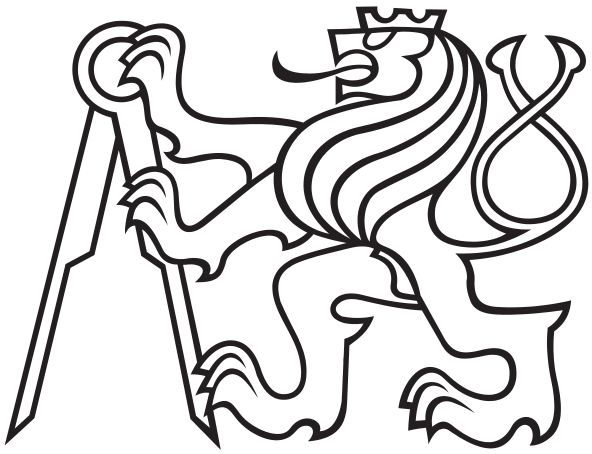
České vysoké učení technické v Praze

Fakulta elektrotechnická

Katedra telekomunikační techniky



Diplomová práce

Systém pro sběr technologických dat v koncepci IoT

Autor: Bc. Jan Hofman

Vedoucí práce: Ing. Bc. Lukáš Vojtěch, Ph.D.

Čestné prohlášení

Jako autor této bakalářské práce dále prohlašuji, že v souvislosti s jejím vytvořením, jsem neporušil autorská práva třetích osob a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb.

V Praze dne 1. 5. 2017 .....

(Bc. Jan Hofman)

Poděkování

Děkuji Ing. Bc. Lukáši Vojtěchovi, PhD. za aktivní pomoc, a to jak při psaní teoretické, tak i praktické části této diplomové práce. Jeho věcné připomínky a postřehy mi velmi usnadnily tvorbu této práce.

Zároveň děkuji své matce a přítelkyni, které mi byly po celou dobu studia oporou. Vytvářely mi kvalitní podmínky ke studiu a byly vždy po ruce, když jsem cokoli potřeboval.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Hofman** Jméno: **Jan** Osobní číslo: **406122**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Sítě elektronických komunikací**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Systém pro sběr technologických dat v koncepci IoT

Název diplomové práce anglicky:

System for technological data collection in the IoT concept

Pokyny pro vypracování:

Navrhněte a realizujte systém pro sběr, základní správu a vizualizaci technologických dat v koncepci IoT. Pro připojení senzorů a snímačů veličin do datového koncentrátoru uvažujte jak kabelová připojení, tak využití vybrané LPWAN/LPN technologie. Uvažované snímače musí být schopny měřit minimálně teplotu vodných roztoků, pH roztoku, stejnosměrné elektrické napětí do 15 V a stejnosměrný elektrický proud do 10 A. Součástí systému bude též datový koncentrátor/centrální sběrná jednotka, obsahující HTTP server, display pro zobrazení dat a datové úložiště s využitím SD karty. Detaily zadání a realizaci scénářů konzultujte s vedoucím práce. Uvažujte také aspekty bezpečnosti a spolehlivosti navrženého řešení. Součástí práce je i testování a dokumentace navrženého řešení.

Seznam doporučené literatury:

[1] Dokumentace dostupná na http://www.iqrfalliance.org [on-line]
[2] Dokumentace dostupná na https://www.lora-alliance.org [on-line]
[3] Discovery kit with STM32F746NG MCU dostupný na http://www.st.com/ [on-line]

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Lukáš Vojtěch Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **17.02.2017** Termín odevzdání diplomové práce: **26.05.2017**

Platnost zadání diplomové práce: **30.09.2018**

Podpis vedoucí(ho) práce	Podpis vedoucí(ho) ústavu/katedry	Podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání	Podpis studenta

Anotace

Tato diplomová práce se zabývá tvorbou univerzálního systému pro sběr technologických dat. Tento systém je navrhnut tak, aby ho bylo možné použít jak v průmyslu, tak v běžné domácnosti. Navržený sběrný bod obsahuje HTTP, TFTP služby, kterými je řízen. Součástí diplomové práce je návrh i konstrukce senzorových přípravků pro otestování sběrného bodu.

Klíčová slova
IoT, HTTP, TFTP, senzorové sítě, ARM, zpracování dat

Abstract

This diploma thesis is focused on designing universal system for collection of technological data. The system is designed for industry and ordinary household usage. Designed collection unit contains HTTP, TFTP protocols used for controlling. Design and construction of sensoric kits for testing of the collection unit was also a part of this thesis.

Keywords
IoT, HTTP, TFTP, senzor network, ARM, processing data

Obsah

Obrázky

Seznam zkratek

AD	Analogově/Digitální
AES	Advanced Encyption Standart
AJAX	Asynchronous Javascript and XML
API	Application Peripheral Interface
ARM	Advanced RISC Machine
BSP	Board Support Package
CBC	Cipher Block Chaining
CGI	Common Gateway Interface
CMSIS	Cortex® Microcontroller Software Interface Standard
ČRa	České Radiokomunikace
ČR	Česká republika
ČSN	Československá norma
ČTÚ	Český telekomunikační úřad
FatFS	File Allocation Table File System
HAL	Hardware Abstraction Layer
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
I2C	Inter-Integrated Circuit
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
js	Javascript
JSON	Javascript Object Notation
JTAG/SWD	Joint Test Action Group/Serial Wire Debug
LCD-TFT	Liquid Crystal Display - Thin-Film
LoRa	Long Range
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
LWIP	LightWeightIP

M2M	Machine to Machine
MaR	Měření a Regulace
M-BUS	Meter BUS
MEMS	MicroElectroMechanical Systems
NB	Narrow Band
OS	Operační systém
OSS	Open Source
RAM	Random Access Memory
RF	Radiofrekvenční
RISC	Reduced Instruction Set Computing
RTC	Real Time Clock
RTOS	Real Time Operating System
SPI	Serial Peripheral Interface
SSI	Server Side Include
SSL	Secure Sockets Layer
SW	Software
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UART	Universal asynchronous receiver/ transmitter
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WSN	Wireless Sensor Network

Kapitola 1

Úvod

S rozvojem elektroniky a přenosových technologii narůstá i poptávka po automatizovaném sběru dat. Pro ulehčení tvorby statistik a ovládání zařízení shromažďují firmy informace např. o výrobě, kvalitě a efektivitě práce na jednom centralizovaném místě. Proto je třeba zabývat se otázkou jakým prostředkem tato data sbírat. Jednou z možností je použití proprietárního rozhraní dodaného výrobcem, které lze propojit komunikačním kanálem do centrálního úložiště. Vzniká však problém nekompatibility s ostatními využívanými systémy. Řešením může být vytvoření komunikačního protokolu ve spolupráci s výrobcem tohoto rozhraní. To je však závislé na ochotě výrobce a míře kvalifikovanosti jeho zaměstnanců. Toto řešení je i finančně nákladné, a proto je nutné zvážit výrobní a vývojové možnosti. Ekonomicky výhodnější a bez závislosti na dodavateli je varianta dodat si na zařízení vlastní senzory [1].

Systémů pro bezdrátovou nízkoenergetickou správu a sběr dat je na trhu mnoho, ať už se jedná přímo o proprietární brány (např. LoRa, SIGFOX) nebo o poskytnutí služeb třetích stran (RehiveTech). Všechny tyto brány využívají online cloud řešení, na které se přenáší data. Existují firmy, které nechtějí data přenášet na úložiště mimo společnost, i když se jedná o šifrovaná spojení. Firma Microrisc umožňuje ukládat data do svého IQRF cloudu i přímo do brány, kterou vyvinula a která sbírá data do interní flash paměti o velikosti 252kB pro příjem a 128kB pro odeslaná data. Celkově lze uložit do této brány 3308 záznamů pro přijatá data a 1680 pro odeslaná data. Po zaplnění paměti se data přepisují. V případě připojení více senzorů by se interní flash paměť rychle přepisovala a uživatel by nemohl získat dlouhodobější statistické údaje [2].

Diplomová práce se zabývá návrhem univerzálního sběrného bodu, který využívá nízkoenergetické přenosové technologie. Hlavní výhodou narozdíl od dostupných systémů je, že nepotřebuje být připojen do žádného vzdáleného cloudu. Veškeré informace jsou uloženy na SD kartě umístěné ve sběrném bodu. Díky variabilní velikosti SD karty se uživatel nemusí obávat, že bude ihned naplněna, a tím ztratí naměřená data. K zamezení ztráty dat je ve sběrném bodu naprogramován mechanismus stahovaní dat k uživateli. Ten si při pravidelném užívání stáhne veškerá data a může si vytvořit více záloh. Sběrný bod dále umožňuje vizualizaci dat a nastavení prahu zobrazených dat. V kritických místech dochází ke zbarvení grafu, a tak je uživatel upozorněn na problémy.

Tato práce je rozdělena do dvou částí:

- První část informuje o vlastnostech drátových i bezdrátových senzorových sítí, konceptu a hrozbách v IoT (Internet of Things) a o dostupnosti LPWAN (Low Power Wide Area Network) sítí v ČR (Česká republika).
- Druhá část se zabývá určením požadavků jednotlivých bloků systémů. Popisuje požadavky na spolehlivost systému. Popisuje konstrukci jednotlivých bloků systému, uvádí důvody pro výběr HW (Hardware), knihoven pro SW (Software) a následná opatření.

Kapitola 2

Senzorové sítě

V rámci rozvoje senzorových technologií došlo i k rozvoji druhé generace senzorů, která umožňuje využití nových materiálů pro senzory, zmenšení jejich rozměrů i váhy a také rozvoj technologií přenosu a zpracování senzorových dat při minimalizaci spotřeby. Tento rozvoj lze shrnout do pojmu multisenzorové systémy a senzorové sítě. Pro jejich další vývoj je nezbytné zvýšit požadavky na kvantitu a kvalitu monitorování fyzikálních veličin, zajistit bezpečnost a zlepšit predikci a rozvoj robotických systémů v odlišných funkcích i podobách [3].

Senzorové sítě, jako takové, umožňují vznik dalších kategorií decentralizovaných systémů, které jsou schopny v určitých funkcích nahradit člověka a to za předpokladu komunikace s nadřazenou úrovní automatického řízení, neboť jsou výrazně samostatněji propojeny s reálným světem než ostatní komunikační systémy [3].

WSN (Wireless Sensor Network) – bezdrátová senzorová síť je složena z velkého množství uzlů, které obsahují odlišné typy senzorů. Pracuje na základě spolupráce moderních technologií s bezdrátovou komunikací, za požadavku malé energetické spotřeby, velkého komunikačního dosahu a dostatečné přenosové rychlosti. V současnosti je výkon WSN obvykle značně omezen napájecími možnostmi a výpočetní kapacitou. Význam WSN se neustále zvyšuje, neboť ji lze navrhovat pro různé účely, např. shromažďování a zpracovávání různých typů dat informací a výskytu možných jevů v daném prostředí, na jejichž základě lze následně vytvořit zpětné akční působení podle navržených algoritmů [3, 4].

Realizaci senzorů pro sítě s miniaturními rozměry a vyšším počtem výkonnějších funkcí umožňují mikroelektronické technologie při využití nanoeletroniky a

nanotechnologií, zvyšující jejich integraci a výkon [3].

Senzory v sítích musí pracovat i za nepříznivých podmínek, např. při velkých teplotních rozdílech, při malé energetické spotřebě a dlouhodobě bez údržby. Dobu činnosti a množství zpracovávaných senzorových dat často omezuje spotřeba elektrické energie. Proto je nezbytné vyvíjet autonomní napájecí systémy – solární, elektrostatické, piezoelektrické, které by zajistily jejich energetickou nezávislost, a tím pádem jejich dlouhý nezávislý provoz. Autonomní napájení mikrosenzorových systémů a mikrosystémů patří do samostatné oblasti – Energy Harvesting, kde se uplatňují mikrosenzory MEMS (MicroElectroMechanical Systems), jejich technologie umožňují nabídku senzorů pro snímání fyzikálních i biochemických veličin [3].

Kapitola 3

Internet věcí

3.1 Úvod

Zjednodušeně se dá říci, že IoT (Internet of Things) je vše, co je připojeno k síti bez potřeby lidské manipulace. Toto propojení, převážně bezdrátové, má za cíl vytvořit moderní domácnosti (spotřebiče pro regulace tepla a vody), zabezpečení aut i komerčních objektů, má i nemalé místo v průmyslové sféře. Nejde ovšem jen o komunikaci a přenos vytvořených dat. Podstatné je efektivně zpracovat, skladovat a používat vyhodnocená data i pro jednotlivce.

IoT není homogenní prostředí, ale každé zařízení („věc“), které má své požadavky a rozdílné vlastnosti.

Existují zařízení, která musí být připojena k síti v reálném čase, mít dostupnost z vnějšku, obousměrnou komunikaci i přenášet větší množství dat k uživateli. Jsou i zařízení, která naopak nepotřebují obousměrnou komunikaci, ale stačí jim jen jednosměrná komunikace a možnost přenášet omezený počet bajtů informací o svém provozním stavu [4].

Další rozdílnost je ve spotřebě elektrické energie. Jsou „věci“, které musí být aktivní řadu let a mají v sobě jen baterii a není možné je neustále nabíjet či měnit.

Zařízení musí být i ekonomicky výhodné, ať už se jedná o větší datové tarify mobilních operátorů či menší M2M (Machine to Machine) tarify, kdy se náklady pohybují v desítkách korun za měsíc.

Z těchto důvodů není možné, aby IoT byl závislý na jedné přenosové technologii jako je mobilní síť , Wi-Fi (Wireless Fidelity), ZigBee atd.. Tyto technologie nejsou efektivní pro spotřebu a nehodí se do zařízení, které je potřeba napájet z baterie [5].

3.2 Využívané frekvenční pásmo v IoT

Z požadavku na malou spotřebu energie a co nejnižší režijní náklady vznikají nové přenosové technologie, které využívají bezlicenční pásmo ISM (Industrial, Scientific and Medical). V Evropě pro IoT je vyhrazené pásmo na 868MHz. I když toto pásmo nezahrnuje paušální poplatky, které se jinak platí za licencovaná pásma a musí být promítnuta v ceně služby či zařízení, má také svá omezení. ISM pásmo spadá pod regulaci správního orgánu, který spravuje radiofrekveční (RF) spektrum v dané zemi. V České republice se o regulace, nařízení, doporučení RF spektra stará ČTÚ (Český telekomunikační úřad). K provozování komunikace v tomto pásmu je nutné splnit následující podmínky [6]:

- část spektra 868,0 – 868,6 MHz umožňuje každému jednotlivému koncovému zařízení v síti komunikovat maximálně 1% v jakékoliv hodině, tedy maximálně 36 sekund. Maximální vysílací výkon je 25 mW.
- část spektra 868,7 – 869,2 MHz umožňuje každému jednotlivému koncovému zařízení v síti komunikovat maximálně 0,1% v jakékoliv hodině, tedy maximálně 3,6 sekund. Maximální vysílací výkon je 25 mW.
- část spektra 869,4 – 869,65 MHz umožňuje každému jednotlivému koncovému zařízení v síti komunikovat maximálně 10% v jakékoliv hodině, tedy maximálně 360 sekund. Maximální vysílací výkon je 500 mW. V průmyslových odvětvích není vždy zaručen přísun napájení. Senzor bude napájen z baterie. Je potřeba zajistit co nejdelší životnost.

Z těchto nařízení vyplývá, že zařízení nemohou komunikovat v reálném čase a je potřeba dbát na dobu vysílání.

3.3 Hlavní oblasti využití IoT

- Nové obchodní modely vytvářejí nové zdroje informací o firmách jako takových, tak i zpětnou vazbu od zákazníků. Firmám tak umožní rychlou a plošnou nabídku svých stávajících produktů (výrobků i služeb) a zároveň se obratem dozví požadavky zákazníků [7].

- Informace v reálném čase z kritických systémů Firmy získávají větší množství informací o své činnosti a podle získaných dat mohou reagovat potřebnou změnou na odchylku od normálu [7].

- Diverzifikace příjmů
  IoT umožní firmám zhodnotit dodatečné služby přidané k jejich produktům, získaná data a jejich propojenost umožní určení potřebných služeb a jejich doručovaní [7].

- Globální viditelnost
  Díky IoT získají firmy možnost dohlížet na svou činnost od začátků až po výsledný produkt i ve vzdálenějších místech [7].

- Efektivní a inteligentní fungování
  Informace od všech zákazníků umožní rychlou reakci v oblastech, které jsou nezbytné pro úspěch – úpravy cen, logistika nebo zavedení nových prvků pro zvýšení prodeje.

Výše uvedené možnosti jsou důsledkem efektivního využíváni internetů věcí. Řadu dalších eventualit nabízí výroba a používání produktů, které IoT vytváří. Například koncové zařízení, komunikační infrastruktura, zabezpečení a systémy pro ukládaní a zpracovávání dat [7].

IoT nemá však pouze pozitivní přínos, ale také představuje možnost řady ohrožení. V první řadě se jedná o hrozbu úniku dat. Jde například o nedostatečné zabezpečení online kamer, díky němuž může dojít ke zveřejnění přístupu k nim, a tím zcela narušit soukromí firem i jednotlivců. Nemalou hrozbu představuje problém s nedostačujícími hesly, šifrováním, přístupovými právy i špatným zabezpečením ovládací webové stránky. Nemalou hrozbou pro internet věcí je i možnost zahlcení

daty, které je závislé na možnosti kam a hlavně jak správně data uložit za pomoci odpovídajících softwarových řešení. V opačném případě IoT činí pouze další nákladovou položku bez přínosu [7].

Obranou proti hrozbám je nutnost zavedení striktních pravidel pro práci s daty, přístup k nim a jejich uložení např. závaznými normami (zákony). Je třeba provést pečlivý výběr a nasazení moderních SW nástrojů, které umožňují mazání, zpracovávání a využívání dat tak, aby mohla být používána ve stávajících systémech firem. Nedílnou součástí obrany je také nutnost přizpůsobení náboru nových zaměstnanců i vzdělávaní stávajících. Při všech možnostech na ochranu dat a jejich správným použitím poskytuje internet věcí velkou příležitost pro růst byznysu [7].

3.4 Zabezpečení IoT

Šifrování a zabezpečení přenosu dat je nedílnou součástí každého dnešního systému. Význam šifrovaní byl znám už před vynálezem jakékoliv elektroniky. Již v 7. st. př. n. l. Řekové používali Skytale, což byla hůl daného poloměru a pruh papíru, která realizovala transpoziční šifru. Používala se především ve válkách. César při svých válečných taženích používal šifrování, kde posunoval písmena o tři místa. V těchto dobách, kdy většina obyvatel neuměla číst ani psát byly tyto techniky dostatečné. V dnešním 21. století, kdy jsme schopni jedním kliknutím vygenerovat miliony kombinací, jsou tyto metody nevyhovující. Díky pokročilé technice přenosu dat je proto nutno vymyslet i důmyslné zabezpečovací praktiky, tzv. moderní šifry. Je třeba dodat, že v dnešních systémech se neřeší jen šifrovaní, ale je nezbytné zajistit, aby data nebyla ztracena nebo změněna. V kryptografii se tomuto pojmu říká integrita.

3.5 Moderní šifry

Moderní šifry dělíme na symetrické a asymetrické.

3.5.1 Symetrické moderní šifry

Symetrická šifra je kryptografický algoritmus, při kterém se k šifrování a dešifrování používá stejný klíč nebo ho lze na straně adresáta jednoduše odvodit.

Tyto symetrické šifry dělíme do dvou tříd. První třída jsou proudové šifry a druhá třída jsou blokové šifry [8].

3.5.1.1 Proudové šifry

Proudové šifry se vyznačují tím, že šifrují data po jednotlivých bitech.

$$c_i = E(z_i, K) \tag{3.1}$$

kde:
c_i je i-tý bit kryptogramu
z_i je i-tý bit zprávy
K je klíč

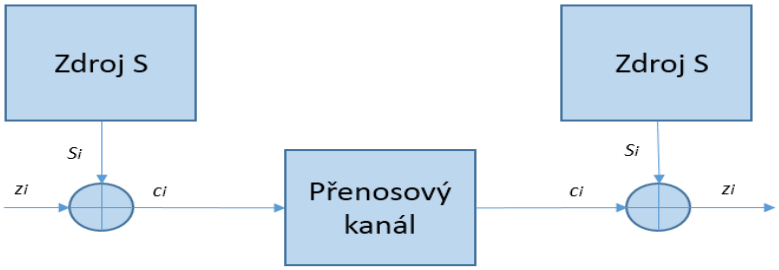
Výhoda proudových šifer spočívá v jednodušší implementaci s vyšší šifrovací a dešifrovací rychlostí. Nevýhodou je nižší odolnost vůči útokům. K šifrovaní a dešifrování se používá šifrovací tok dat, který musí být na obou stranách shodný. Tento tok se generuje deterministickým způsobem, nebo může být čten z jiného zdroje. Šifrování probíhá podle následujícího vztahu: [8]

$$c_i = z_i \oplus s_i \tag{3.2}$$

kde:
c_i je i-tý bit kryptogramu
z_i je i-tý bit zprávy
s_i je i-tý bit šifrovací posloupnosti

a dešifrování podle následujícího:

$$z_i = c_i \oplus s_i \tag{3.3}$$

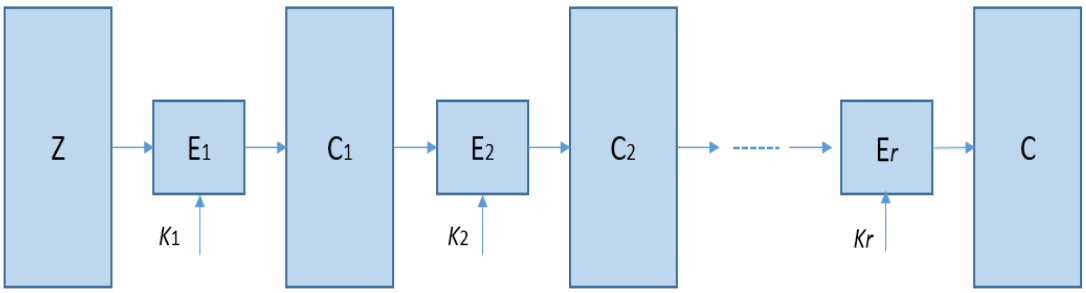


Obr. 3-1: Proudová šifra [8]

3.5.1.2 Blokové šifry

Na rozdíl od proudových šifer blokové šifry šifrují po blocích s pevně danou délkou bitů. Principem blokových šifer je, že každý výstupní bit je závislý na všech bitech vstupu (difuze) a také na všech bitech klíče (konfuze). To značně komplikuje útočníkovi kryptoanalýzu [8].

Dnešní moderní šifry se konstruují z kaskády šifer. Kaskáda šifer znamená spojení více šifer (zpravidla stejných), kdy výstup z jedné šifry je vstup do další. Poslední šifra je výsledný kryptogram. Používá se varianta stejných šifer (iterační šifra), kde se na základě šifrovacího klíče odvodí dílčí klíče pro transformace, která se zpravidla používá jako jednoduchá šifra, která je přetransformována kombinací blokových operací (substituce, rotace a aritmetické operace). Po jedné iteraci se výsledek přivádí na vstup dalšího bloku, než dojde na poslední blok. Dešifrování se provádí stejně jako u šifrování, jen se provádí inverzní transformace [8].



Obr. 3-2: Princip blokové kaskádní šifry [8]

3.5.2 Asymetrické šifry

Asymetrické šifry používají k šifrování a dešifrování zcela odlišné klíče. Nejpoužívanější metoda pro asymetrické šifry je využívání veřejného klíče, kterým uživatel šifruje. K dešifrování používá soukromý klíč. Tím je zaručeno, že zprávu může číst pouze jen majitel soukromého klíče. Tak se eliminují složité výměny klíčů, ale toto šifrování je pomalé. Proto se v dnešní době využívá kooperace symetrických a asymetrických šifer [8].

Principem asymetrických šifer je zatím neřešitelný matematický problém. V dnešních systémech se používá faktorizace čísel (RSA), nebo problém diskrétního logaritmu (Diffie – Hellmanův protokol) atd. [8].

3.6 Integrita dat

V dnešních sdílených přenosových kanálech není potřeba jen šifrovat. Příjemce musí také vědět, že dostal všechna data od odesílatele anebo, že data někdo během přenosu nezměnil. K tomuto opatření se nejvíce používají především jednosměrné funkce.

Jednosměrná funkce je taková funkce, pro kterou lze snadno vypočítat výstup, ale je obtížné z výstupu dostat vstup. Jednosměrné funkce mohou mít pevnou délku výstupu nebo volitelnou délku výstupu.

Jednosměrné funkce s pevnou délkou výstupu vytvoří výstup s určitou délkou, který reprezentuje daný vstup. Tato funkce se nazývá hašovací funkce. Umožňuje libovolně dlouhému vstupu přiřadit konkrétní reprezentační výstup. Uživatel tedy dostane data s tímto výstupem a zkontroluje si, zda spočítaná funkce se rovná výsledku. Pokud se rovnají, prošla data komunikačním kanálem bez chyby. V opačném případě by přenos musel proběhnout opakovaně [8].

Kapitola 4

Přenosové technologie LPWAN sítí

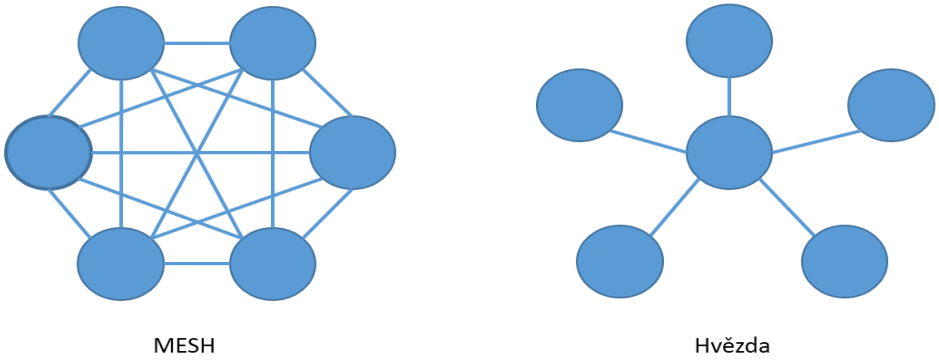
Cílem této části je zhodnotit přenosové LPWAN (Low Power Wide Area Network) sítě z pohledu spotřeby, bezpečnosti a možností režimu topologie sítě a nezávislosti připojení systému.

Systém je napájený z baterie a je nutné, aby přenosová technologie byla energeticky efektivní a měla dlouhou životnost. Není možné, aby uživatel musel často nabíjet nebo měnit baterie. Takový systém by nebyl na trhu žádaný.

Důležitým aspektem LPWAN sítě je bezpečnost. V případě prolomení přenosové technologie vzniká nebezpečí, ať už se jedná o sběr dat, kdy útočník může zjistit, že v domě klesla spotřeba elektřiny, či klesla teplota a například naplánovat loupež, nebo získat možnost ovládání části domu.

Nezávislost připojení systému a topologie je závislá na odpovídajícím návrhu systému. Nezávislost připojení systému znamená možnost uživatele postavit si vlastní soukromou síť bez poskytovatele a neplatit tak paušál za připojená zařízení. Musí jen dodržovat nařízení ČTÚ. Topologie je důležitá, aby síť mohla pracovat v plném rozsahu. Všechny uzly musí mít dostatečnou sílu signálu, aby všechny informace byly přeneseny bez chyby, nebo nedošlo k rozpadu spojení mezi uzly. V sítích LPWAN se nejčastěji využívá hvězda a MESH síť (Obr. 4-1.) Hvězda využívá více transceiverů, které vysílají k jednomu sběrnému bodu. Hlavním negativem této topologie je, že transceiver musí mít dosah na sběrný bod. Pokud ho nemají, je nutné do sítě dodat opakovače, které zvyšují cenu sítě. Na rozdíl od toho MESH síť používá transceivery i jako opakovače v síti, které znají mapu sítě a předávají si zprávy ke koncentrátoru. Na rozdíl od hvězdy zaručuje plnou dostupnost sítě, pokud je alespoň vidět vždy jeden

transceiver. Nevýhodou této sítě je zvýšení odezvy přenosu zpráv ke koncentrátoru. S každým hopem (skokem) se prodlužuje čas přenosu zprávy, protože transceivery neslouží jen k jejich přeposlání, ale musí zpracovat i ostatní funkce, ke kterým je určen. Také se zvyšuje výpočetní náročnost na směrovaní v síti, protože každý transceiver musí znát mapu sítě.



Obr. 4-1: Topologie MESH a Hvězda

4.1 Porovnání LPWAN sítí dostupných v ČR

V současnosti v ČR jsou dostupné čtyři technologie LPWAN Sigfox, LoRa (Long Range), IQRF,Wireless M-BUS (Meter BUS) a plánuje se NB (Narrow Band)-LTE (Long Term Evolution).

Pro správné fungování sítě je potřeba vybudovat kvalitní síť s dostatečným pokrytím. Kroky různých firem pro budování sítí se liší. Žádná ze společností, které produkují LPWAN nemá ambice, ani prostředky pro budování služeb a projektů pro koncové zákazníky od začátku do konce. Každá společnost má jinou strategii a plán tvorby sítě, jiné partnery pro výstavbu a různé topologie sítí.

4.2 Sigfox

Firma Sigfox se vydala směrem budování sítí po celém světě za spolupráce s velkými operátory. Jedinou výjimkou je její domovská země Francie, kde si celoplošnou síť postavila a provozuje sama.V České republice firma Sigfox spolupracuje na testovacím provozu a následně i na výstavbě sítě s T-Mobile, který je v současné

době největším mobilním operátorem u nás. Spolupráce firmy Sigfox a českého T-Mobile vznikla v roce 2015 a byla pro obě firmy velice výhodným krokem. Praha se stala jednou z prvních 12-ti evropských metropolí, kde byl pilotní projekt zprovozněn. Testovací provoz byl spuštěn na několika vysílačích po dobu 3 měsíců a v případě kladných výsledků měření se technologie začne využívat v dalších zemích, kde působí Deutche Telekom a jeho dceřiné společnosti V současné době technologie Sigfox pokrývá více než 80% území ČR [5, 9].

4.3 LoRa

Technologie LoRa má podobnou strategii jako Sigfox. Zatímco Sigfox se po celém světě specializuje pouze na mobilní operátory, LoRa tento požadavek nemá. Spolupracuje s každým, kdo má vybudované stožáry tak, že splňují pokrytí pro pásmo 868MHz. Mobilní operátoři mají velmi často tuto síť nadbytečně hustou, protože pracují na jiných frekvencích a také mají z hlediska kapacity zákazníků několikanásobně vyšší datové provozy. Dalším důležitým požadavkem, který má technologie LoRa na výběr partnera pro budování sítě je již vytvořený komunikační tunel mezi jednotlivými vysílači a datovými centry se zabezpečením jak proti fyzickému vniknutí osob, tak zabezpečením z hlediska kybernetické bezpečnosti.V České republice si aliance LoRa vybrala za partnera České Radiokomunikace. České Radiokomunikace disponují dostupnou technologií a správným umístěním stožárů po vypnuté analogové televizi, která byla provozována na blízké frekvenci technologie LoRa. Na modifikaci celé infrastruktury nebylo proto potřeba vynaložit tolik finančních prostředků [10].

4.4 IQRF

Technologie IQRF je zcela odlišná od dvou předchozích. IQRF využívá nejčastěji topologii sítí typu MESH. Může být ale i v režimu Hvězda. Topologie MESH má největší výhody v dosahu pokrytí. Tato topologie nemá striktně dané uspořádání zařízení v síti. Dojde-li k tomu, že adresát koncový bod (nod) je mimo dosah hlavní bodu (koordinátora), paket je tomuto koncovému bodu doručen pomocí sousedních bodů. Jeden aktivní systém může obsahovat pouze jednoho koordinátora a až 240 Nodů. Síť se může dále řetězit, takže může mít neomezené množství zařízení. Síť pracuje tak, že koordinátor řídí nody, které sbírají informace ve své síti, komunikují mezi sebou a posílají informace koordinátorovi. Koordinátor zpracovává informace ze své sítě a odesílá je ven do světa. Tato síť díky přenosům informací od sousedních bodů má velmi redundantní přenos dat v síti a tedy je velmi spolehlivá. Nedosahuje

ale tak velkých přenosových vzdáleností, jako u předchozích technologií. Mezi jednotlivými body může být v otevřeném prostoru vzdálenost až 500 m. Při tomto rozmístění se ale ztrácí výhoda redundance dat sítě typu MESH. Technologie IQRF se využívá na takové aplikace, které obsahují mnoho senzorů na jednom místě nebo na místech, kde je problém se šířením radiofrekvenčního signálu, jako jsou různé šachty a podobně. Při problému s pokrytím lze do sítě zařadit i nadbytečné členy, které nejsou osazeny žádnými technologiemi, ale budou pouze předávat zprávy vzdálenějšímu nodu [11, 12].

4.5 Wireless M-BUS

Technologie Wireless M-BUS vznikla v roce 2007 rozšířením průmyslové datové sběrnice M-BUS. Jedná se o specializovanou drátovou síť, která je určena především pro oblast měření spotřeby a MaR (Měření a Regulace). Starší varianta M-BUS sloužila hlavně v průmyslových podnicích, kde byla jednotlivá zařízení (např. podružné vodoměry či elektroměry) propojena drátovou datovou sběrnicí. V dnešním moderním a uspěchaném světě je třeba instalace provádět rychle a hlavně bez stavebních úprav. Proto je kladen důraz na vývoj bezdrátové varianty zařízení pro vzdálené měření a dálkové odečty [13].

Komunikace v technologii Wireless M-BUS má hvězdicovou strukturu. Síť je tvořena několika měřícími jednotkami a jedním koncentrátorem. Komunikaci vždy zahajuje měřící jednotka, tím se minimalizuje spotřeba. Měřící jednotky snímají data a následně je odesílají do koncentrátoru. Ten shromažďuje a zpracovává data od měřících jednotek, následně je odesílá na předem určené místo. Komunikace mezi koncentrátorem a měřícími jednotkami probíhá na 12-ti kanálech v bezlicenčním pásmu ISM okolo frekvence 868MHz. Zařízení má více režimů rádiového přenosu. Ty jsou označovány S, T a R a reprezentují rozdílné přenosové rychlosti. Pro různé aplikace se hodí i různé rychlosti přenosu informace. Existují aplikace, při kterých je vyžadován pouze jednosměrný tok (označení 1) informací i aplikace vyžadující obousměrný [13].

Přenosová rychlost [kb/s]	Označení jednosměrné komunikace	Označení obousměrné komunikace
4,8	není	R2
32,768	S1/S1m	S2
100	T1	T2

Tab. 4.1: Tabulka režimů komunikace Wireless M-BUS [13]

4.6 NB-LTE

V současné době se v ČR plánuje nástup další technologie, na které pracuje O2 společně s Nokií a Huaweiem. Jedná se o technologii NB (Narrow Band)-LTE (Long Term Evolution), kde se využije současné pokrytí v LTE pásmu a provede se pouze softwarová úprava na základnových stanicích a v systémech provozovatelů sítě. Nemusí se tedy přidávat žádná další technologie, ani soutěžit o nová pásma. Softwarová úprava na základnových stanicích provede takovou změnu, že vyčlení část spektra pro LPWAN síť. Tato vyhrazená část spektra se musí umístit doprostřed pásma LTE, protože by jinak rušila sousední kmitočty cizích operátorů. Vyhrazené pásmo má vyšší úroveň signálu než klasické LTE [14].

4.7 Shrnutí vlastností LPWAN sítí

V tabulce 4.1 jsou shrnuty vlastnosti jednotlivých technologií, které je potřeba zajistit při návrhu zadaného systému.

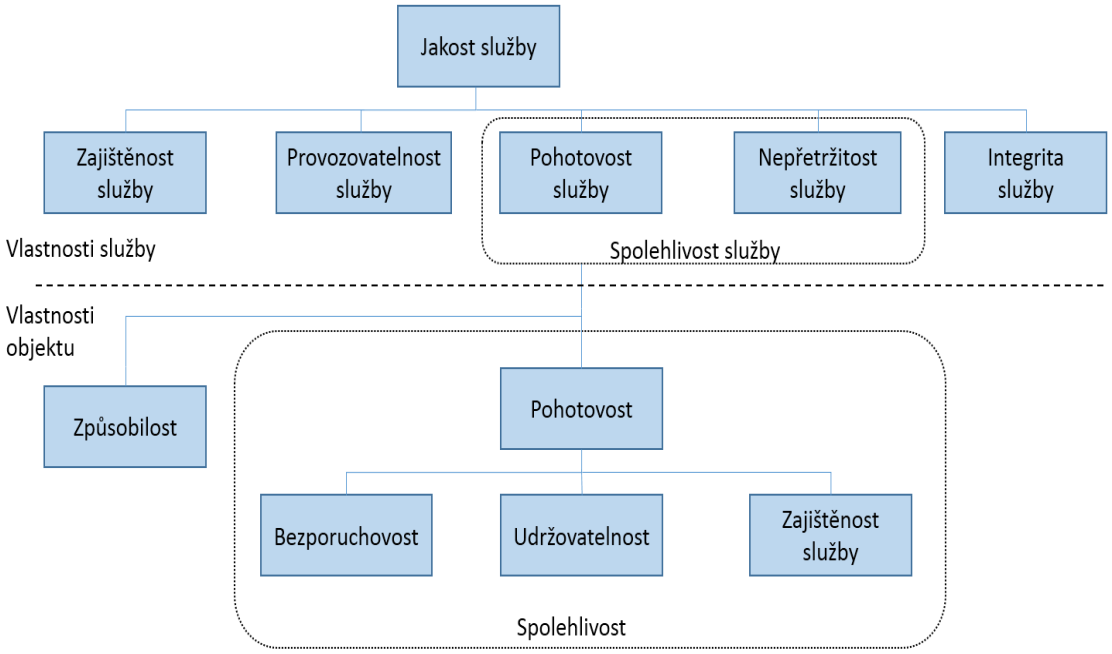
	IQRF	M-BUS	SIGFOX	LORA
Spotřeba	Tx = 8-22 mA Spánek = 1.7uA	Tx=37mA Spánek=0.1uA	Tx=5-45mA Spánek=1-2 uA	Tx = 40mA Spánek=1-2uA
Bezpečnost	AES128	AES128	certifikát,hash, šifr. apl. úrovně	AES128
Topologie	Hvězda,MESH	Hvězda	Hvězda	Hvězda
Nezávislost systému	Ano	Ano	Ne	Ano/Ne

Tab. 4.2: Vlastnosti LPWAN sítí [13,15,16,17]

Kapitola 5

Spolehlivost služby

Spolehlivost služby je vlastnost systému (výrobku), který plní definované funkce ve stanovené době při jasně daných provozních parametrech. Je dána normou ČSN (Československá norma) IEC (International Electrotechnical Commission) 50 (191) a skládá se z několika vzájemně ovlivňujících bloků. Viz Obr. 5-1.



Obr. 5-1: Jakost služby [18]

Podle uvedené normy jsou bloky definované [18]:

- Spolehlivost služby
  Znamená poskytnout stanovenou službu v definovaných mezích v požadované době.
  Člení se na:
  - Pohotovost služby - Poskytnutí služby v definovaných mezích po vyžádaní uživatelem. Závisí na zařízení, kterým je služba poskytována.
  - Nepřetržitost služby – Poskytnutí služby v definovaných mezích v požadované době.

- Integrita služby
  Získaná služba musí pracovat s definovanými vlastnostmi bez zhoršení kvality.

Hlavním činitelem spolehlivosti služby jsou vlastnosti objektů, díky kterým se služba poskytuje a nezáleží o jakou část se jedná. Do spolehlivosti služby může být zahrnut i lidský faktor. Vlastnosti objektů nejvíce ovlivňují způsobilost a spolehlivost [19, 20].

- Způsobilost
  Plnění požadavků s definovanými kvantitativními charakteristikami v jasně daných vnitřních podmínkách.

- Spolehlivost
  Slouží pro popis pohotovostí a činitelů. Patří sem bezporuchovost, udržovatelnost a zajištění služby.

- Pohotovost
  Stav objektu, kdy musí být schopen plnit své funkce v definovaných podmínkách v daném čase.

- Udržovatelnost
  Setrvat v požadovaném stavu nebo se vrátit do požadovaného stavu po provedení údržby.

- Zajištěnost údržby
  Zajištění požadované údržby podle definovaných podmínek podle koncepce údržby.

5.1 Zálohování systému

Největšího zvýšení spolehlivosti dosáhneme dostatečným zálohováním prvků systému. Zálohování je paralelní uspořádaní prvků a dělíme jí na:

- Stálou
  Záloha pracuje ve stejným režimu jako primární prvek.

- Substituční
  Využívá se až po výpadku primárního prvku. Tato záloha se dále dělí na :
  - Nezatíženou (studená záloha) - není vůbec zapojena v soustavě.
  - Odlehčenou (horká záloha) - pracuje v odlehčeném pracovním režimu.

5.2 Pohotovost

Je nutné počítat s možností selhání některého prvku soustavy, kdy následně nemůže plnit svou funkci. V případě vyhodnocení vlivu poruchovosti na pohotovost služby je třeba znát stacionární hodnotu pohotovostního objektu. Ta znamená pravděpodobnost, kdy je objekt v režimu, kdy může pracovat – součinitel pohotovosti – R, nebo kdy nemůže pracovat, je v poruše – součinitel nepohotovosti Q.
Tyto pravděpodobnosti se dají vyjádřit vztahem [19, 20]:

$$R = \frac{\mu}{\lambda + \mu} \tag{5.1}$$

$$Q = \frac{\lambda}{\lambda + \mu} \tag{5.2}$$

kde:
λ intenzita poruch(1/hod), určuje bezporuchovost.
μ intenzita obnovení provozuschopnosti(1/hod), určuje udržovatelnost.

Soustavy či systémy se obvykle skládají z více prvků. Tyto prvky mohou být složeny sériově nebo paralelně. Sériové řazení způsobí to, že v případě selhání jednoho prvku ze systému selže celý systém.

Pro výslednou hodnotu součinitele pohotovosti plyne [19, 20]:

$$R = \prod_{i=1}^{n} R_i = \prod_{i=1}^{n} (1 - Q_i) \tag{5.3}$$

Součinitel nepohotovosti se v tomto případě rovná:

$$Q = 1 - \prod_{i=1}^{n} R_i = 1 - \prod_{i=1}^{n} (1 - Q_i) \tag{5.4}$$

Druhým způsobem, jak řadit prvky systému je paralelní. Systém přestane pracovat jen v případě výpadku všech prvků v systému. Pro výslednou hodnotu součinitele pohotovosti plyne [19, 20]:

$$R = 1 - \prod_{i=1}^{n} Q_i = 1 - \prod_{i=1}^{n} (1 - R_i) \tag{5.5}$$

a pro součinitel nepohotovosti:

$$Q = \prod_{i=1}^{n} Q_i = \prod_{i=1}^{n} (1 - R_i) \tag{5.6}$$

Pro zvýšení součinitele pohotovosti poruch se systémy navrhují se zálohami. Poté se tyto vztahy změní na : [19, 20]

$$Rs = 1 - \frac{(L+M)!}{(M+1)!(L-1)!} Q^{M+1} \tag{5.7}$$

pro zatížené zálohy.

A pro odlehčené zálohy [19, 20]:

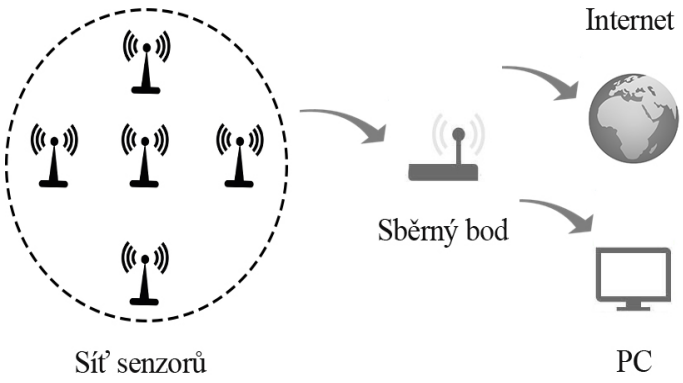
$$Rs = 1 - \frac{(LQ)^{M+1}}{(M+1)!}; Qs = 1 - Rs \tag{5.8}$$

kde:
L je primární prvek.
M je záložní prvek.

Kapitola 6

Stanovení požadavků systému

Cílem této diplomové práce je navrhnout systém, který bude přijímat data z navržené bezpečné senzorové sítě do sběrného bodu, která je schopna výsledky nejen zobrazit, ale také uložit hodnoty a vytvořit z nich vhodný výstup. Systém se rozděluje do tří vrstev, kde každá vrstva má své požadavky, které musí být splněny.



Obr. 6-1: Schématické znázornění senzorové sítě

Požadavky na senzorovou síť:

- Přípojení senzorů do transceiverů
  Výběr digitálních senzorů, které podporují běžné sběrnice transceiverů (SPI - Serial Peripheral Interface, UART-Universal asynchronous receiver/ transmitter, I2C-Inter-Integrated Circuit)
  Analogové senzory nemají žádná omezení.

- Přesnost / odchylka
  Senzor, který splňuje přesnost a odchylku měření za přijatelnou cenu.

- Malá spotřeba
  V průmyslových odvětvích není vždy zaručen přísun napájení. Senzor bude napájen z baterie. Je potřeba zajistit co nejdelší životnost.

Požadavky na přenosové médium:

- Odolnost vůči rušení
- Nezávislost topologie sítě
  Každá topologie je vhodná pro jiné účely a je potřeba, aby daná technologie měla více možnosti propojení.
- Dostačující šifrování

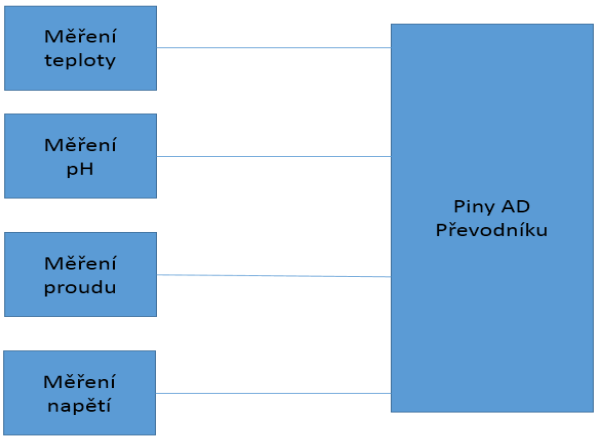
Požadavky na sběrný bod:

- Propojení s transceiverem
  Sběrný bod musí komunikovat pomocí sériových sběrnic (UART, SPI), které jsou běžně využívány v transceiverech. Jednotka musí podporovat komunikaci po Ethernetu z důvodu propojení do lokální sítě.
- Souborový systém
  Je nutné, aby software uměl číst a zapisovat na vyměnitelné médium, a tak umožnil měnit konfigurační soubor a ukládat naměřená data.
- Víceúlohové prostředí
  Programové vybavení by mělo podporovat nezávislé procesy, které jsou řízeny plánovačem úloh.
- Hodiny reálného času
  Hodiny by se měly synchronizovat pomocí externího zdroje nezávisle na programu.
- Grafický displej
  Na grafickém displeji by se měla zobrazovat konfigurace sběrného bodu (IP[Internet Protocol] adresa, nastavení hodin reálného času) a hodnoty senzorů v reálném čase.

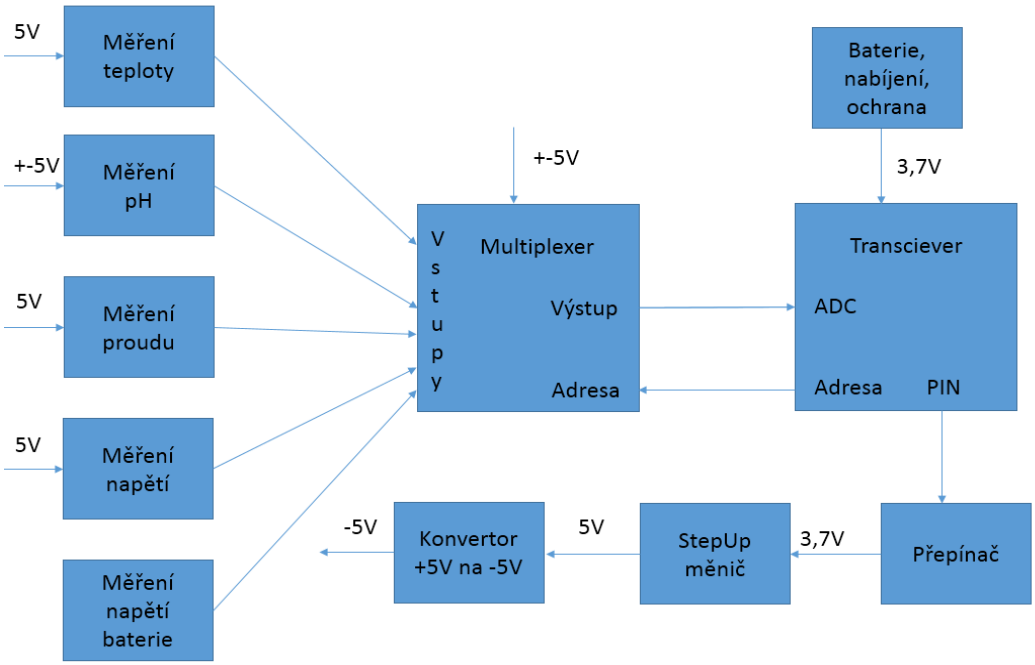
Kapitola 7

Navržený senzorový přípravek

K otestování systému sběrného bodu jsou navrženy dva senzorové přípravky. Jeden lze napojit drátovým připojením na piny AD (analogově/digitálního) převodníku ve sběrném bodě, druhý je připojen na transceiver (Node), který následně pošle hodnoty do transceiveru (Koordinátor) spojeného se sběrným bodem přes rozhraní UART. Blokové schéma přípravků na Obr. 7-1. a Obr. 7-2.



Obr. 7-1: Drátové připojení do sběrného bodu



Obr. 7-2: Bezdrátové připojení do sběrného bodu

7.1 Přípravek s drátovým připojením na sběrný bod

Přípravek obsahuje snímače na měření teploty, pH roztoků, stejnosměrného elektrického napětí do 15V a elektrického proudu do 30A. V případě, kdy sběrný bod je napájen ze sítě, není potřeba žádná režie ohledně napájení. Senzory jsou neustále zapnuté a měří. Ve sběrném bodu si lze navolit kanál AD převodníku, ze kterého se vyčítají data.

7.1.1 Měření teploty

Pro měření teploty je vybrán senzor od firmy Analog Devices TMP36GT9Z. Tento senzor má široké pracovní napětí od 2.7 – 5,5 V se spotřebou 50 uA. Snímač je z výroby kalibrován na °C.

7.1.2 Měření pH

Pro měření pH vodných roztoků se využívá metody potenciometrie. Tato metoda měří rovnovážné napětí článku, který obsahuje měrnou a referentní elektrodu. Pro přesné měření se používá skleněná elektroda jako měrný člen. Při měření musí

referentní elektrodě zůstat elektrický potenciál konstantní i při změně prostředí [21]. Postup pro měření pH se řídí doporučeným schématem [21]. Skládá se ze tří fází:

- 1. Fáze - Přizpůsobení vstupní impedance, zesílení
  Měřící elektrody pro pH jsou měkkým zdrojem pro měřící obvod a je nutné, aby vstupní impedance byla co největší. Používá zapojení s operačním zesilovačem, který má vysokou vstupní impedanci. Symetrické napájení je vytvořeno obvodem konvertorem ICL7660 z dodaných 5V.
- 2.Fáze - Filtrace a zesílení pro AD převodník. Senzor, který splňuje přesnost a odchylku měření za přijatelnou cenu.
- 3. Fáze – Ochrana AD převodníku.

7.1.3 Měření stejnosměrného elektrického napětí do 15V

AD převodníky mikroprocesorů nejsou schopny měřit tato napětí přímo. Obvykle se jedná o 10bitové nebo 12bitové převodníky s maximálním napětím 3,3V nebo 5V. Proto je nutné předřadit vysokoimpedanční dělič, aby zbytečně neprocházel proud obvodem a v AD převodníku bylo maximální povolené napětí. Z důvodu ochrany AD převodníku kvůli maximálním hodnotám je zařazena do obvodu Zenerova dioda.

7.1.4 Měření elektrického proudu do 30A

Pro měření vysokých proudů se využívají magnetoelektrické systémy většinou s Hallovou sondou, kde průchodem elektrického proudu se generuje elektrické napětí na základě působícího elektromagnetického pole. Firma Allegro Microsystems dodává senzor ACS712 ve variantách 5A, 20A, 30A jak pro stejnosměrný, tak pro střídavý proud. Tento obvod obsahuje galvanické oddělení, takže je možné na jeho vstup připojit měřený proud bez omezení. Výstupní svorky je možno připojit přímo na AD převodník.

7.2 Přípravek s bezdrátovým připojením na sběrný bod

V případě, že není možné kabelové připojení senzorů ke sběrnému bodu (např. v místě není elektrická síť), je navrhnut přípravek s bezdrátovým přenosem pomocí

IQRF (více v kapitole 9). Přípravek používá stejné senzory, ale řízení je odlišné. Přípravek je napájen z baterie, tudíž není možné, aby se měřilo neustále. Pokud transceiver dostane ze sběrného bodu zprávu, že má měřit, přepne spínač a do step-up měniče připojí napájení z baterie. Tím dodá obvodu potřebných 5V. Transceiver nemá dostatečný počet kanálů pro měření všech veličin. Z těchto důvodu je přidán do přípravku multiplexer s nízkou spotřebou. Na multiplexer jsou připojeny adresové vodiče z transceiveru, které si řídí z jakého senzoru zpracují data. Přípravek také obsahuje kontrolu stavu nabití baterie, který posílá do sběrného bodu. Pokud si uživatel nevšimne nízkého stavu baterie, může dojít k jejímu nenávratnému poškození. Z těchto preventivních důvodů je do obvodu dodána ochrana, která ji odpojí při výrazném poklesu napětí.

Kapitola 8

Vybraná přenosová technologie

Do navrženého systému je zvolena technologie IQRF, protože systém bude mít hlavní využití ve výrobních halách a továrnách, kde jsou velké problémy se šířením rádiového signálu skrz kovové konstrukce. I když má technologie menší vysílací výkon může využít výhody své IQMESH sítě a přes ostatní transceivery přenést informaci ke koncentrátoru. Dalším porovnávaným aspektem je uzavřenost. IQRF a M-BUS není potřeba zavádět do cizí sítě (nemusí být dostupná v dané lokalitě) a shromažďovat data na jiném cloudu. Není tedy potřeba platit paušální poplatky za připojený senzor. Technologie LoRa umožňuje vybudovat si svoji privátní síť, ale je potřeba pořídit speciální koncentrátor, který stojí 10x více než transceiver IQRF a navíc takto postavená síť by fungovala v topologii hvězda a mohl by nastat problém se spolehlivostí sítě. Sigfox tuto možnost nepodporuje.

8.1 Aplikace v IQRF modulech

Všechny IQRF moduly nejsou naprogramovány za použití stejného programu. Každý samostatně (nebo i více v případě řetězení sítě) musí plnit funkci koordinátora, který bude řídit MESH síť. Ostatní moduly jsou naprogramovány ve funkci nodu. V testovací síti se předpokládá viditelnost všech nodů navzájem, není tedy potřeba dodávat do sítě opakovače. Další předpoklad je, že IQRF moduly jsou nabondovány (zpárovány). V této verzi sběrného bodu není možné spravovat síť přes webové rozhraní.

8.2 Programové vybavení koordinátora

Koordinátor komunikuje se sběrným bodem prostřednictvím sériové linky. Vykonává příkazy od sběrného bodu, který zpracovává data ze vzdálených senzorů. Koordinátor přijme rovnou připravená data pro přenos komunikačním kanálem. Po odeslání dat čeká na odpověď. Po příjmu odpovědi ji pouze přepošle do sběrného bodu, který vše zpracuje.

8.3 Programové vybavení nodu

V testovacím senzorickém přípravku je nutné měřit více veličin než je možné připojit přímo do IQRF modulu. Po přijmutí paketu musí node zjistit identifikaci měřeného senzoru. Jakmile toto zjistí, musí zapnout napájení z baterie do obvodu. Napájení z baterie se dostane do step-up měniče. Ten zajistí napájecí napětí pro senzory. Následně node může zadat adresu vyžádaného senzoru na multiplexor, který ho propojí. Modul změří hodnotu na AD převodníku a tuto hodnotu bez jakýkoli úprav přepošle. Je bezpodmínečně nutné co nejvíce šetřit baterii a minimalizovat počet operací, které není nutné provádět na nodech a poslat je ke zpracování na sběrný bod. K informaci ze senzoru se ještě přidá hodnota změřeného napětí z baterie, aby uživatel věděl, zda má node nabít. Veškerá bezdrátová komunikace je šifrována pomocí AES128 v režimu CBC (Cipher Block Chaining).

Kapitola 9

Sběrný bod

V této části je popsán výběr hardwaru pro sběrný bod. Požadavky na sběrný bod jsou definovány výše. Kromě vhodného hardwaru je také třeba vybrat vhodné open-source nástroje pro kompilaci, ladění a nahrávání softwaru do sběrného bodu. V rámci požadavku na HTTP (Hypertext Transfer Protocol) server je nutné vybrat zařízení s dostatečnou velikostí interní flash paměti. Je potřeba ukládat větší množství dat jako HTML (HyperText Markup Language) nebo js (javascript) soubory, které se mohou pohybovat v řádu stovek KB. Z pohledu funkčního a bezpečnostního aspektu není doporučeno ukládat webové stránky na vyměnitelné médium. Pokud by došlo ke ztrátě či poškození, funkčnost systému by byla ztracena či velice omezena.

Vývojář může jít cestou výběru s použitím proprietárních architektur (Industry Standard Architecture), které jsou optimální pro daný typ aplikace. Zásadní nevýhodou je však závislost na výrobci, který může vývoj ukončit a produkt se tak ocitne bez podpory a možnosti získaní náhradních součástek pro vestavěný systém. Také se může stát, že konkurence začne nabízet lepší produkt, jehož využití je při zvýšení nákladů neefektivní.

Pro vývoj vestavěných systémů je proto nejvhodnější vybírat mikrokontroléry s architekturou ARM (Advanced RISC [Reduced Instruction Set Computing] Machine). Společnost ARM přímo nevyrábí mikrokontroléry, pouze dodává know-how ostatním výrobcům. Vývojář může přecházet mezi výrobci bez zásadní změny vývojového prostředí či absolvování kurzů. Jádro zůstává u všech výrobců stejné, ale liší se pouze implementací jednotlivých periférii, pamětí atd. Stejná zůstává i instrukční sada.

Je potřeba si dobře rozmyslet, kterou cestou se vývojář vydá. Pokud podcení parametry, systém nebude mít dostatečný výkon a neprorazí na trh. Jakmile však parametry přecení bude mít sice systém se skvělými parametry, ale cenově pro koncové uživatele nedostupný.

9.1 Vybraný mikrokontrolér

Mikrokontroléry s těmito požadavky vyrábí většina firem zabývající se touto problematikou. Pro sběrný bod byl vybrán kit 32F746GDiscovery od firmy STM. Výběr byl ovlivněn předchozí zkušeností s těmito mikrokontroléry a kity. Kit 32F746GDiscovery obsahuje procesor STM32F746NG, který obsahuje jádro CORTEX M7. Tento kit má široké uplatnění v aplikacích audia, senzorových sítí, grafiky aj. Hlavní vlastnosti [22]:

- Interní FLASH paměť 1MB
- Interní RAM (Random Access Memory) 340KB
- Obsahuje ST-LINK pro nahrávání a ladění programu přímo na kitu a není nutné připojovat externí JTAG/SWD (Joint Test Action Group/Serial Wire Debug) programátor.
- 4.3-Palcový 480x272 barevný LCD-TFT (Liquid Crystal Display - Thin-Film Transistors) s kapacitním dotykovým displejem
- Konektor pro microSD kartu
- Ethernet konektor v souladu IEEE-802.3-2002
- Hodiny reálného času (RTC)
- Vyvedené komunikační sběrnice SPI, UART

9.2 Výběr Open source nástrojů

Vývojové nástroje musí zvládnout kompletní řetězec operací nutný pro vývoj softwaru (tvorba zdrojového kódu, přeložení, linkovaní, nahrání do zařízení a ladění programů). Vývojové nástroje lze rozdělit do tří druhů:

- Komerční
  Plně placená vývojová sada, kde hlavně uživatel platí za okamžitou technikou podporu a kvalitní technickou dokumentaci.

- Open Source (OSS)
  Volná distribuce všech prostředků, kde uživatel má přístup na nejnižší vrstvy a podle svých potřeb si je upravuje.

- Open Source s komerčními prvky
  Dnešní výrobci se spíše zaměřují na toto řešení. Nástroje jsou založeny na open source nástrojích, kde je možno si koupit prvky navíc nebo kompletní technickou podporu. Toto řešení je prospěšné jak pro stranu OSS, tak pro stranu vývojářů. OSS je vylepšována ve velkých firmách a tyto vylepšení může ihned vyzkoušet velké množství uživatelů.

Pro vývoj na STM32 jsou dostupné tyto nástroje:

Toolchain	Společnost	Kompilátor	Informace
EWARM	IAR Systems	IAR C/C++	www.iar.com 30-denní zkušební verze Jen pro Windows
MDK-ARM	Keil	ARMCC	www.keil.com MDK-Lite Velikost kódu omezena na 32Ko Jen pro Windows
TrueStudio	Atollic	GNUC	www.atollic.com 30-denní zkušební plná verze Velikost kódu omezena na 32Ko Jen pro Windows
SW4STM32	AC6	GNUC	www.openstm32.org Bez limitu

Tab. 9.1: Vývojové nástroje pro STM32 [23]

Pro potřeby sběrného bodu, kde kód může mít velikost v řádu 100Kbytů, připadá v úvahu jen toolchain SW4STM32, který nemá žádný limit pro velikost kódu. Na stránkách openstm32.org je k dispozici ke stažení i doporučené integrované vývojové prostředí SYSTEM WORKBECH FOR STM32, které je vhodné k použití s tímto toolchainem. Prostředí je založeno na Eclipse. Program je napsaný v jazyce Java, proto ho lze využít v systémech GNU/Linux, MS Windows a MacOS.

9.3 Struktura programového vybavení

Při řešení komplexních úloh je nutné určit hranici, při které je daný problém stále řešitelný v rámci jednotlivce nebo týmu. Pokud se úloha stává příliš složitou, je vhodné ji rozdělit na dílčí problémy (vrstvy), které se řeší nezávisle na sobě a následně se spojují do jednoho celku, který má hiearchické uspořádaní. Rozdělení úlohy do vrstev má řadu výhod:

- Zjednodušení systému
  Není potřeba znát veškeré programové vybavení systému. Stačí být obeznámen s vrstvou, na které se pracuje. Příkladem je aplikační programátor, který zažádá o otevření souboru na disku. Aplikační vrstva se spojí s nižší vrstvou, která má na starosti periferie pro otevření souboru a následné vrácení výsledku bez toho, aby programátor znal práci na nižších vrstvách.

- Rozdílná implementace vrstev
  Záměna vrstev aplikace umožní přenos na jiný hardware s tím, že nepozná záměny nižších vrstev a chod aplikace zůstává nezměněn.

- Efektivní testování
  Rozdělení na menší bloky a simulace jednotlivých funkcí dle potřeby.

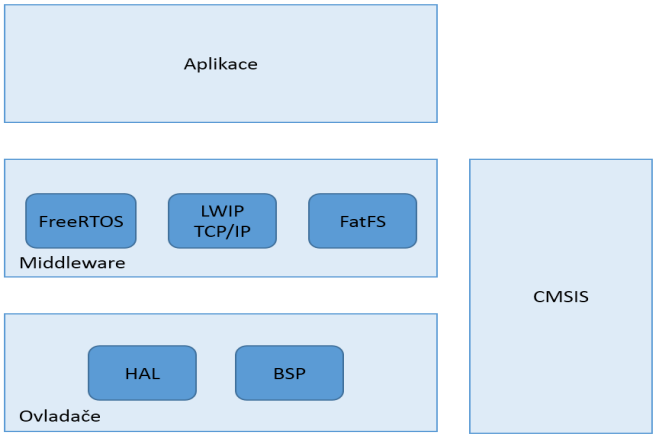
Nevýhody vrstvového modelu:

- Kaskádové změny
  Změna implementace nižší vrstvy, která používá vyšší vrstvu vyžaduje změnu i vyšší vrstvy a to z důvodu správné funkce.

- Snížení výkonu
  Každá vrstva obsahuje datové struktury, předává do dalších vrstev, zpracovává je a tím dojde ke zpomalení systému.

9.4 Vrstvy modelu

Na Obr. 9.1. je zobrazen vrstvový model pro aplikaci sběrného bodu.



Obr. 9-1: Vrstvový model

HAL (Hardware Abstraction Layer),
BSP (Board Support Package),
CMSIS (Cortex® Microcontroller Software Interface Standard),
RTOS (Real Time Operating System),
LWIP TCP/IP (LightWeight TCP[Transmission Control Protocol]/IP),
FatFS (File Allocation Table File System)

9.4.1 Aplikační vrstva

Vrstva je definována funkcemi se stanovenými vstupy a výstupy. Proto je možná záměna funkcionality nižší vrstvy a jsou schovány detaily implementace. Tato vrstva poskytuje programátorovi rozhraní operačního systému, knihoven a k periferií API (Application Peripheral Interface).

9.4.2 Middleware

Software, který propojuje aplikační vrstvu a ovladače, umožňuje přenos dat mezi komponenty nad rámec operačního systému. Usnadňuje práci vývojářům, kteří se zaměřují jen na vstup a výstup. Na základě požadavku systému jsou implementovány tyto softwarové balíky:

Název Middleware	Zdroj
LWIP TCP/IP Stack	http://savannah.nongnu.org/projects/lwip/
FatFS souborový systém	http://elm-chan.org/fsw/ff/00index_e.html
FreeRTOS	http://www.freertos.org/

Tab. 9.2: Middleware balíky

9.4.3 Ovladače

Ovladače zařizují přístup operačnímu systému k dané hardwarové periférii. Tato vrstva se dělí na vrstvy HAL a BSP [25].

9.4.3.1 HAL

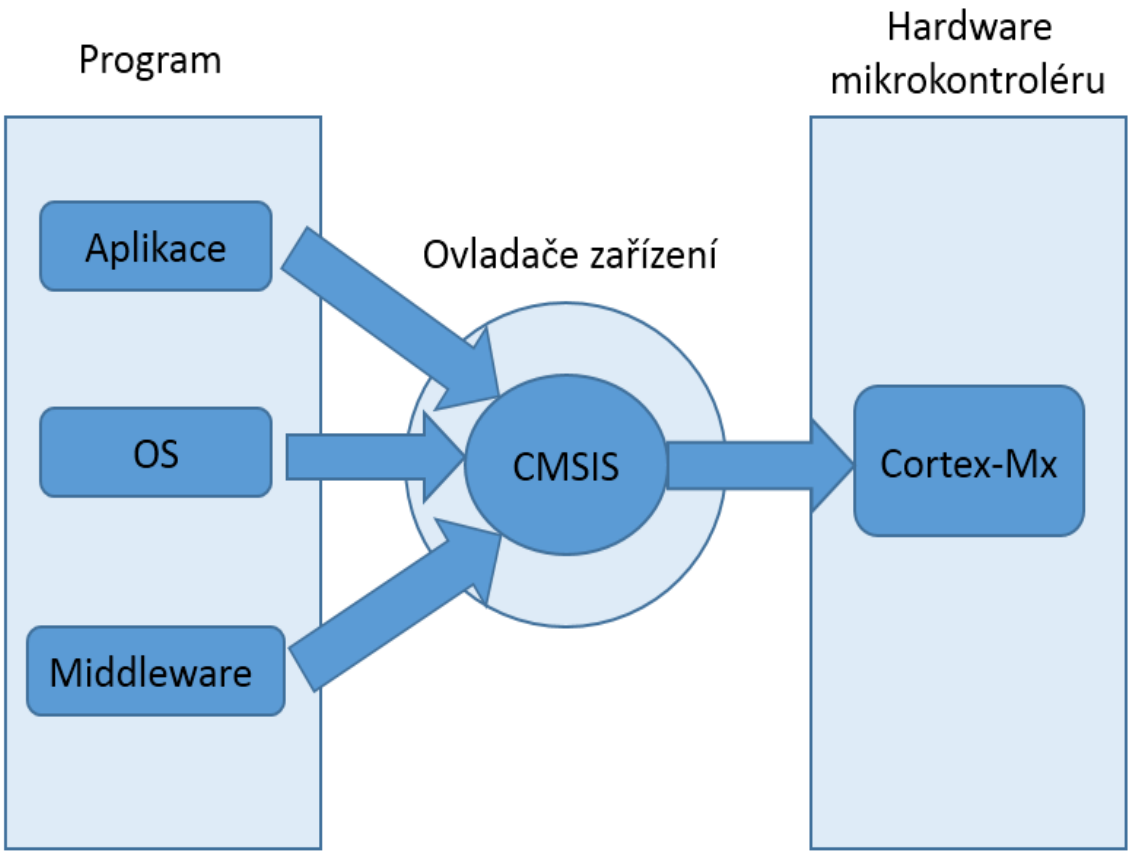
HAL komunikuje přímo s hardwarem. Definuje virtuální (abstraktní) hardware, ke kterému jádro přistupuje, pokud se potřebuje dostat k zařízení. Vrstva transformuje abstraktní příkazy na příkazy, které systém ve skutečnosti využívá [25].

9.4.3.2 BSP

BSP obsahuje specifikace architektury desky, knihoven požadovaných operačním systémem. Systém musí být před předáním řízení aplikaci už inicializován. Pokud se zjistí, že máme BSP pro jinou desku, je nutné zablokovat spuštění aplikace, aby se předešlo zničení ostatních periferií a pádům aplikace [25].

9.4.4 CMSIS

Použitím CMSIS se zjednodušuje vývoj, umožňuje použití kódových šablon, které jsou kompatibilní od různých dodavatelů middleware programů, různého operačního systému a aplikací. Hlavní výhodou je přenositelnost a možnost opětovného použití. Je také možné migrovat mezi jinými Cortex jádry, což má za následek rapidní pokles času a ceny vývoje. Schéma CMSIS je zobrazeno na Obr.9-2. [24, 25, 26].



Obr. 9-2: CMSIS [26]

9.5 Programové vybavení sběrného bodu

9.5.1 Inicializace

Ke správné funkčnosti systému se musí nejprve inicializovat než se předá řízení uživatelské aplikaci. Skládá se definice vektoru přerušení inicializace periferií, ovladačů časovačů atd.. V navrhnutém systému má inicializace dvě fáze - inicializace před spuštěním OS (Operační systém) a po spuštění OS.

9.5.1.1 Inicializace systému před spuštěním OS

Probíhá ihned po validním nahrání programu do procesoru. V této chvíli ještě není spuštěn RTOS (Real Time Operating Systém) a nelze využívat jeho funkce. Tím je zaručeno, že nenastane přerušení vykonávaného kódu a nespustí se funkce, která

použije ještě nezinicializované periférie a piny.
Má za úkol:

- Zapnutí vyrovnávacích pamětí
  Procesor obsahuje zvlášť vyrovnávací paměť pro instrukce a data. Díky tomu může procesor zpracovávat instrukce a data paralelně. Toto uspořádaní pamětí zvyšuje výkon procesoru.
- Inicializace HAL vrstvy, ovladačů.
- Zapnutí a nastavení ovladačů, které se používají na vybraném kitu.
- Mapování SD karty k přečtení konfigurace pro danou aplikaci.
- Inicializace hodin reálného času. Nastavení frekvence hodin.
  STM32F746NG je ve výchozím stavu řízen z interního RC oscilátoru o frekvenci 16MHz. V této aplikaci je potřeba mít co nejvyšší výkon, takže v procesoru je upravena konfigurace na rychlý vnější externí krystal. Frekvence krystalu je modifikována děličkami a násobičkami na nejvyšší možnou frekvenci procesoru na 216MHz
- Vytvoření a dynamická alokace globální proměnné pro sdílení parametrů.
- Nahrání konfigurace z inicializačního souboru
  Aplikace je navrhnuta tak, aby parametry, které se mění od zákazníka k zákazníkovi, nemusel měnit programátor v aplikaci a přehrával se sběrný bod. Aby aplikace nemusela procházet soubor od začátku až do konce, inicializační soubor obsahuje sekce, které jsou ze začátku vyhledání a následně se třídí data. Struktura souboru je na Obr. 9-3.

```
[global]

IpAddress = 192.168.0.10
NetMask   = 255.255.255.0
IpDefGw   = 192.168.0.1

[time]

Date = 5.11.16
Time = 20:30:00
```

Obr. 9-3: Struktura inicializačního souboru

- Definice a spuštění úloh pro procesor
  V této fázi má procesor nainicializované všechny periférie a ovladače. Definuje se startovací proces pro konfiguraci úloh pro uživatelskou aplikaci jako je IP adresa, počáteční čas RTC Proces je ukončen po nakonfigurování ostatních procesů.

9.5.1.2 Inicializace systému po spuštěním OS

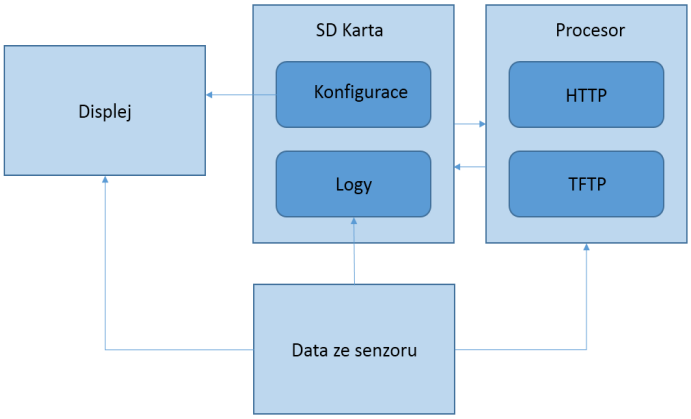
Po spuštění plánovače naběhne startovací proces. Ten neslouží jen ke konfiguraci procesů, jak již bylo zmíněno, ale také vytvoří a spustí další procesy uživatelské aplikace HTTP server, sběr a zpracování dat, RTC pro kontinuální zobrazení času na displej.

9.6 Aplikace na sběrném bodu

Tato kapitola popisuje chování sběrného bodu a jeho možnosti režimu. V první části je popsána obecná funkce sběrného bodu. V dalších se řeší jednotlivé implementace bloků.

9.6.1 Obecná funkcionalita

Po nainicializování sběrného bodu se předá řízení uživatelské aplikaci. Konfigurace aplikace se nachází na inicializačním souboru na SD kartě. Sběrný bod tedy může pracovat i v offline režimu bez připojení na síť. Tento způsob umožní sběrnému bodu pracovat i v případě výpadku, nebo pokud není možné použít síťový kabel k sběrnému bodu. Nevýhodou offline režimu je to, že uživatel musí být u změny konfiguračního souboru či získání dat ze senzoru fyzicky přítomen. Výhodnější způsob je připojení sběrného bodu na síť. Na sběrném bodu je nasazen http server, který po přihlášení umožňuje měnit konfiguraci, stáhnout si data a zobrazit je v grafu. Umožňuje také oboustranný přenos souborů díky TFTP (Trivial File Transfer Protocol) protokolu. Zobrazení konfigurace a současné naměřené hodnoty je možno sledovat online i offline na displeji sběrném bodu. Struktura aplikace je zobrazena na Obr. 9-4.



Obr. 9-4: Struktura aplikace sběrného bodu

9.6.2 Sběr dat

Sběr dat řídí samostatná úloha. Tato úloha musí být správně nakonfigurovaná, aby sběrný bod věděl, jestli má měřit v lokálních, vzdálených nebo z obou typů senzorů najednou. Nesmí se opomenout s jakou periodou má měřit. Pokud by aplikace byla špatně nakonfigurovaná a měřila z lokálních senzorů, výsledkem by byla náhodná data vyčtená z pinu AD převodníku, na které jsou senzory napojeny. U vzdálených senzorů by tento problém nenastal, protože jsou řízeny metodou server-klient. Proces by sice posílal příkazy na sběrnici, ale nedostal by nikdy odpověď a nic by nezapsal. Data se zapisují v nastavené periodě do fronty. Po vyzvednutí informace z fronty se ihned mažou.

9.6.3 HTTP server

Součástí systému je integrovaný HTTP server, který usnadňuje uživateli práci se sběrným bodem. Nemusí tedy řešit instalace dalších SW a druh zařízení. Stačí, aby měl jakékoliv chytré zařízení bez ohledu na jeho operační systém. Responzivní vzhled stránky podporuje zařízení s jakýmkoliv rozlišením.

Interakce mezi uživatelem a sběrným bodem je implementována pomocí SSI (Server Side Include) – tvorba stránek před odesláním uživateli a CGI (Commom Gateway Interface) – propojení aplikace s webovým serverem. Ty jsou jednoznačně identifikovány pomocí tagů. Pro přihlášení uživatele je z bezpečnostních důvodu využita metoda POST, která v prohlížeči nezobrazuje vyplněné hodnoty.

Do HTTP serveru jsou implementovány open source nástroje ke zpracování (jQuery), uložení (SQLite) a zobrazení (RGRAPH). Tyto nástroje jsou uloženy na interní flash paměti sběrného bodu. Ke klientovi jsou odeslány až v případě potřeby využití knihoven. Klient tedy nemusí být připojen k internetu, aby mohl využívat tento systém.

9.6.3.1 jQuery

jQuery je javascriptová knihovna,která zprostředkovává interakci mezi js a HTML. Tato knihovna je volně šiřitelná pod licencí MIT (Massachusetts Institute of Technology). V systému je využita, protože obsahuje AJAX (Asynchronous Javascript and XML), který načítá data ze serveru bez aktualizace webové stránky.

9.6.3.2 SQLite

SQLite je relační databáze, založena na tabulkách s položkami jednoho typu. Výhodou SQLite je, že neběží jako služba, ale je to jen knihovna nástrojů. Databáze se ukládá do jednoho souboru přenositelného na jakýkoliv počítač. Soubor se otevře v SQLite manažeru, kde lze data prohlížet a vkládat SQL dotazy k filtrování.

9.6.3.3 RGRAPH

RGRAPH je javascriptová knihovna pro tvorbu grafů. Obsahuje více než 50 možností vykreslení grafů. Výhodou je, že každý typ grafu má vlastní malý soubor, který se dá implementovat do procesoru bez jakýkoliv problémů a bez nutnosti přístupu k internetu. RGRAPH je volně šiřitelný pod licencí MIT.

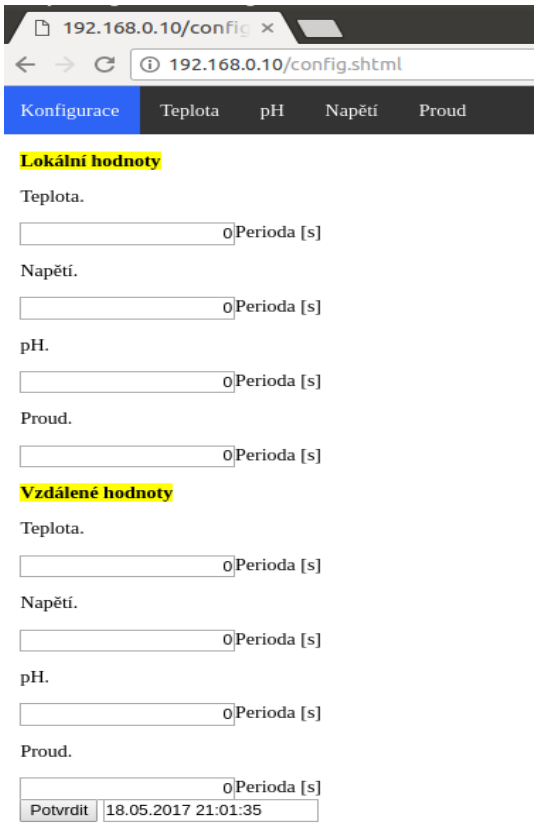
9.6.3.4 Aplikace na HTTP serveru

Po zadání příslušné IP adresy (doménového jména) se zobrazí přihlašovací stránka (Obr. 9-5.), kde uživatel zadá uživatelské jméno a heslo. V případě správného zadání je vpuštěn do systému, v opačném případě se opět zobrazí přihlašovací stránka. Po přihlášení se ihned stahují knihovny pro plné využití sběrného bodu. Po stažení těchto knihoven a před tím, než uživatel klikne na jakoukoli záložku, je v pozadí zadán požadavek na stažení posledních záznamů z SD karty do SQLite databáze, která je vytvořena u klienta na chytrém zařízení. Tím se zajistí redundance uložení dat a menší pravděpodobnost ztráty dat v případě pravidelného stahovaní.

Obr. 9-5: Úvodní stránka aplikace

9.6.3.5 Konfigurace sběrného bodu

Uživatel může změnit konfiguraci sběrného bodu pomocí webového rozhraní. V záložce pro konfiguraci jsou připravené formuláře viz Obr. 9-6. Po vyplnění a potvrzení těchto formulářů se přes CGI handler odešlou data do procesoru, který zapne měření a spustí časovače. Na pozadí s odeslaným formulářem se posílá aktuální čas a datum pro synchronizaci RTC hodin v procesoru. Hodnoty časovačů se uloží do session v prohlížeči, a to z důvodu synchronizovanosti odběru hodnot z procesoru v reálném čase.



Obr. 9-6: Konfigurace aplikace

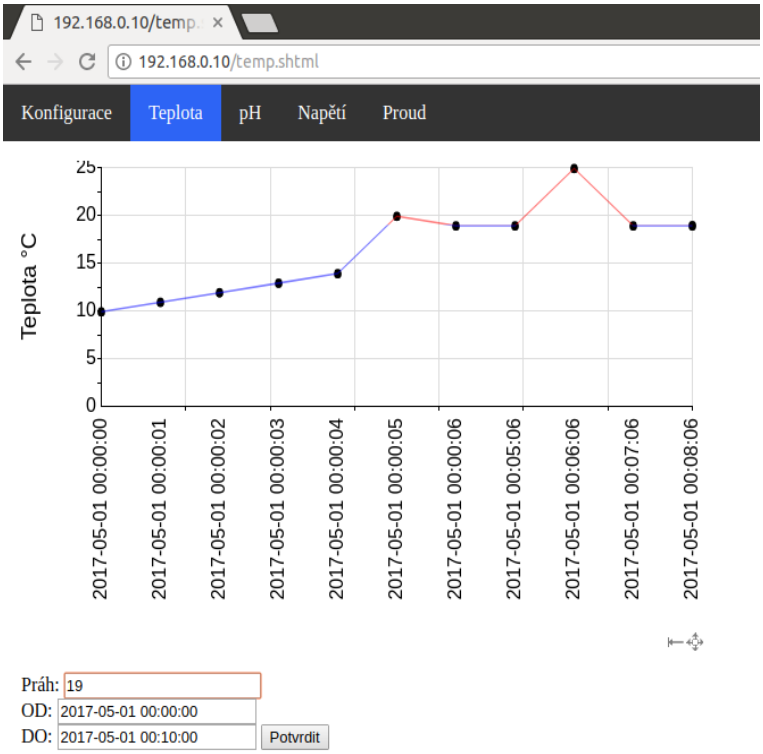
9.6.3.6 Přenos senzorických dat na HTTP server

Jak už bylo uvedeno, přenos prvotních dat probíhá bez vědomí uživatele. Ten získá rovnou aktuální data a nemusí čekat na počáteční hodnoty. Na vyžádaní se stahují všechna senzorická data z SD karty do klientské SQLite databáze. K přenosu těchto informací je použit AJAX. Ten spustí a stáhne stránku sync.html. Po aktivaci stránky se v procesoru spustí callback funkce, která vyčte data uložena ve frontě a pošle je s vhodným tagem SSI ke klientovi. AJAX tuto stránku načte, najde příslušný tag a vytáhne užitečné informace. Data jsou uložena ve formátu JSON (Javascript Object Notation), který je čitelný a snadno rozdělitelný v javascriptu do dílčích objektů.

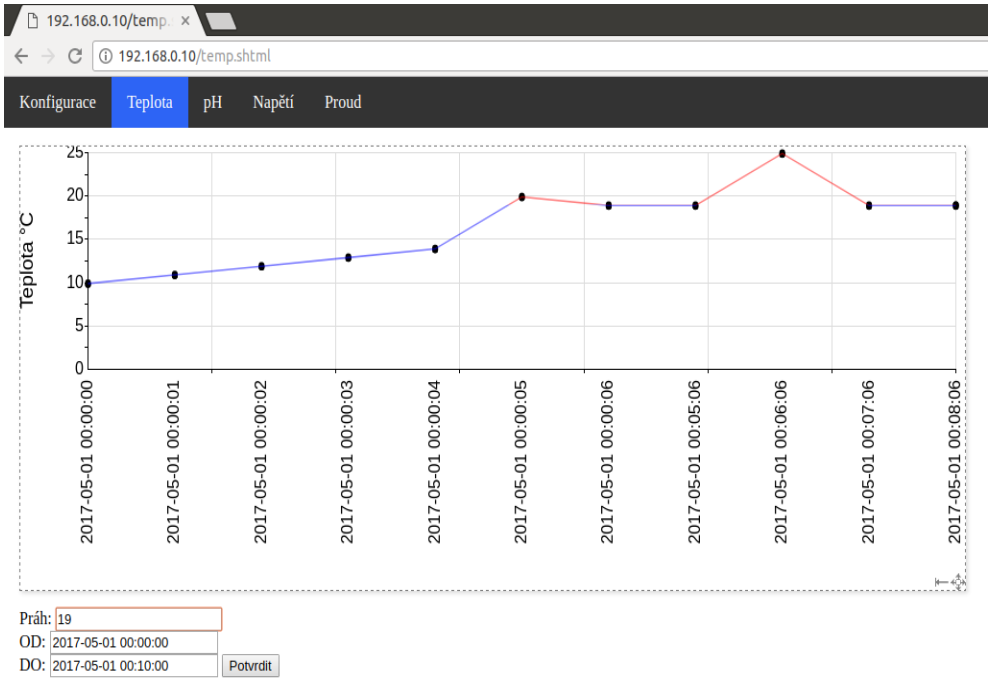
9.6.3.7 Zobrazení z SQLite databáze

Pro zobrazení hodnot z odlišných senzorů jsou na stránce vytvořeny jednotlivé záložky tak, aby graf mohl být co největší a nemuselo se zbytečně rolovat a hledat potřebný graf senzoru. Graf lze libovolně zvětšovat či zmenšovat podle potřeby uživatele. Nemůže se stát, že by vykreslený graf byl větší než plocha displeje.

HTTP server zobrazí nejen aktuální data, ale umožňuje i výběr starších dat. Po nastavení data se vygeneruje patřičná query pro databázi a graf se automaticky překreslí. Dále si uživatel může nastavit práh, který ho upozorní na vzniklé problémy.



Obr. 9-7: Graf s prahem bez přiblížení



Obr. 9-8: Graf s prahem a přiblížením

9.6.4 TFTP protokol

TFTP je jednoduchý protokol pro přenos souboru, který je využíván tam, kde je omezená paměť. Uživatel si může stáhnout konfigurační soubor a upravit dle své potřeby. Může stáhnout jakýkoliv soubor logu s daty. Nevýhodou řešení TFTP je, že uživatel musí znát přesné názvy souborů, které chce stáhnout nebo poslat na sběrný bod, aby tato funkce měla smysl. Soubory budou mít jasně definované názvy jako v manuálu. Pro stažení souboru je vyvinut dostatek volně dostupných klientů s grafickým rozhraním. V těchto klientech se zadá, kam a odkud se mají informace stáhnout.

Kapitola 10

Spolehlivost a zabezpečení systému

Systém je konstruovaný tak, aby se snížila pravděpodobnost ztráty dat nebo poruchy celého systému. Nezabývá se matematickými modely a výpočty pravděpodobnosti spolehlivosti.

10.1 Zamezení ztráty dat

Ztráta dat patří mezi nejrizikovější faktory. Může vzniknout cizím zaviněním např. poruchou úložiště nebo vlastním smazáním dat. Ke snížení pravděpodobnosti ztrát dat je systém navrhnut tak, že data jsou uložena i ve sběrném bodu. Po spuštění webového rozhraní jsou nahrána klientovi. Tím je zajištěna potřebná redundance a zamezení ztráty dat.

10.2 Zamezení nefunkčnosti systému

Tento systém umožňuje připojit do sítě více sběrných bodů s odlišnou IP adresou. Funguje buď jako stálá záloha, kdy pracuje ve stejném režimu jako primární prvek, nebo ve studené záloze, kdy se stačí připojit do elektrické sítě a použít vhodný konfigurační soubor. Anebo v horké záloze, kdy může sběrný bod fungovat, ale nebude sbírat data. Po vypadnutí primárního prvku by stačilo ve webovém rozhraní zapnout senzory. V případě výpadku lokální sítě sběrný bod může stále sbírat data. Po obnovení sítě si nová data uživatel stáhne.

Pro případ, že dojde k nefunkčnosti SD karty jsou webové stránky uloženy na interní flash paměti, aby systém nepřestal fungovat. Uživateli sice nebudou ukládána data, ale bude mít možnost prohlížení předešlých dat z lokálního úložiště.

Pro možnost vzdáleného měření ze senzoru musí být baterie dostatečně nabita. Informace o nabití se zobrazují na webovém rozhraní a na displeji sběrného bodu. V případě, že by se baterie dostala na kritickou hodnotu napětí, je automaticky odpojena od obvodu. Tím se baterie chrání před nenávratným zničením.

10.3 Zabezpečení systému

Sběrný bod je primárně umístěn v intranetové síti. V tomto typu sítě má uživatel (administrátor) plnou kontrolu nad stavem sítě. Při dodržování bezpečnostních aspektů sítě by se do intranetu neměl dostat nikdo nežádoucí, a proto není nutné spouštět na sběrném bodě HTTPS (Hypertext Transfer Protocol Secure). Pokud by uživatel chtěl získat data z internetu, musel by se sběrný bod připojit do směrovače, který by se o toto šifrování postaral. Může vytvořit například privátní virtuální síť (VPN - Virtual Private Network) nebo zašifrovaný tunel (SSL/TLS - Secure Sockets Layer/Transport Layer Security).

Bezdrátový přenos dat je šifrován pomocí AES128 v režimu CBC, a to jak v případě bondování tak i šifrování na aplikační úrovni.

Kapitola 11

Závěr

Cílem této diplomové práce je navržení a implementace systému pro sběr technologických dat. Práce zahrnuje návrh drátového a bezdrátového senzorového přípravku. Oba přípravky obsahují měření teploty vodných roztoků, pH roztoku, stejnosměrné napětí do 15 V a stejnosměrný elektrický proud do 10 A. Teplotní senzory nejsou přímo na desce, ale jsou vyvedeny dráty mimo desku a zaizolovány tak, aby mohly být vloženy do vodného roztoku. PH roztoků je měřeno externí skleněnou baňkou. Pro tuto baňku je na deskách připraven BNC konektor. Navrženým obvodem je možno měřit pH v rozmezí 0-14. Stejnosměrné napětí je měřeno pomocí vysoko ohmového děliče, aby nezatěžoval měřící obvod. K děliči je připojena Zenerova dioda pro ochranu AD převodníku před přepětím. Měření stejnosměrného proudu do 10 A je rozšířeno i o měření střídavého proudu. Obvod je navržen tak, aby měřil proudy maximálně 10 A. Desky jsou ale osazeny ACS712 s měřícím prahem až 30 A. Zvýšení maximální měřené hodnoty proudu lze dosáhnout zmenšením napájecího napětí, aby se zmenšilo výstupní napětí při nulovém proudu.

Bezdrátový přípravek obsahuje LPWAN technologii IQRF, která ho řídí. Zapíná napájení senzorů a adresuje multiplexor, který propojuje výstupy ze senzoru na vstup AD převodníku IQRF modulu. Adresy jsou definovány konkrétní zprávou z koncentrátoru. Po přečtení změřené hodnoty ji pošle zpět ke koncentrátoru a následně vypne napájení přípravku, tím šetří baterii. Baterie je ochráněna před zničením odepínacím obvodem, který hlídá její napětí. Kritický stav baterie je odeslán na sběrný bod.

Změřené (přijaté hodnoty) jsou uloženy na SD kartě. Soubory jsou členěny podle typu senzoru a data měření. Aktuální hodnoty jsou zobrazeny na LCD displeji

sběrného bodu a odeslány do fronty na http server. Ve sběrném bodě je naprogramován mechanismus pro kontrolu zaplnění SD karty a následné smazaní nejstarších souborů.

Sběrný bod obsahuje integrovaný HTTP server. Všechny potřebné knihovny pro zobrazení a načítání dat jsou naprogramovány do interní flash paměti. Není tedy nutné sběrný bod připojovat k internetu. Po správném zadání uživatelského jména a hesla se ihned spustí skript na stažení nejnovějších záznamů uložených na SD kartě. Hodnoty z předešlých dnů si uživatel může vyžádat přes webové rozhraní. Pokud soubor existuje, jsou data přenesena k uživateli. Ten si je může zobrazit, vyfiltrovat a nastavit práh zobrazených hodnot.

Stažené hodnoty z SD karty se ukládají do SQLite databáze uložené u klienta. Z této databáze se následně vybírají hodnoty, které chce uživatel zobrazit. Ukládaní hodnot do dalšího úložiště výrazně zmenšuje pravděpodobnost ztráty dat.

Základní konfigurace sběrného bodu (IP adresa, uživatelské jméno a heslo atd.) se provádí přes inicializační soubor, aby tyto hodnoty nebyly natrvalo v procesoru a uživatel si je mohl sám měnit dle potřeby bez přeprogramování procesoru. Konfigurace period měření senzorů se provádí přes webové rozhraní. To je po potvrzení odesláno do sběrného bodu spolu s aktuálním časem, pro synchronizaci hodin reálného času.

Na sběrném bodě je implementován TFTP protokol. Ten umožní uživateli přenášet soubory bez jakékoliv manipulace s SD kartou. Stačí mu pouze znát umístění souborů a jejich strukturu.

Všechny komponenty systému jsou navrženy a otestovány tak, aby splnily stanovené cíle. Výjimkou je otestování měření pH. K obvodu byla totiž dodána nefunkční pH sonda (vyschlý druhý roztok v elektrodě). Obvod byl tedy otestován pouze elektricky, kdy na vstup byl připojen měkký zdroj napětí a sledovalo se chování navrženého obvodu. Výsledky testu ověřily zadané požadavky. Aplikace na HTTP serveru je vytvořena pro funkci ve všech prohlížečích, které podporují nejnovější HTML5 databáze (Safari, Chrome a Opera 10.50). Uložená databáze má při stejném obsahu jen jiné umístění. Veškeré zpracování dat probíhá ve sběrném bodě a to z důvodu šetření spotřeby. Má zaveden komunikační protokol s identifikátory jednotlivých pracovišť a senzorů. Délka komunikačního protokolu je navržena co

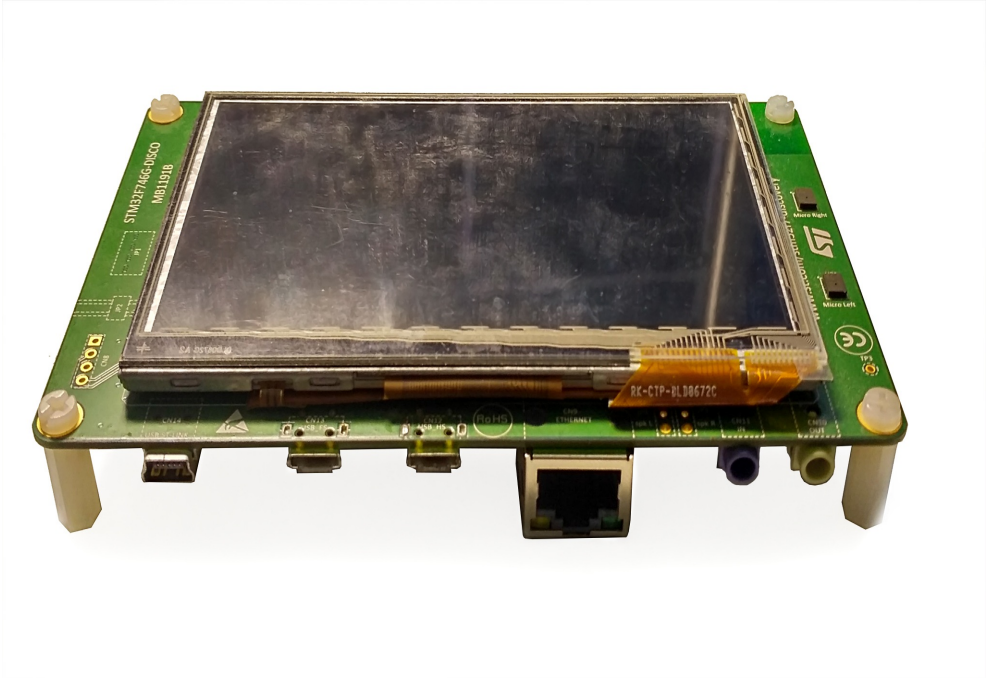
nejkratší, aby se snížila spotřeba elektrické energie, protože přenos bezdrátovým řetězcem nejvíce zatěžuje baterii.

Systém lze rozšířit o zabezpečený HTTPS server, aby sběrný bod mohl být připojen do vnější sítě i bez využití šifrování směrovače. Pro HTTPS je nutné softwarově (hardware je obsažen ve sběrném bodu) dodat externí paměti, protože interní paměť není pro tuto implementaci dostatečně velká.

V současném řešení se již počítá s připravenou sítí a pro větší univerzálnost je vhodné na sběrném bodě umožnit správu bezdrátové sítě (přidat, odebrat uzly), zobrazit tuto síť atd..

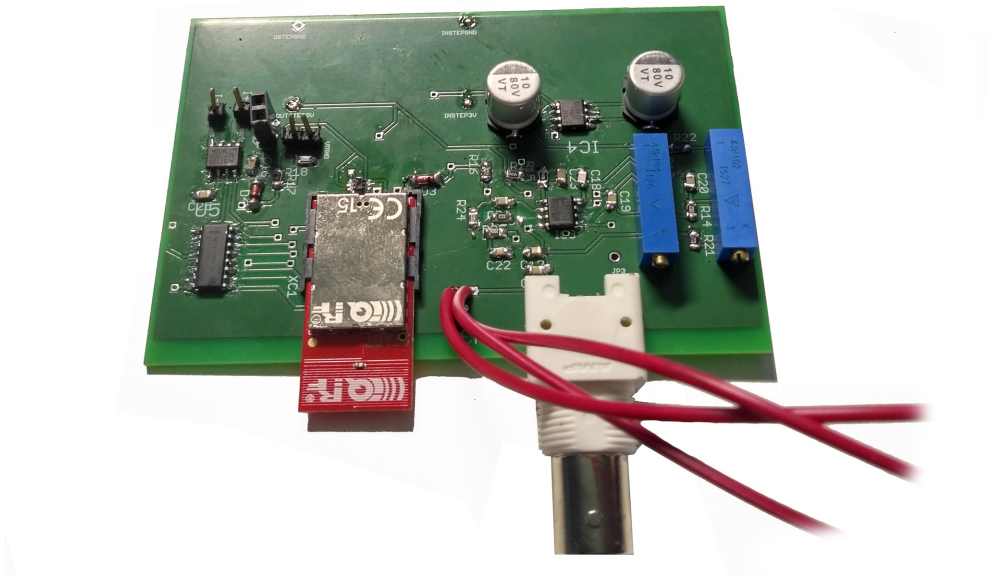
Kapitola 12

Přílohy

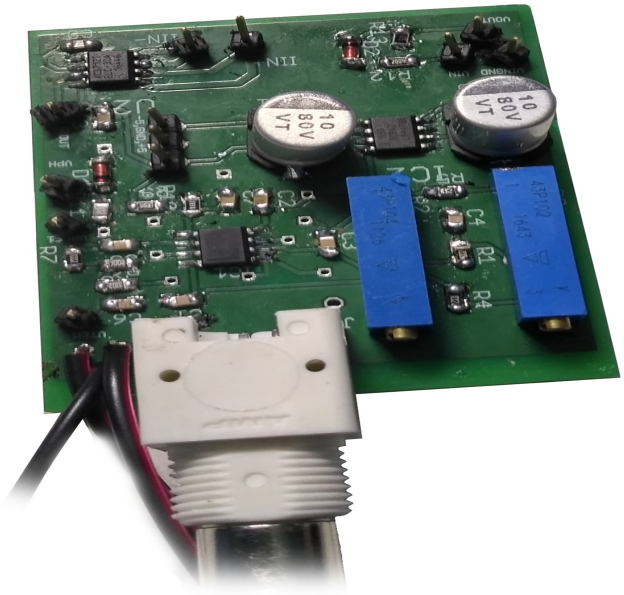


Obr. 12-1: Sběrný bod

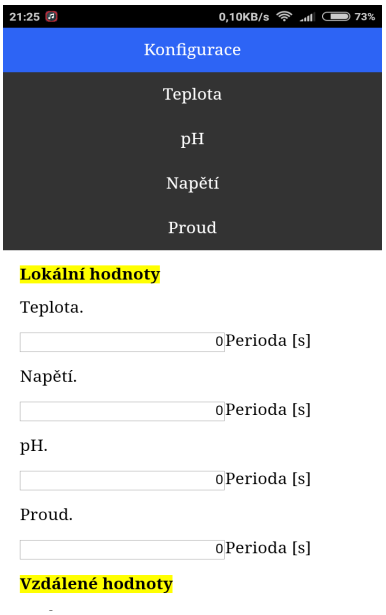
Obr. 12-2: Zobrazení konfigurace a naměřených dat



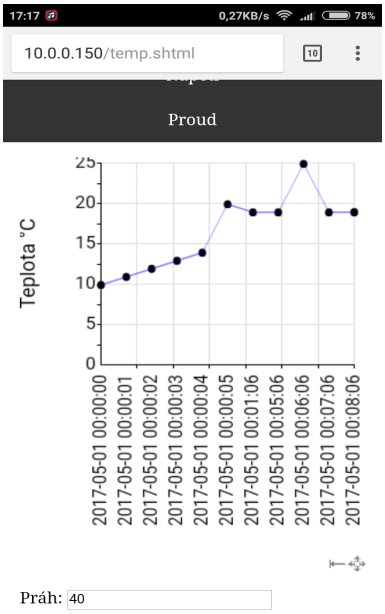
Obr. 12-3: Navržená bezdrátová senzorová síť



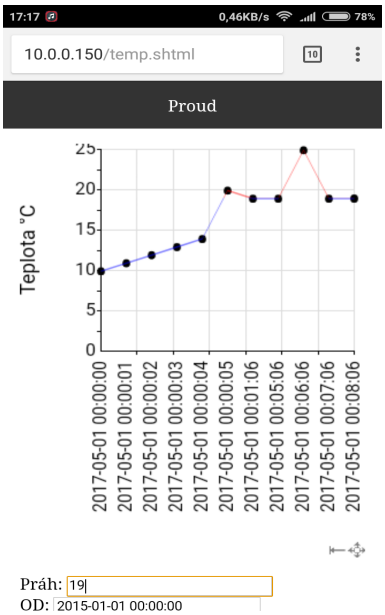
Obr. 12-4: Navržená senzorová síť



Obr. 12-5: Zobrazení konfigurace na mobilním zařízení



Obr. 12-6: Zobrazení grafu na mobilním zařízení



Obr. 12-7: Zobrazení grafu na mobilním zařízení s prahem

Literatura

[1] Úvod do automatizovaného sběru dat ve výrobě. SystemOnline [online]. [cit. 2017-05-07]. Dostupné z:
https://www.systemonline.cz/clanky/uvod-do-automatizovaneho-sberu-dat-ve-vyrobe.htm

[2] IQRF Brána. IQRF [online]. [cit. 2017-05-11]. Dostupné z:
http://www.iqrf.org/products/gateways/gw-eth-02a

[3] Mikrosenzorové technologie pro inteligentní senzorové sítě. DPS-AZ [online]. [cit. 2017-05-07]. Dostupné z:
http://www.dps-az.cz/vyvoj/id:18068/mikrosenzorove-technologie-pro-inteligentni-senzorove-site

[4] Internet of Things: Wireless Sensor Networks. IEC [online]. [cit. 2017-05-07]. Dostupné z:
http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

[5] SIGFOX: Internet věcí bez internetu a jen pro některé věci Lupa [online]. [cit. 2017-05-07]. Dostupné z:
http://www.lupa.cz/clanky/sigfox-internet-veci-bez-internetu-a-jen-pro-nektere-veci/

[6] Všeobecné oprávnění č. VO-R/10/05.2014-3. ČTÚ [online]. [cit. 2017-05-07]. Dostupné z:
https://www.ctu.cz/cs/download/oop/rok_2014/vo-r_10-05_2014-03.pdf Internet

věcí: Nové příležitosti i hrozby. BusinessIT [online]. [cit. 2017-05-07]. Dostupné z: http://www.businessit.cz/cz/internet-veci-nove-prilezitosti-i-hrozby.php

[8] BURDA, Karel. Úvod do kryptografie. Brno: Akademické nakladatelství CERM, 2015. ISBN 978-80-7204-925-7.

[9] SIGFOX: NOVÁ BEZDRÁTOVÁ SÍŤ PRO „INTERNET VĚCÍ“ V ČESKÉ REPUBLICE. T-PRESS [online]. [cit. 2017-05-07]. Dostupné z: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/sigfox -nova-bezdratova-sit-pro-internet-veci-v-ceske-republice.html

[10] Technologie LoRa z pohledu Českých Radiokomunikací. Telmag [online]. [cit. 2017-05-07]. Dostupné z: http://telmag.cz/technologie-lora-z-pohledu-ceskych-radiokomunikaci/

[11] Malé, chytré, české... Bezdrátová platforma IQRF. Vyvoj.hw [online]. [cit. 2017-05-07]. Dostupné z: http://vyvoj.hw.cz/rf/male-chytre-ceske-bezdratova-platforma-iqrf.html

[12] IQRF - bezdrátová technologie, která láme bariéry. Soselectronic [online]. [cit. 2017-05-07]. Dostupné z: https://www.soselectronic.cz/articles/iqrf/iqrf-iqrf-bezdratova-technologie-ktera-lame-bariery-1342

[13] Sbernice-wireless-mbus-jde-i-bezdratove. automatizace.hw.cz [online]. [cit. 2017-05-22]. Dostupné z: http://automatizace.hw.cz/sbernice-wireless-mbus-jde-i-bezdratove

[14] V Praze otestovali sestřičku LTE, příští rok možná pokryje celé Česko. Technet.idnes [online]. [cit. 2017-05-07]. Dostupné z: http://technet.idnes.cz/site-lp-wan-testovani-praha-internet-veci-fgf-/tec_technika.aspx?c=A161212_081214_tec_technika_nyv

[15] TR-72D datasheet. IQRF [online]. [cit. 2017-05-07]. Dostupné z: http://www.iqrf.org/products/transceivers/tr-72d

[16] Semtech SX1272. Semtech [online]. [cit. 2017-05-07]. Dostupné z:
http://www.semtech.com/wireless-rf/rf-transceivers/sx1272/

[17] Technologie-Sigfox. Simplecell [online]. [cit. 2017-05-07]. Dostupné z:
https://www.simplecell.eu/technologie-sigfox/

[18] Norma ČSN IEC 50(191) (010102) + změny z1, z2, platné od 1.4.2003. Medzinárodný elektrotechnický slovník. Kapitola 191: Spoľahlivosť a akosť služieb.

[19] Chodounský, J. Projektování spolehlivosti telefonního přenosu. Praha: NADAS 1983, 167 s.

[20] Chodounský, J. Spolehlivost služby v telekomunikacích. Praha: Česká společnost pro jakost, 1995, 60 s.

[21] PhDuino. Github [online]. [cit. 2017-05-07]. Dostupné z:
https://github.com/hephesto/phduino

[22] Info Discovery kit [online]. [cit. 2017-02-17]. Dostupné z:
http://www.st.com/en/evaluation-tools/32f746gdiscovery.html

[23] UM2052 Getting started with STM32 MCU Discovery Kits software development tools [online]. [cit. 2017-02-17]. Dostupné z:
http://www.st.com

[24] PM0253 Programming manual [online]. [cit. 2017-02-17]. Dostupné z:
http://www.st.com

[25] YIU, Joseph. The definitive guide to ARM® Cortex®-M3 and Cortex-M4 processors. Third edition. ISBN 01-240-8082-0.

[26] YIU, Joseph. The definitive guide to the ARM Cortex-M3. 2nd ed. Amsterdam: Newnes, 2010. ISBN 978-1-85617-963-8.