dopadl dobře. Jelikož je zařízení popsané v této diplomové práci navrhováno podobným způsobem (tedy vložením pomocných odrušovacích filtrů, stíněním, navrženým layoutem DPS, užitím spínaných zdrojů s využitím rozprostřeného spektra), předpokládá se, že výsledky budou obdobné. Pravé EMC testy však prozatím ani na jednom typu zařízení doposud nebyly provedeny.

EMC testování probíhá před uvedením na trh a je tedy jednorázovým nákladem, je nezbytné, aby výrobce udržel stejnou kvalitu po celou dobu výroby.

4.7.7 Kompletace

Jakmile je zařízení vyrobeno, je zapotřebí zkontrolovat jeho kvalitu, následně zabalit a odeslat případnému zákazníkovi.

4.8 Porovnání s konkurencí

V této kapitole bude provedena komparace navrženého zařízení Meteos s vybranými meteostanicemi, které jsou dostupné na českém trhu.

Byly vybrány dvě meteostanice, které disponují podobnými funkcemi jako navržené zařízení Meteos.

4.8.1 Netatmo Smart Home Weather Station

Netatmo Smart Home Weather Station je chytrá meteostanice do domácnosti, která obsahuje hlavní (vnitřní) stanici a sondu, která se umisťuje do exteriéru.

Vnitřní stanici je možné připojit k lokální Wi-Fi síti a data je možné prohlížet na chytrém mobilním telefonu, což je také jediný možný způsob ovládání, jelikož stanice neobsahuje žádný displej.

Vnitřní stanice měří teplotu, vlhkost, kvalitu vzduchu a hluk.

Vnější sonda měří teplotu, vlhkost, kvalitu vzduchu a barometrický tlak.

K systému je možné jako modul dokoupit anemometr a srážkoměr.

Maloobchodní cena hlavní stanice a sondy je **3 789,- Kč včetně DPH** a jedná se o druhý nejprodávanější produkt v kategorii meteostanic v internetovém obchodě alza.cz.[22]

Interiérový modul je napájen USB adaptérem, sondy jsou napájeny 2 AAA bateriemi.

[22]Cena i žebříček prodávanosti převzat z internetového obchodu alza.cz ke dni 17.3.2021

Obrázek 36: Netatmo Smart Home Weather Station
Vlevo: Hlavní obrazovka aplikace sloužící pro ovládání meteostanice, aplikace je v angličtině (dle alza.cz)
Vpravo: Pohled na skutečnou podobu vnitřní meteostanice (větší) a sondu (menší)
Zdroj: Netatmo.com

Meteos a Netatmo si jsou velmi podobné, avšak Meteos v současné době nemá dodatečné moduly. Rovněž Netatmo umí měřit hladinu hluku, Meteos stejně jako Netatmo obsahuje mikrofon, pomocí kterého je také možné měřit zvukovou hladinu, nicméně tato funkcionalita není prozatím ve firmwaru navrženého zařízení implementována.

Netatmo rovněž obsahuje senzor CO2. Meteos byl navržen takovým způsobem, že měření kvality ovzduší (VOC) je možné velmi jednoduše přidat, nicméně tato funkcionalita není v aktuální verzi implementována.

Informace o přenosovém protokolu Netatmo nebyly nalezeny, interval měření není možné u Netatmo nastavit (je napevno nastaven na 5 minut), u navrženého zařízení Meteos je interval možné měnit i v průběhu měření.

Meteos umí navíc měřit UV index a intenzitu osvětlení a obsahuje dotykový displej. Je možné jej napájet napětím ve značném rozsahu, proto je možno jej používat například i v autě nebo obytném voze bez aktivního adaptéru.

K hlavní stanici Netatmo je možné připojit 3 interiérové moduly, 1 srážkoměr a 1 anemometr. Meteos umožňuje připojit až 255 sond.

Velikost vnitřní paměti Netatmo nebyla nalezena, paměť pro naměřená data u navrženého zařízení může být v současné revizi maximálně 2 Gbit.

Netatmo má hliníkový plášť, Meteos má jednoduchou krabičku vytvořenou na 3D tiskárně.

4.8.2 GARNI 2055 Arcus

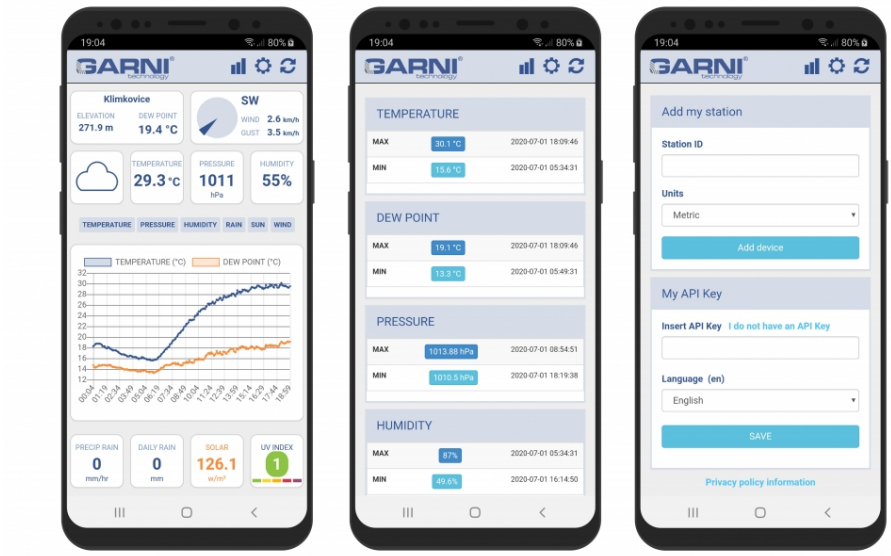
GARNI 2055 Arcus je vlajkovou lodí české společnosti Garni a.s. a se svou cenou **8 689,- Kč**[23] je nejdražší meteostanicí v nabídce obchodu alza.cz

Stanice Arcus umožňuje měřit stejné fyzikální veličiny jako Meteos, avšak navíc v základní verzi má i měření větru a srážek.

Arcus obsahuje barevný displej, který však není dotykový a neumožňuje provádět složitější nastavení a zobrazovat grafy z naměřených hodnot tak jako tomu je u stanice Meteos.

Hlavní jednotka Arcus je napájena síťovým adaptérem, avšak může být napájena i záložními bateriemi (3 ks 1.5V AAA), sonda je napájena stejně jako Meteos sonda 2 ks 1.5V AA.

Dle stránek výrobce trval vývoj meteostanice rok a byla uvedena na trh v červenci 2020.



Obrázek 37: GARNI 2055 Arcus ovládací aplikace
Zdroj: garni-meteo.cz

[23] Stav ke dni 18.3.2021 u obchodu alza.cz

4.8.3 Tabulkové srovnání

	Netatmo	Garni	Meteos
Senzor teploty	✓	✓	✓
Senzor vlhkosti	✓	✓	✓
Senzor tlaku	✓	✓	✓
Senzor osvětlení	✗	✓	✓
Senzor UV indexu	✗	✓	✓
Hlukoměr/mikrofon	✓	✗	✓
Senzor CO2	✓	✗	✗
Senzor VOC	✗	✗	✗[24]
Senzor větru (směr, síla)	✗[25]	✓	
Senzor srážek		✓	
Reproduktor (hlas/hudba)	✗	✗	✓
Bezdrátový přenos dat	✓	✓	✓
Barevný displej	✗	✓	✓
Dotykový displej	✗	✗	✓
Možnost napájení z palubní sítě automobilu	✗[26]	✗[27]	✓
Zapamatování času při přerušení napájení	✗	✓[28]	✓
Záložní baterie	✗	✓	✗
USB připojení k PC (stažení dat atp.)	?	?	✓
Wi-Fi	✓	✓	✓
Bluetooth	✗	✗	✓[29]
Vnitřní paměť pro zobrazení naměřených dat	✗	✓[30]	✓[31]
Možnost odeslání dat do cloudu	✓	✓	✓[32]
Nastavení doby měření	✗	✗	✓
Šifrovaný přenos dat	?	?	✓

Tabulka 24: Tabulkové srovnání hlavních funkcí meteostanic

[24] Je možné dodat v budoucnu bez změn ve výrobních výkresech hlavní meteostanice
[25] Dostupné jako dodatečný modul
[26] Pouze s převodníkem
[27] Pouze s převodníkem
[28] Pokud jsou v hlavní stanici záložní baterie
[29] HW osazen, v současné verzi FW neimplementováno
[30] Posledních 24 hodin s rozlišením 1 hodina
[31] Počet hodnot v závislosti na osazené paměti a četnosti měření
[32] V současné verzi firmwaru pouze na testovací server v lokální síti

	Netatmo	Garni	Meteos
Frekvence přenosu	868 MHz	868 MHz	240 - 930 MHz[33]
Maximální počet sond	3+1+1+1[34]	7	255
Rozsah měřené teploty	-40 °C až 65 °C	-40 °C až 80 °C	-40 °C až 85 °C
Přenost měření teploty	±0.3 °C	± 0.4 °C až ± 1.9 °C[35]	± 0.5 °C až ± 1.5 °C[36]
Rozsah měřené vlhkosti	0 % až 100 %	1 % až 99 %	0 % až 100 %
Přesnost měření vlhkosti	±3 %	± 3.5 % až ± 6.5 %	± 3 %
Rozsah měřeného tlaku	260 hPa až 1260 hPa	540 hPa až 1100 hPa	300 hPa až 1100 hPa
Přesnost měření tlaku	±1 hPa	± 5 hPa až ± 8 hPa	± 1.0 až 1.7 hPa [37]
Rozsah měření osvětlení	✗	0 klx až 200 klx	0 klx až 128 klx
Přesnost měření osvětlení	✗	?	100 mlx

Tabulka 25: Tabulkové srovnání vybraných parametrů meteostanic
Pozn.: Symbol otazníku značí, že k podpoře dané funkcionality nejsou dostupné informace

4.9 Cílová skupina

Navržená IoT meteostanice Meteos je vzhledem ke svým funkcím a možnostem určena pro náročnější klientelu, která má zálibu v technologiích. Zákazníci mohou být uživateli chytrých domácností či jiných zařízení IoT. Jedná se z velké části o uživatele s vysokoškolským nebo vyšším odborným vzděláním.

Meteos mohou samozřejmě používat i uživatelé běžných meteostanic, protože navržené zařízení všechny jednoduché funkce podporuje, ale vzhledem k ceně se předpokládá, že uživatelé budou spíše náročnější, ochotni investovat do pokročilé meteostanice.

[33] V závislosti na povolených frekvencích v daném státě
[34] 3 interiérové moduly, 1 srážkoměr, anemometr a venkovní modul
[35] +55 až +60°C ±0.5°C, +10 až +55°C 0.4°C, -20 až +10°C ±1.3°C, -40 až -20°C ±1.9°C
[36] Při pokojové teplotě (25 °C) ± 0.5 °C, 0 až +65 °C ± 1.0 °C, -20 °C až 0 °C ± 1.25 °C, -40 °C až -20 °C ± 1.5 °C
[37] 300 hPa až 1100 hPa při -20 °C až 0 °C ± 1.7 hPa, 300 hPa až 1100 hPa při 0 °C až +65 °C ± 1.0 hPa, 1100 hPa až 1250 hPa při 25 °C až 40 °C ± 1.5 hPa

5 Výsledky a diskuze

Diplomová práce se zabývá návrhem a konstrukcí prototypu IoT zařízení schopného bezdrátově přijímat a vyhodnocovat údaje ze sond nacházejících se v exteriéru a interiéru.

Nejprve bylo potřeba stanovit požadavky kladené na zařízení. Tyto požadavky byly porovnány s výsledky prezentovanými v bakalářské práci pod názvem Bezdrátová senzorová stanice. Byla provedena rešerše, výběr a zhodnocení mikrokontroléru pro stavbu obou typů zařízení. Požadavky na hlavní stanici a sondu byly rozdílné z důvodu jiných nároků na architekturu dle preferovaných parametrů a ceny. Na základě porovnání bylo rozhodnuto, že původní architektura AVR je v tomto případě pro hlavní stanici nedostatečná. Tato architektura však mohla být ponechána pro sondu. Pro hlavní stanici byla následně vybrána architektura ESP32 od společnosti Espressif. Jedná se o dvoujádrový mikrokontrlér, jehož výhodou je, že je přímo určen pro IoT projekty, je velmi levný, má slušný výkon, Wi-Fi a Bluetooth jsou implementovány přímo na čipu. Mikrokontrolér spolu s anténou, externí flash a RAM pamětí jsou k dispozici ve formě modulů, které je možné připájet k základní desce. Velké množství knihoven je portováno přímo do vývojového frameworku výrobce, včetně síťových knihoven a modifikovaného operačního systému FreeRTOS, což podstatně zjednodušilo vývoj.

Hlavní stanice se nachází v interiéru a měří zde teplotu, tlak, vlhkost, osvětlení a UV index. Má ochranu proti přepětí, nesprávné polaritě, podpětí a zkratu, obsahuje mikrofon a reproduktor. Součástí je rovněž modul pro bezdrátový přenos dat mezi hlavní stanicí a přidruženými sondami. Ke stanici je možno připojit až 255 sond.

Velkou výhodou celé hlavní stanice je enormní modulárnost konstrukce a velké množství funkcí, které se u většiny meteostanic na trhu běžně nevyskytují. Patří k nim například interní paměť pro ukládání naměřených hodnot, odolnost všech vstupů a výstupů, USB rozhraní pro případnou komunikaci s nadřízeným systémem (osobním počítačem) či integrování obvodu reálného času schopného uchovat čas i v případě ztráty napájení. Sonda má vyspělý spínaný zdroj, který je schopen vybít baterie až na hodnotu 0.15 V na článek, díky čemuž se šetří životní prostředí. Zajímavostí je rovněž možnost napájet hlavní stanici ze zásuvky automobilu.

Pro výpočet předpovědi počasí z naměřených dat byl využit modifikovaný algoritmus Zambretti. Pro výpočet fází Měsíce byl zvolen naivní přístup - výpočet synodického měsíce neboli lunace. Pomocí algoritmu "Sunrise equation" byla implementována předpověď východu a západu Slunce (počítá s aktuálním juliánským dnem, pozicí na zeměkouli atp.).

Aby zařízení reflektovalo poslední trendy v rámci internetu věcí, došlo k navržení dalších funkcionalit, které jsou pro tato inteligentní zařízení nezbytná. Byl navržen vlastní informační systém

využívající databázi SQLite, který je poměrně neobvykle napsán v jazyce C. Naměřená data je možné prohlížet buď přes webové rozhraní meteostanice připojené k lokální Wi-Fi síti nebo pomocí dotykového barevného displeje.

Byl navržen nový protokol pro polo-duplexní přenos. Protokol umožňuje spárovat nové sondy s hlavní stanicí pomocí "rendez-vous" frekvence, těmto sondám je poté možné odesílat nastavení. Sondy naopak v nastavených intervalech odesílají na hlavní stanici naměřená data. Stanice potvrzuje příjem a případně odesílá změněné nastavení dané sondy, které drží ve vyrovnávací paměti.

Velmi důležité pro IoT je šifrování dat, pro tuto meteostanici byla zvolena šifra XXTEA z toho důvodu, že je malá, její implementace je snadná a není zatížena žádnými patenty.

Jednotlivé části zařízení byly při vývoji průběžně testovány pro odhalení případných chyb, byla ověřena správnost funkce všech hardwarových prvků a jednotlivých softwarových částí, které byly psány v rámci firmwaru.

Rovněž byla provedena kalkulace nákupní ceny součástek a ceny za výrobu desek plošných spojů a šablon jak sondy, tak hlavní stanice. Tato cena závisí na konkrétním dodavateli a pohybuje se v rozmezí od 1 914, Kč do 7 398,- Kč bez DPH za jeden prototyp sondy a hlavní stanice.

Zařízení je porovnatelné s vybranými konkurečními výrobky disponujícími podobnými funkcemi. Jedná se o meteostanice Netatmo Smart Home Weather Station a GARNI 2055 Arcus. Parametry meteostanic jsou srovnatelné, některé funkcionality chybí konkurenčním zařízením, některé naopak navrženému prototypu. Vzhledem k modulárnosti konstrukce je ale přidání těchto funkcionalit možné, neboť při vývoji byl brán zřetel na možnost snadného rozšíření požadovaných funkcí.

Mezi funkcionality, které mohou být do zařízení přidány a prozatím nebyly implementovány, patří například možnost komunikace s ostatními zařízeními nacházejícími se v chytré domácnosti, ať už souvisejí či nesouvisejí s počasím (hlásiče požáru, inteligentní osvětlení, chytré zásuvky atd.). Dále se předpokládá, že by zařízení mohlo být využito jako centrální prvek chytré domácnosti (možnost poslouchání rádia, ovládání ostatních chytrých zařízení). V neposlední řadě by také bylo vhodné, kdyby zařízení umělo přečíst naměřené hodnoty pro uživatele s vizuálním hendikepem, hardwarově k tomu již vybavené je, nicméně firmware by musel být modifikován.

Vzhledem k tomu, že se jedná o implementaci Meteorologického systému, bylo zařízení pojmenováno Meteos, bylo vytvořeno logo a předpokládá se jeho komerční využití. Zařízení bylo navrhováno v souladu s právními předpisy EU a aby mohlo být v EU prodáváno, potřebuje označení CE, kterému předcházejí EMC testy (testování elektromagnetické kompatibility). Dále je potřeba navrhnout novou designovou krabičku a vytvořit podmínky pro zahájení sériové výroby.

6 Závěr

Hlavním cílem této práce bylo navržení funkčních prototypů IoT meteostanice a přidružených sond.

Úvodní teoretická část se zabývá definicí internetu věcí a samotné meteostanice, dále základními aspekty meteorologie a popisem některých měřených veličin (teplota, vlhkost, tlak, osvětlení, UV index) a veličin dopočítávaných (rosný bod, předpověď počasí). V oblasti astronomie jsou popsány algoritmy pro výpočet lunárních fází a východu a západu Slunce. Teoretická část rovněž obsahuje informace týkající se architektury systému, firmwaru a také bezdrátového přenosu dat mezi sondami a hlavní stanicí. Jelikož riziko zneužití dat je v IoT zařízeních značné, bylo nutné se v teoretické části rovněž věnovat oblasti šifrování, která je nezbytná pro konstrukci přenosového protokolu.

V praktické části byla popsána samotná konstrukce hlavní stanice a sondy, počínaje zvážením alternativ pro konstrukci, výběrem vhodné architektury přes návrh hardwaru a firmwaru až po protokol přenosu dat a využití šifrovací nádstavby. Vlastní práce se rovněž zabývá postupem výroby, zhodnocením ekonomické stránky a porovnáním zařízení s konkurenčními výrobky.

Pro úspěšné splnění cílů bylo nezbytné využít definice, poznatky a algoritmy z teoretické části a aplikovat je na vývoj prototypů.

Byla navržena meteostanice, která je schopná se připojit k Wi-Fi síti, obsahuje webserver s webovým rozhraním, je možné ji ovládat barevným dotykovým displejem a bezdrátově komunikuje se sondami pomocí šifrovaného protokolu.

Na základě teoretických poznatků byla analyzována vhodná architektura systému a pro hlavní stanici bylo zvoleno řešení postavené na technologii ESP32, které pomocí sběrnic komunikuje s ostatními součástkami. Pro sondu byla zvolena architektura AVR.

Zařízení umožňuje rychlý náhled jak na hodnoty změřené přímo hlavní stanicí, tak sondami. Zajímavostí je, že ke stanici lze připojit až 255 sond, které mohou snímat teplotu, tlak, vlhkost, osvětlení či UV index. Přenos dat může probíhat na libovolné frekvenci v rozsahu 240 - 930 MHz pomocí nově navrženého šifrovaného protokolu.

Meteostanice umožňuje také na základě implementovaných algoritmů jednoduchou předpověď počasí z naměřených dat, předpověď fází Měsíce a východu a západu Slunce.

Zařízení je srovnatelné s vybranými konkurenčními zařízeními disponujícími podobnými funkcemi a předpokládá se možnost komerčního nasazení této inteligentní meteostanice.

7 Seznam použitých zdrojů

Reference

ALMANAC. *Moon Phases and Lunar Calendar* [online]. Yankee Publishing, 2021. [cit. 17.2.2021]. Dostupné online: https://www.almanac.com/astronomy/moon/calendar.

ALMANAC. *Moon Phase* [online]. Wikimedia, 2007. [cit. 17.2.2021]. Dostupné online: https://en.wikipedia.org/wiki/File:Moon_phase_0.svg.

AMETSOC. *Meteorology* [online]. 2012. [cit. 20.12.2017]. Dostupné online: http://glossary.ametsoc.org/wiki/Meteorology.

AMETSOC. *Weather* [online]. 2015. [cit. 20.12.2017]. Dostupné online: http://glossary.ametsoc.org/wiki/Weather.

BAYER, Amanda. – IERSEL, Marc. – CHAPPELL, Matthew. *What is a Weather station and Can it Benefit Ornamental Growers?* [online]. University of Georgia, 2017. [cit. 10.3.2021]. Dostupné online: https://ag.umass.edu/sites/ag.umass.edu/files/fact-sheets/pdf/b_1475_2.pdf.

BELLARE, Mihir. – ROGAWAY, Philip. *Introduction to Modern Cryptography* [online]. 2005. [cit. 9.9.2020]. Dostupné online: https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

BERNSTEIN, Daniel J.. *The Salsa20 family of stream ciphers* [online]. University of Illinois, 2007. [cit. 12.3.2021]. Dostupné online: https://cr.yp.to/snuffle/salsafamily-20071225.pdf.

BERNSTEIN, Daniel J.. *Protecting communications against forgery* [online]. 2008. [cit. 9.9.2020]. Dostupné online: https://cr.yp.to/antiforgery/forgery-20080501.pdf.

BERNSTEIN, D. J. et al. *Post-quantum RSA* [online]. 2017. [cit. 9.9.2020]. Dostupné online: https://cr.yp.to/papers/pqrsa-20170419.pdf.

BIGGS, Norman. *Codes : an introduction to information communication and cryptography*. London : Springer, 2008. ISBN 9781848002739.

Bootstrap developers. *Twitter Bootstrap Under Firefox 32* [online]. Wikimedia, 2014. [cit. 12.9.2020]. Dostupné online: https://commons.wikimedia.org/wiki/File:Twitter_Bootstrap_Under_Firefox_32.png.

BRAIN, Marshall. *How Microcontrollers Work* [online]. HowStuffWorks, 2000. [cit. 15.9.2020]. Dostupné online: https://electronics.howstuffworks.com/microcontroller1.htm.

BRITANNICA. *Julian period* [online]. Britannica, 2021. [cit. 10.3.2021]. Dostupné online: https://www.britannica.com/science/Julian-period.

BRITANNICA. *Celsius temperature scale* [online]. 2014. [cit. 20.12.2017]. Dostupné online: https://www.britannica.com/technology/Celsius-temperature-scale.

BROžKOVá, Radmila. *Jak spočítat počasí* [online]. Vesmír), 2010. [cit. 18.9.2020]. Dostupné online: https://vesmir.cz/cz/casopis/archiv-casopisu/2010/cislo-12/jak-spocitat-pocasi.html.

BURNETT, Colin M.L.. *SPI three slaves* [online]. Wikimedia, 2006a. [cit. 5.9.2020]. Dostupné online: https://upload.wikimedia.org/wikipedia/commons/f/fc/SPI_three_slaves.svg.

BURNETT, Colin M.L.. *I2C* [online]. Wikimedia, 2006b. [cit. 5.9.2020]. Dostupné online: https://commons.wikimedia.org/wiki/File:I2C.svg.

CANNIERE, Christophe De. – PRENEEL, Bart. TRIVIUM Specifications. *eSTREAM, ECRYPT Stream Cipher Project*. 2006.

CHRISTIANSEN, Grant. *Data whitening and Random TX Mode* [online]. Texas instruments, 2010. [cit. 25.2.2021]. Dostupné online: https://www.ti.com/lit/an/swra322/swra322.pdf.

COLLEY, Stephen. *What Is Brown Out Reset in Microcontrollers? How to Prevent False Power-Downs* [online]. All about circuits, 2019. [cit. 7.9.2020]. Dostupné online: https://www.allaboutcircuits.com/technical-articles/what-is-brown-out-reset-microcontroller-prevent-false-power-down/.

CONSTANTIN, Lucian. *Microsoft continues RC4 encryption phase-out plan with .NET security updates* [online]. computerworld, 2014. [cit. 22.2.2021]. Dostupné online:

https://www.computerworld.com/article/2489395/microsoft-continues-rc4-encryption-phase-out-plan-with--net-security-updates.html.

CYPRESS. *Inter-IC Sound Bus (I2S)* [online]. 2016. [cit. 5.9.2020]. Dostupné online: https://www.cypress.com/file/133906/download.

DAEMEN, Joan. – RIJMEN, Vincent. *Rijndael* [online]. NIST, 2003. [cit. 25.2.2021]. Dostupné online: https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf#page=1.

DONCESCU, Andrei. *The Central Processing Unit: What Goes on Inside the Computer* [online]. LAAS-CNRS, 2020. [cit. 12.3.2021]. Dostupné online: https://homepages.laas.fr/adoncesc/Lectures-OS/Lecture2-ArchitecturesOS.pdf.

EHRSAM, W. F. et al. *Message verification and transmission error detection by block chaining* [online]. International Business Machines Corp, 1976. [cit. 14.9.2020]. Dostupné online: https://patents.google.com/patent/US4074066A/en.

ESPENAK, Fred. *Length of the Synodic Month: 2001 to 2100* [online]. Astropixels, 2019. [cit. 22.2.2021]. Dostupné online: http://www.astropixels.com/ephemeris/moon/synodicmonth2001.html.

Espressif. *ESP32 Series Datasheet* [online]. 2020. [cit. 12.9.2020]. Dostupné online: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf.

ESPRESSIF. *ESP-IDF Programming Guide* [online]. Espressif, 2020. [cit. 13.9.2020]. Dostupné online: https://docs.espressif.com/projects/esp-idf/en/latest/esp32.

FIOLETOV, Vitaly. – KERR, James B.. – FERGUSSON, Angus. The UV Index: Definition, Distribution and Factors Affecting It. *Canadian journal of public health*. 2010, 101, 4, s. 5–9. Dostupné online: http://journal.cpha.ca/index.php/cjph/article/viewFile/1905/2203.

GABZDYL, Pavel. *Fáze Měsíce* [online]. astronomie.cz, 2020. [cit. 10.3.2021]. Dostupné online: http://mesic.astronomie.cz/faze-mesice.htm.

GAD, Vinaya. – GAD, Rajendra. – NAIK, Gourish. Configurable CRC Error Detection Model for Performance Analysis of Polynomial: Case Study for the 32-Bits Ethernet Protocol. 08 2015. doi: 10.1007/978-3-319-23126-6_46.

HILL, G. C.. *An Introduction to Microcontrollers, Assembly Language, and EmbeddedSystems* [online]. California State University, Long Beach, 2021. [cit. 10.3.2021]. Dostupné online: http://web.csulb.edu/~hill/ee346/Lectures/02%20Intro%20Microcontroller.pdf.

HILL, Jonathan. *Weather architecture*. London New York : Routledge, 2012. ISBN 978-0415668613.

HOANG, Viet Tung. – ROGAWAY, Phillip. *On Generalized Feistel Networks* [online]. 2018. [cit. 9.9.2020]. Dostupné online: https://eprint.iacr.org/2010/301.pdf.

JAIKARAN, Chris. *Encryption: Frequently Asked Questions* [online]. Congressional Research Service, 2016. [cit. 9.9.2020]. Dostupné online: https://fas.org/sgp/crs/misc/R44642.pdf.

JOYCE. *Co je WiFi?* [online]. Joyce, 2010. [cit. 12.3.2021]. Dostupné online: http://joyce.cz/co-je-wifi.html.

KISS-VAMOSI, Gabor. *LVGL - Light and Versatile Graphics Library* [online]. Github, 2020. [cit. 12.9.2020]. Dostupné online: https://github.com/lvgl/lvgl/blob/master/README.md.

KOTLER, Philip. *MARKETING MANAGEMENT*. Děčín : VICTORIA PUBLISHING, a.s., 1992. ISBN 80-85605-08-2.

KOříNEK, Viktor. *Co máme a jiní ne: Meteorologická stanice* [online]. izun.eu, 2010. [cit. 12.3.2021]. Dostupné online: https://www.izun.eu/univerzita/co-mame-a-jini-ne-meteorologicka-stanice.

KRENT, Brian. *Espressif ESP-WROOM-32 Wi-Fi & Bluetooth Module* [online]. Wikimedia, 2017. [cit. 13.9.2020]. Dostupné online: https://commons.wikimedia.org/wiki/File:Espressif_ESP-WROOM-32_Wi-Fi_%26_Bluetooth_Module.jpg.

LAI, C. S. et al. A Review of Technical Standards for Smart Cities. *Clean Technologies*. Aug 2020, 2, 3, s. 290–310. ISSN 2571-8797. doi: 10.3390/cleantechnol2030019. Dostupné online: http://dx.doi.org/10.3390/cleantechnol2030019.

LAU, Derek. – CHENG, Y.H.. *Brown-out Protection for S08 MCU's* [online]. NXP Semiconductor, 2011. [cit. 7.9.2020]. Dostupné online: https://www.nxp.com/docs/en/application-note/AN4366.pdf.

LEEUWEN, J. *Handbook of theoretical computer science*. Amsterdam New York Cambridge, Mass : Elsevier MIT Press, 1990. ISBN 978-0-444-88071-0.

MAHDAL, Alois. *Algorithm diagram for XXTEA cipher* [online]. Wikimedia, 2013. [cit. 25.2.2021]. Dostupné online: https://commons.wikimedia.org/wiki/File:Algorithm_diagram_for_XXTEA_cipher.svg.

Mark Otto. *Bootstrap from Twitter* [online]. 2011. [cit. 12.9.2020]. Dostupné online: https://blog.twitter.com/developer/en_us/a/2011/bootstrap-twitter.html.

MAXIM. *Manchester Data encoding for Radio Communications* [online]. Maxim, 2005. [cit. 22.2.2021]. Dostupné online: https://pdfserv.maximintegrated.com/en/an/AN3435.pdf.

MEISER, G. et al. Efficient implementation of eSTREAM ciphers on 8-bit AVR microcontrollers. 07 2008, s. 58 – 66. doi: 10.1109/SIES.2008.4577681.

MENEZES, A.. – OORSCHOT, P.. – VANSTONE, S.. *Block Ciphers* [online]. CRC Press, 1996. [cit. 14.9.2020]. Dostupné online: http://cacr.uwaterloo.ca/hac/about/chap7.pdf.

METEOCENTRUM. *Teplota vzduchu* [online]. Meteocentrum.cz, 2020. [cit. 10.3.2021]. Dostupné online: https://www.meteocentrum.cz/encyklopedie/teplota-vzduchu.

MICROCHIP. *ATTINY84* [online]. Microchip, 2021. [cit. 10.3.2021]. Dostupné online: https://www.microchip.com/wwwproducts/en/ATtiny84.

MILLS, Adrian. *Manchester encoding using RS-232* [online]. Quickbuilder, 2009. [cit. 22.2.2021]. Dostupné online: http://www.quickbuilder.co.uk/qb/articles/index.htm.

MULLEN, G.L.. – MUMMERT, C.. *Finite Fields and Applications*. Student mathematical library. Toulouse : American Mathematical Soc. Dostupné online: https://books.google.cz/books?id=yDgWctqWL4wC. ISBN 9780821884614.

MULLINS, Paul. *Introduction to computers: Hardware and Software* [online]. Slippery Rock University, 2014. [cit. 10.3.2021]. Dostupné online: http://cs.sru.edu/~mullins/cpsc100book/module02_introduction/module02-03_introduction.html.

NIST. *Announcing the ADVANCED ENCRYPTION STANDARD (AES)* [online]. NIST, 2001. [cit. 25.2.2021]. Dostupné online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

NXP Semiconductors. *I2C-bus specification and user manual* [online]. 2014. [cit. 6.9.2020]. Dostupné online: https://www.nxp.com/docs/en/user-guide/UM10204.pdf.

PANTHER. *Ural-1 front view* [online]. Wikimedia, 2009a. [cit. 18.9.2020]. Dostupné online: https://commons.wikimedia.org/wiki/File:Ural-1_Indicators.jpg.

PANTHER. *Ural-1 front view* [online]. Wikimedia, 2009b. [cit. 18.9.2020]. Dostupné online: https://commons.wikimedia.org/wiki/File:Ural-1_front_view.jpg.

Philips Semiconductors. *I2S Bus specification* [online]. 1996. [cit. 5.9.2020]. Dostupné online: https://web.archive.org/web/20070102004400/http://www.nxp.com/acrobat_download/various/I2SBUS.pdf.

POPOV, Andrej. *Prohibiting RC4 Cipher Suites* [online]. Internet Engineering Task Force (IETF), 2015. [cit. 12.3.2021]. Dostupné online: https://tools.ietf.org/html/rfc7465.

ROUSE, Margaret. *Internet of things (IoT)* [online]. Techtarget, 2016. [cit. 19.9.2020]. Dostupné online: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

RUSSELL, Matthew D.. *Tinyness: An Overview of TEA and Related Ciphers* [online]. University of York, 2004. [cit. 25.2.2021]. Dostupné online: https://web.archive.org/web/20070812222155/http://www-users.cs.york.ac.uk/~matthew/TEA/.

SABIR, Esasaid. *Advances in ubiquitous networking : proceedings of the UNet'15*. Singapore : Springer, 2016. ISBN 978-981-287-989-9.

SAIFEE, Akbar Ali S.F.A. *How accurate are the computed timings for sunrise and sunset?* [online]. icoproject.org, 2016. [cit. 15.2.2021]. Dostupné online: http://www.icoproject.org/pdf/saifee_2106.pdf.

SAMELI, Ioan. *Intel 8742 153056995* [online]. Wikimedia, 2003. [cit. 15.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:Intel_8742_153056995.jpg.

SAXENA, S. et al. Various Types of Circuit Breakers used in Power System for Smooth Working of the Transmission Line. *MIT International Journal of Electrical and Instrumentation Engineering*. 2012, 2, 2, s. 106–111. Dostupné online: https://pdfs.semanticscholar.org/0691/8326da2b2ac6fd80620d88961b68554b72ed.pdf.

Schneider Electric. *Overcurrent Protection* [online]. Schneider Electric, 2012. [cit. 5.9.2020]. Dostupné online: https://download.schneider-electric.com/files?p_enDocType=Data+Bulletin&p_File_Name=0600DB0301.pdf&p_Doc_Ref=0600DB0301.

SCOTT, Kevin. *Zambretti* [online]. Meteormetrics, 2010. [cit. 19.9.2020]. Dostupné online: https://web.archive.org/web/20100518184824/http://www.meteormetrics.com/zambretti.htm.

SHASHIKANTH, Rahul. *Ball Grid Array (BGA): Features, Soldering Technique and X-Ray Inspection* [online]. Protoexpress, 2020. [cit. 19.9.2020]. Dostupné online: https://www.protoexpress.com/blog/bga-features-soldering-x-ray-inspection/.

SQLite. *What is SQLite?* [online]. SQLite.org, 2020a. [cit. 12.9.2020]. Dostupné online: https://www.sqlite.org/index.html.

SQLite. *SQLite Is A Zero-Configuration Database* [online]. SQLite.org, 2020b. [cit. 12.9.2020]. Dostupné online: https://sqlite.org/zeroconf.html.

STALLINGS, W.. *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice-Hall : Prentice Hall, 1999. Dostupné online: https://books.google.cz/books?id=Dam9zrViJjEC. ISBN 9780138690175.

STOSIC, Lazar. RC4 stream cipher and possible attacks on WEP. *International Journal of Advanced Computer Science and Applications (IJACSA)*. 01 2012, 3, s. 110–114.

STROUS, Louis. *Astronomy answers position of the Sun* [online]. 2020. [cit. 15.2.2021]. Dostupné online: https://www.aa.quae.nl/en/reken/zonpositie.html.

SUBSYSTEMS. *Calculate the Moon Phase* [online]. Subsystems, 2017. [cit. 22.2.2021]. Dostupné online: https://www.subsystems.us/uploads/9/8/9/4/98948044/moonphase.pdf.

TECHOPEDIA. *Julian date* [online]. Techopedia, 2021. [cit. 10.3.2021]. Dostupné online: https://www.techopedia.com/definition/16719/julian-date.

TIšNOVSKý, Pavel. *Externí sériové sběrnice SPI a I²C* [online]. Root.cz, 2008. [cit. 5.9.2020]. Dostupné online: https://www.root.cz/clanky/externi-seriove-sbernice-spi-a-i2c/#k01.

TOTALPHASE. *7-bit, 8-bit, and 10-bit I2C Slave Addressing* [online]. 2013. [cit. 6.9.2020]. Dostupné online: https://www.totalphase.com/support/articles/200349176.

TRAORE, Issa. *Basic Networking Concepts* [online]. University of Victoria, 2021. [cit. 12.3.2021]. Dostupné online: https://www.ece.uvic.ca/~itraore/elec567-13/notes/dist-03-4.pdf.

UNSöLD, Albrecht. – BASCHEK, Bodo. *The New Cosmos*. Berlin : Springer, 2002. ISBN 978-3-540-67877-9.

WESTLUND, Harold B.. *NIST reports measurable success of Advanced Encryption Standard* [online]. NIST, 2002. [cit. 25.2.2021]. Dostupné online: https://web.archive.org/web/20071103105501/http://findarticles.com/p/articles/mi_m0IKZ/is_3_107?pnum=2&opg=90984479.

WHEELER, David J.. – NEEDHAM, Roger M.. *Correction to xtea* [online]. Cambridge University, 1998. [cit. 12.3.2021]. Dostupné online: http://www.movable-type.co.uk/scripts/xxtea.pdf.

WHITETIMBERWOLF. *CBC decryption* [online]. Wikimedia, 2013a. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:CBC_decryption.svg.

WHITETIMBERWOLF. *CBC Encryption* [online]. Wikimedia, 2013b. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:CBC_encryption.svg.

WHITETIMBERWOLF. *CFB Decryption* [online]. Wikimedia, 2013c. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:CFB_decryption.svg.

WHITETIMBERWOLF. *CFB Encryption* [online]. Wikimedia, 2013d. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:CFB_encryption.svg.

WHITETIMBERWOLF. *ECB decryption* [online]. Wikimedia, 2013e. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:ECB_decryption.svg.

WHITETIMBERWOLF. *ECB encryption* [online]. Wikimedia, 2013f. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:ECB_encryption.svg.

WHITETIMBERWOLF. *OFB Decryption* [online]. Wikimedia, 2013g. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:OFB_encryption.svg.

WHITETIMBERWOLF. *OFB Encryption* [online]. Wikimedia, 2013h. [cit. 14.9.2020]. Dostupné online: https://en.wikipedia.org/wiki/File:OFB_encryption.svg.

WILLIAMS, Ed. *Sunrise/Sunset Algorithm* [online]. Nautical Almanac Office, 1990. [cit. 15.2.2021]. Dostupné online: https://www.edwilliams.org/sunrise_sunset_algorithm.htm.

WRIGHT, A. *Electric fuses*. London, UK : Institution of Electrical Engineers, 2004. ISBN 978-0-86341-399-5.

YUN, Aaram. – PARK, Je Hong. – LEE, Jooyoung. *Lai-Massey Scheme an Quasi-Feistel Networks* [online]. University of Minnesota, 2010. [cit. 13.9.2020]. Dostupné online: https://eprint.iacr.org/2007/347.pdf.

ČERNIKOVSKý, Libor. – BROžKOVá, Radmila. *Superpočítače v meteorologii a klimatologii* [online]. Český hydrometeorologický ústav (CHMI), 2019. [cit. 18.9.2020]. Dostupné online: http://slideplayer.cz/slide/17826396/.

8 Přílohy

8.1 Příloha A - zdrojové kódy

8.1.1 RC4

```
1  void RC4(unsigned char* data,long dataLen, unsigned char* key, long keyLen,unsigned char* result)
2  /* Function to encrypt data represented in array of char "data" with length represented in
       dataLen using key which is represented in "Key" with length represented in keyLen, and result
       will be stored in result */
3  {
4      unsigned char T[256];
5      unsigned char S[256];
6      unsigned char  tmp; // to be used in swaping
7      int j = 0,t= 0,i= 0;
8
9
10     /* S & K initialization */
11     for(int i = 0 ; i < 256 ; i++)
12     {
13         S[i]=i;
14         T[i]= key[i % keyLen];
15     }
16     /* State Permutation */
17     for(int i = 0 ; i < 256; i++)
18     {
19         j = ( j + S[i] + T[i] ) % 256;
20
21          //Swap S[i] & S[j]
22         tmp = S[j];
23         S[j]= S[i];
24         S[i] = tmp;
25     }
26     j =0; // reintializing j to reuse it
27     for(int x = 0 ; x< dataLen ; x++)
28     {
29         i = (i+1) % 256; // using %256 to avoid exceed the array limit
30         j = (j + S[i])% 256; // using %256 to avoid exceed the array limit
31
32         //Swap S[i] & S[j]
33         tmp = S[j];
34         S[j]= S[i];
35         S[i] = tmp;
36
37         t = (S[i] + S[j]) % 256;
38
39         result[x]= data[x]^S[t]; // XOR generated S[t] with Byte from the plaintext / cipher and
               append each Encrypted/Decrypted byte to result array
40     }
41 }
```

Zdroj: https://github.com/kmohamed2020/rc4/blob/master/RC4.c (11.9.2020)

8.1.2 Zdrojový kód šifry XXTEA v jazyce C

```
#define MX ((z>>5^y<<2) + (y>>3^z<<4) ^ (sum^y) + (k[p&3^e]^z))

long btea(long* v, long n, long* k) {
  unsigned long z=v[n-1], y=v[0], sum=0, e, DELTA=0x9e3779b9;
  long p, q ;
  if (n > 1) {          /* Coding Part */
    q = 6 + 52/n;
    while (q-- > 0) {
      sum += DELTA;
      e = (sum >> 2) & 3;
      for (p=0; p<n-1; p++) y = v[p+1], z = v[p] += MX;
      y = v[0];
      z = v[n-1] += MX;
    }
    return 0 ;
  } else if (n < -1) {  /* Decoding Part */
    n = -n;
    q = 6 + 52/n;
    sum = q*DELTA ;
    while (sum != 0) {
      e = (sum >> 2) & 3;
      for (p=n-1; p>0; p--) z = v[p-1], y = v[p] -= MX;
      z = v[n-1];
      y = v[0] -= MX;
      sum -= DELTA;
    }
    return 0;
  }
  return 1;
}
```

Zdroj: (Wheeler – Needham, 1998), modifikovaná verze převzata z anglické wikipedie pod heslem „XXTEA“[38]

8.1.3 Kompenzace kombinovaného senzoru teploty/vlhkosti/tlaku

Kompenzace probíhá z důvodů výpočetní náročnosti na hlavní stanici, koeficienty pro kompenzaci jsou odeslány při párování sondy s hlavní stanicí tak, jak bylo uvedeno v kapitole č.4.6.5 (Paket kompenzačních koeficientů).

[38] Dne 10.9.2020

```
1  //vypocitava pomocnou teplotu ktera se pouziva ke kompenzaci tlaku a vlhkosti
2  double bme280_calculate_t_fine(int32_t adc_T, uint16_t dig_T1, int16_t dig_T2, int16_t dig_T3) {
3      double var1, var2;
4      var1 = (((double) adc_T) / 16384.0 - ((double) dig_T1) / 1024.0) * ((double) dig_T2);
5      var2 = ((((double) adc_T) / 131072.0 - ((double) dig_T1) / 8192.0) * (((double) adc_T) /
           131072.0 - ((double) dig_T1) / 8192.0)) * ((double) dig_T3);
6      return var1 + var2;
7  }
8
9  //vraci teplotu ve stupnich celsia
10
11 double bme280_compensate_T_double(double t_fine) {
12     return t_fine / 5120.0;
13 }
14
15 //vraci tlak v pascalech
16 double bme280_compensate_P_double(int32_t adc_P, double t_fine, uint16_t dig_P1, int16_t dig_P2,
       int16_t dig_P3, int16_t dig_P4, int16_t dig_P5,
17         int16_t dig_P6, int16_t dig_P7, int16_t dig_P8, int16_t dig_P9) {
18     double var1, var2, p;
19     var1 = (t_fine / 2.0) - 64000.0;
20     var2 = var1 * var1 * ((double) dig_P6) / 32768.0;
21     var2 = var2 + var1 * ((double) dig_P5) * 2.0;
22     var2 = (var2 / 4.0) + (((double) dig_P4) * 65536.0);
23     var1 = (((double) dig_P3) * var1 * var1 / 524288.0 + ((double) dig_P2) * var1) / 524288.0;
24
25     if (var1 == 0) {
26         return 0; //vyhnuti se vyjimky, aby se nedelilo nulou
27     }
28
29     p = 1048576.0 - (double) adc_P;
30     p = (p - (var2 / 4096.0)) * 6250.0 / var1;
31     var1 = ((double) dig_P9) * p * p / 2147483648.0;
32     var2 = p * ((double) dig_P8) / 32768.0;
33     p = p + (var1 + var2 + ((double) dig_P7)) / 16.0;
34     return p;
35 }
36
37 //vraci vlhkost v procentech
38 double bme280_compensate_H_double(int32_t adc_H, double t_fine, uint8_t dig_H1, int16_t dig_H2,
       uint8_t dig_H3, int16_t dig_H4, int16_t dig_H5, int8_t dig_H6) {
39     double var_H;
40     var_H = t_fine - 76800.0;
41     var_H = (adc_H - (((double) dig_H4) * 64.0 + ((double) dig_H5) / 16384.0 * var_H)) *
42             (((double) dig_H2) / 65536.0 * (1.0 + ((double) dig_H6) / 67108864.0 * var_H * (1.0 +
                    ((double) dig_H3) / 671008864.0 * var_H)));
43     var_H = var_H * (1.0 - ((double) dig_H1) * var_H / 524288.0);
44
45     if (var_H > 100.0) {
46         var_H = 100.0;
47     } else if (var_H < 0.0) {
```

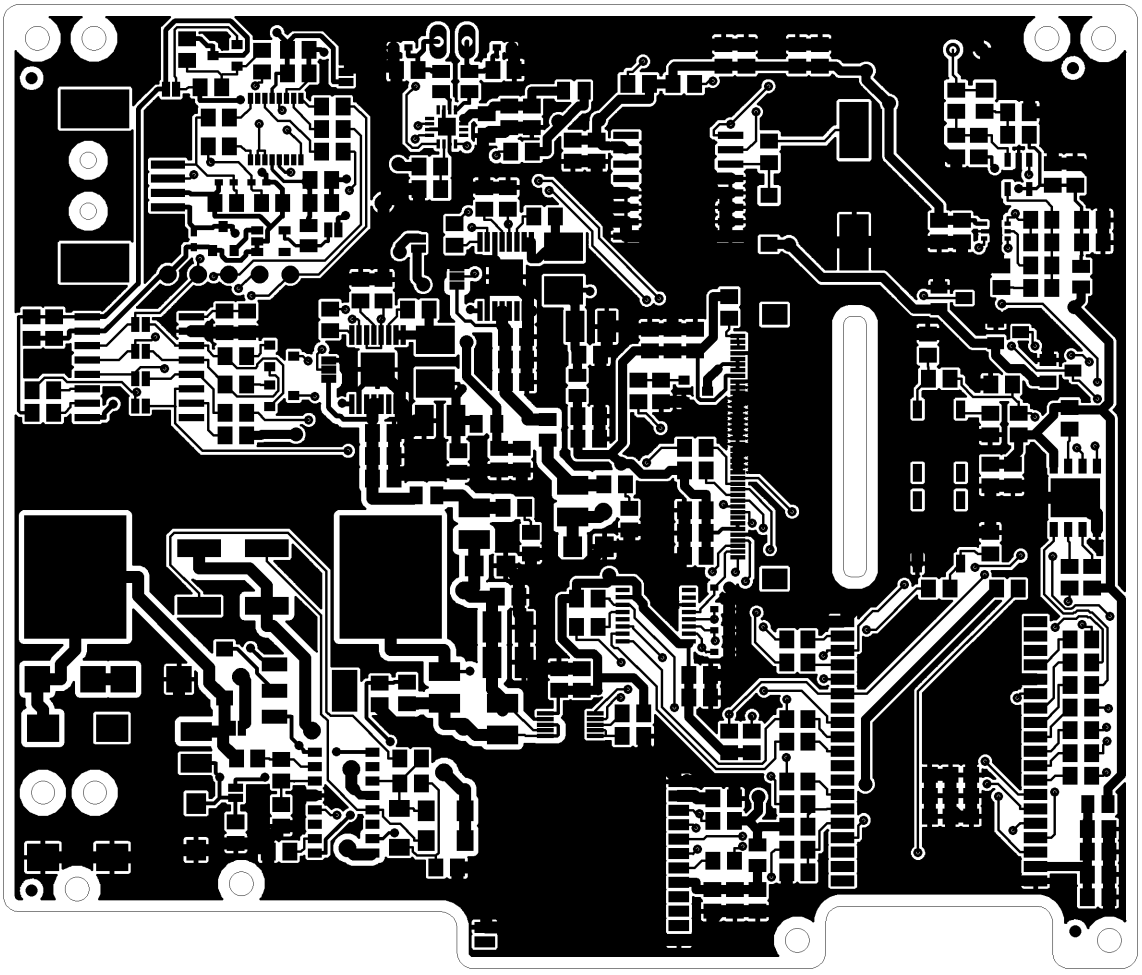
```
48            var_H = 0.0;
49        }
50        return var_H;
51    }
```

8.2 Příloha B - výrobní výkresy DPS

8.2.1 Hlavní stanice

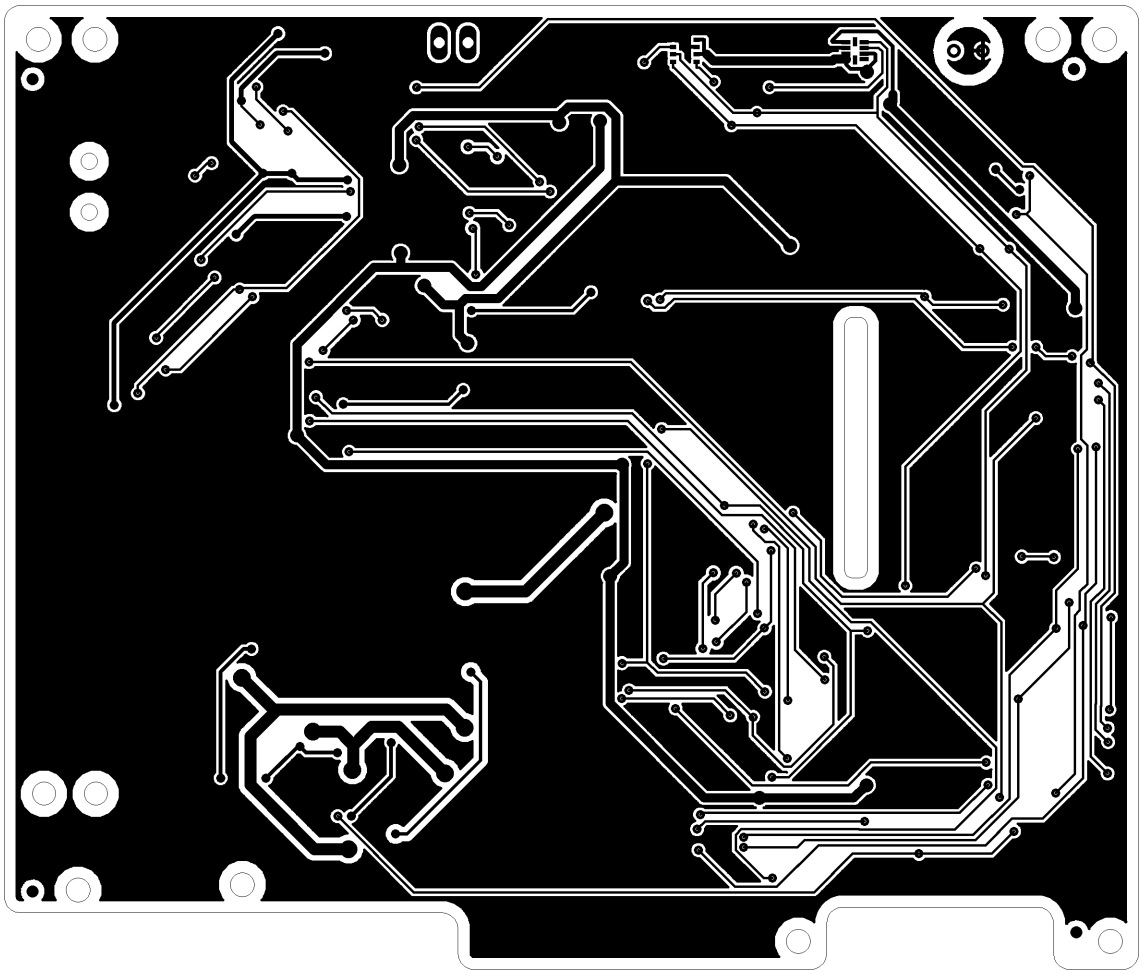
Měřítka výkresů jsou 1.5:1

8.2.1.1 Vrchní strana spojů hlavní stanice



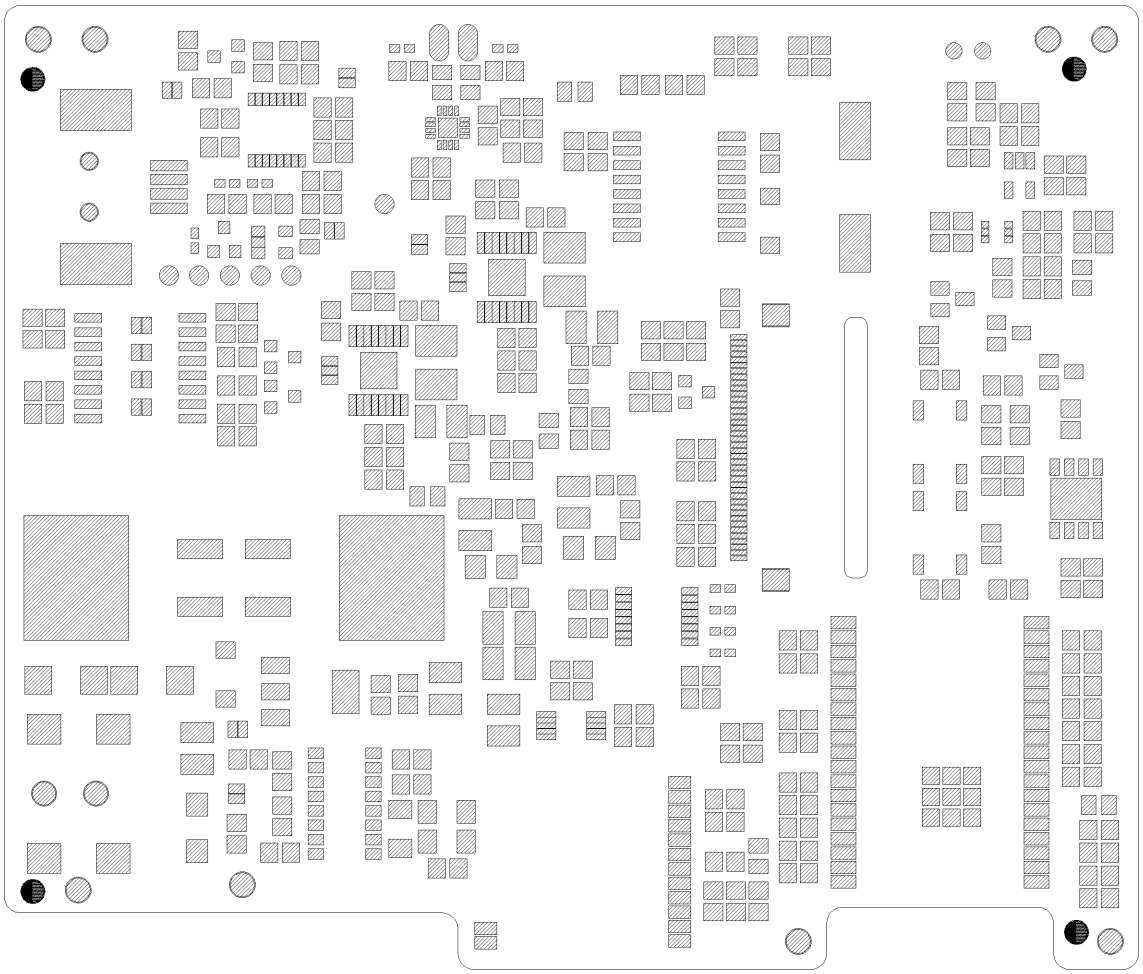
Obrázek 38: Vrchní strana spojů hlavní stanice

8.2.1.2 Spodní strana spojů hlavní stanice



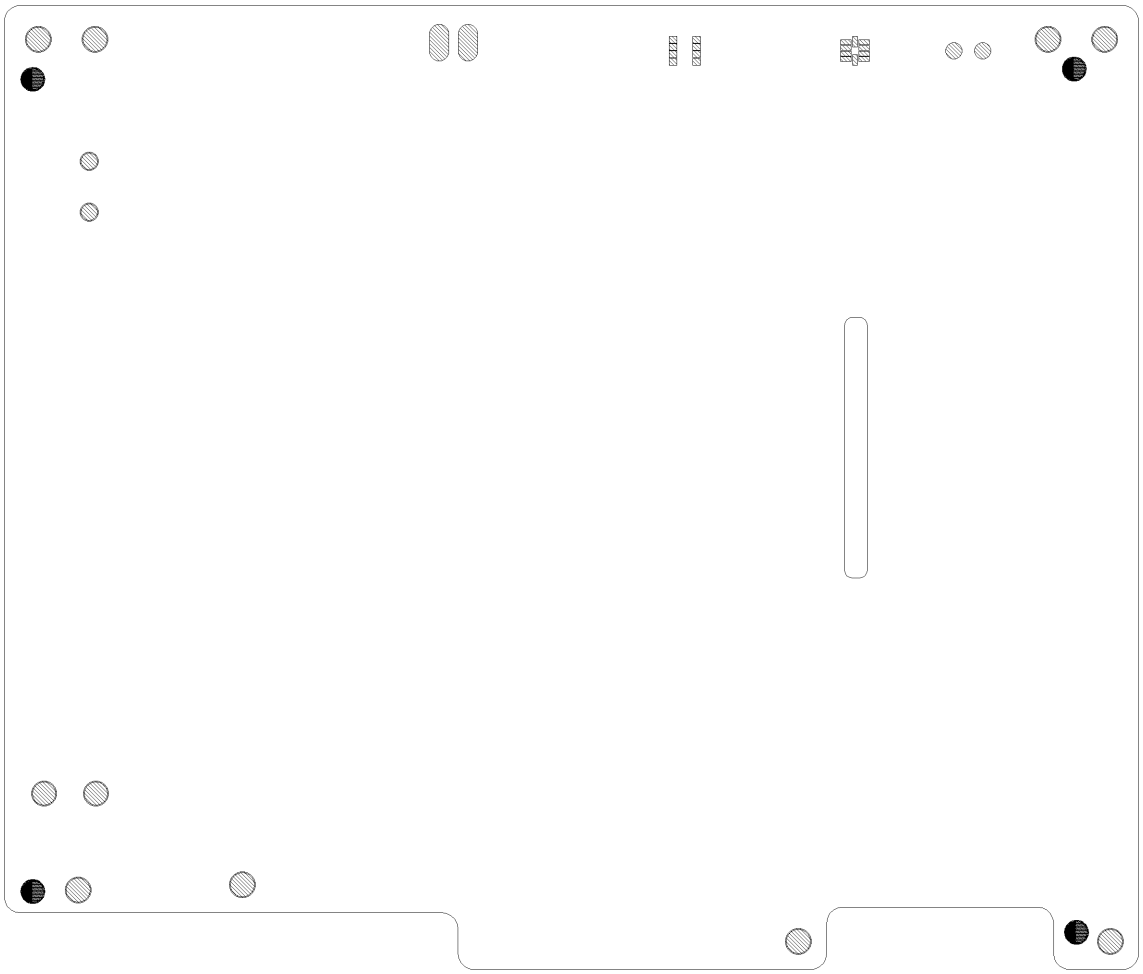
Obrázek 39: Spodní strana spojů hlavní stanice

8.2.1.3 Vrchní strana masky hlavní stanice



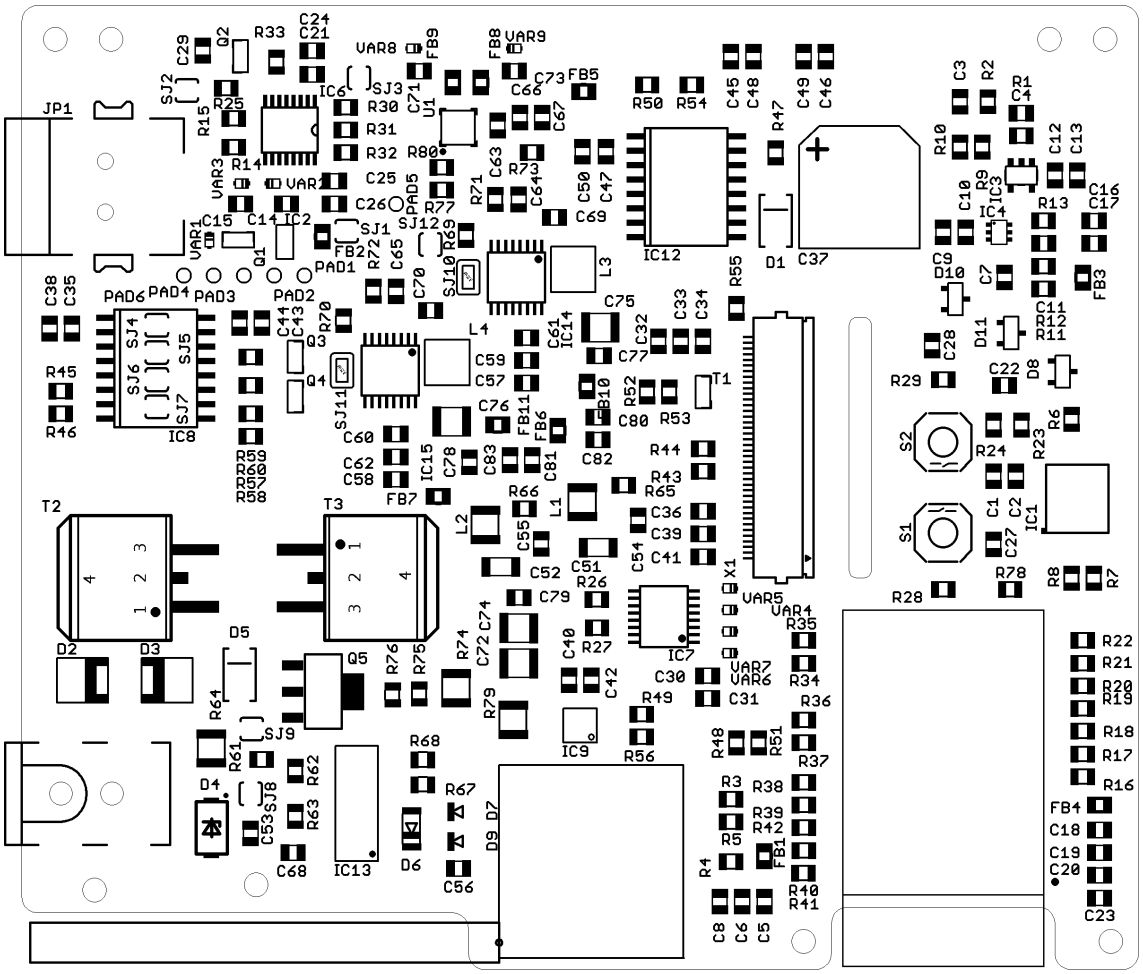
Obrázek 40: Vrchní strana masky hlavní stanice

8.2.1.4 Spodní strana masky hlavní stanice



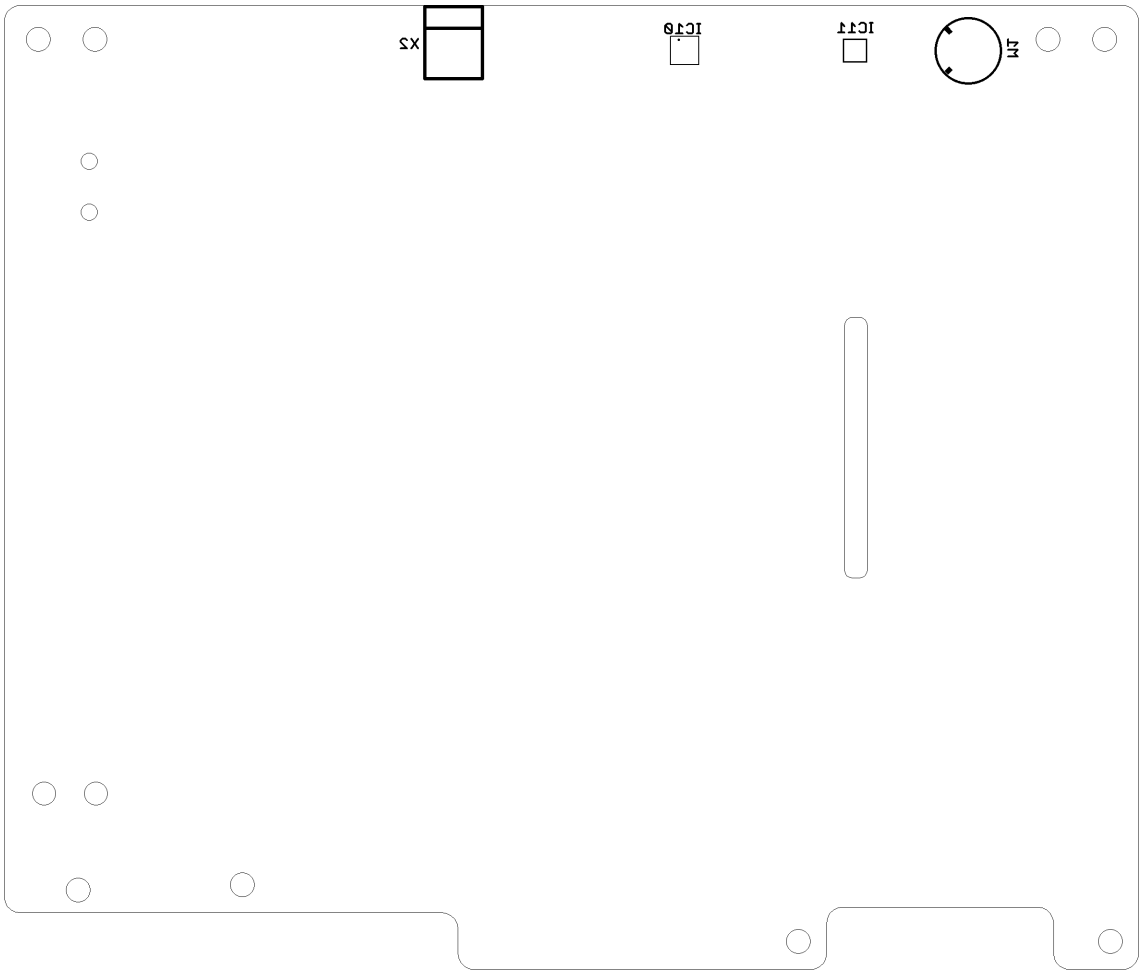
Obrázek 41: Spodní strana masky hlavní stanice

8.2.1.5 Vrchní strana potisku hlavní stanice



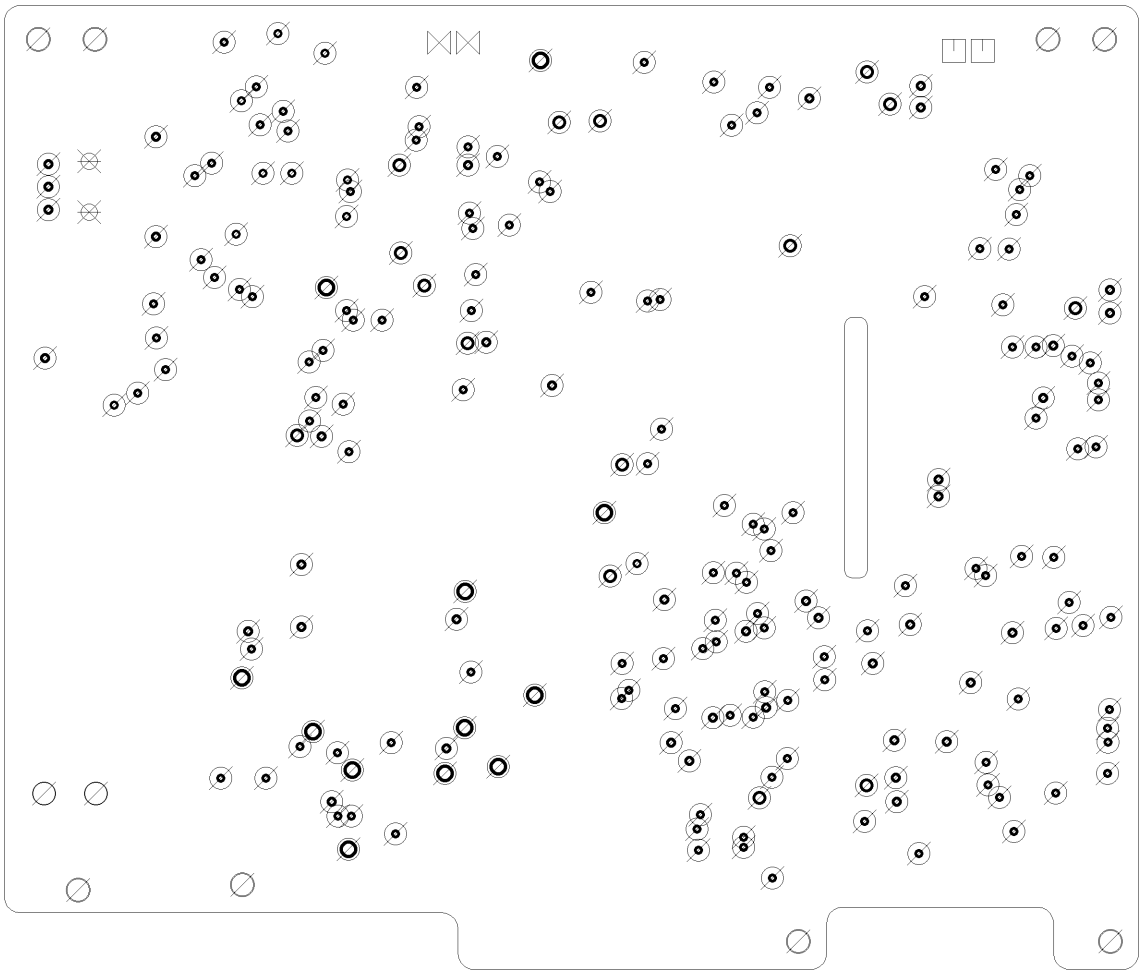
Obrázek 42: Vrchní strana potisku hlavní stanice

8.2.1.6 Spodní strana potisku hlavní stanice



Obrázek 43: Spodní strana potisku hlavní stanice

8.2.1.7 Vývrty hlavní stanice

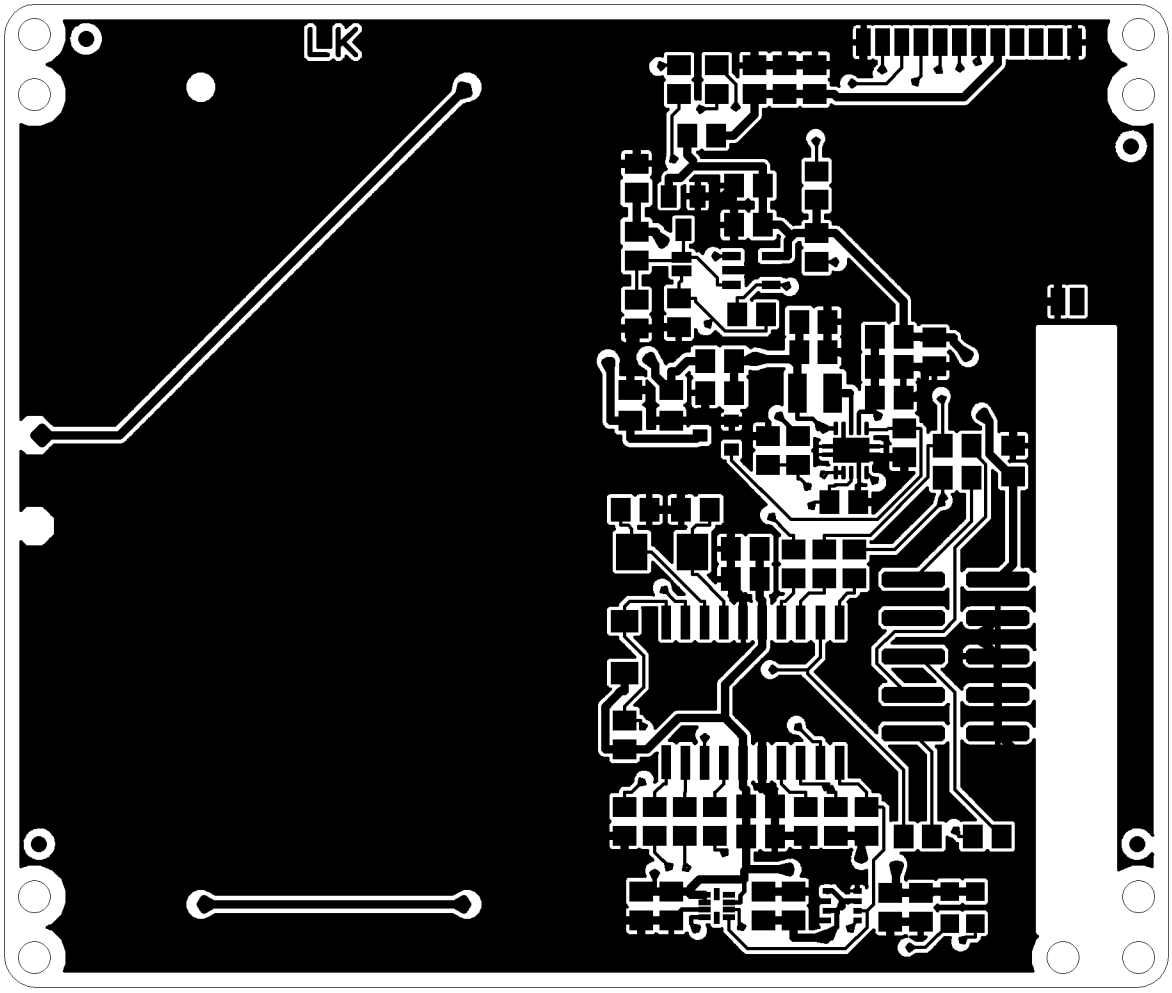


Obrázek 44: Vývrty hlavní stanice

8.2.2 Sonda

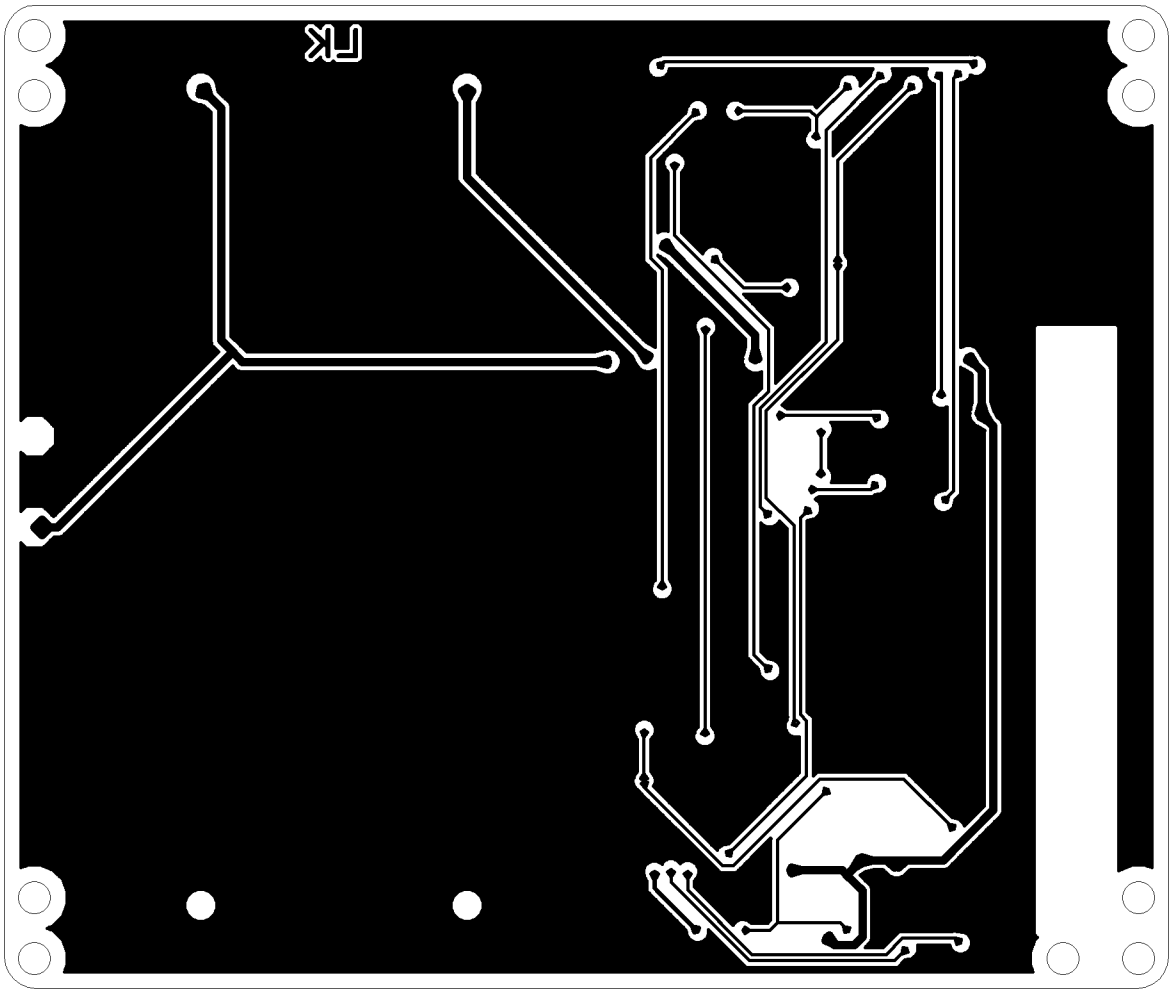
Měřítka výkresů jsou 2:1

8.2.2.1 Vrchní strana spojů sondy



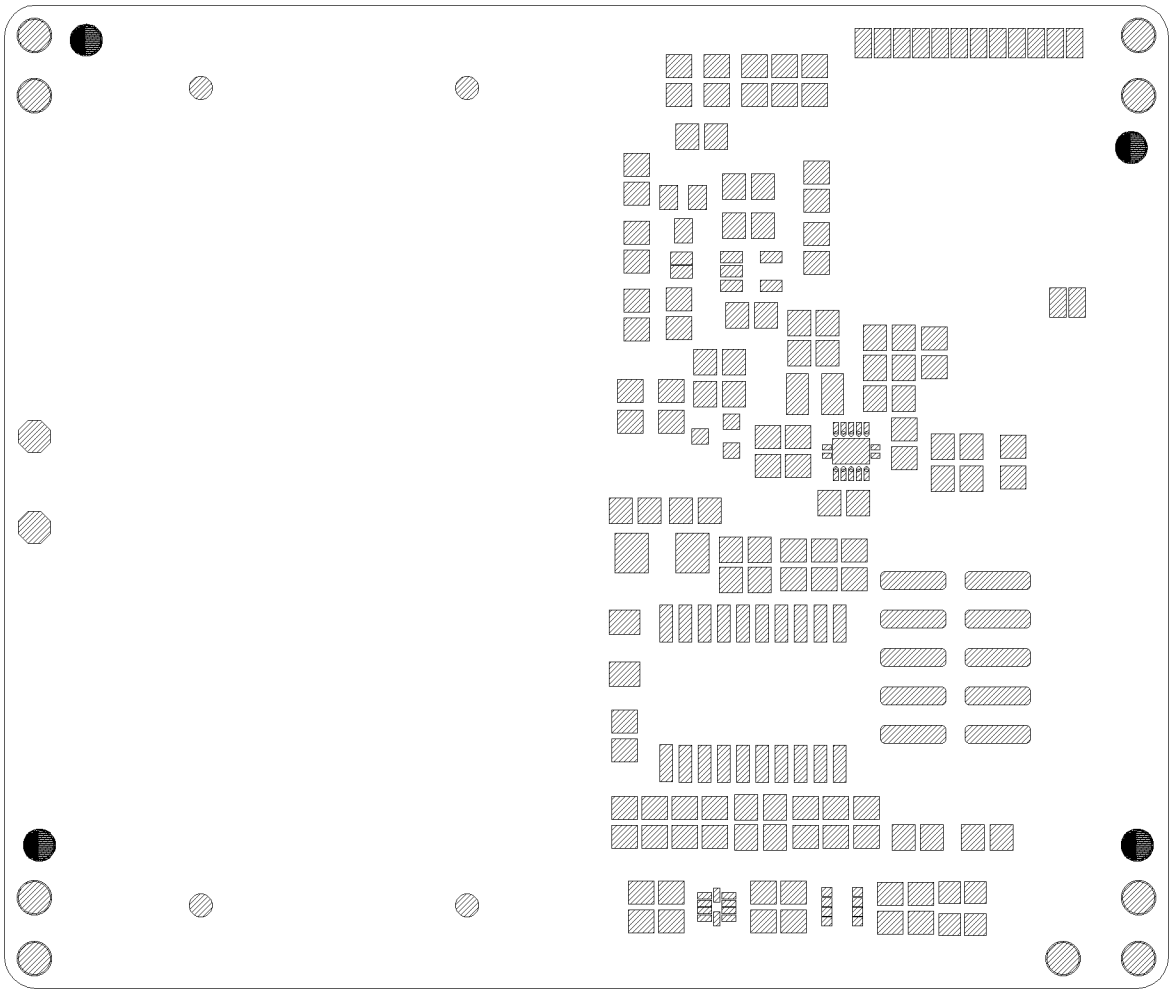
Obrázek 45: Vrchní strana spojů sondy

8.2.2.2 Spodní strana spojů sondy



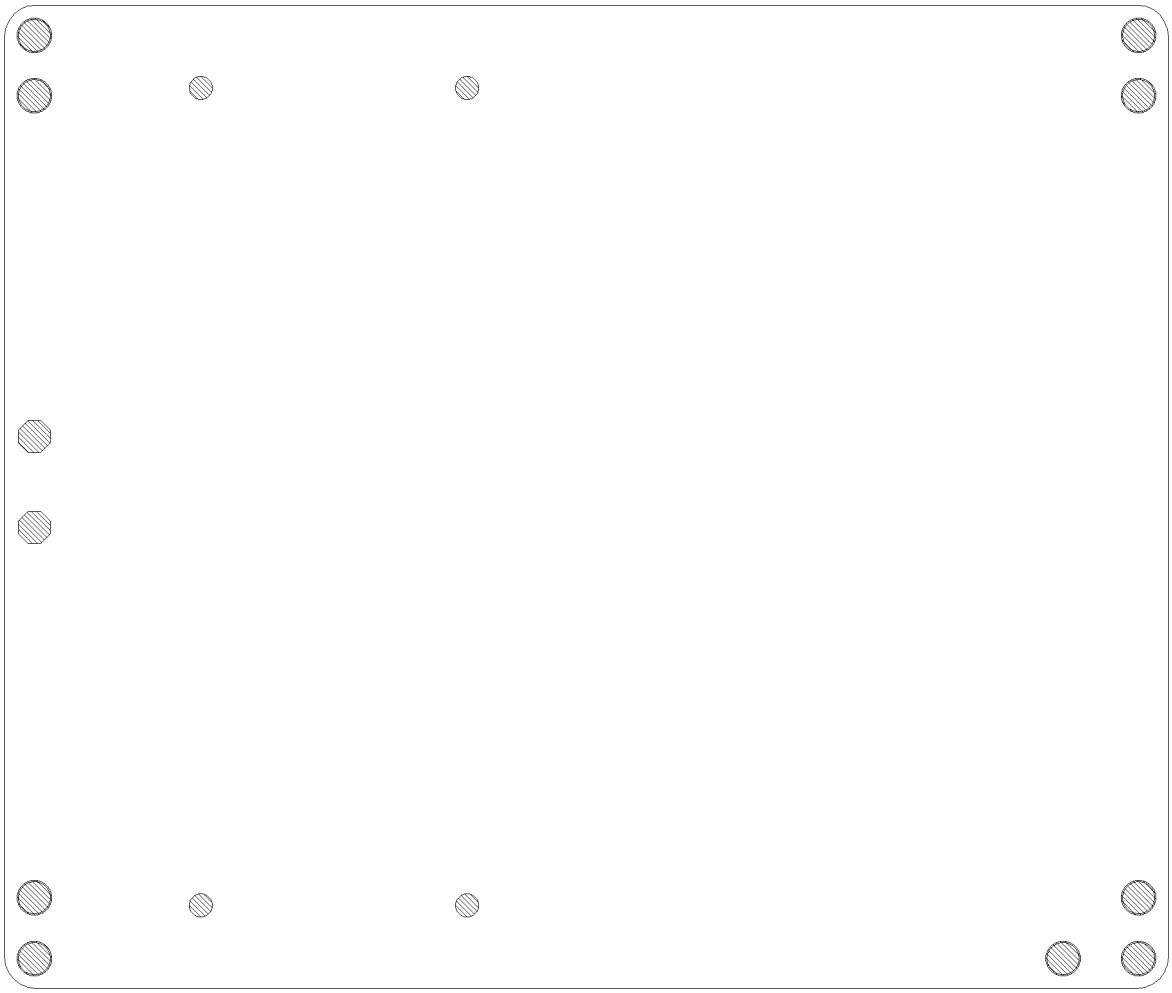
Obrázek 46: Spodní strana spojů sondy

8.2.2.3 Vrchní strana masky sondy



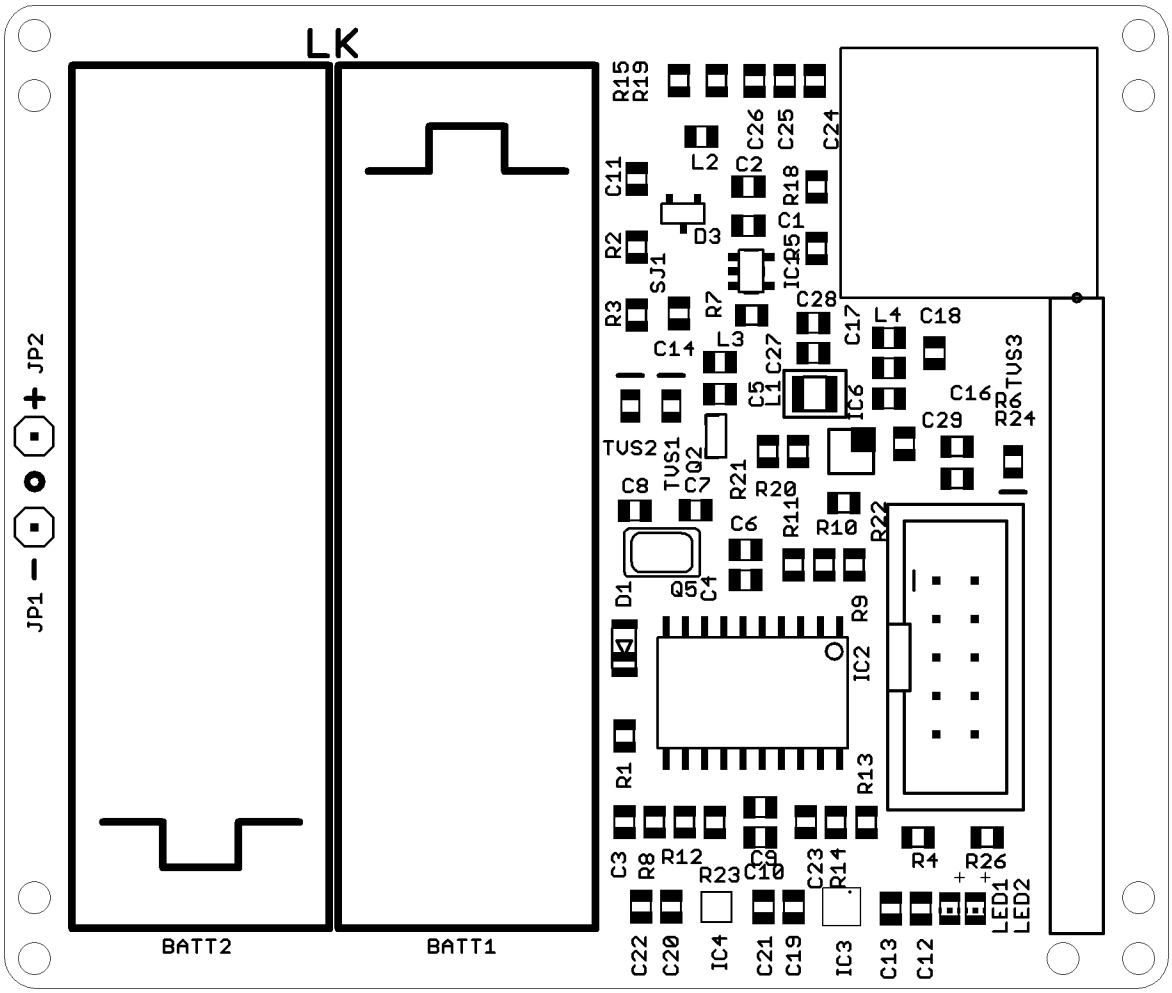
Obrázek 47: Vrchní strana masky sondy

8.2.2.4 Spodní strana masky sondy



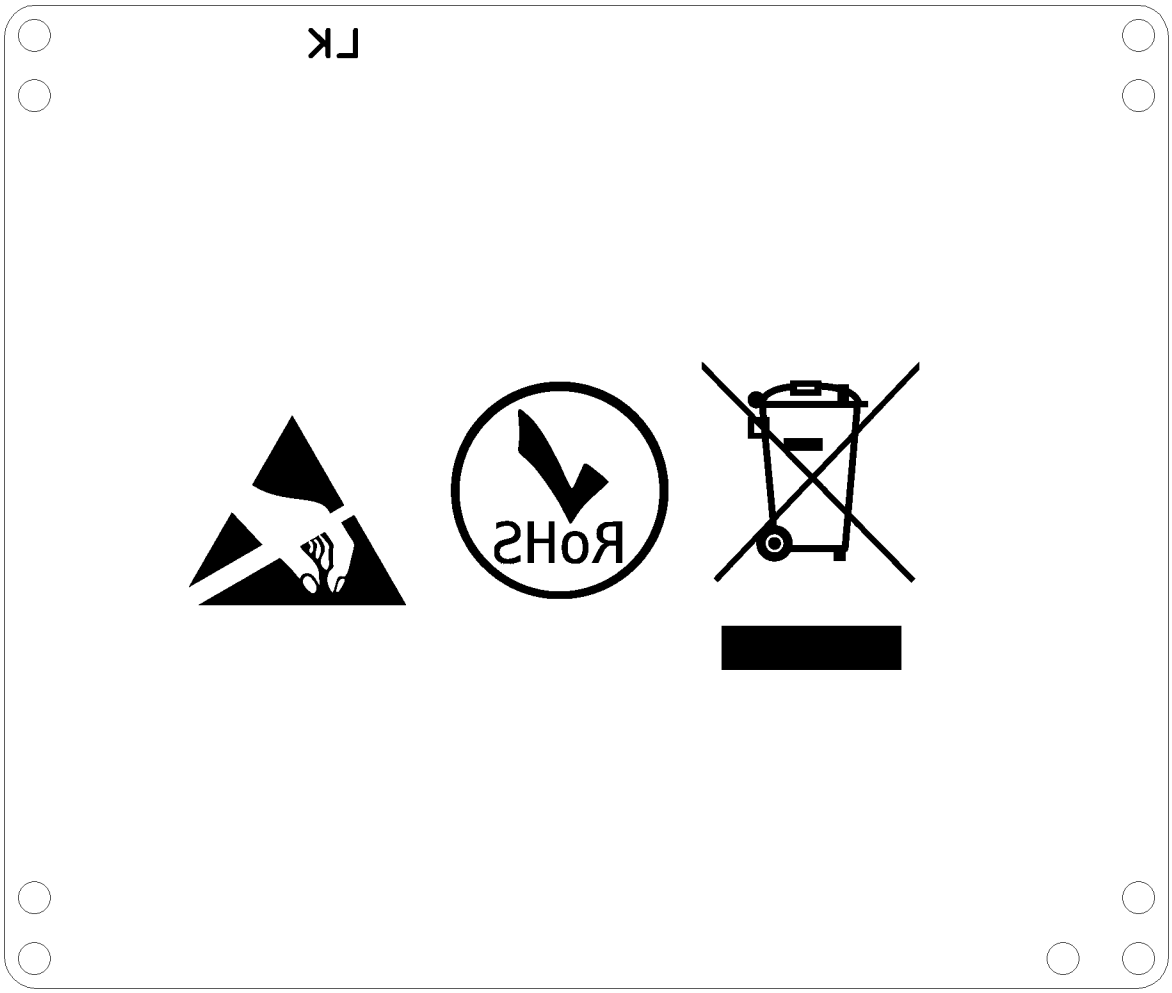
Obrázek 48: Spodní strana masky sondy

8.2.2.5 Vrchní strana potisku sondy



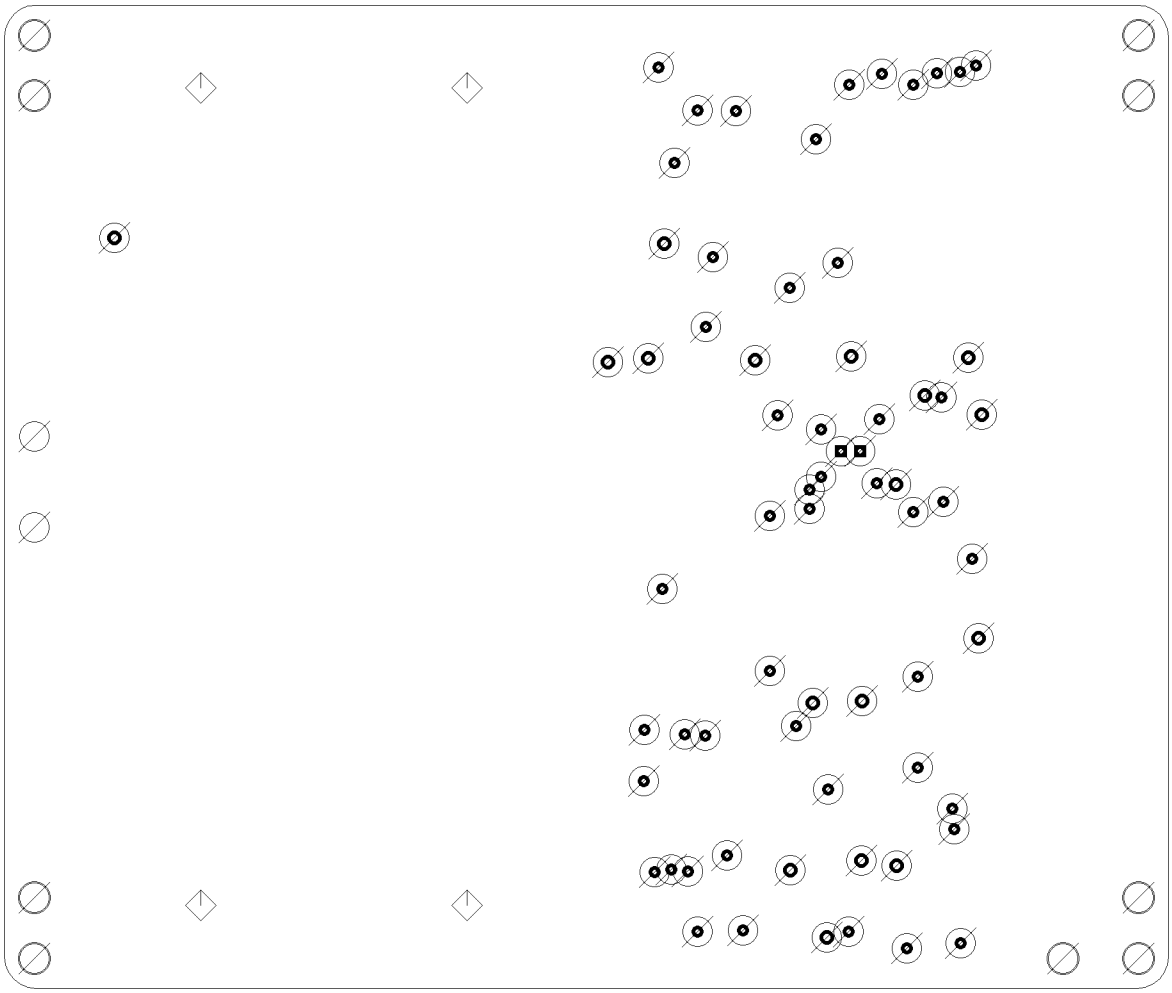
Obrázek 49: Vrchní strana potisku sondy

8.2.2.6 Spodní strana potisku sondy



Obrázek 50: Spodní strana potisku sondy

8.2.2.7 Vývrty sondy



Obrázek 51: Spodní strana vývrtů sondy