Česká zemědělská universita v Praze

Technická fakulta

Realizace výukových úloh na základě bezdrátové platformy IQRF

bakalářská práce

Vedoucí práce: Ing. Miloslav Linda, Ph.D.

Autor práce: Luboš Muchna

Praha 2017

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Luboš Muchna

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Realizace výukových úloh na základě bezdrátové platformy IQRF

Název anglicky

Implementation in IQRF Wireless Communication Platform

Cíle práce

Cílem práce je realizace výukových úloh komunikace modulů zabezpečovací technicky, přenášení procesních signálů a regulace v inteligentních domech s využitím bezdrátové platformy IQRF.

Metodika

Rozbor možností komunikace bezdrátové platformy IQRF v různých oblastech použitelnosti. Seznámení se s konkrétní aplikací přenášení dat mezi moduly zabezpečovací techniky, přenášení procesních signálů (teplota, vlhkost, tlak atp.) a přenášení signálů v oblasti regulace (např. akční členy ventilů topných členů). Celkem realizujte tři vybrané úlohy.

Doporučený rozsah práce

45 stran, bez příloh

Klíčová slova

zabezpečovací technika, IQRF, měření, bezdrátová komunikace

Doporučené zdroje informací

Bazydło, Piotr; Dąbrowski, Szymon; Szewczyk, Roman, Distributed temperature and humidity measurement system utilizing iqmesh wireless routing algorithms, (2015), Advances in Intelligent Systems and Computing , vol. 352, p. 1-9

Bazydło, Piotr; Dąbrowski, Szymon; Szewczyk, Roman, Wireless temperature measurement system based on the IQRF platform, (2015), Advances in Intelligent Systems and Computing, vol. 317, p. 281-288

Hajovsky, Radovan; Pies, Martin, Use of IQRF technology for large monitoring systems, (2015), IFAC Proceedings Volumes (IFAC-PapersOnline) , vol. 48 (4), p. 486-491

Jaros, David; Kuchta, Radek, New location-based authentication techniques in the access management, (2010), Proceedings – 6th International Conference on Wireless and Mobile Communications, ICWMC 2010, p. 426-430

Kuchta, Radek; Vrba, Radimir; Sulc, Vladimir, IQRF smart wireless platform for home automation: A case study, (2009), 5th International Conference on Wireless and Mobile Communications, ICWMC 2009, p. 168-173

Kuchta, Radek; Vrba, Radimir; Sulc, Vladimir, Smart platform for wireless communication – Case study, (2008), Proceedings – 7th International Conference on Networking, ICN 2008, p. 117-120

Seflova, Petra; Sulc, Vladimir; Pos, Jiri; Spinar, Rostislav, IQRF wireless technology utilizing IQMESH protocol, (2012), 2012 35th International Conference on Telecommunications and Signal Processing, TSP 2012 – Proceedings, p. 101-104

Předběžný termín obhajoby

2016/17 LS – TF

Vedoucí práce

Ing. Miloslav Linda, Ph.D.

Garantující pracoviště

Katedra elektrotechniky a automatizace

Konzultant

Ing. Zdeněk Votruba, Ph.D.

Elektronicky schváleno dne 24. 2. 2016

prof. Ing. Jaromír Volf, DrSc.

Vedoucí katedry

Elektronicky schváleno dne 2. 3. 2016

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 06. 03. 2017

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Realizace výukových úloh na základě bezdrátové platformy IQRF“ vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze:..... Podpis:.....

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Miloslavu Lindovi, Ph.D. za odborné vedení a podmětné připomínky, které mi pomohly při psaní této práce. Dále chci poděkovat konzultantovi Ing. Zdeňku Votrubovi, Ph.D. za podnětné připomínky a pomoc při realizaci úloh, také chci poděkovat své rodině a kolegům, kteří mě podporovali, a byli nápomocni, kdykoliv bylo zapotřebí.

Abstrakt: Bakalářská práce je zaměřena na rozbor možností použití bezdrátového přenosu informací pomocí technologie IQRF. V úvodu práce je představena technologie IQRF. Jsou rozebrány její části, vlastnosti a možnosti komunikace, které jsou potřebné pro další část práce. V další části práce je proveden rozbor použitelnosti zvolené technologie IQRF pro oblasti použití, které definuje zadání práce. Poslední část se věnuje návrhu a realizaci tří výukových úloh z těchto vybraných oblastí postavených na technologii IQRF. V závěru práce je obsaženo zhodnocení použitelnosti v daných oblastech použití.

Klíčová slova: měření, IQRF, mesh, zabezpečovací technika, bezdrátová komunikace

IMPLEMENTATION IN IQRF WIRELESS COMMUNICATION PLATFORM

Summary: This bachelor thesis focuses on wireless data transmission using IQRF technology. The first chapter provides basic introduction to IQRF including detailed description of different aspects of IQRF ecosystem utilized in this thesis. Next chapters analyse range of application of IQRF technology in given areas and its results are used to form three educational tasks including their proposed solution using IQRF platform. Last chapter reviews utilization of these solutions in the given areas.

Key words: measurement, IQRF, mesh, security technology, wireless communication

Obsah

1 ÚVOD 1

2 CÍLE PRÁCE 2

3 IQRF 3

3.1 IQRF HARDWARE 4
3.1.1 Transceivery, komunikační moduly 4
3.1.2 DCS brány 6
3.2 OPERAČNÍ SYSTÉM IQRF 7
3.2.1 Sítě mesh 8
3.2.2 Protokol IQMESH 10
3.2.3 DPA Framework 15
3.3 VÝVOJOVÉ NÁSTROJE 16
3.3.1 Hardware pro vývoj 16
3.3.2 Softwarové prostředky 18
3.4 POROVNÁNÍ S KONKURENCÍ 18

4 TEORETICKÁ VÝCHODISKA 22

4.1 ZABEZPEČOVACÍ TECHNIKA 22
4.1.1 PIR čidlo 23
4.1.2 Legislativa 24
4.1.3 Návrh použití IQRF 25
4.1.4 Zhodnocení použitelnosti IQRF 28
4.2 PŘENOS PROCESNÍCH VELIČIN 29
4.2.1 Sítě WSN 29
4.2.2 WSN a IoT 30
4.2.3 Návrh použití IQRF 31
4.2.4 Zhodnocení použitelnosti IQRF 34
4.3 DOMOVNÍ AUTOMATIZACE 34
4.3.1 Návrh použití IQRF 35
4.3.2 Zhodnocení použitelnosti IQRF 36

5 PRAKTICKÁ ČÁST PRÁCE 37

5.1 POTŘEBNÉ VYBAVENÍ 37
5.2 PŘÍPRAVA TRANSCEIVERŮ 38
5.3 REALIZACE JEDNODUCHÉHO PIR ČIDLA 40
5.4 REALIZACE MĚŘENÍ TEPLOTY A VLHKOSTI 42
5.4.1 DPA Custom Handler 43
5.5 REALIZACE PŘENOSU DVOUSTAVOVÉHO POVELU 43
5.6 SOFTWARE PRO KOMUNIKACI S MODULY 45

6 ZÁVĚR 47

7 CITOVANÁ LITERATURA 50

8 SEZNAM OBRÁZKŮ 52

9 SEZNAM TABULEK 52

10 PŘÍLOHY 54

Seznam symbolů a zkratek

IQRF ..... (Intelligent Radio Fervency) platforma pro bezdrátovou komunikaci

WSN..... (Wireless Sensor Network) bezdrátová měřící síť

MEMS..... (Micro Electromechanical System) systémy s mikrorozměry

IoT..... (Internet Of Things) internet věcí

OS ..... (Operation system) operační systém

DPA..... (Direct Peripheral Access) framework pro komunikaci s periférіemy

HW..... (Hard Ware) hardware

RF..... (Radio Frequency) rádiové pásmo

MESH ..... (Mesh) typ topologie komunikační sítě

MCU ..... (Micro Controller Unit) mikroprocesor

GPIO ..... (General Pin Output Input) universální vstupně výstupní port

DCS..... (Data Collecting Station) brána systému IQRF

1-WIRE..... (One Wire) jednovodičová komunikační sběrnice

PZTS ..... Poplachové, zabezpečovací a tísňové systémy

PCO..... Pult centrální ochrany

PIR ..... (Passive Infra Red Sensor) pohybové čidlo

DPA..... (Direct Accesss Protokol) protokol pro přímý přístup k periférііm

CSMA ..... (Carrier Sense Multiple Access) pravděpodobnostní protokol přístupu k médiu

EEPROM ..... (Electrically Erasable Programmable Read-Only Memory) elektricky mazatelná semipermanentní (nevolatilní) paměť

FH ..... (Frequency Hopping) algoritmus frekvenčních skoků

SoC..... (System On Chip) integrovaný obvod, který zahrnuje všechny součásti elektronického systému

UART..... (Universal Asynchronous Reciever/Transmiter) asynchronní komunikační rozhraní

SPI..... (Serial Peripheral Interface) sériové periferní rozhraní

TWI..... (Two Wire Interface) dvouvodičová sběrnice

ADC ..... (Analog Digital Converter) analogově digitální převodník

PWM..... (Pulse Width Modulation) diskrétní modulace pro přenos analogového signálu

USB..... (Universal Serial Bus) univerzální sériová sběrnice

1 Úvod

Tato bakalářská práce se zabývá rozborem možností použití bezdrátové platformy IQRF. IQRF je jednou z bezdrátových platforem podporující nové standardy vyrobená v České republice, která se snaží prorazit v konkurenci technologií jako je ZigBee a další.

Úvod této práce je věnován seznámením se s touto platformou. Platforma se skládá z hardware použitého pro bezdrátovou komunikaci, operačního systému, protokolu pro komunikaci v mesh sítích a vývojových nástrojů. Všechny tyto části systému jsou představeny a jsou popsány jejich hlavní vlastnosti důležité pro realizaci výukových úloh.

V další části práce jsou shrnuty vlastnosti platformy a navržena možná implementace ve vybraných oblastech použití. Těmi oblastmi jsou zabezpečovací technika, přenos procesních signálů a domovní automatizace.

Poslední částí práce je návrh a realizace tří výukových úloh z jednotlivých oblastí použití. Jedná se o konstrukci jednoduchého PIR čidla, konstrukci bezdrátového teploměru a konstrukci přenosu digitálního povelu.

V závěru práce jsou shrnuty naměřené výsledky v jednotlivých úlohách a zhodnocena využitelnost platformy IQRF.

2 Cíle práce

1. Rozbor možností využití IQRF v zabezpečovací technice,

2. Rozbor možností využití IQRF v přenosu procesních veličin,

3. Rozbor možností využití IQRF v domovní automatizaci,

4. Realizace jednoduchého PIR čidla,

5. Realizace měření teploty a vlhkosti,

6. Realizace přenosu dvoustavového povelu,

7. Realizace SW pro čtení a zápis hodnot v realizovaných úlohách.

3 IQRF

IQRF je platforma pro bezdrátovou komunikaci vyvinutá českou společností Microrisc s.r.o. Platforma je navržena pro přenášení malých objemů dat, při malých rychlostech, na krátké vzdálenosti v rozmezí desítek, ve speciálních případech až stovek metrů. [1]

Bezdrátový přenos zajišťují komunikační moduly transceiverů, které mají velikost SIM karty. Tyto transceivery spolu komunikují v bezlicenčním frekvenčním pásmu na frekvenci 868 MHz, nebo volitelně na frekvenci 433 MHz. V pásmu 868 MHz je možno využívat 62 kanálů se šířkou 100 kHz. [1]

Transceiver moduly mají vestavěný operační systém (OS), který lze plně programovat pomocí jazyka C. Požadované uživatelské funkce lze programovat buďto jako pluginy, anebo lze využít framework DPA. DPA framework pomáhá vytvořit požadovanou funkcionalitu bez programování spouštěním předpřipravených hardwarových profilů HWP. [2]

IQRF OS podporuje několik typů síťové topologie a směrování. O to se stará implementace komunikačního protokolu IQMESH. IQMESH protokol podporuje paketově orientovaná schémata komunikace point-to-point a složitější, komplexnější topologie jako hvězda a mesh. Tento protokol umožňuje vytvářet rozlehlé mesh sítě jejich vzájemným spojováním. Jedná se o tzv. network chaining. V takovéto síti může být až 65 000 zařízení a může být rozprostřena na velké ploše. Jeden transceiver je v tomto případě součástí dvou podsítí a dochází na něm k přesměrování.

IQRF platforma je navržena jako nízkospotřebová. Úspora energie transceiverů je systémem realizována režimem spánku. Tento režim je aktivován, pokud modul nevysílá, nebo nečeká na přijetí dat. Optimalizace vysílání a přijímaní je součástí implementace IQRF OS.

IQRF platforma byla vyvinuta a je doporučována pro použití v těchto odvětvích:

- Sběr dat,
- Automatizace,
- Inteligentní domy,
- Internet věcí (IoT).

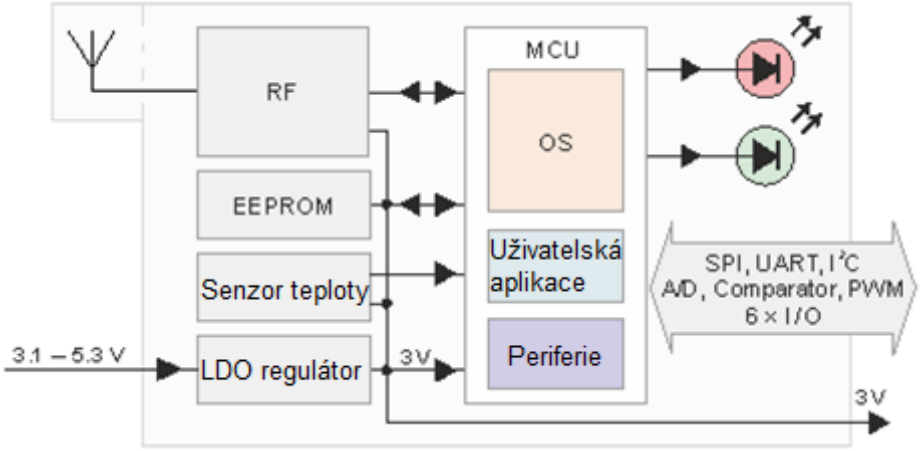
3.1 IQRF Hardware

Komunikaci v platformě IQRF zajišťují transceivery. Transceivery jsou zabudovány do koncových zařízení, například senzor teploty a tvoří tak autonomní měřící jednotku. Z těchto zařízení je pak sestavena síť. Měřící zařízení se v mesh síti stává komunikačním uzlem – node. V jedné síti je jeden koordinátor a maximálně 240 nodů – autonomních měřících zařízeních.

Koordinátor je transceiver připojený jedním z dostupných komunikačních rozhraní (SPI, UART, I^2C) s jednotkou, která data sbírá a dále zpracovává. Tato jednotka se nazývá DCS – *Data Collecting Station*, česky brána.

3.1.1 Transceivery, komunikační moduly

Na ploše velikosti SIM karty je umístěn procesor MCU, RF obvod, LDO regulátor a EEPROM jak je vidět na obrázku *Obr. 1*. Dalším volitelným vybavením je anténa, nebo teploměr. Díky velmi nízké spotřebě je toto zařízení vhodné pro napájení z baterie.



Obr. 1 Blokové schéma modulu [3]

Modul je vybaven kromě RF modulu rozhraními pro komunikaci po standardizovaných sběrnicích, jako je SPI, I^2C, nebo UART. Modul může být napájen napětím 3,1 V až 5,3 V díky LDO regulátoru. Díky tomuto regulátoru je také možné napájet jiné periférie. A to výstupem 3 V 100 mA.

Nyní jsou na trhu dvě řady transceiverů označené počátečním číslem 5 a 7. Jedná se o dvě různé generace, které se mezi sebou liší výkonem RF obvodu a velikostí paměti. V novějších

modulech řady 7 je 256 kb EEPROM, zatímco ve starších modulech řady 5 jen 16 kb EEPROM. Porovnání vlastností RF čipu je v tabulce *Tab. 1*. [3]

Tab. 1 Porovnání hardware RF obvodů řady 7 a řady 5 [3]

Specifikace	**Řada 7**	**Řada 5**
RF obvod	SPIRIT1	MRF49XA
RF obvod výrobce	STMicroelectronics	Microchip
RF pásmo	433/868/916 MHz	433/868/916 MHz
RF modulace	GFSK	FSK
Přenosová rychlost	19,836 kb/s	19,836 kb/s
RFIC RF citlivost	-106 dBm	-110 dBm
RFIC výstupní výkon	11 dBm	7 dBm
RF dosah	500 m	300 m

Všechny transceivery jsou velikosti SIM karty. Vyrábí se v provedení pro SMD montáž a pro uchycení do držáku SIM karty. Moduly mohou být vybaveny vnitřním teploměrem a dále se rozlišují podle druhu antény. Existují tři druhy anténního připojení:

- Bez antény – anténa není připojena, modul obsahuje plošku pro připojení,
- Vnitřní anténa – anténa je vytvořena přímo na desce modulu,
- U. FL konektor – konektor pro připojení externí antény.

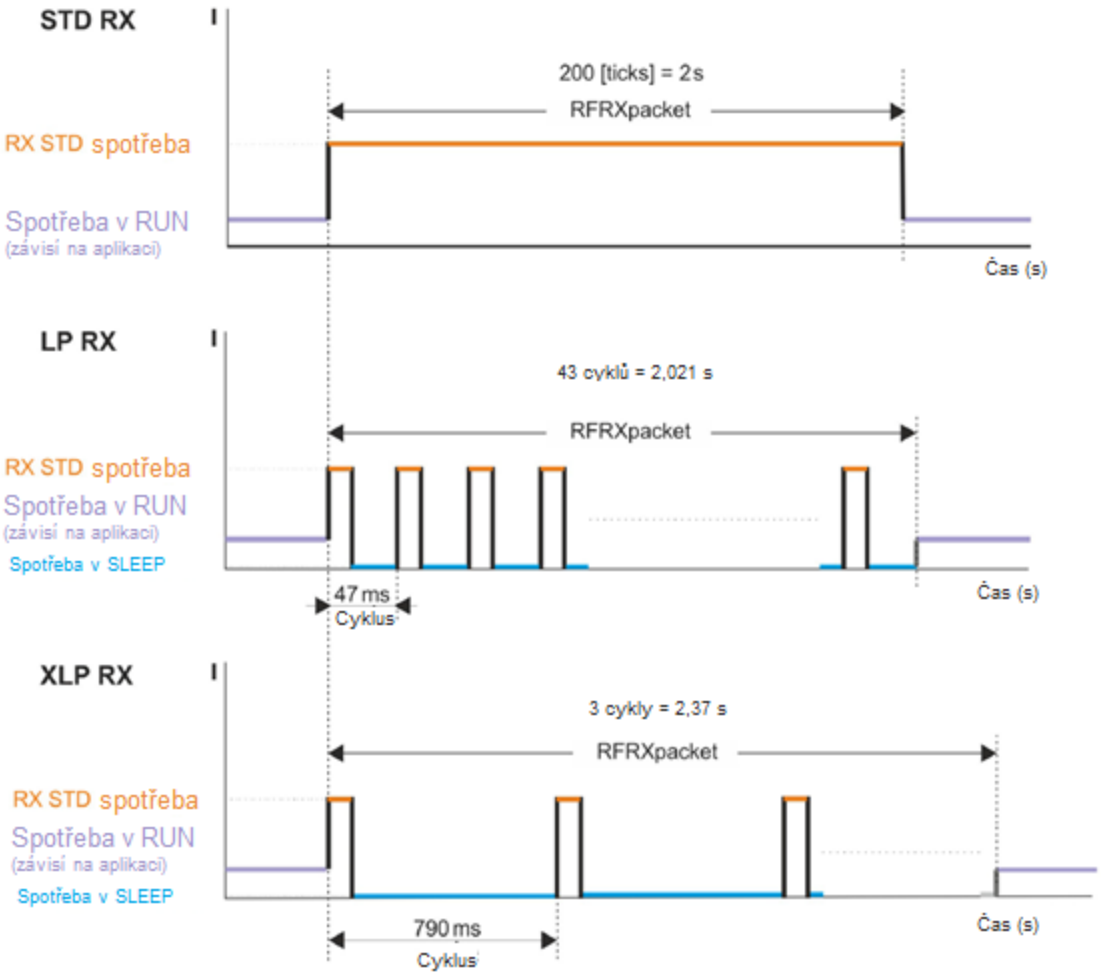
Moduly jsou dodávány s nahraným operačním systémem IQRFOS. U transceiverů řady 7 může OS upgradovat uživatel sám. Tato možnost u řady 5 není dostupná. Transceivery se dále vyrábějí ve dvou verzích OS. Verze s označením DCTR obsahuje DPA framework. Verze, která DPA framework neobsahuje, je označena jako TR. [3]

Transceiver má velmi nízkou spotřebu, která závisí na stavu modulu, ve kterém se nachází, a na požadovaném výkonu při vysílání. Nízká spotřeba modulu je dána využíváním režimu spánku MCU, využíváním spánku RF modulu a dále pak nastavením režimu spotřeby ve stavu, kdy modul čeká na přijetí dat – RX režim. Teoretické spotřeby v jednotlivých režimech udávané výrobcem jsou shrnuty v tabulce *Tab. 2*. [2]

Tab. 2 Spotřeby modulů v jednotlivých režimech [3]

Režim modulu		**Spotřeba**	**Poznámka**
Sleep mode		2,9 µA	Režim spánku celého modulu
Run mode	RF sleep	1,2 mA	Režim běhu modulu s uspaným RF obvodem
	RF ready	3 mA	Režim běhu modulu s připraveným RF obvodem
RX mode	STD	12,3 mA	Režim čekání na data, mód spotřeby standard
	LP	234 µA	Režim čekání na data, mód spotřeby nízká spotřeba
	XLP	16 µA	Režim čekání na data, mód spotřeby velmi nízká spotřeba
TX mode		8,3-19 mA	Režim vysílání závisí na výkonu max. 12,5 mW

Pro RX režim je možné definovat tři módy spotřeby. Módy spotřeby se liší tím, jak často RF modul naslouchá a jak často se nachází v režimu spánku. To je vysvětleno na obrázku *Obr. 2*. Na tomto obrázku je graficky znázorněno, v jakých časových cyklech je RF modul uspán a kdy je vzbouzen. [2]



Obr. 2 Módy spotřeby v RX režimu modulu [2]

Moduly jsou konstruovány s rozšířenou operační teplotou. Dokumentace [3] udává -40 °C až +85 °C. Díky jejich nízké spotřebě, malým rozměrům a možnosti připojení externí antény je celkem snadné je zabudovat do krytu s vyšším krytím IP. Tyto vlastnosti umožňují moduly používat ve venkovních podmínkách a v průmyslu.

3.1.2 DCS brány

Účelem brány je sbírat a zpracovávat a dále předávat naměřená data z IQRF sítě. Proto je brána vybavena komunikačním rozhraním pro komunikaci s nadřazenými systémy. [1]

Komunikace je zpravidla přenášena pomocí GSM modemu, nebo je brána vybavena síťovým (*Ethernet*) rozhraním. V IoT konceptu pak brána funguje jako připojení k internetu, po kterém zařízení (věci) sdílí data s ostatními zařízeními (věcmi), nebo cloudovými nástroji pro archivaci a analýzu dat. [1]

Brány jsou zpravidla napájeny externím zdrojem. Baterie jsou jen jako krátkodobý záložní zdroj. Je to z důvodu vysoké spotřeby GSM a z důvodu přenosu velkých dat. [1]

IQRF nabízí několik svých řešení bran jak s GSM modemem, WiFi, nebo ethernet rozhraním. Tato zařízení jsou poměrně drahá a data umí ukládat jen do IQRF Cloudu. Dalším typem brány je USB brána, kterou budu využívat pro realizaci výukových úloh. [1]

USB brána je převodník mezi UART, nebo SPI rozhraním na straně IQRF a USB na straně nadřazeného systému, kterým pro řešení výukových úloh bude PC. Tato brána neobsahuje žádné další vestavěné funkce ani podporu IQRF Cloudu. [1]

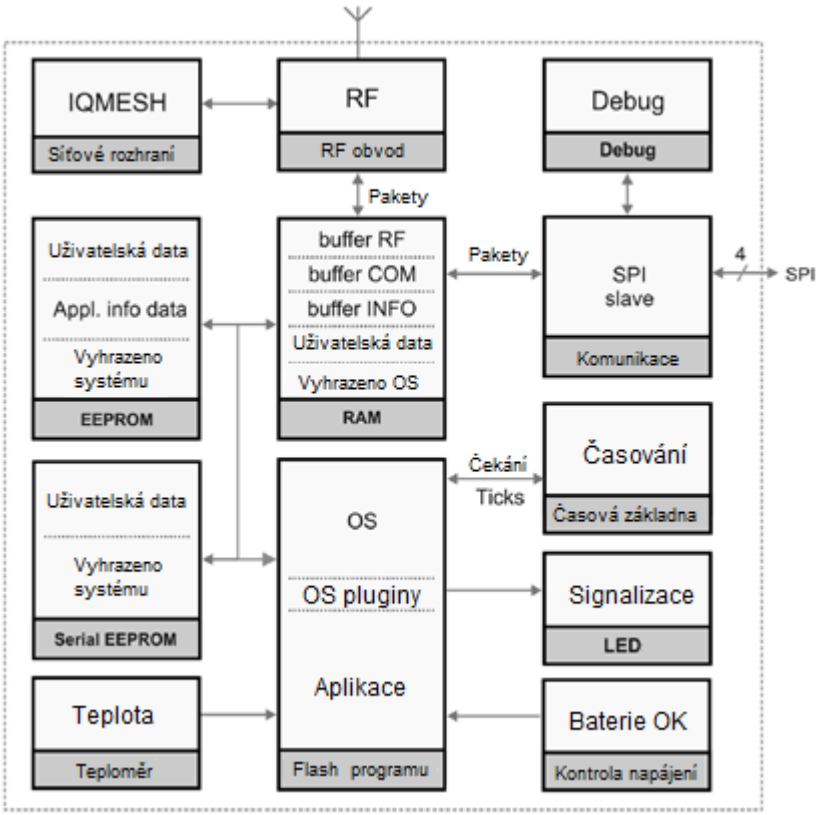
3.2 Operační systém IQRF

Transceivery obsahují vestavěný operační systém OS, který je plně programovatelný v jazyce C. Pomocí volání funkcí systému je možné přistupovat a ovládat jednotlivé periférie transceiveru jako je RF obvod a rozhraní SPI. Operační systém nabízí plnou podporu IQMESH protokolu. Vlastní systém neobsahuje implementaci linkové vrstvy, její realizace je ponechána na uživateli v rámci uživatelské aplikace. Ve funkcích OS nejsou zpřístupněny ostatní periferie modulu jako I^2C, UART, 1-WIRE. Obsluha těchto rozhraní musí být naprogramována v uživatelské časti aplikace. [2]

IQRF OS může být rozšířen o novou funkcionalitu pluginy OS. Pluginy většinou vytváří výrobce v závislosti na nových vlastnostech hardware. Více pluginů může být použito na jednom zařízení najednou. Detailní architektura operačního systému je na obrázku *Obr. 3.* [2]

Operační systém automaticky poskytuje všechny potřebné služby při komunikaci na těchto úrovních: [2]

- Na přenosové úrovni: HW setup, kódování, kontrola timeoutů a další,
- Na paketové úrovni: kódování, kontrola konzistence a další,
- Na síťové úrovni: routování, filtrování, discovery a další.



Obr. 3 Architektura operačního systému IQRF [2]

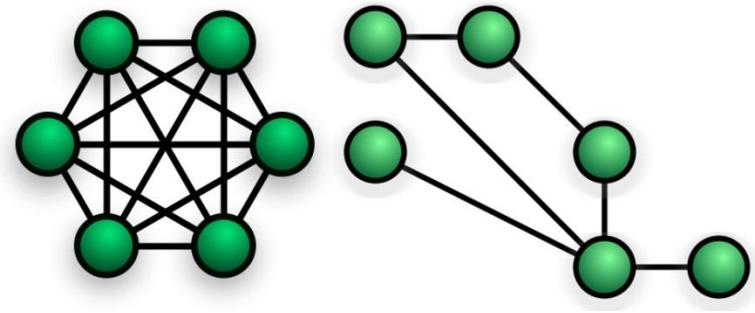
Podporované typy sítí v OS jsou: [2]

- Peer-to-peer: nejméně dvě zařízení jsou v síti bez koordinátora. Pakety posílané v síti jsou dostupné všem zařízením,
- IQMESH: topologie mesh sítě s jedním koordinátorem, při použití zřetězení sítí je možné vytvářet strukturu s až 65 000 koncových zařízení.

Bezpečnost systému je ve verzí OS do 3.08 realizována pomocí proprietárního kryptování odesílaných paketů v rámci sítě IQMASH. Popis kryptování není veřejně přístupný. V nové verzi OS 4.0 je plánováno používat 128bitové šifrování AES. Tento operační systém není v současné době dostupný, měl by být výrobcem uvolněn v 1. kvartálu tohoto roku.

3.2.1 Sítě mesh

Mesh sítě dnes hrají velmi významnou roli v konceptu IoT. Topologie síťe mesh je definována jako uspořádání komunikujících uzlů (nodes). Podle toho, jak jsou jednotlivé uzly spolu propojeny, se jedná o úplnou mesh síť, nebo částečnou mesh síť. Rozdíly jsou patrné z obrázku *Obr. 4.* [4]



Obr. 4 Úplná mesh a částečná mesh síť

V síti typu full mesh jsou mezi sebou spojeny všechny uzly. To znamená, že jedno zařízení se spojí přímo s libovolným dalším zařízením. V částečné síti mesh jsou spolu spojena jen některá zařízení. Spojení mezi zařízeními, která nejsou přímo spojena, pak probíhá přes mezilehlé uzly, se kterými spojení existuje. [5]

Síla mesh topologie spočívá v její obecnosti. Při poruše jednoho z uzlů není přerušena komunikace mezi ostatními uzly. Pokud dojde k poruše uzlu v částečné mesh síti a tento uzel spojuje mezi sebou jiné dva uzly, najde se nová cesta tak, aby byla dostupnost ostatních uzlů zachována. Spolehlivost pak závisí na počtu nodů v síti. Nevýhodou sítí mesh je složité routování, složité vyhledávání cest a zajištění odolnosti proti směrovacím smyčkám. [5]

Zasílání dat v sítích mesh je realizováno pomocí zasílání zpráv. Algoritmy pro zasílání zpráv využívají dvě možné techniky. Jednou z nich je zaplavení sítě.

Zaplavovací algoritmus *Flooding* pracuje tak, že všechny příchozí zprávy zašle na všechny odchozí spojení. Tím se zpráva šíří dokud není zaplavena celá síť. Algoritmus zaplavení může být buďto řízený, nebo neřízený. [4]

Další možností je routování – směrování. Směrovací algoritmus nalezne cestu dle svojí definice a zpráva pak putuje přes jednotlivé uzly sítě až k cíli. Cestování zprávy od jednoho nodu k dalšímu je *hooping*. Jeden přeskok mezi dvěma nody se pak nazývá *hop*. [4]

Mesh topologie je nejčastěji používána v bezdrátových sítích, které jsou pak označovány zkratkou WMN. Tuto topologii sítě dnes využívá řada výrobců a mesh sítě se staly součástí některých norem. Jednou z nich je ZigBee, které je založeno na standardu IEE 802.1.5.4 a je dnes ve verzi 3.0.

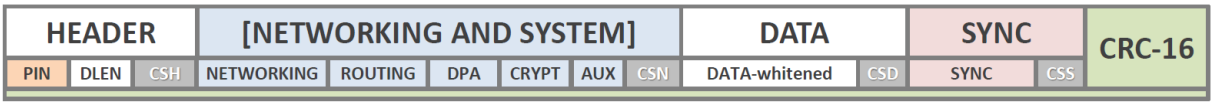
3.2.2 Protokol IQMESH

IQMESH (Intelligent Mesh) protokol byl vyvinut v roce 2005, jako základní komunikační protokol platformy IQRF. IQMESH je založen na topologii mesh sítě. Do jedné takové sítě je možné připojit až 240 zařízení. Mesh sítě se pomocí IQMESH protokolu dají řetězit, tím lze celkově připojit až 65 000 zařízení. [1]

V jedné mesh síti může být jeden koordinátor (C) a až 239 slave nodů (N) připojených ke koordinátorovi. IQMESH protokol podporuje dva způsoby adresace zařízení v síti a to individuální a skupinovou. Dále podporuje rozesílání broadcastových zpráv. Pro adresování je použit jeden byte, díky tomu je možné adresovat až 240 zařízení a maximálně 15 skupin v jedné síti. [6]

3.2.2.1 Pakety v síti IQMESH

IQMESH protokol podporuje paketově orientované komunikační schéma. Pakety pro komunikaci peer-to-peer jsou složeny ze tří bloků: *PATH, DATA* a *CRC*. Pakety v IQMESH sítích mají o jeden blok více a to *NTWINFO* jak je vidět na obrázku *Obr. 5*. Každá část paketu má svůj kontrolní součet. v síti je možné posílat jak peer – to – peer pakety, tak IQMESH pakety [2]



Obr. 5 Složení paketu IQMESH [2]

PATH – je hlavičkou paketu, má velikost 3 byty a obsahuje základní informace o paketu. Jsou to tyto základní informace: [2]

- pro jaký druh sítě je paket určen (peer-to-peer, IQMESH),
- směrování, které je použito,
- přímá adresa zařízení,
- algoritmus kryptování, který byl použit,
- požadavek potvrzení přijetí paketu.

NTWINFO – je blok obsahující informace o IQMESH síti jako je použitý algoritmus směrování, data směrování, topologie sítě, adresa zařízení kterému je paket v dané síti určen,

adresa odesílajícího zařízení, identifikace paketu a části využívané OS. Tento blok je nastavován odesílajícím a je předán všem příjemcům. [2]

DATA – Uživatelská data o maximální velikosti 64 B. Na jejich velikosti a typu sítě pak závisí doba potřebná k vyslání dat a tím i spotřeba nodu. [2]

V tabulce *Tab. 3* Doba potřebná pro vyslání paketu jsou výrobcem udávané doby odeslání paketu. Měřena byla doba odesílání paketu v různých typech sítě pro různé velikosti uživatelských dat. Měření byla provedena při komunikační rychlosti 19,2 kb/s [2]

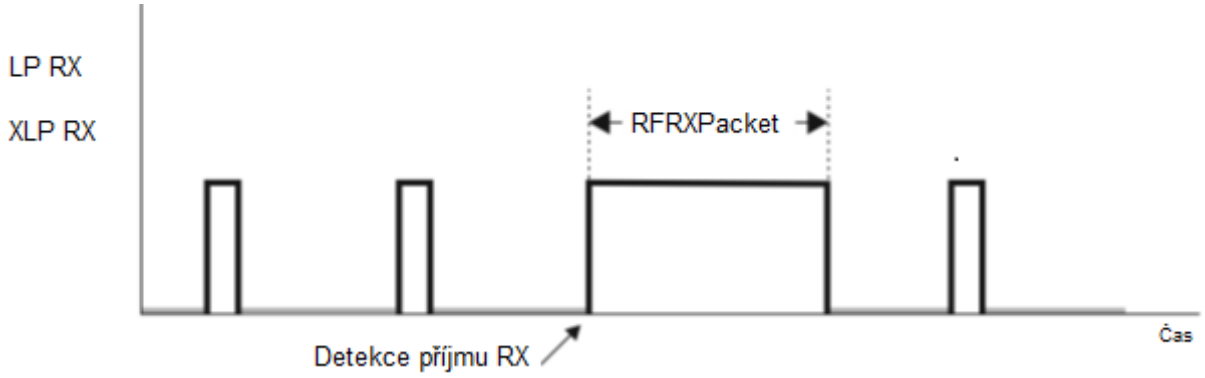
Tab. 3 Doba potřebná pro vyslání paketu [2]

Délka DLEN (B)	Peer-to-peer (ms)	IQMESH bez směrování (ms)	IQMESH se směrování (ms)
1	10	13	16
10	12	15	18
64	35	39	42

V systému jsou definovány tři režimy spotřeby:

- STD – standartní režim,
- LP – nízká spotřeby,
- XLP – velmi nízká spotřeba.

Časový průběh a princip snížení spotřeby je vysvětlen na obrázku *Obr. 2* v kapitole 1.2.1. Na obrázku *Obr. 6* je znázorněna odezva systému na příjem paketu.

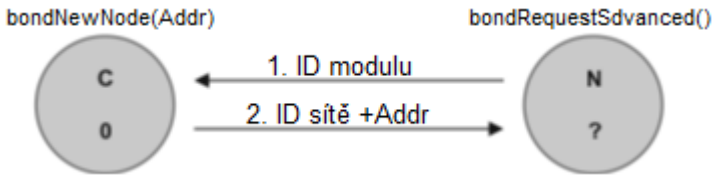


Obr. 6 Reakce na příjem paketu

3.2.2.2 Bonding

Bonding znamená přiřazování nodů ke koordinátorovy a tím vytváření struktury sítě. Při bondingu je koordinátorem přiřazena konkrétnímu nodu adresa. Adresu může specifikovat uživatel, jinak je adresa rovna počtu nodů v síti, které jsou nabondovány, plus jedna.

Tato adresa pak může být použita při směrování. Průběh bondingu je zobrazen na obrázku *Obr. 7*. [2]



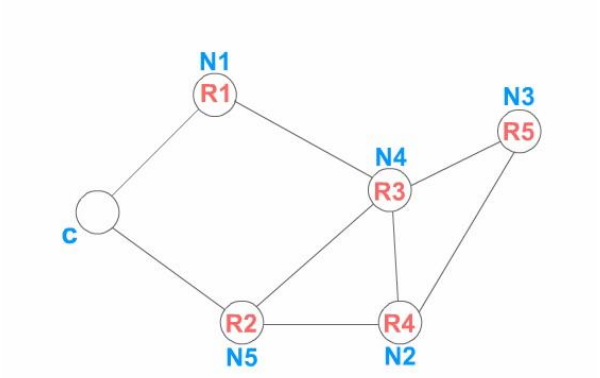
Obr. 7 Průběh bondingu [2]

V případě, že chceme některé zařízení, které je nabondováno na koordinátor, přemístit a nabondovat na jíný koordinátor, je za potřebí provést unbond. To je v podstatě opačný postup bondu, kdy si koordinátor smaže z EEPROM paměti záznam o přiřazeném nodu a nodu je smazána přiřazená adresa. [2]

3.2.2.3 Discovery

Při rozmísťování již bondovaných zařízení v topologii sítě může být dodržen statický vektor sítě a zařízení jsou podle adres postupně rozmisťována od koordinátora dále, nebo jsou rozmístěna náhodně. Pokud jsou rozmístěna náhodně je zapotřebí provést discovery, tj. průzkum sítě. [2]

V průběhu discovery je nodům přiřazena virtuální adresa, která může být použita ke směrování v některých algoritmech. V obrázku *Obr. 8* je znázorněn stav sítě po discovery. Modré adresy jsou adresy přiřazené po bondu. Červené jsou virtuální adresy přiřazené pomocí discovery. Discovery se provádí až po rozmístění a instalaci zařízení na svoje místo. Bond se dá provádět před instalací tzv. na stole.



Obr. 8 Discovery

Discovery rozdělí a setřídí nody do skupin a to tak, aby v jedné skupině byly všechny nody dostupné koordinátorem stejným počtem hopů. Počet skupin může být uživatelem limitován. Discovery by mělo být provedeno při každé změně topologie sítě. [2]

3.2.2.4 Směrování

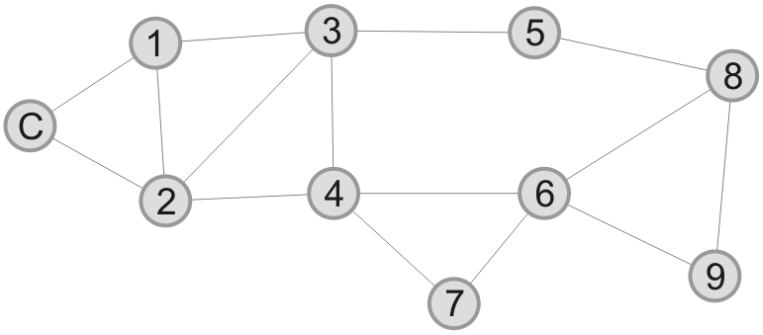
Směrování umožňuje zasílání paketů zařízením, která nemají přímou cestu k odesílateli. Odesílání paketů je pak prováděno pomocí jiných nodů, které jsou po cestě k požadovanému zařízení. Každý z těchto nodů po cestě, přesměrovává paket pouze jednou, aby nedošlo ke smyčkám. Směrování je nezávislé na adresování. Paket je směrován skrze nody v daném pořadí, to se nazývá vektor směrování (routing vector). Odesílání musí probíhat v definovaném timeslotu s definovanou periodou. Protokol dovoluje paket ignorovat všem zaříním která se nenacházejí v definovaném vektoru. [2] [6]

V efektivně postavené IQMESH síti by mělo mít každé zařízení v dosahu alespoň dvě jiná zařízení, tak aby při poruše jednoho z nich mohlo dojít ke změně směrování a zachování dostupnosti ostatních zařízení. Směrovací algoritmus by měl být vybrán podle požadované rychlosti odezvy a podle nároků na spotřebu. [2]

V IQRF protokolu je definováno několik typů směrování, a to: [6]

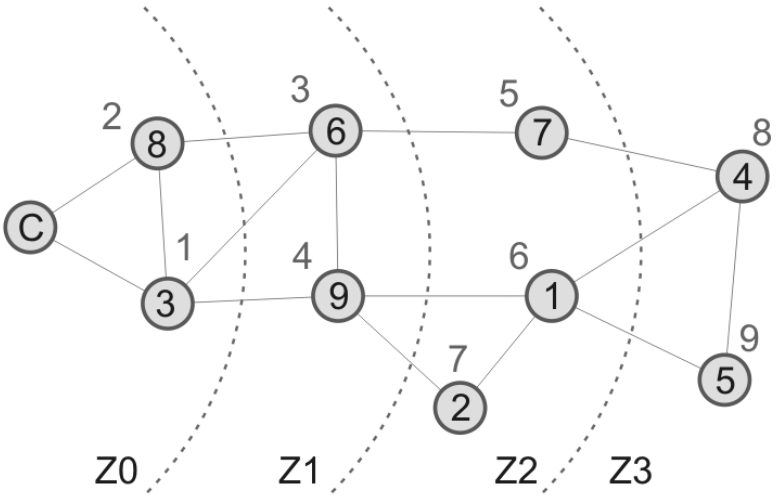
- SFM (Static Full Mesh),
- DFM (Discovered Full Mesh),
- DFM2B (Discovered Full Mesh, 2B),
- Tree.

SFM algoritmus pracuje na principu zaplavení popsaném v kapitole 1.3.1. V síti kde je použit tento algoritmus lze adresovat až 240 zařízení. Směrovací vektor má fixní a pořadí. Rozmístění zařízení musí respektovat pořadí adres. V tomto případě se neprovádí discovery. Adresy se počítají od koordinátora, tak jak je to vidět na obrázku *Obr. 9*. [2] [6]



Obr. 9 Topologie a adresování sítě při použití SFM [2]

DFM algoritmus je podobný SFM algoritmu jen se nepoužívají adresy zařízení, ale virtuální adresy přiřazené pomocí discovery. V jedné síti může být až 240 zařízení, z toho jeden koordinátor a 239 nodů. Před instalací se provede bonding. Nody jsou pak rozmísťovány náhodně. Po rozmístění nodů se spustí discovery. Discovery se pak musí provádět při každé změně sítě. Na obrázku *Obr. 10* je síť rozdělená do skupin a adresovaná virtuálními adresami po provedení discovery. [2]



Obr. 10 Přeadresovaná síť [2]

DOM je speciální případ DFM algoritmu. Liší se v tom, že cesty jsou optimalizovány počtem hopů. [2]

DFM2B je podobný algoritmus jako DFM. Používá 2B adresaci na rozdíl od DFM a SFM kde je adresa 1B. Tímto algoritmem lze adresovat až 65 000 zařízení, 256 v páteřní síti. Tento algoritmus se využívá v zřetězených sítích mesh.

Posledním směrovacím algoritmem je strom. Tento algoritmus postrádá redundanci. Je nejrychlejší cestou jak posílat data od nodu na koncentrátor. Bohužel v aktuální verzi OS není plně implementován a testován. [2]

Dalším silným nástrojem IQRF protokolu je implementace různých typů sběru dat. Prvním je standardní dotazování se na určité zařízení. To je výhodné při potřebě číst data jednotlivých nodů selektivně.

Další možností je typ sběru dat FRC (Fast Response Command). Tento typ sběru dat je využíván tam, kde je zapotřebí rychlá odpověď a čtou se stejná data z celé sítě, nebo podsítě. Systém definuje několik druhů FRC. Jsou to: [2]

- standard FRC – od každého nodu jsou v paketu přenášeny jen 2 B dat,
- rozšířený FRC – od každého nodu mohou být přenášena data až 30 B.

Dále se FRC může chovat jako selektivní a neselektivní. Selektivní FRC přenáší data jen o požadovaných nodů uživatelem. Neselektivní pak od všech. [2]

Standartní FRC má omezený počet dotazovaných nodů, podle velikosti přenášených dat jak je uvedeno v tabulce *Tab. 4.* V tabulce *Tab. 5* je uvedeno porovnání časů přenosu dat standardního FRC s rozšířeným FRC. [2]

Tab. 4 Omezení standard FRC

Délka dat	**Počet nodů selektivní FRC**	**Počet nodů neselektivní FRC**
2 bit	-	239
1 byte	62 vybraných z adres 1-239	prvních 62, adresa 1-62
2 byte	30 vybraných z adres 1-239	prvních 30, adresa 1-30

Tab. 5 Rychlost odezvy FRC

Počet nodů	**Standard FRC**	**Rozšířený FRC**	
		Standard spotřeba	**Nízká spotřeba**
10	1,59 s	1,83 s	2,43 s
239	31,36 s	36,18 s	48,23 s

3.2.3 DPA Framework

DPA framework zabezpečuje komunikaci mezi moduly pomocí protokolu DPA a umožňuje využívat hardwarové profily. DPA framework je nadstavba OS, která

zjednodušuje přístup k datům v síti IQRF, kde mohou být použita zařízení různých výrobců, tím snižuje čas potřebný na vývoj a nasazení IQRF.

HWP (Hardware Profile) se využívá ke konfiguraci koncových zařízení bez dodatečného programování. Profil je stažen ze stránek výrobce a nahrán do zařízení. Tím je zařízení nastaveno pro dané použití. HWP zpravidla vydávají výrobci zařízení na platformě IQRF.

DPA (Direct Accesss Protokol) je jednoduchý protokol pro ovládání zařízení v IQMESH síti. Koordinátor a nody mohou být ovládány přes SPI, nebo UART rozhraní. DPA protokol lze využívat jen u modulů s označením DCTR. [7]

Rozdíl při použití DPA oproti psaní uživatelské aplikace v OS je ten, že v uživatelské aplikaci si musí uživatel napsat a zabezpečit linkovou vrstvu komunikace v IQRF síti. DPA framework již tuto linkovou vrstvu má implementovánu a odladěnu s ohledem na rychlost komunikace a nízkou spotřebu.

Pro obsluhu vlastních zařízení lze v DPA naprogramovat Custom DPA handler. Ten je psána v jazyce C a dovoluje volat funkce DPA frameworku pomocí DPA API. V Custom DPA handleru je možné implementovat vlastní logiku aplikace koncového zařízení, obsluhovat události systému a pracovat s perifériemi zařízení. [7]

DPA framework je velmi silný nástroj jak pro vzdálenou správu sítě, tak pro rychlý vývoj aplikací. Velkou výhodou je implementace odzkoušené linkové vrstvy optimalizované na nízkou spotřebu a maximální rychlost přenosu dat.

3.3 Vývojové nástroje

IQRF platforma má několik startovacích sad pro rychlé seznámení se s hardwarem a softwarem pro vývoj.

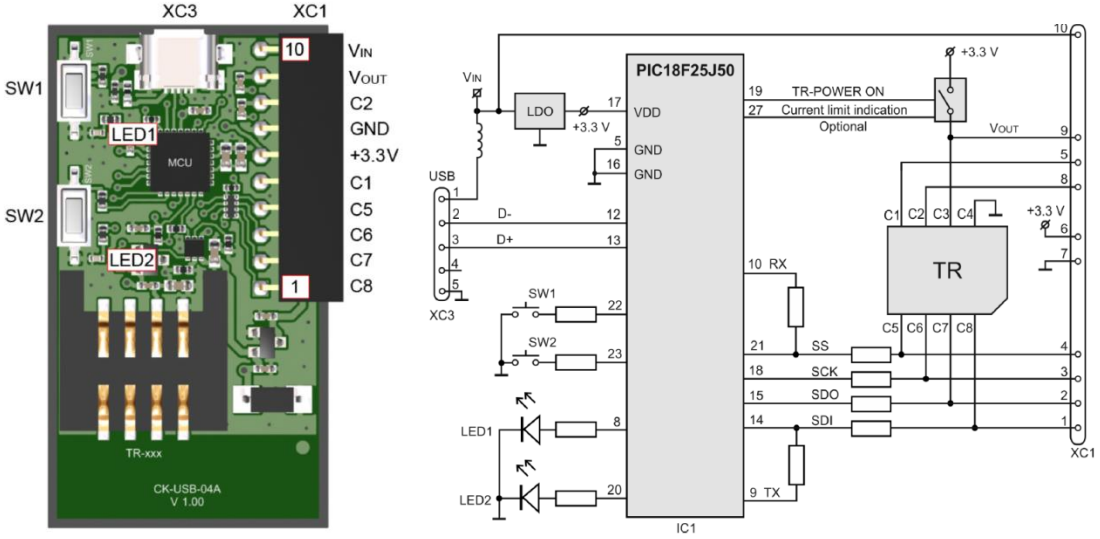
3.3.1 Hardware pro vývoj

Základním hardware pro vývoj aplikací je programátor CK-USB04A, který je na obrázku *Obr. 11*. Pomocí tohoto programátoru lze programovat a nahrávat uživatelské aplikace. Programátor lze využít také jako USB bránu pro testování IQRF sítě. Společně s programovacím nástrojem lze testovat i aplikace využívající SPI a UART. Vše se konfiguruje v programovacím nástroji IQRF IDE. Programátor je k počítači s vývojovým

nástrojem připojen pomocí USB, které je na obrázku *Obr. 11* označeno XC3. Programátor je vybaven dvěma tlačítky SW1 a SW2 jejich funkce je podrobně popsána v manuálu [8]. LED diody LED1 a LED2 signalizují stav modulu. Svorkovnici XC1 lze využít pro napájení programátoru, nebo externího zařízení. Dále jsou na této svorkovnici piny C1 až C8. Jejich funkce závisí na tom v jakém režimu se programátor a transceiver nachází, viz tabulka *Tab. 6.* [8]

Tab. 6 Tabulka funkcí PIN C1 až C8

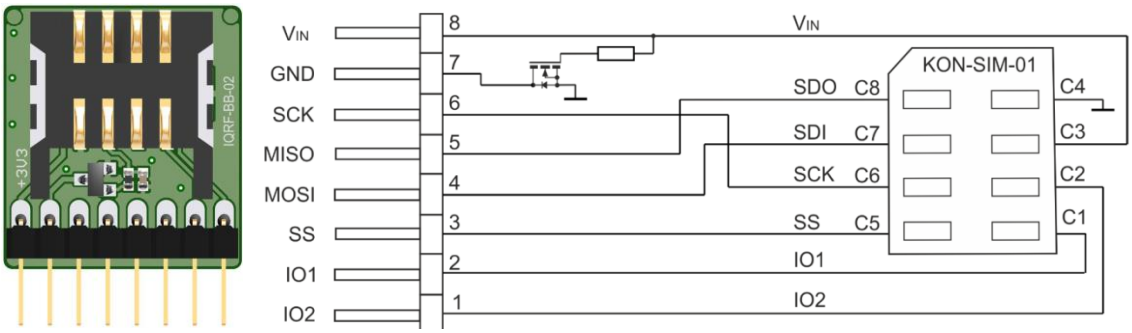
PIN	Funkce
C1	IO/RX/SDO-
C5	IO/TX/SS
C6	IO/SCK
C7	IO/SDI
C8	IO/RX/SDO



Obr. 11 Programátor CK-USB-04A [8]

Dalším potřebným hardwarovým vybavením pro vývoj na platformě IQRF jsou adaptéry pro housing transceiverů. Adaptérů je celá řada a jejich výběr závisí na zvolené aplikaci.

Jedním typem adaptéru je IQRF-BB-01, který je na obrázku *Obr. 12.* Tento adaptér je vhodný pro vývoj prototypů na nepájivých polích. Byl vyvinut speciálně pro vývoj aplikací na platformách jako je BeagleBone, Raspberry Pi, nebo Arduino. [9]



Obr. 12 Adaptér IQRF-BB-01 [9]

3.3.2 Softwarové prostředky

IQRF platforma nabízí kromě vlastního vývojového prostředí ještě mnoho příkladů, jak s využitím DPA frameworku, tak uživatelských aplikací pro OS. Všechny aktuální verze se dají stáhnout na stránkách výrobce.

Pro překlad kódu psaného v jazyce C je využíván volně dostupný překladač CC5X. Tento překladač je speciálně vyvinut pro programování PIC čipů, které jsou použity na transceiverech.

Dále je výrobcem poskytováno IQRF IDE (Intergrated Development Enviroment). Je to nástroj pro správu IQRF sítě, vytváření IQRF aplikací, ladění aplikací a nahrávání programu do modulů pomocí programátora CK-USB-04A.

IQRF IDE je nástroj ve kterém je možné plně programovat všechny druhy aplikací. Lze v něm spravovat a nahrávat do modulů HWP profily, vytvářet uživatelkou aplikaci pro moduly, psát DPA Custom handler aplikace a ladit je. IDE při překladu kódu volá nainstalovaný kompiler CC5X a vrací jeho výstup. IDE má několik velmi užitečných nástrojů. Jedním z nich je správa a vytváření sítě. V tomto modulu lze provádět bond a discovery vytvořené sítě která, je pak graficky znázorněna.

3.4 Porovnání s konkurencí

Vybraní konkurenti pro porovnání s platformou IQRF jsou ZigBee a Z-Wave. Jsou to bezdrátové technologie pro přenos malých a středních dat na krátké vzdálenosti při malých rychlostech. Jsou navrženy pro vzdálený monitoring a řízení.

ZigBee je otevřený komunikační protokol pro bezdrátovou komunikaci založený na standardu IEEE 802.15.4. Z tohoto standardu přebírá 1. a 2. vrstvu komunikačního protokolu.

První vrstva zabezpečuje fyzickou vrstvu sítě PHY a druhá kontrolu nad přenosovým médiem sítě MAC. ZigBee standard nad těmi vrstvami zabezpečuje síťovou a aplikační vrstvu. [10]

Stejně jako IQRF i ZigBee dovoluje používat mesh sítě, ale také standardní topologie typu strom a hvězda. Tato technologie dovoluje adresovat více než 65 000 zařízení. ZigBee pracuje v bezlicenčních pásmech. Nejčastěji na 2,4 GHz kde má nejvyšší přenosovou rychlost 250 kbit/s. Na pásmu 868 MHz, které je nejčastěji používané v Evropě, je přenosová rychlost 20 kbit/s s použitou BPSK modulací. [10]

Standard ZigBee je vyvíjen aliancí „ZigBee.org“. Tato aliance je sdružením organizací, které podporují vývoj standardu a jeho propagaci. Pokud chce někdo vyvíjet platformu pro ZigBee, musí tato platforma projít certifikací. [10]

Jelikož je ZigBee otevřený standard, tak vývojové sady a zařízení implementuje mnoho výrobců. Pro porovnání byl zvolen EM357 SoC výrobce SiliconLabs. Stejně tak jako s hardware je to i se softwarem pro vývoj. Ten dodává výrobce platformy podle hardware, na kterém má software běžet.

Z-Wave není otevřeným standartem tak jako ZigBee. Tato technologie byla vyvinuta společností Zensys jako proprietární bezdrátový komunikační standard. Standard je přístupný jen členům asociace Zensys/Sigma Design. Všechny výrobky, které jsou na platformě Z-Wave postaveny musí být certifikovány. [11]

Stejně tak jako předešlé technologie, Z-Wave pracuje s mesh topologií sítě. Rozdílem v implementaci vůči IQRF je to, že každé zařízení může komunikovat s libovolným dalším zařízením v síti přímo. V případě IQRF toto nelze, komunikaci evokuje koordinátor. V síti je možné adresovat 232 zařízení. V Evropě je pro komunikaci používáno pásmo 868 MHz. V tomto pásmu je možné přenášet 9600 kbit/s a 40 kbit/s. Je použita GFSK modulace. [11]

Jelikož je Z-Wave uzavřeným standardem, tak hardware a vývojové sady vyrábí jen jedna organizace – Sigma Design. Pro naše porovnání je vybrán modul ZM4102 SoC. V následující tabulce *Tab. 7* jsou porovnány vlastnosti jednotlivých platforem.

Každá platforma má svoje výhody a nevýhody. Platformy ZigBee a Z-Wave jsou náročné na vývoj hardwaru a softwaru. Nelze je použít bez programování. Programování je složité

a vyžaduje testování, což prodražuje vývoj. Dále ho prodražuje nutnost certifikace a vstup do aliance.

Tab. 7 Porovnání HW konkurence [11] [10] [3]

Název	**EM 357 ZigBee**	**ZM4102 Z-Wave**	**DCTR72D IQRF**
Procesor	ARM cortex M3, 32 bit 6/12/24 MHz	8051 CPU	PIC16LF1938–I/MV, 8 bit, 32 MHz
Paměť flash	192 kB	128 kB	256 kB EEPROM
Paměť RAM	12 kB	16 kB SRAM	1 kB
Kryptování	AES128	AES128	proprietální
Periférie	UART/SPI/ TWI/ADC	USB/UART/SPI/ PWM/ADC	UART/SPI/I^2C/ 1-Wire/ADC/PWM
GPIO	24	30	2
RF pásmo	2,4 GHz/868 MHz	868 MHz	433/868 MHz
RF modulace	OQPSK/BPSK	GFSK	GFSK
Přenosová rychlost	250 kbit/s, 20 kbit/s	9.6 kbit/s	19,836 kbit/s
RFIC RF citlivost	-102 dBm	-105 dBm	-106 dBm
RFIC výstupní výkon	8 dBm	6 dBm	11 dBm
RF dosah	30 m uvnitř, 100 m venku	30 m uvnitř, 100 m venku	100 m uvnitř, 500 m venku
Spotřeba SLEEP	400 nA	1 µA	2,9 µA
Spotřeba RX	26 mA	32 mA	12,3 mA
Spotřeba TX	31 mA	32 mA	19 mA
Napájení	2,1-3,6 V	2,3-3,6 V	3,1-5,3 V
Montáž	SMD	SMD	Do SIM držáku
Provedení	SoC	SoC	DPS velikosti SIM
Cena	245 Kč	178 Kč	326 Kč

Vývoj v IQRF je v porovnání s konkurencí jednoduchý, některé úlohy lze udělat i bez programování a při použití DPA frameworku jsou implementovány všechny síťové vrstvy. Tím odpadá testování v různých modelech nasazení. Vývoj je jednodušší, mnohem rychlejší a levnější. Vstup do aliance není podmínkou a certifikace není nutná.

ZigBee je nejuniverzálnější platforma pokrývající nejširší spektrum využití. Pomocí technologie Zigbee je možné postavit rozsáhlé sítě, kde může být více jak 65 000 zařízení. Testovaný hardware je nejvýkonnější, s nejlepší spotřebou.

Z-Wave je platforma s nejdokonalejší implementací mesh sítí. Testovaný hardware není tak výkonný jako ZigBee a má nejhorší spotřebu. Dále má velmi nízkou rychlost přenosu a srovnatelný dosah s platformou ZigBee.

Platforma IQRF není tak univerzální jako ZigBee, implementace mesh protokolu není tak robustní jako v předešlých technologiích a má nejhorší výkon, co se týká hardware. Naproti tomu vyniká délkou dosahu komunikace při příznivé spotřebě. Její implementace mesh je jednodušší a tím snadněji implementovatelná. I přes vyšší cenu modulu, je nakonec cena vývoje hardware levnější, protože jeho montáž na DPS je velmi jednoduchá. Zvládne ji i domácí kutil.

Technologii IQRF bych zvolil vždy tam, kde není nutná vysoká spolehlivost komunikace, vysoké zabezpečení a zařízení nevykonávají složité činnosti. Jednoznačně je vývoj v této platformě jednodušší, rychlejší a levnější. V následující tabulce *Tab. 8* je závěrečné hodnocení platforem.

Tab. 8 Závěrečné hodnocení

Vlastnost	**ZigBee**	**Z-Wave**	**IQRF**
Hardware	+++	+	+
Vývoj hardware	+	+	+++
Vývoj software	+	+	+++
Zabezpečení	+++	+++	+
Implementace mesh	+++	+++	+
Aliance	nutná	nutná	není nutná
Certifikace	nutná	nutná	není nutná

4 Teoretická východiska

Tato část práce se zabývá teoretickým návrhem řešení úloh v jednotlivých oblastech použitelnosti. Jsou to tyto oblasti:

- Zabezpečovací technika,
- Přenos procesních signálů,
- Domovní automatizace.

V těchto oblastech bude zhodnocena použitelnost platformy IQRF s ohledem na splnění norem a trendů pro dané oblasti použitelnosti.

4.1 Zabezpečovací technika

Bezdrátové poplachové, zabezpečovací a tísňové systémy jsou na trhu velice žádané širokou veřejností vzhledem k jednoduchosti jejich instalace.

Bezdrátové PZTS se stejně tak jako drátové skládají z několika základních částí. Těmito částmi jsou:

- Ústředna je nejdůležitější částí zabezpečovacího systému, obsahuje několik komunikačních rozhraní: jedno pro bezdrátovou komunikaci s detektory, další pak pro komunikaci s PCO, nebo přímo s majitelem. Umožňuje ovládání a indikaci stavu PZTS.
- Čidlo (detektor) je to zařízení, které pomocí bezdrátové komunikace přenáší informace do ústředny. Přenáší informace o svém stavu a o stavu střeženého objektu, nebo prostoru.
- Signalizační zařízení je zařízení, které zajišťuje indikaci výstupních informací z ústředny. Signalizace je akustická a optická.
- Doplňkové ovládací zařízení je zařízení, které dovoluje ústřednu ovládat a uvádět do stavu zastřežení, nebo do klidového stavu.

Detektory jsou z pravidla napájeny z vestavěných baterií, proto je u nich kladen vysoký důraz na nízkou spotřebu a dlouhou životnost baterie. Ústředna je většinou napájena z externího zdroje, baterie využívá jen jako záložní zdroj napájení.

Komunikace mezi detektory, signalizačním zařízením, doplňkovým ovládacím zařízením a ústřednou probíhá bezdrátově zpravidla v bezlicenčním pásmu na frekvencích 868 MHz

nebo 433MHz. Dosah komunikace je závislý na vlivu prostředí a zvolené frekvenci. Ve venkovním prostředí to jsou stovky metrů, uvnitř budov se dosah razantně zkracuje. Komunikace mezi ústřednou a čidlem se dělí na jednosměrnou a obousměrnou.

Jednosměrná komunikace je vyvolávána na straně čidla. Při narušení čidlo posílá informaci na ústřednu a ta ji zpracuje. Nevýhodou této komunikace je, že ústředna neví nic o aktuálním stavu svých čidel. Pokud dojde k sabotáži čidla, ať už zarušením nebo fyzickým poškozením, ústředna to nezjistí. Výhodou je, že čidla komunikují jen v případě narušení, což výrazně prodlužuje životnost baterie. Tato nevýhoda se ošetřuje pravidelnou komunikací čidla jednou za definovaný čas, tak aby ústředna věděla, že je čidlo v pořádku. S ohledem na životnost baterie, je ale tato komunikace prováděna zřídka a ústředna vyhodnocuje poruchový stav až po několika neúspěšných intervalech. Tím se doba zjištění sabotáže nebo poruchy čidla prodlužuje.

Obousměrná komunikace funguje na principu, že aktivně komunikují všechna zařízení v síti. Komunikace probíhá na dvou kanálech, na jednom komunikují čidla a na jednom ústředna. Pokud dojde k zarušení signálu, zařízení se přeladí na jiný kanál. Tento typ komunikace se nazývá duplexní. Ústředny jsou odolnější k sabotážím a poruchám čidel.

U obou typů komunikace může dojít ke kolizi při komunikaci – vysílá více zařízení najednou a ústředna není schopna přijmout data.

Čidla se dají dělit pomocí mnoha hledisek – pro výukovou úlohu bylo zvoleno jednoduché PIR čidlo. Na většinu čidel z hlediska přenášené informace lze nahlížet jako na digitální dvoustavovou hodnotu. Existují i čidla přenášející analogovou hodnotu, ale nebudeme je v této práci do návrhu uvažovat.

4.1.1 PIR čidlo

PIR (Passive Infra Red Sensor) čidlo patří mezi nejčastěji používané čidlo. Čidlo funguje na principu pyroelektrického jevu, při kterém se pyroelektrické materiály deformují vlivem změny teploty. Změna teploty vyvolá deformaci a tím se díky piezoelektrickému jevu indukuje na povrchu materiálu elektrický náboj. [12]

Na povrch pyroelektrického materiálu je optickou soustavou promítán obraz okolí (Fresnelova čočka). Pokud v okolí nastane tepelná změna, např. projde člověk, je materiál

změnou teploty v části povrchu deformován a je možné detekovat indukovaný náboj na jeho povrchu. [12]

Využití senzoru pro detekci pohybu se stalo velice populárním v zabezpečovací technice a v aplikacích pro úsporu energie. Přestože je možné využívat i jiné typy senzorů (termistory, termočlánky), jsou senzory založené na pyroelektrickém jevu v těchto odvětvích využívány téměř výhradně pro svou jednoduchost, nízkou cenu, vysokou spolehlivost a velký rozsah tepelných změn. [12]

4.1.2 Legislativa

Prvky systému EZS musí být certifikovány. Certifikaci provádí zkušebna dle předepsaných požadavků. Tyto požadavky jsou dány souborem norem ČSN EN 50131. Normy jsou vypracovány evropskou komisí CENELEC/TC79. V České republice jsou schvalovány Úřadem pro technickou normalizaci, metrologii a zkušebnictví. [12]

V normě ČSN EN 50131-1 ed. 2 jsou uvedeny technické stupně bezpečnosti, viz tabulka Tab. 9. Tyto technické stupně stanovují kritéria na výbavu a funkci jednotlivých komponent.

Tab. 9 Technické stupně zabezpečení z normy ČSN EN 50131-1 ed.2

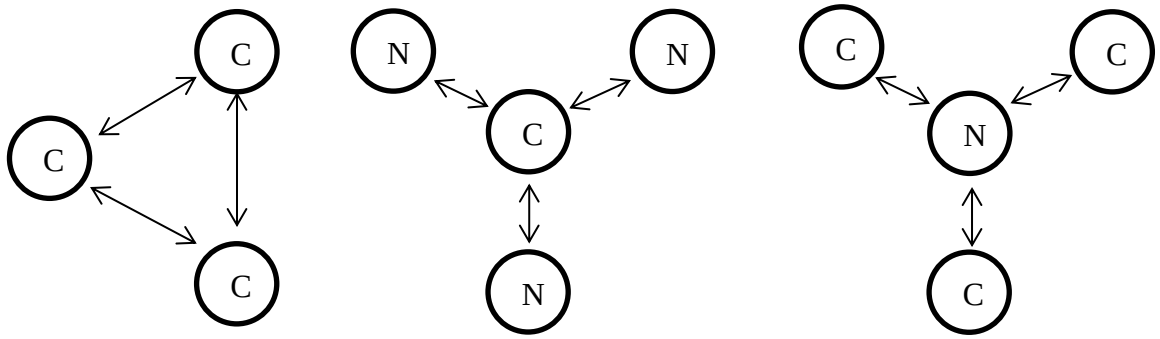
Stupeň	Míra rizika	Typ narušitele
1	nízké	Narušitel má malou znalost PZTS, omezený sortiment snadno dostupných nástrojů
2	nízké až střední	Narušitel má určité znalosti PZTS a používá základní sortiment nástrojů a přenosných přístrojů
3	střední až vysoké	Narušitel je obeznámen s PZTS a má úplný sortiment nástrojů a přenosných elektrických zařízení
4	vysoké	Narušitel má možnost zpracovat podrobný plán vniknutí a má kompletní sortiment zařízení v četně prostředků pro náhradu rozhodujících prvků v PZTS.

Jelikož se práce zabývá využitím bezdrátové technologie, bude nás ze zmíněného souboru norem zajímat norma ČSN EN 50131 – 5 – 3, která se nazývá „Poplachové systémy – elektrické zabezpečovací systémy – Část 5-3: Požadavky na zařízení využívající bezdrátové propojení“. V této normě jsou shrnuty požadavky na bezdrátové PZTS systémy pro jednotlivé stupně zabezpečení.

4.1.3 Návrh použití IQRF

Pomocí platformy IQRF jsme schopni implementovat oba typy komunikace jak jednosměrnou, tak obousměrnou.

Jednosměrnou komunikaci je možné v IQMESH protokolu definovat jako síť peer-to-peer. Nelze však použít topologii hvězdy, kterou IQMESH protokol obsahuje. Tuto topologii nelze použít proto, že v IQMESH se hvězda skládá z jednoho koordinátora a až z 239 nodů. Komunikaci řídí a podněcuje koordinátor a asynchronní komunikace z nodů není autory IQMESH doporučována kvůli kolizím. Porovnání sítí je na obrázku *Obr. 13*. Případ pro řešení jednosměrné komunikace EZS je obrácený. To znamená, že střed sítě tvoří ústředna, definovaná jako node, a koncové senzory, které mají vlastnosti koordinátora.

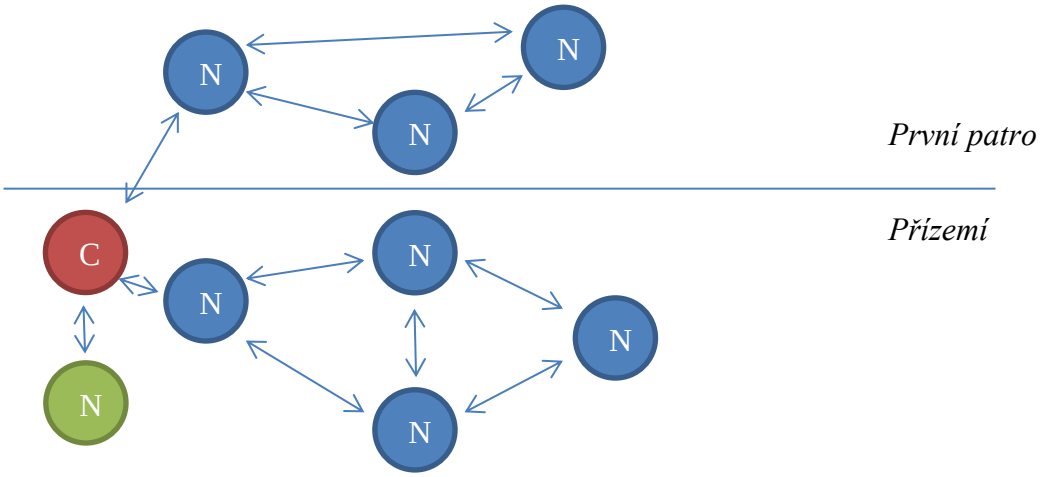


Obr. 13 Topologie peer-to-peer, topologie IQMESH star, topologie potřebná pro realizaci úlohy jednosměrné komunikace EZS

V takovéto síti bude docházet ke kolizím. Proto bude nutné vyžadovat potvrzení přijetí informace ústřednou.

V datech o senzoru by se přenášel jeden byte, kde by jednotlivé bity nesly informaci o stavu čidla. Čidla by se po definovaném čase automaticky hlásila ústředně. Pokud by se čidlo neohlásilo po dobu definovaného násobku času ústředně, pak by ústředna vyhlásila závadu na čidle. Z hlediska spotřeby je posílání tak malých datových rámců velice úsporné. Nevýhodou v tomto případě je, že se pro tuto síť nedá použít DPA framework – autor by si musel naprogramovat linkovou vrstvu komunikace a odladit vzhledem ke spotřebě a spolehlivosti sám. Další nevýhodou této topologie je, že všechny senzory musejí být v dosahu ústředny. Nelze tak využívat výhod sítě mesh a její optimalizace pro úsporu napájení.

Obousměrnou komunikaci je možné realizovat pomocí mesh sítě, po které s jednotlivými čidly komunikuje ústředna. Informace o narušení zasílají senzory ústředně asynchronně. Asynchronní přenos není výrobcem platformy IQMESH doporučován kvůli kolizím. V mesh síti lze na vyčítání stavů jednotlivých senzorů používán hromadný dotaz FRC. Komunikace by probíhala v nastavené periodě. Data jsou stejná jako u jednosměrné komunikace. Topologie sítě může být složitější a vypadat tak jak je uvedena na obrázku *Obr. 14*.



Obr. 14 Topologie mesh sítě EZS

Na tomto obrázku je vidět topologie mesh, kde koordinátorem je ústředna – červená buňka, nody jsou jednotlivá čidla – modré buňky, a doplňkové ovládací zařízení (klávesnice) je také nodem – zelená buňka. Doplňkové ovládací zařízení se nachází v přízemí, kde je i ústředna a skupina čidel zabezpečující tento prostor. V prvním patře jsou jen čidla zabezpečující prostor prvního patra. V prvním a druhém patře je jeden node – čidlo, které propojuje ústřednu s dalšími čidly. To je právě výhodou mesh sítí, ve kterých nemusí mít čidla přímé spojení s ústřednou.

Na toto řešení je možné využít DPA frameworku. Tím se ušetří čas vývoje a testováním linkové vrstvy. Další výhodou je možnost použití režimů nízké spotřeby. Problémem zůstávají kolize. Platforma IQRF dovoluje vysílání jen po jednom kanálu, proto je riziko kolizí při nekoordinovaném asynchronním vysílání poměrně velké. Řešením by bylo mít v ústředně zabudovány dva transceivery. Jeden na realizaci IQMESH pro přenos periodických FRC dotazů. Druhý transceiver by naslouchal na jiném kanálu a přijímal asynchronní zprávy od koncových zařízení. Koncová zařízení by před odesláním asynchronní zprávy přeladila na druhý kanál, kde naslouchá ústředna, a odeslala zprávu. Po přijetí potvrzení, že ústředna alarm přijala, by se koncové zařízení přeladilo zpět na kanál IQMESHe. Kolize se v tomto

případě musejí řešit jen na asynchronním kanálu. Čas potřebný na nahlášení alarmu by nenesl riziko zpoždění při kolizi s FRC telegramem.

Co se týká rychlosti odezvy, je závislá na počtu nodů v síti. V extrémním případě, kdy bude v síti 239 zařízení, může při režimu velmi nízké spotřeby trvat odezva na hromadný dotaz FRC, který sbírá data ze všech senzorů, až jednu minutu. Pokud v této době na jednom z těchto čidel nastane alarm a dojde ke kolizi, bude čidlo čekat na dokončení FRC, než bude alarm přenesen na ústřednu, tedy až jednu minutu.

Spotřeba v obousměrném režimu komunikace bude také násobně vyšší než u jednosměrné komunikace. Je to dáno jak dotazem FRC, tak tím, že nody propojující ostatní nody na patře s ústřednou budou více vytěžovány komunikací. Přenáší se přes ně komunikace z – a na koncové nody. Na druhou stranu bude možné využít režim nízké spotřeby DPA frameworku, což by mělo energii uspořit.

S ohledem na normu ČSN EN 50131-5-3 a její požadavky na jednotlivé stupně bezpečnosti nejsme bez vlastní implementace linkové vrstvy, vyřešení kolizí, detekce zarušení a dalších předepsaných požadavků schopni splnit ani první stupeň bezpečnosti.

Z hlediska možných kolizí komunikace v obou případech použití je zapotřebí implementovat protokol pro detekci a ošetření kolizí. Například CSMA, nebo CSMA/CD. Jsou to pravděpodobnostní protokoly pro synchronizaci přístupu k přenosovému médiu pomocí naslouchání na lince před zahájením vysílání. Při obsazeném médiu je náhodně vygenerován timeout, po kterém se pokus opakuje.

Dále je zapotřebí vyřešit bezpečnost systému a odolnost vůči zarušení. V OS IQRF je možné měnit kanály programově. Měl by se tedy implementovat algoritmus automatického přelaďování kanálů. Například protokol FH (Frekvence Hooping) který využívá technologie BlueTooth. Problémem je vlastní detekce zarušení. V případě jednosměrné ani obousměrné komunikace nejsme schopni rozeznat chybu čidla od sabotáže – zarušení senzoru, nebo zarušení vlivem přehlcení frekvenčního pásma. Pak je otázkou, zda je dobrým řešením přelaďovat celý systém na jiný kanál automaticky. U sítě s peer-to-peer topologií je toto možné provést. U mesh sítí je tato operace nebezpečná a může při ní dojít k rozpadu sítě.

Zabezpečení dat přenášených v síti je řešeno výrobcem IQRF platformy. Je možné použít proprietární šifrování. Popis tohoto šifrování není veřejný. Jelikož obě dvě sítě fungují na jednom kanále, je jednoduché odposlechnout jejich rámec, nebo ji zarušit.

V každém případě pokud by se měly do zařízení implementovat algoritmy CSMA, nebo algoritmy automatického přeladění kanálu, bylo by nutné je programovat na úrovni uživatelské aplikace za využití volání funkcí OS. V rámci této aplikace by bylo nutné naprogramovat linkovou vrstvu komunikace v síti a odladit ji. Nepoužitím DPA frameworku, nebo IQMESH protokolu přicházíme o velkou část platformy IQRF a v podstatě používáme z platformy jen hardware.

4.1.4 Zhodnocení použitelnosti IQRF

Implementace IQMESH se principiálně neshoduje s potřebami pro použití v zabezpečovací technice. Není navržena a implementována pro asynchronní přenosy dat. Komunikaci řídí a vyvolává vždy jeden prvek sítě a to je koordinátor.

Vzhledem k požadavku na jednoduchost instalace PZTS jsou mesh sítě nevhodné a implementace IQMESH taktéž. Pro správný návrh, který by zabezpečil kritéria předepsaná legislativou, je nutná znalost jak mesh sítí obecně, tak jejich implementace v IQMESH. Parametry jako je rychlost odezvy a délka životnosti baterií jsou dány právě návrhem sítě a počtem zařízení v síti. Proto by se musela posuzovat každá aplikace zvlášť, nebo by systém musel být navržen tak, aby nabízel jen jednu možnost nasazení. Tím by pak byla jasně daná počitatelná omezení obecné maximální aplikace daného systému.

Sám výrobce IQRF platformy neuvádí, že by platforma byla vyvíjena pro oblast použití v elektronických zabezpečovacích systémech. Po konzultaci s výrobcem a hledáním v různých zdrojích, jsem nenašel žádnou referenci na komerční certifikované využití této platformy pro PZTS. Z tohoto důvodu docházím k závěru, že platforma, tak jak je nyní navržena – bez úprav a vlastní implementace linkové vrstvy, není vhodná pro toto využití. Úlohy v ní implementované, jako jsou PIR čidla, magnetické kontakty atd. jsou zařaditelné spíše do kategorie inteligentních domů (Smart Home). Výrobce IQRF stále vyvíjí operační systém a dává mu nové funkce. Nyní je před vydáním OS verze 4, která by mohla některé problémy řešit.

4.2 Přenos procesních veličin

Sběru dat a přenosu procesních veličin se věnuje koncept WSN (Wireless Sensor Network). WSN je distribuovaný systém skládající se z malých autonomních zařízení, která poskytují data o měření veličin fyzického světa. Je založena na principu sběru dat pomocí bezdrátové komunikace mezi těmito malými autonomními zařízeními. [13]

4.2.1 Sítě WSN

WSN nejčastěji využívají bezlicenční pásmo na frekvencích 433 MHz a 868 MHz. Požadavky na zařízení používaných pro měření jsou velmi dlouhá životnost baterie, jednoduchost a nízká cena zařízení. Měřící zařízení se ve WSN nazývají senzory. Senzory měří vlastnosti fyzických objektů reálného světa. Jednotlivé senzory mohou komunikovat mezi sebou, nebo vytvářet části sítě. Jeden senzor měří jen omezené množství veličin reálného světa. Pokud tyto senzory spojíme do sítě, můžeme dostat větší množství různých dat popisující určitý segment. Tento segment (malá síť), může být součástí další sítě, tím vznikne komplexní nástroj pro sběr dat z dané oblasti. Nad jednotlivými daty je pak možné vytvářet agregace a dostávat různá analytická data z dané oblasti. [13]

Využití WSN je možné od malých aplikací sběru dat v rámci výrobní haly až po rozsáhlé aplikace snímání fyzikálních veličin z důvodu varování před požáry, zemětřesením atd. Příklad využití WSN: [13]

- Zemědělství – Měřením teploty a vlhkosti půdy lze řídit například zavlažovací systémy. Pomocí sítě lze určit, jaké množství vody je zapotřebí pro různé oblasti a tím šetřit vodu.
- Inteligentní budovy – Při řízení klimatu v inteligentních budovách dochází k velkým energetickým ztrátám kvůli regulaci vnitřní teploty, vlhkosti a kvality vzduchu. Vzduchotechniky větrající velké prostory většinou s jinou strukturou jako chodby, kanceláře, sociální zázemí atd. mají často málo referenčních měření pro efektivní řízení. Proto se nasazují WSN které měří kvalitu prostředí a dávají řídicímu systému VZT lepší informace pro řízení. Dále je možné monitorovat tyto prostory dlouhodobě a takto naměřená data použít tvorbu modelů chování budovy. Pomocí těchto modelů lze systémy větrání a vytápění řídit prediktivně a maximálně efektivně.

Možností použití je celá řada. Většina základních vlastností WSN sítí je společná, některé se ale řídí podle typu aplikace WSN. Dle typu aplikace rozdělujeme WSN na: [14]

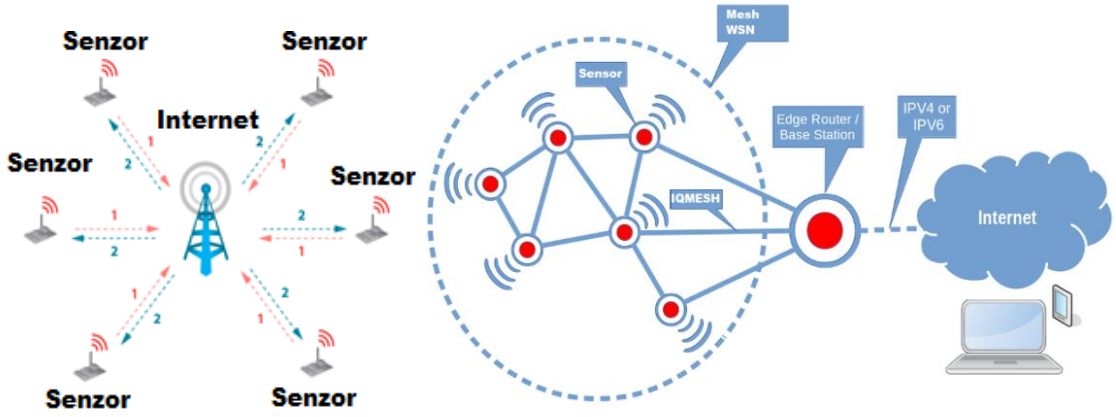
- Sítě pro detekci poruch – senzory měří hlídanou fyzikální hodnotu a při překročení systém nahlásí událost. Na události se podílí jeden senzor, nebo skupina sousedních senzorů.
- Sítě pro periodické měření – používají se na sběr dat v pravidelných intervalech. Příkladem jsou teplotní mapy prováděné jako kontrola vlastností prostředí ve skladech s léčivy.
- Sítě pro zjištění funkce změny a předpověď špiček – podle měřených vlastností a jejich změn se určuje matematická funkce změny a dosažení špiček. To se pak dá použít pro predikci chování.
- Sítě pro sledování polohy a rychlost – používá se pro řízení dopravy ve městech.

4.2.2 WSN a IoT

Sítě WSN mají velmi blízko ke konceptu IoT (internetu věcí). V podstatě se dá říct, že každá brána WSN připojená k internetu a odesílající data je v konceptu IoT věcí. Za věc se v IoT považuje zařízení, které je připojeno k internetu a odesílá data ke zpracování buďto na server, nebo jiné věci. V IoT se v dnešní době objevuje mnoho nových technologií jako je LoRa, nebo SigFox, které jsou cenově dostupné a mají velice nízkou spotřebu. Na základě těchto technologií jsou stavěny senzory, se kterými lze měřit mnoho základních veličin jako je teplota, vlhkost, tlak atd. Nevýhodou těchto technologií je topologie jejich sítě, viz *Obr. 15*. Topologie dává velkou výhodu WSN, jejíž senzory tvoří autonomní multihop síť a až brána je propojuje s vnějším světem. Proto lze WSN použít v průmyslových halách, nebo nepřístupných oblastech. V následující tabulce je porovnání technologií LoRa, SigFox a IQRF.

Tab. 10 Porovnání technologií IoT [15] [16] [1]

	LoRa	**SigFox**	**IQRF**
Frekvenční pásmo	868, 433 MHz	868 MHz	868, 433 MHz
Dosah	20 km	50 km mimo město, 10 km ve městě	500 m
Přenosová rychlost	50 kbit/s	100 kbit/s	19,836 kbit/s
Topologie	Hvězda	Hvězda	Mesh
Modulace	LoRa (FSK)	UNB	GFSK
RF výkon	18 dBm	14 dBm	11 dBm
Výdrž baterie	až 10 let	až 20 let	Standard: 9 dní Nízká spotřeba: 1,68 roku Velmi nízká spotřeba: 11,4 let

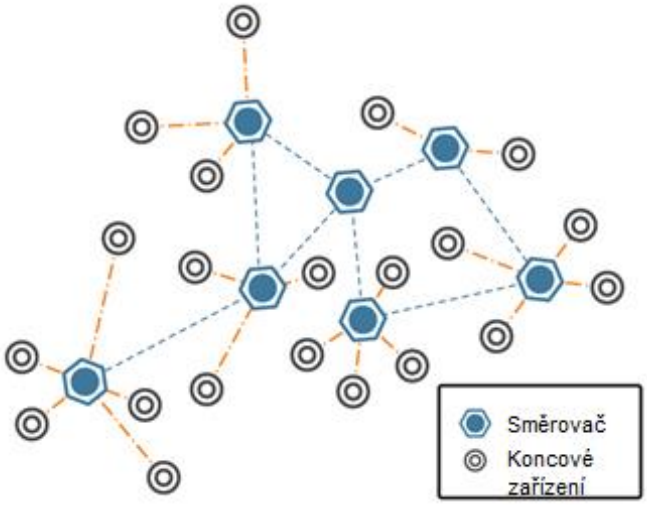


Obr. 15 Porovnání konceptu IoT a WSN

4.2.3 Návrh použití IQRF

Platforma IQRF je vhodná pro použití ve všech typech aplikací WSN. Pro všechny aplikace je nejvhodnější využít topologie sítě mesh. Při požadavku na připojení více než 239 senzorů by se mesh síť rozdělila do segmentů. Tyto segmenty mohou tvořit zřetězené podsítě, tak jak je zobrazeno na obrázku *Obr. 16*. Tím je možné adresovat až 65 000 zařízení.

Pro tvorbu vlastního senzoru stačí použít transceiver, který má dostatečně výkonný MCU a dostatek paměti pro operace s měřenými daty. Dále disponuje sběrnicí I^2C, přes kterou lze připojit inteligentní čidla různých výrobců, například čidlo teploty a vlhkosti. Tento postup je použit při realizaci druhé výukové úlohy.



Obr. 16 Řetězená IQMESH

Další možností jak měřit analogový signál, je použít zabudovaný 10bitový A/D převodník. Ten lze použít po přizpůsobení signálu k měření výstupu aktivních čidel nebo přirozeného signálu odporových čidel teploty. K napájení senzoru stačí tři kusy baterií AA. To je možné díky LDO regulátoru, který je v transceiveru integrován a dovoluje transceiver napájet napětím 3,1–5,2 V.

Pro realizaci ústředny lze použít PC, nebo jednodeskové počítače jako jsou např. RaspBerry nebo BeagleBone. Tyto platformy disponují dostatečným výkonem pro zpracování velkých dat. Jsou vybaveny připojením na ethernet, u některých modelů i WiFi modulem, a přes USB je možné k nim připojit GSM modem. Transceiver lze k bráně připojit pomocí sběrnice SPI. K připojení je vhodný adaptér IQRF-BB-01, který je na obrázku *Obr. 12*.

Komunikaci je možné realizovat pomocí DPA frameworku. Data se na straně senzoru zpracují v naprogramovaném Custom DPA Handleru. Při příchodu požadavku na zaslání dat se data přečtou z realizované periferie, uloží do paměti transceiveru a odešlou po síti IQMESH. Velikost dat je závislá na měřené veličině. Maximální velikost dat, která se dají vložit do jednoho komunikačního rámce je 64 bytů. Čím budou data větší, tím pomaleji se budou přenášet a to bude mít za následek větší nároky na spotřebu, tudíž kratší životnost baterií.

Na straně brány lze vytvořit program v jakémkoli jazyce přeložitelném pod operačním systémem Linux přizpůsobeném pro ARM procesory. Úkolem programu je periodicky

vyvolávat komunikaci, obsluhovat transceiver brány přes SPI sběrnici a přijatá data dál zpracovával.

Jako směrovací algoritmus je vhodné použít DFM2B pro rozlehlé zřetězené sítě, nebo DOM pro malé sítě s potřebou rychlejší odezvy. Pro dotazování na data při periodickém čtení je výhodný FRC telegram. U dat čtených v různých intervalech po skupinách lze použit selektivní FRC telegram. Při čtení dat jako reakce na nějakou událost nebo požadavek by bylo použito přímého dotazu.

Jelikož WSN sítě nemají požadavek na rychlost komunikace, lze použít režim velmi nízké spotřeby implementovaný v DPA frameworku. Tento režim sice prodlužuje hromadný FRC dotaz, ale zároveň násobně šetří spotřebu.

Při přenášení velkých uživatelských dat a častému periodickému dotazování v malých a středních sítích je použití FRC nevýhodné z hlediska spotřeby. FRC dotaz se chová jako vláček jedoucí přes jednotlivá zařízení v síti, do kterého tato zařízení vkládají svá data. Vláček má jen jedny koleje, to znamená, kudy přijede, tudy se vrací. Nody v takovém případě přenášejí data dvakrát – jednou při cestě tam a pak při cestě zpět. Při zpáteční cestě jsou data největší. Proto je vhodné tento dotaz používat na periodické dotazy s dlouhou periodou anebo na velké sítě, kde by selektivní dotazování znamenalo velký počet dotazů.

Jelikož komunikace řízená DPA frameworkem za použití DPA protokolu, má implementovánu linkovou vrstvu, není ji třeba programovat. Tím se ušetří mnoho času implementace linkové vrstvy a hlavně testování v různých scénářích použití.

Přidávání a odebírání senzorů v síti může být častá operace. Při použití jedné topologie sítě jakou je IQMESH, je přidávání jednoduché. Nové čidlo se spáruje s bránou, uloží na místo určení a potom brána provede prozkoumání sítě. O trochu složitější je toto v zřetězených sítích, kde se musí senzor spárovat s příslušným koordinátorem, ke kterému patří, poté se opět provede prozkoumání sítě.

Bezpečnost přenášených dat zajišťuje proprietární šifrování, ke kterému není veřejný popis.

4.2.4 Zhodnocení použitelnosti IQRF

Platforma IQRF je pro nasazení v sítích WSN přímo navržena a odpovídá všem požadavkům pro realizaci WSN.

Vývoj hardware pro nasazení je velmi snadný a rychlý díky velice dobře navrženému a vybavenému transceiveru, který disponuje řadou standardních rozhraní.

Softwarové vybavení nodu se dá velice rychle napsat díky hotovým příkladům DPA Custom Handlerů, které jsou součástí volně dostupného SDK pro vývoj na platformě IQRF. Díky použití DPA frameworku není zapotřebí psát linkovou vrstvu a starat se o spotřebu. To za nás dělá framework sám. Tím se rapidně zkracuje doba vývoje a odpadá testování linkové vrstvy v různých scénářích nasazení.

Jak v některých svých materiálech výrobce udává, byla technologie WSN uplatněna při realizaci na některých komerčních projektech. Z předchozích závěrů je jasné, že toto je oblast použití, pro kterou je platforma IQRF vyrobená.

4.3 Domovní automatizace

Domovní automatizace, jinak také chytré domy (Smart Homes), je soubor technických prostředků umožňujících uživateli stavby ovládat, programovat a monitorovat technologie zde instalované. Jedná se především o ovládání a programování komfortu prostředí v domě ať už lokálně nebo dálkově. Dále mohou být součástí systému ovládání a monitoring EZS systémů, ovládání světel a ovládání audiovizuální techniky.

V domovní automatizaci se dají zařízení rozdělit do těchto skupin: [17]

- Kontrolovaná zařízení – všechna zařízení, která domovní automatizace řídí. Ať už jsou to zařízení vybavená některým druhem protokolu pro přímé připojení k domovní automatizaci jako celku nebo zařízení, která ovládáme prostým vypnutím napájení dané zásuvky.
- Senzory – jednoduchá zařízení, která systému zprostředkovávají požadované měřené vlastnosti ovládaného prostředí (teplota, vlhkost, tlak, osvit) nebo binární stavy zařízení (otevřené okno, světlo svítí)
- Aktuátory – zařízení, jejichž pomocí systém řídí akční členy regulace nebo ovládá stav zařízení.

- Komunikační síť – prostředek, po kterém komponenty systému navzájem komunikují. Komunikace může probíhat bezdrátově, po stávajících rozvodech, nebo po fyzické komunikační lince.
- Kontrolér – zařízení, které sbírá měřené veličiny, zpracovává je, komunikuje s uživatelem, a dle jeho požadavků, nebo pomocí programu řídí připojená zařízení. Komunikace mezi uživatelem může být lokální pomocí zobrazovací jednotky, nebo vzdálená pomocí příkazů ze vzdáleného zařízení např. chytrý telefon. Pro domovní automatizaci je to zpravidla jedno zařízení. Pro složitější celky to může být distribuované řízení pomocí více kontrolérů.
- Zařízení pro dálkové ovládání – v dnešní době jsou to zpravidla chytré telefony, tablety případně PC. Komunikace a ovládání nejčastěji probíhá pomocí webových služeb implementovaných na straně kontrolérů připojených k internetu. Další možností je hlášení a ovládání pomocí SMS. Využívá se nejčastěji ve spojení se EZS pro hlášení narušení hlídaného objektu.

Porovnání vybraných komunikačních standardů je uvedeno v následující tabulce *Tab. 11*.

Tab. 11 Porovnání standardů domovní automatizace

	Z-Wave	**ZigBee**	**IQRF**	**EnOcean**
Frekvenční pásmo	868 MHz	2,4 GHz, 868 MHz	868, 433 MHz	868 MHz
Dosah	30 m	30 m	100 m	30 m
Přenosová rychlost	9,6 kbit/s	250 kbit/s, 20 kbit/s	19,836 kbit/s	až 125 kbit/s
Modulace	GFSK	QPSK	GFSK	ASK

4.3.1 Návrh použití IQRF

Tvorba komponent pomocí platformy IQRF by byla velice podobná jako u WSN. Pro rodinné domy předpokládám, že v jedné síti nebude více než 250 zařízení. V kancelářských budovách, kde je možné předpokládat více zařízení, by se síť musela rozdělit do více segmentů a s ohledem na bezpečnost systému by zde mělo být i více kontrolérů – distribuované řízení.

Jako kontrolér by bylo možné použít některé z řady PLC na trhu vhodné pro domovní automatizaci jako je UniPi, Domat iPLC a další. Pro připojení IQRF k PLC je nutné realizovat převodník mezi IQRF platformou a některým komunikačním standardem, který podporují vybraná PLC. Tím může být například ModBus-RTU.

Další možností je vytvořit vlastní kontrolér, k tomu by opět stejně jako u WSN posloužily platformy BeagleBone, nebo RaspBerry. IQRF transceiver je možné připojit přes SPI. Vývoj univerzálního software pro řízení by byl ale velice nákladný, proto by bylo výhodnější na hardware portovat některou již existující platformu.

Koncová zařízení lze vyvinout na základě transceiveru IQRF. Přes komunikační sběrnici I^2C nebo SPI je možné připojit čidla různých výrobců. Pro aktuátory je možné využít PWM výstup, nebo chytrý DAC převodník řízený po těchto standardních sběrnicích. V třetí výukové úloze je realizován jednoduchý aktuátor. Ten ovládá pomocí GPIO transceiveru bistabilní relé. Tak je možné přenášet dvoustavový logický povel.

Nejvhodnější topologie sítě by byla mesh síť. Pro domovní automatizaci je vhodné použít směrování DOM optimalizované na počet hopů. Periodické čtení dat ze senzorů můžeme realizovat selektivním FRC dotazem. Zápis hodnot na aktuátory je z hlediska bezpečnosti provedení povelu provést selektivně a čekat na potvrzení odpovědi.

Pro realizaci sítě je nevhodnější a nejrychlejší řešení použít DPA framework. Pokud čidlo, nebo aktuátor na straně transceiveru používá GPIO není nutné pro něj programovat DPA handler. Ve většině případů je možné použít existující HWP dodávaný výrobcem IQRF. Pokud je na čidle, nebo aktuátoru použita komunikace s externím hardwarem je nutné naprogramovat DPA Custom Handler pro obsluhu zařízení.

4.3.2 Zhodnocení použitelnosti IQRF

Technologie IQRF je vhodná pro použití v domovní automatizaci. Hardwarové i softwarové požadavky na tento typ aplikace platforma splňuje a přináší výhodu rychlého vývoje zařízení. Některé společnosti prodávají vlastní čidla postavené na této technologii vhodná pro domovní automatizaci jako například TERA Systems, DATmo a další. Více informací je dostupných na stránkách aliance.

Vývoj hardware včetně obslužného software pro aplikaci v domovní automatizaci je rychlý a při řešení standardních úloh i levný. Největší zastoupení má IQRF v ovládání osvětlení.

5 Praktická část práce

V této části práce je popsán návrh realizace tří výukových úloh. Z každé hodnocené oblasti použitelnosti byla zvolena jedna úloha. Jedná se o:

- Jednoduché PIR čidlo,
- Měření teploty a vlhkosti,
- Přenos dvoustavového povelu.

Pro dané úlohy je navržen hardware a software, který zabezpečuje obsluhu jednotlivých zařízení. Poslední částí je tvorba aplikace pro zápis a čtení dat z realizovaných zařízení.

5.1 Potřebné vybavení

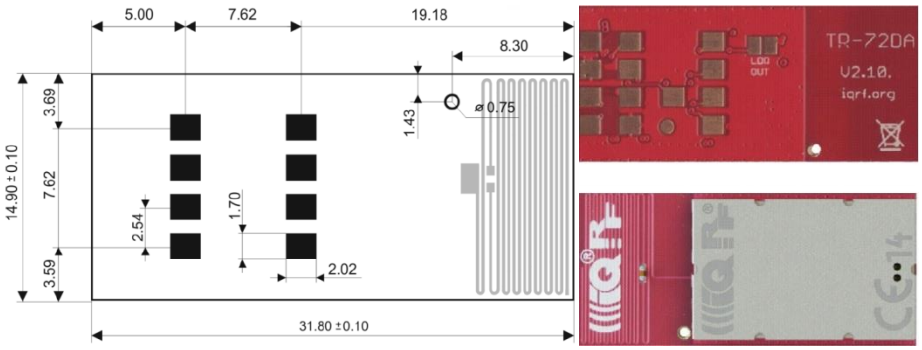
Programování a nastavování transceiverů bude realizováno pomocí programátoru CK-USB 04A. Jeho popis je uveden v kapitole 3.3.1, kde je vyobrazen na obrázku *Obr. 11* Programátor CK-USB-04A. Tento programátor je využit pro konfiguraci a nahrávání software do transceiverů použitých v jednotlivých úlohách.

Dalším hardware je GW-USB-06 viz obrázek *Obr. 17* Brána GW-USB-06. Tato USB brána je použita ke komunikaci počítače se zařízeními realizovanými v jednotlivých úlohách.

Obr. 17 Brána GW-USB-06

Brána obsahuje transceiver DCTR 72DA a funguje jako převodník UART – USB. UART transceiveru je v PC přístupný jako virtuální COM port. Při komunikaci bude brána zastupovat roli koordinátora sítě.

Pro správnou funkci brány je nutné mít nainstalovány příslušné drivery, které jsou dostupné na stránkách výrobce nebo v balíčku IQRF SDK.



Obr. 18 TRANSCEIVER DCTR 72DA

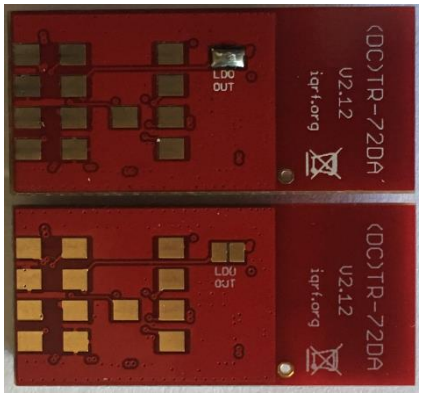
Balíček IQRF SDK obsahuje nástroje pro vývoj aplikací pro platformu IQRF, HWP pro transceivery a mnoho užitečný příkladů kódu. Aktuální balíček se též nachází na stránkách výrobce IQRF.

Pro realizaci jednotlivých úloh budou použity transceivery řady 7. Přesné označení je DCTR-72D a jsou zobrazeny na obrázku *Obr. 18*. Tyto transceivery mají vestavěnou anténu.

5.2 Příprava transceiverů

Před použitím tranceiverů v realizovaných úlohách je zapotřebí na nich provést úpravy, nastavit jim základní komunikační vlastnosti a nahrát HWP.

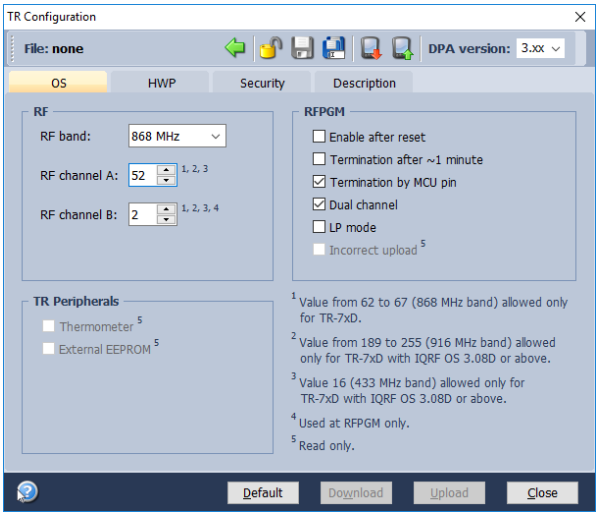
Na transceiverech pro realizaci prvních dvou úloh, jednoduchého PIR čidla a měření teploty a vlhkosti, je nutné umožnit napájení externích zařízení z LDO vestavěného na modulu. To se provede spojením dvou plošek pro tento účel připravených na DPS transceiveru které se jmenují LDO OUT. Spojení plošek je zobrazeno na obrázku *Obr. 19*.



Obr. 19 Upravená a neupravená verze transceiveru

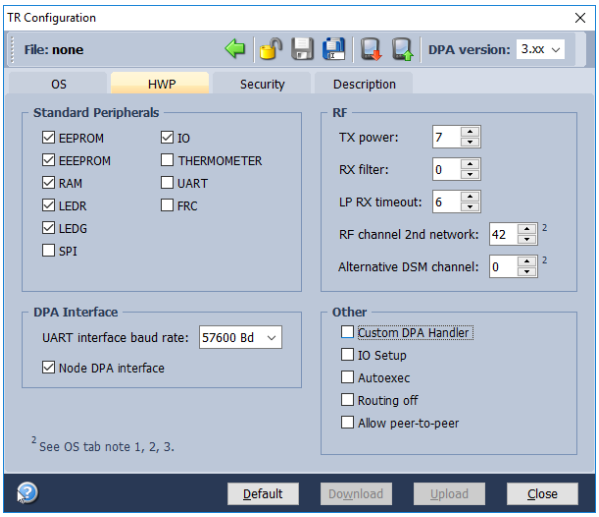
Nastavení základních vlastností komunikace bude nastaveno pomocí IQRF IDE. Postup nastavení hardware a nahrávání HWP je podrobně popsáno a vysvětleno ve video tutoriálech na stránkách výrobce IQRF.

Důležité vlastnosti komunikace, které musíme nastavit pro všechny transceivery a bránu tak, aby bylo možné vytvořit síť, jsou frekvenční pásmo a kanál A. Nastavení je vidět na obrázku *Obr. 20* v části RF. Ostatní nastavení můžeme pro testování nechat nastavené defaultně.



Obr. 20 Nastavení RF vlastností

Pro možnost použití DPA protokolu je nutné modulu brány, který se bude chovat jako koordinátor nastavit DPA Interface jako UART. To je vidět na obrázku *Obr. 21* v regionu DPA Interface.



Obr. 21 Nastavení DPA Interface a Custom DPA Handler

Pro transceiver, který bude použit pro měření teploty a vlhkosti, musíme nastavit použití Custom DPA Handleru, které je na tom samém obrázku *Obr. 21* v sekci Others.

Poslední operací je nahrání HWP profilu do všech transceiverů. Tento profil je pro všechny transceivery stejný. Profily jsou obsaženy v balíčku SDK, kde je jich několik. Z těchto profilů si můžeme vybrat jakýkoliv začínající názvem „GeneralHWP-Node…“. Zbytek názvu specifikuje pro jaký režim je profil nastaven, případně jaké zařízení je v něm podporováno.

Tím máme připraveny síťové prvky IQRF. Bránu, která reprezentuje koordinátora, a tři transceivery pro jednotlivé úlohy.

5.3 Realizace jednoduchého PIR čidla

Realizace jednoduchého PIR čidla je založena na transceiveru a miniaturním PIR senzoru výrobce OEM, které je na obrázku *Obr. 22*.

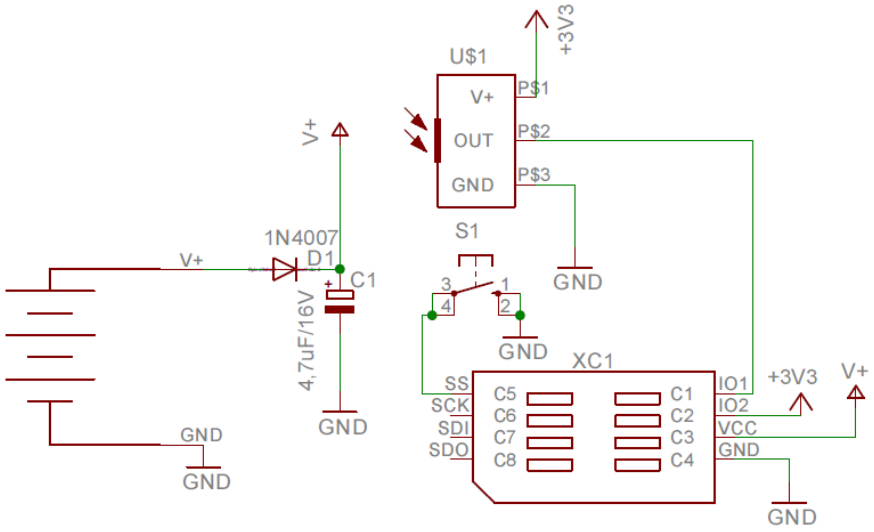
Obr. 22 Micro PIR senzor

Micro PIR senzor je předpřipravený polotovar. Je to nejmenší kompletní PIR čidlo s digitálním výstupem. Níže jsou uvedeny jeho specifikace:

- Napájení: DC 3 – 12 V,
- Odběr v klidu: <0,1 mA,
- Retenční čas: 2 ms,
- Výstup: digitální 0 V–3 V,
- Detekční oblast: 3 až 5 m,
- Detekční úhel: až 100°,
- Celkové rozměry: 12 x 25 mm.

Transceiver použitý na realizaci je, jak již bylo uvedeno, DCTR-72DA. Pro tuto aplikaci je důležité neopomenout úpravu DPS transceiveru tak, aby byl zapnut výstup vnitřního LDO. Tak jak je to popsáno v kapitole 5.2.

Navržené čidlo bude detekovat pohyb pomocí PIR senzoru. Stav čidla bude přenášen pomocí DPA protokolu do koordinátoru a zobrazován na PC.



Obr. 23 Schéma zapojení PIR čidla

Princip funkce navrženého zařízení je následující. Pokud se v prostoru PIR senzoru danému charakteristikou Fresnelovy čočky zaznamená pohyb, PIR senzor svým výstupem sepne universální vstup transceiveru IO1 vyvedený na držáku SIM XC1 na PINu C2.

Celé zařízení je napájeno třemi bateriemi AA, to je celkem 3,6 V až 4,5 V. Za zdrojem je dioda D1 jako ochrana proti přepólování napájení a filtrační kondenzátor. PIR čidlo je napájeno z LDO transceiveru, který je vyveden na PINu C2 držáku SIM XC1. Výstup interního LDO je 3,1 V.

Rezistor R1 a kondenzátor C2 plní funkci nízkoúrovňového filtru pro stabilizaci napájecího napětí PIR čidla. Rezistorem R3 se určuje klidový proud výstupního FET tranzistoru PIR senzoru.

DPS je vybavena tlačítkem S1. Toto tlačítko je použito pro spárování s koordinátorem při konfiguraci a tvorbě sítě, tzv. bondovací tlačítko.

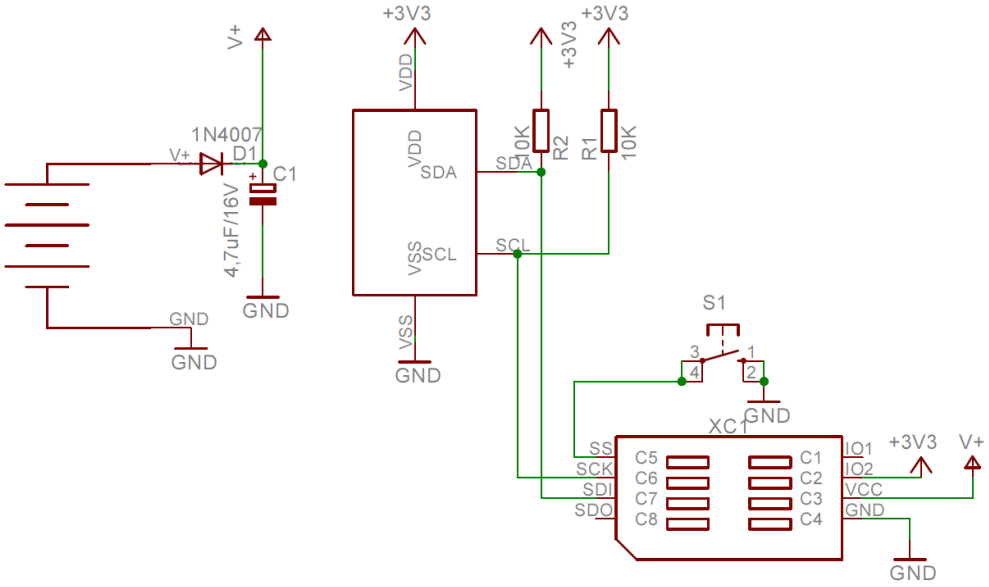
5.4 Realizace měření teploty a vlhkosti

Měření teploty a vlhkosti je opět postaveno na transceiveru DCTR-72DA. K tomuto transceiveru je na sběrnici I^2C připojeno čidlo teploty a vlhkosti SHT21 výrobce SENSIRION.

Čidlo je dodáváno pro povrchovou montáž jeho parametry jsou uvedeny níže:

- Napájení: 2,1–3,6 V
- Výstup: I^2C, PWM, SDM
- Přesnost měření vlhkosti: ± 2 %
- Přesnost měření teploty: ± 0,3 °C

Měření teploty a vlhkosti má v transceiveru naprogramován DPA Custom Handler pro komunikace s SHT21 přes I^2C sběrnici. Měření v zařízení neprobíhá kontinuálně, ale jen na dotaz od koordinátora, tím je snížena spotřeba baterie. Pro tuto úlohu je nutné použít transceiver s připojeným výstupem interního LDO. Do transceiveru musí být nahrán DPA Custom Handler a v nastavení zaškrtnuto jeho spuštění. To je uvedeno v kapitole 5.2.



Obr. 24 Schéma zapojení měření teploty a vlhkosti

Na schématu je vidět, že zařízení bude napájeno třemi bateriemi AA 1,2 V až 1,5 V. Za bateriemi je ochranná dioda D1 proti přepólování zdroje a kompenzační kondenzátor C1. Transceiver je propojen sběrnicí I^2C s obvodem pro měření teploty a vlhkosti SHT21. Na každém signálu sběrnice jsou pull-up rezistory R1 a R2. Obvod SHT21 je napájen z interního

LDO transceiveru. Součástí návrhu je tlačítko S1, které je použito při párování transceiveru s koordinátorem sítě.

5.4.1 DPA Custom Handler

Senzor SHT21 použitý při realizaci této úlohy není přímo podporován DPA frameworkem. Proto je zapotřebí napsat vlastní DPA handler, který se nahraje do MCU senzoru. V tomto handleru se čte hodnota teploty a vlhkosti prostřednictvím I^2C sběrnice z obvodu SHT21, a dále předává v rámci IQMESH sítě.

Do původní šablony DPA handleru, která je součástí balíčku IQRF SDK, je přidána obsluha pro dotaz na uživatelskou periferii s číslem 20 h. Struktura příkazů vysílaná na I2C pro získání aktuální teploty a vlhkosti z čidla je k dispozici v návodu SHT21.

Hodnota přijatá od senzoru SHT21 po sběrnici I^2C má délku 14 bitů. Je implementována rutina pro kontrolu kontrolního součtu CRC přijatých dat. Výsledných 14 bitů je předáno do 16bitové proměnné, tu pak transceiver vrací jako výstup uživatelského příkazu. Horní dva bity, které nejsou využité, nastavujeme následovně:

- bit 16 je vždy nastaven na logickou 1,
- bit 15 obsahuje logickou 1, pokud nebyla data přijatá po I^2C validní z hlediska CRC.

S tímto formátem je potřeba počítat v rámci konverzních rutin v aplikaci.

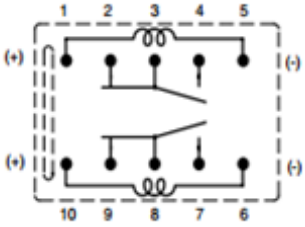
5.5 Realizace přenosu dvoustavového povelu

Úloha přenosu dvoustavového povelu je opět založena na transceiveru DCTR-72DA a dvoucívkovém bistabilním paměťovém relé AZ850P2-3 výrobce Zettler. Relé je spínáno univerzálními digitálními výstupy IO1 a IO2 transceiveru pomocí spínacích tranzistorů. Tranzistory jsou použity z toho důvodu, že výstup transceiveru nedokáže přenést proud potřebný pro sepnutí cívky relé.

Bistabilní relé bylo zvoleno s ohledem na požadovanou nízkou spotřebu, schéma je na obrázku *Obr. 25* Bistabilní relé AZ850P2. Provedení tohoto relé má následující parametry:

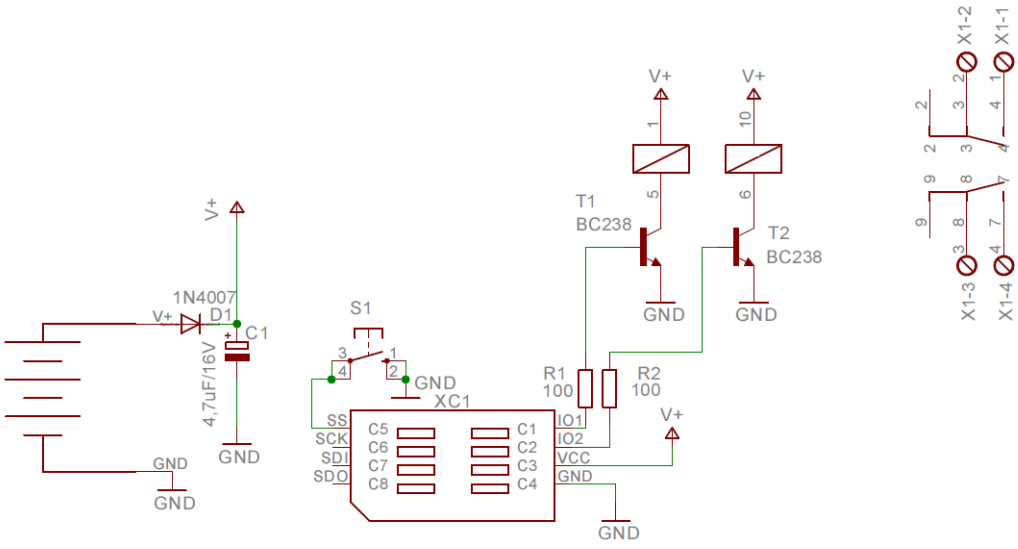
- Nominální napájení: 3 V
- Minimální operační napájení: 2,3 V

- Odpor cívky: 45 Ohm
- Maximální spínaný proud: 1 A
- Maximální spínané napětí: 220 VDC nebo 250 VAC



Obr. 25 Bistabilní relé AZ850P2

V této úloze bude použit transceiver, který nemá vyvedené napájení z obvodu LDO. Do transceiveru bude nahrán standardní HWP a nebude používán DPA Custom Handler.



Obr. 26 Schéma zapojení přenosu dvoustavové hodnoty

Jak je vidět na schématu, funkce tohoto zařízení je velice jednoduchá. Pokud transceiver přijme povel na zápis, sepne na definovanou dobu požadovaný výstup a tím i požadovanou cívku bistabilního relé K1 pomocí spínacích tranzistorů. Po definované době výstup opět rozepne. Je to ovládání pomocí impulzu.

Napájecí část je řešena stejně jako u předchozích modulů. Na prvním univerzálním výstupu IO1 je připojena první cívka. Její spínací kontakty jsou vyvedeny na šroubovací svorkovnici X1 pro snadné připojení ovládaného zařízení. Druhá rozpínací cívka je ovládána výstupem IO2 a její spínací kontakty jsou také vyvedeny na šroubovací svorkovnici X1. Tím

máme na šroubovací svorkovnici vyvedenu kombinaci kontaktů jako u standardního relé (sepnuto, rozepnuto).

5.6 Software pro komunikaci s moduly

Software pro komunikaci s moduly je realizován ve vývojovém prostředí Visual Studio 2015, nad platformou .NET v jazyce C#. IQRF standardně nedodává vývojovou knihovnu DPA protokolu pro .NET framework. Není to významnější překážka. Vzhledem k charakteru úlohy stačí implementovat jen minimální část DPA. Primárně je software určen pro běh na platformě Windows, ale vzhledem k portfoliu použitých knihoven ho lze spustit na platformě Linux pod frameworkem Mono.

Rutiny, které se týkají linkové a aplikační vrstvy DPA, jsou umístěny do samostatného modulu – dynamické knihovny DLL. Modulární návrh umožní snadněji navázat a rozšířit práci a obecně zpřehledňuje architekturu. Modul dynamické knihovny je umístěn v samostatném projektu IqrfDpaLib a skládá se z následujících tříd, z nichž každá řeší konkrétní část komunikace:

- HdlcLayer – Vzhledem k tomu, že s modulem komunikujeme přes UART rozhraní, je při přenosu dle DPA dokumentace použit HDLC formát rámců. Třída obsahuje základní rutiny pro kódování a dekódování HDLC rámce, před jeho posláním nebo po jeho přijetí ze sběrnice.
- OneWireCrc – Třída obsahuje metody pro výpočet a kontrolu cyklického součtu, který slouží k ověření integrity a je součásti každého rámce. DPA používá jednobytové CRC, používané rovněž na sběrnicích 1-Wire.
- IqrfUartComm – Třída poskytuje nadstavbu nad implementací sériového portu v .NET framework. Metody pro vysílání a příjem dat na sériovou linku přebírají jako parametr datové buffery a pomocí tříd výše vytvářejí korektní formát rámců DPA protokolu pro komunikaci přes UART rozhraní.
- DpaFrame – Třída obsahuje rutiny pro vytváření a zpracování rámců DPA protokolu, kterou jsou nezbytné pro implementaci ukázkových úloh. Parametrem rutiny je vždy buffer, který slouží buďto jako cíl pro vytvoření DPA rámce, nebo jako zdroj pro validaci a zpracování odpovědi. Další parametry vždy závisí na konkrétním typu rámce.

Vlastní spustitelný program využívající předpřipravenou DLL knihovnu je umístěn v projektu IqrfComm. Na začátku programu je inicializován sériový port představující UART rozhraní DPA frameworku. Následuje nastavení parametrů IO rozhraní jednotlivých modulů. Dále následuje hlavní smyčka: v každém průchodu dochází k detekci stisknuté klávesy a k čekaní v délce 100 ms. Počet průchodů cyklu je monitorován, po definované periodě je vyčten aktuální stav veličin na modulu se senzorem teploty a aktuální stav digitálního vstupu na PIR čidle. Pokud je ve smyčce zaznamenán stisk klávesy, dojde k vyslání rámce s povelem na změnu IO na modulu s relé. Řešení s jednou hlavní smyčkou lze nahradit separátním vláknem nebo časovačem.

6 Závěr

Cílem této práce bylo seznámit se s platformou IQRF, posoudit možnosti jejího nasazení a realizovat tři výukové úlohy s touto platformou.

Seznámení s platformou proběhlo na všech úrovních a to jak hardware, tak implementace komunikačního protokolu a v neposlední řadě možnost, vývoje a programování na této platformě. Informace byly převážně čerpány z návodů a datasheetů k jednotlivým součástem platformy, ale také z dobře zpracovaných videotutoriálů a animací, které jsou na stránkách výrobce. Nejasnosti, které se vyskytly v průběhu práce s IQRF, byly konzultovány přímo s oddělením podpory výrobce.

Platforma byla porovnána s nejznámější technologicky srovnatelnou konkurencí. Výsledkem porovnání bylo, že IQRF je velice dobře použitelná na jednoduší typy aplikací, kde není vyžadováno silné zabezpečení a asynchronní přenos informací z koncových zařízení. I když se platforma jeví dražší než její konkurence, tak s ohledem na provedení transceiverů a rychlý vývoj aplikací tomu tak není. Nejsilnějšími stránkami IQRF je kvalita provedení vlastních transceiverů a rychlost vývoje pomocí DPA frameworku. Oproti konkurenčním řešením vidím jako jedno z největších pozitiv velmi dobrý dosah komunikace vůči malé spotřebě realizované díky volitelný režimům spotřeby. Další konkurenční výhodou je jednoduchý a rychlý vývoj pomocí DPA frameworku, kde je možné využívat hardwarové profily a tak vyvíjet aplikace bez dlouhého programování a testování, které za nás provedl výrobce. Za slabé stránky se dá považovat absence asynchronního posílání zpráv mezi zařízeními a s tím související chybějící algoritmy MAC vrstvy.

Bylo analyzováno možné nasazení platformy ve třech oblastech použití. První oblastí byla zabezpečovací technika, kde se aplikace IQRF nejeví jako nejlepší řešení. A to z důvodů nízkého zabezpečení, odolnosti vůči zarušení a především výše zmíněné absenci asynchronní komunikace koncových zařízení v mesh síti. Při použití jiné topologie ztrácí platforma svoje největší výhody. Pro použití v této oblasti by bylo nutné doprogramovat vlastní linkovou vrstvu, MAC vrstvu, zabezpečení vysílaných dat a ošetřit odolnost vůči zarušení systému. Aplikace v této oblasti jako jsou PIR senzory, magnetické kontakty a další bych spíše zařadil do domovní automatizace.

Další hodnocenou oblastí použití byl přenos procesních veličin. Touto oblastí se zabývá problematika bezdrátových senzorických sítí WSN. Toto je oblast, pro kterou je IQRF navrženo. Díky jednoduché implementaci mesh sítě, možnosti tvořit sítě obsahující až 65 000 zařízení a implementaci hromadného dotazování pomocí FRC dotazů je IQRF platforma pro tuto oblast použití vhodná. Problematika WSN sítí souvisí s dalším rychle se šířícím konceptem, kterým je internet věcí (IoT). Zde bylo provedeno porovnání s vybranou konkurencí a diskutovány výhody a nevýhody těchto technologií.

To samé platí o třetí oblasti použití, kterou je domovní automatizace. Aplikace je podobná jako u WSN. U sítí používaných v domovní automatizaci se neuvažuje takové množství koncových zařízení jako u WSN. Jelikož jsou součástí sítě aktuátory, je vyžadována i větší spolehlivost doručení paketů v síti. Toho lze v IQRF jednoduše dosáhnout kombinací hromadných FRC dotazů se selektivním povelováním aktuátorů. U selektivního povelování je požadováno potvrzení přijetí povelu.

Pro obě dvě oblasti použití, domovní automatizaci a WSN, platí stejné výhody IQRF platformy. Těmi jsou dostatečně vybavený transceiver, velký dosah komunikace a implementace mesh sítě, o kterou se stará DPA framework. Díky tomuto frameworku není nutné programovat linkovou vrstvu komunikace. Tím je mnohem jednodušší, rychlejší a levnější vývoj zařízení.

Pro každou oblast použití byla navržena a sestavena jedna úloha. Jsou to úlohy:

- Jednoduché PIR čidlo
- Měření teploty a vlhkosti
- Přenos dvoustavového povelu

Při návrhu úloh byl brán ohled na jednoduchost návrhu pokud možno bez nutnosti programování vlastní obsluhy zařízení, nízkou spotřebu a využití různých možností transceiverů. Úlohy byly navrženy a realizovány.

Testování jednotlivých zařízení bylo provedeno pomocí software naprogramovaného v jazyce C# pro .NET framework. Aplikace byla napsána tak, aby se její kód dal dále používat a rozvíjet. Skládá se z několika částí, a to z obsluhy sériového portu, vlastního programu s výstupem na konzolu a DLL knihovny, která obaluje zapouzdření API funkcí DPA frameworku.

Výstupem práce je seznámení se s platformou IQRF, porovnání jejích parametrů s konkurencí, diskuze nad použitelností platformy IQRF v jednotlivých oblastech použití a návrh výukových úloh.

7 Citovaná literatura

1. MICRORISC. www.iqrf.org. *IQRF Technical quide.* [Online] 20. 10. 2016. [Citace: 3. 3. 2017]. http://www.iqrf.org/support/download&kat=51&ids=474.

2. MICRORISC. www.iqrf.org. *IQRF OS User's Guide.* [Online] 9. 21. 2017. [Citace: 3. 3. 2017]. http://www.iqrf.org/support/download&kat=35&ids=155.

3. MICRORISC. www.iqrf.org. *(DC)TR-72D Transceiver Module Data Sheet.* [Online] 2. 4. 2016. [Citace: 3. 3. 2017]. http://www.iqrf.org/weben/downloads.php?id=337.

4. Akyildiz, Ian, Xudong, Wang a Weilin, Wang. *Wireless mesh networks: a survey.* Atlanta : The International Journal of Computer and Telecommunications Networking, 2005. 1389-1286.

5. Hynčica, Ondřej. Bezdrátové sítě typu mesh. Děčín : Automa – časopis pro automatizační techniku, s. r. o., 2005, Sv. 5.

6. Sulc, Vladimir, Kuchta, Radek a Vrbata, Radim. Microrisc s.r.o. *IQMESH implementation in IQRF wireless communication platform.* [Online]

7. MICRORISC. www.iqrf.org. *DPA Framework Technical Guide.* [Online] 12. 9. 2016. [Citace: 12. 3. 2017]. http://www.iqrf.org/support/download&kat=54&ids=481.

8. MICRORISC. www.iqrf.com. *CK-USB-04A User's Guide.* [Online] 21. 8. 2015. [Citace: 10. 3. 2017]. http://www.iqrf.org/support/download&kat=41&ids=328.

9. MICRORISC. www.iqrf.org. *IQRF-BB-02 User's guide.* [Online] 24. 11. 2015. [Citace: 17. 3. 2017]. www.iqrf.org/weben/downloads.php?id=447.

10. ZigBee, Aliance. www.zigbee.org. *Introducing ZigBee 3.0.* [Online] 2. 12. 2014. [Citace: 10. 3. 2017]. http://www.zigbee.org/zigbee-for-developers/zigbee/#.

11. SIGMA DESIGN. www.z-wave.com. *ZM 5101.* [Online] [Citace: 27. 3. 2017]. http://z-wave.sigmadesigns.com/wp-content/uploads/ZM5101_br.pdf.

12. Křeček, Stanislav. *Příručka zabezpečovací techniky.* Blatná: Critetus, 2003. 80-902-9382-4.

13. Waltenegus, Dargie a Poellabauer, Christiian. *Fundamentals of Wireless Sensor Networks.* místo neznámé : Wiley, 2010. 978-0-470-99765-9.

14. Holger, Karl a Willig, Andreas. *Protocols and Architectures for Wirelles Sensor Networks.* místo neznámé : Wiley, 2005. 0-470-09510-5.

15. SigFox. www.sigfox.com. *About Sigfox.* [Online] [Citace: 27. 3. 2017]. http://makers.sigfox.com/about/.

16. Alliance, Lora. www.lora-alliance.org. *LoRa Technology.* [Online] [Citace: 27. 3. 2017].

http://www.lora-alliance.org/What-Is-LoRa/Technology.

17. Kyas, Otmar. *How To Smart Home.* Wyk : Concept Press e.K., 2013. 978-3-944980-00-3.

8 Seznam obrázků

Obr. 1 Blokové schéma modulu 4
Obr. 2 Módy spotřeby v RX režimu modulu 6
Obr. 3 Architektura operačního systému IQRF 8
Obr. 4 Úplná mesh a částečná mesh síť 9
Obr. 5 Složení paketu IQMESH 10
Obr. 6 Reakce na příjem paketu 11
Obr. 7 Průběh bondingu 12
Obr. 8 Discovery 12
Obr. 9 Topologie a adresování sítě při použití SFM 14
Obr. 10 Přeadresovaná síť 14
Obr. 11 Programátor CK-USB-04A 17
Obr. 12 Adaptér IQRF-BB-01 18
Obr. 13 Topologie peer-to-peer, topologie IQMESH star, topologie potřebná pro realizaci úlohy jednosměrné komunikace EZS 25
Obr. 14 Topologie mesh sítě EZS 26
Obr. 15 Porovnání konceptu IoT a WSN 31
Obr. 16 Řetězená IQMESH 32
Obr. 17 Brána GW-USB-06 37
Obr. 18 TRANSCEIVER DCTR 72DA 38
Obr. 19 Upravená a neupravená verze transceiveru 38
Obr. 20 Nastavení RF vlastností 39
Obr. 21 Nastavení DPA Interface a Custom DPA Handler 39
Obr. 22 Micro PIR senzor 40
Obr. 23 Schéma zapojení PIR čidla 41
Obr. 24 Schéma zapojení měření teploty a vlhkosti 42
Obr. 25 Bistabilní relé AZ850P2 44
Obr. 26 Schéma zapojení přenosu dvoustavové hodnoty 44

9 Seznam tabulek

Tab. 1 Porovnání hardware RF obvodů řady 7 a řady 5 5
Tab. 2 Spotřeby modulů v jednotlivých režimech 5
Tab. 3 Doba potřebná pro vyslání paketu 11

TAB. 4 OMEZENÍ STANDARD FRC 15
TAB. 5 RYCHLOST ODEZVY FRC 15
TAB. 6 TABULKA FUNKCÍ PIN C1 AŽ C8 17
TAB. 7 POROVNÁNÍ HW KONKURENCE 20
TAB. 8 ZÁVĚREČNÉ HODNOCENÍ 21
TAB. 9 TECHNICKÉ STUPNĚ ZABEZPEČENÍ Z NORMY ČSN EN 50131-1 ED.2 24
TAB. 10 POROVNÁNÍ TECHNOLOGIÍ IOT 31
TAB. 11 POROVNÁNÍ STANDARDŮ DOMOVNÍ AUTOMATIZACE 35

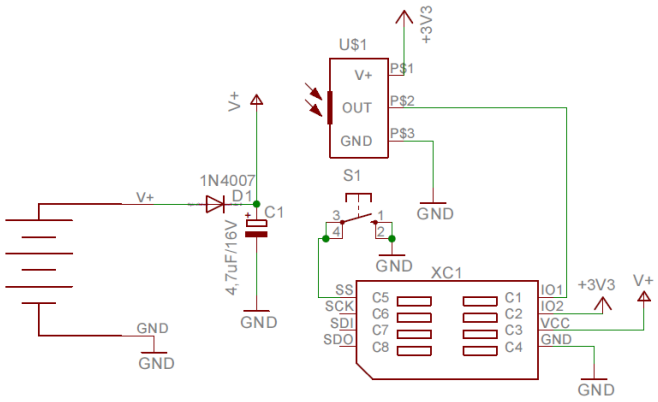
10 Přílohy

Příloha 1 Schéma zapojení PIR čidla a návrh plošného spoje

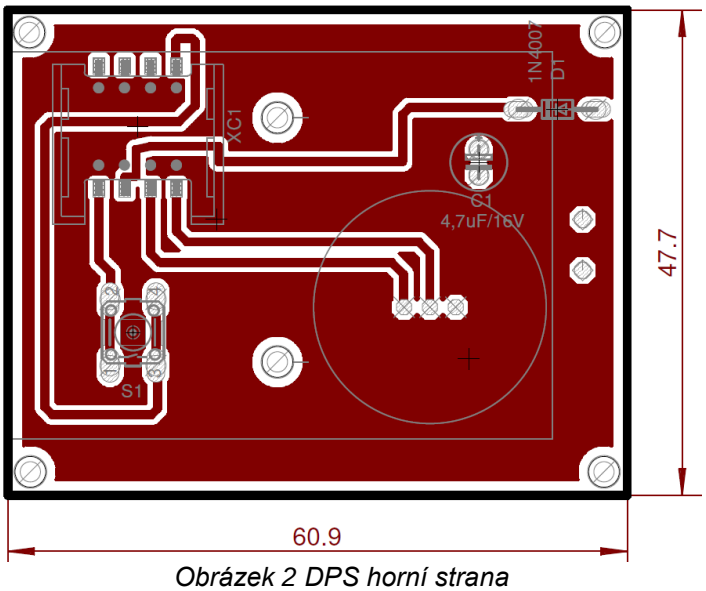
Příloha 2 Schéma zapojení měření teploty a vlhkosti a návrh plošného spoje

Příloha 3 Schéma zapojení ovládání bistabilního relé a návrh plošného spoje

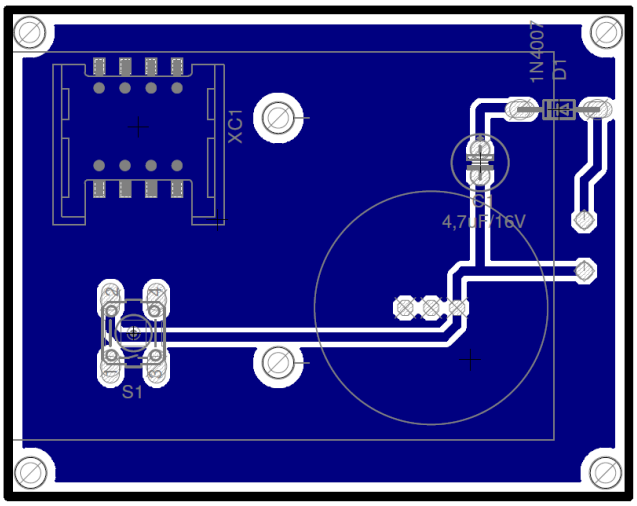
Příloha 1 Schéma zapojení PIR čidla a návrh plošného spoje



Obrázek 1 Schéma zapojení

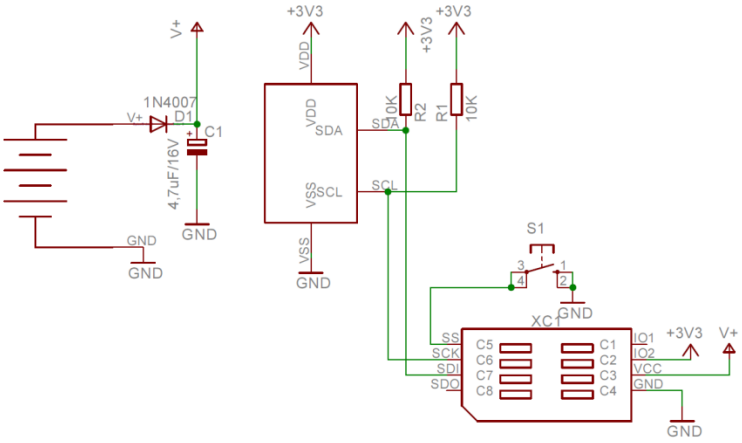


Obrázek 2 DPS horní strana

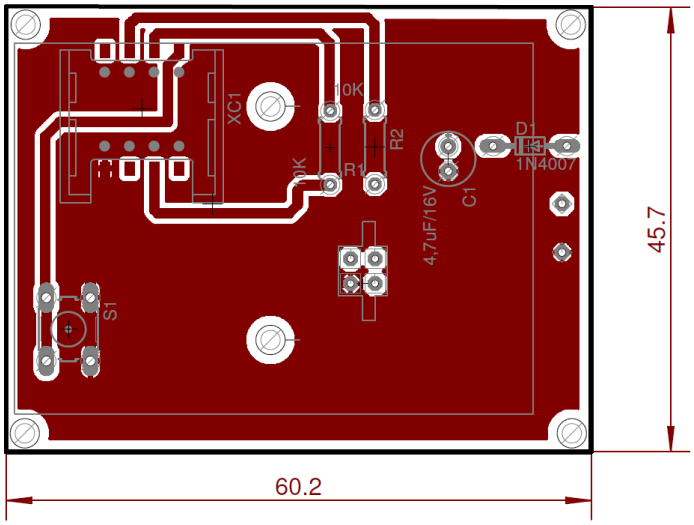


Obrázek 3 DPS spodní strana

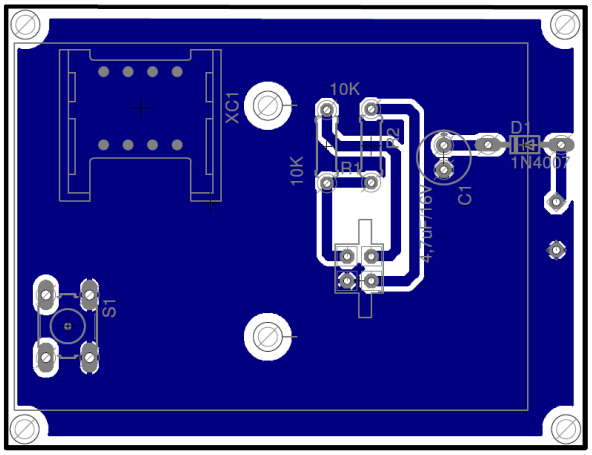
Příloha 2 Schéma zapojení měření teploty a vlhkosti a návrh plošného spoje



Obrázek 4 Schéma zapojení

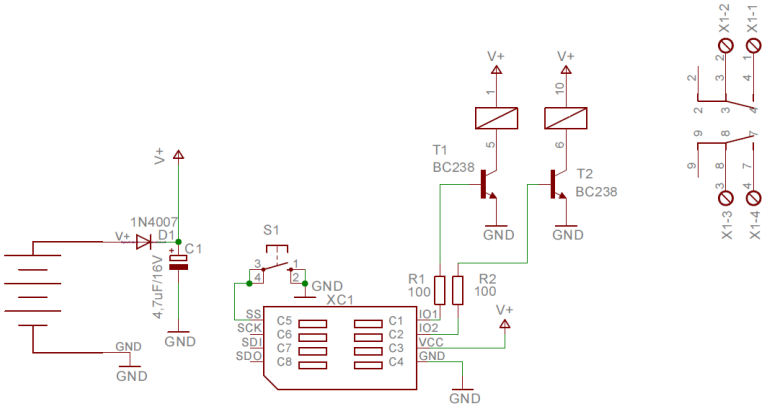


Obrázek 5 DPS horní strana

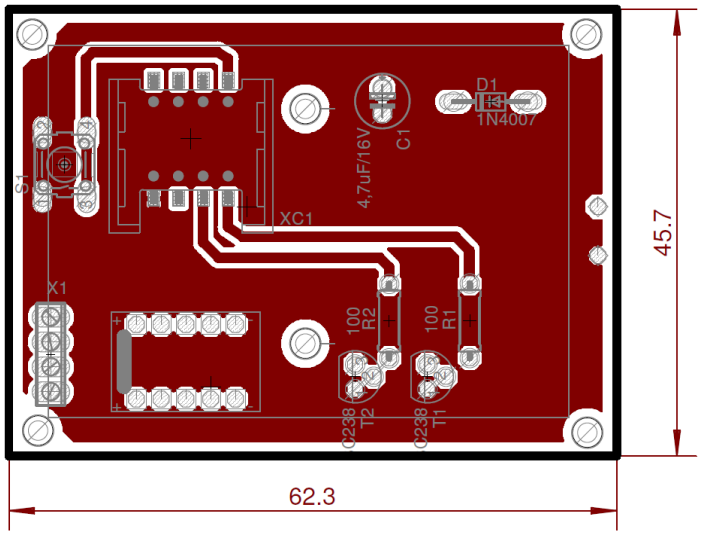


Obrázek 6 DPS spodní strana

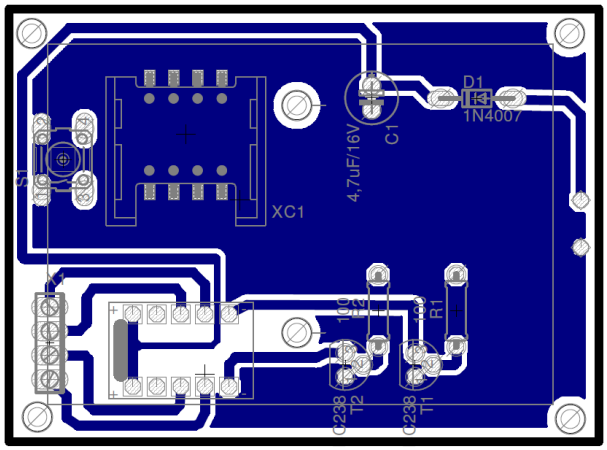
Příloha 3 Schéma zapojení ovládání bistabilního relé a návrh plošného spoje



Obrázek 7 Schéma zapojení



Obrázek 8 DPS horní strana



Obrázek 9 DPS spodní strana