VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY
DEPARTMENT OF CONTROL AND INSTRUMENTATION

APLIKACE SENZORŮ PRACUJÍCÍCH V OBLASTI MILIMETROVÝCH VLN V ZABEZPEČOVACÍ TECHNICE
SECURITY APPLICATION OF MMWAVE SENSORS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Lukáš Petržela
AUTHOR

VEDOUCÍ PRÁCE — Ing. Soběslav Valach
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Automatizační a měřicí technika**
Ústav automatizace a měřicí techniky

Student: Lukáš Petržela ***ID:*** 186802
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Aplikace senzorů pracujících v oblasti milimetrových vln v zabezpečovací technice

POKYNY PRO VYPRACOVÁNÍ:

Cílem projektu je prozkoumat využití senzorů pracujících v oblasti mm vln (frekvence 80GHz) pro využití v zabezpečovací technice. Primárně se jedná o zabezpečení perimetru a náhradu klasických PIR senzorů. Předpokládá se detekce narušitele, odhad velikosti, postu narušitelů, jejich rychlosti a směru.
Postupujte dle následujících bodů:
1) Prostudujte principy a techniky radarové technologie.
2) Seznamte se s řešením dodávaným společností Texas Instruments.
3) Navrhněte vhodné uspořádání senzorů se zaměřením na cílovou aplikaci.
4) Navrhněte vhodný komunikační protokol.
5) Zpracujete data získaná ze senzoru a vizualizujte vhodným způsobem.
6) Analyzujte spolehlivost a funkčnost navrženého řešení.

DOPORUČENÁ LITERATURA:

http://www.ti.com/sensors/mmwave/iwr/overview.html

Termín zadání: 4.2.2019 ***Termín odevzdání:*** 20.5.2019

Vedoucí práce: Ing. Soběslav Valach
Konzultant:

doc. Ing. Václav Jirsík, CSc.
předseda oborové rady

Abstrakt

Tato bakalářská práce se zabývá možným využitím senzorů od společnosti Texas Instruments v zabezpečovací technice, především pro zabezpečení perimetru. Obsahuje přehled principů radarové technologie a popis principu radarů od společnosti Texas Instruments. Bylo navrženo a implementováno vhodné umístění senzorů a byl navržen komunikační protokol. Byla provedena měření ověřující funkčnost a spolehlivost navrženého řešení. Dosažené výsledky jsou zanalyzovány a vyhodnoceny

Klíčová slova

FMCW, radar, vysílač, přijímač, vzdálenost, frekvence, Texas Instruments

Abstract

This bachelor thesis is focused on possible use of Texas Instrument´s sensors in security systems, especially for perimeter securing. It includes the overview of radar technology principles and describe of Texas Instrument´s radars principle. Appropriate sensors location has been designed and implemented, and a communication protocol has been designed. The functionality and reliability of the proposed solution has been verified. The results are analyzed and evaluated.

Keywords

FMCW, radar, transmitter, receiver, distance, frequency, Texas Instruments

Bibliografická citace:

PETRŽELA, Lukáš. *Aplikace senzorů pracujících v oblasti milimetrových vln v zabezpečovací technice.* Brno, 2019. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/119602. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav automatizace a měřicí techniky. Vedoucí práce Soběslav Valach.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma Aplikace senzorů pracujících v oblasti mm vln v zabezpečovací technice jsem vypracoval samostatně pod vedením vedoucí/ho bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne: .....

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Soběslavu Valachovi za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé diplomové práce.

V Brně dne: ……

podpis autora

Obsah

Seznam obrázků

1. ÚVOD

Jedním z nejmodernějších typů radarů jsou tzv. FMCW radary na které se v této práci zaměřuji. V dnešní době se u radarů klade důraz především na rychlost, přesnost, rozlišitelnost. V práci se soustředím především na FMCW radary vyráběné společností Texas Instruments. Tyto radary mají velmi široké možnosti využití např. v automobilovém průmyslu (řízení autonomních aut, senzory v autech), nebo ve statistice (doprava, fronty). Tato práce se zabývá především využití těchto radarů v zabezpečovací technice, kde mohou radary sloužit jako náhrada klasických PIR čidel, s tím, že mohou vykonávat více funkcí a v horších podmínkách.

Cíl teoretické části této práce je podat přehled o fungování základních typů radarů, vysvětlit jaké druhy existují, najakém principu fungují a kde se využívají. Následně čtenáře seznámit podrobně s FMCW radary, jakým způsobem vysílají a přijímají signál, jakým způsobem vyhodnocují data, jak vypadá konkrétní řešení od společnosti Texas Instrument, tzn. z jakých bloků je radar složen, jakým způsobem lže uživatelsky programovat, jak vypadá tok dat v čipu radaru a jakým způsobem radar komunikuje. Jelikož se práce věnuje využití těchto senzorů v zabezpečovací technice, je také nutné se zmínit o aktuálně nejpoužívanějším způsobu zabezpečování objektů proti vniknutí narušitele a to je pomocí PIR čidel.

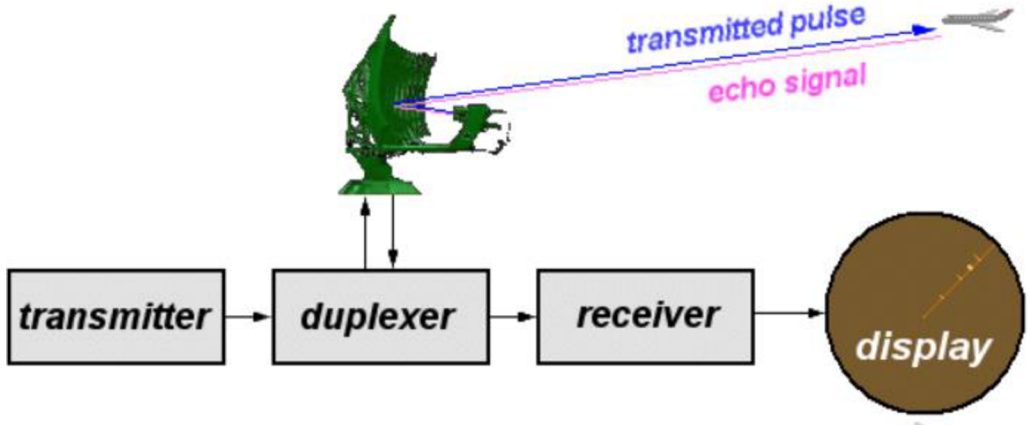
V praktické části se práce věnuje návrhu konkrétní zabezpečení objektu pomocí radaru od společnosti Texas Instruments a to konkrétně radaru IWR1642. Předpokládá se návrh vhodné umístění senzorů, návrh vhodného komunikačního protokolu a následné praktické měření a získávání dat. Po této části následuje část s vyhodnocením a analýzou dat, ve které bude shrnuto a odůvodněno, zda je toto řešení funkční a spolehlivé

2. PRINCIPY A TECHNIKY RADAROVÉ TECHNOLOGIE

2.1 Základy radarové technologie

Radar, zkratka z anglických slov Radio detection and ranging, česky radiové rozpoznávání a určování vzdálenosti, je systém pracují na principu vysílání vysokofrekvenčních signálů a to nejčastěji v podobě buď elektromagnetických vln, nebo ultrazvuku, jejich odrazu, následném příjmu a vyhodnocení přijaté odražené vlny (některé typy radarů, tzv. pasivní radary nevysílají signál, jen přijímají). Jelikož je známa rychlost šíření signálu, je možné měřit čas mezi vysláním a opětovném přijetí signálu a z této doby zjistit vzdálenost objektu, který vlnu odráží. Tímto způsobem fungovaly radary při jejich nástupu a je také znázorněn na obrázku 2.1. Dnes je již velké množství různých druhů radarů, které fungují na jiných principech, ty nejpoužívanější jsou zmíněny v následujících podkapitolách. [1]

První radary se začaly objevovat v první polovině 20. století a největší pokrok ve výzkumu radarů nastal při druhé světové válce. Do té doby se přítomnost letadel zjišťovala pouze vizuálně a zachycováním zvuků, podle kterých se pak rozlišovaly typy letadel. S příchodem radarů se nepřátelské objekty daly detekovat na mnohem větší vzdálenosti, s větší přesností, téměř nonstop, při jakémkoliv počasí či jiných nepříznivých podmínkách. [1] [2]



Obr. 2.1 Jeden ze základních principů radaru [1]

Popis jednotlivých bloků z obrázku 2.1:

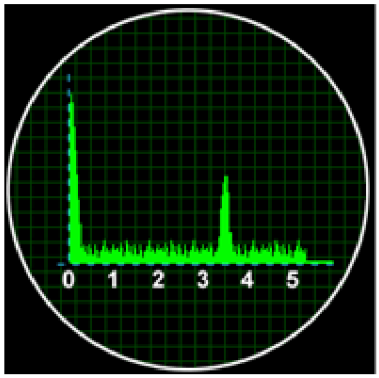
Transmitter (vysílač) vytváří vysokofrekvenční krátký impuls, který je anténou přenášen do okolí.

Duplexer (přepínač) přepíná anténu mezi režimem vysílání a přijímání signálu, tudíž u radarů fungujících na tomto principu stačí pouze jedna anténa. Antény používají

vysoké frekvence především kvůli vyššímu rozlišení (čím menší vlnová délka, tím menší objektu může radar detekovat) a také kvůli velikosti antény (čím je vyšší frekvence, tím může být anténa menší a zachová si zesílení) [1]

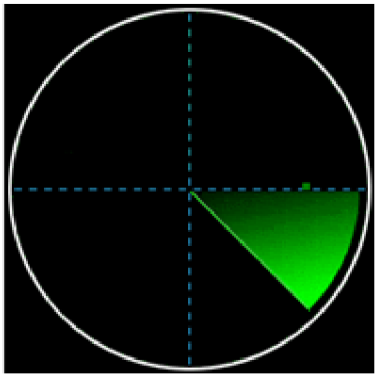
Receiver (přijímač) zesiluje a demoduluje přijatý signál, který je následně zpracován a jednoduše a srozumitelně zobrazen na displeji, který je připojen jak k vysílači, tak k přijímači. [1]

Dříve byly nejčastěji používané displeje monitory osciloskopu, jako je na obrázku 2.2. První špička značí vyslaný signál, druhá špička přijatý signál, x-ová osa displeje je v takovém měřítku, aby doba přijetí signálu odpovídala vzdálenosti, kterou signál urazil (respektive polovině vzdálenosti). Na obrázku se tedy vyslaný signál odrazil od objektu ve vzdálenosti 3,5 km. Nevýhodou ovšem bylo, že radar poskytl informaci jen o vzdálenosti, nikoliv o úhlu (přesné poloze) objektu. [2]



Obr. 2.2 Příklad displeje radaru (obrazovka osciloskopu) [2]

Aby bylo možné určit přesnou polohu objektu, začaly se používat kruhové displeje, příklad takového displeje je znázorněn na obrázku 2.3. Anténa se otáčí o 360° a neustále střídavě vysílá a přijímá signál, aktuální natočení antény zobrazuje zelená plocha a pokud radar zachytí odražený signál, je znázorněn zelenou tečkou (na obrázku vidět v pravé části x-ové osy). [1] [2]



Obr. 2.3 Příklad kruhového displeje radaru [2]

2.2 Typy radarů

Radary lze rozdělit z mnoha hledisek. Jedno ze základních dělení je na radary aktivní a pasivní. Aktivní radary vysílají vlastní elektromagnetické vlny, pasivní radary vlny pouze přijímají, zatímco vlna je vysílána jiným objektem. [3]

Mezi aktivní radary patří například radar ultrazvukový, který detekuje přítomnost objektů pomocí známé rychlosti vysílaného ultrazvuku a doby letu signálu. Rychost objektu zjišťuje pomocí změny frekvence přijatého signálu (Dopplerův efekt). Tyto radary mají využití například pro měření rychlosti automobilů. Měříme-li dobu návratu signálu, můžeme také zjišťovat i výšku vozidla (pokud radar vysílá signál kolmo na silnici), například pro statistické účely.

Další druh aktivního radaru je radar mikrovlnný, ty se dále dělí na 3 základní typy, podle toho jakým způsobem signál vysílají a to:

- Radar s pulzní vlnou – Většinou mívají jen jednu anténu, která se v pravidelných intervalech přepíná na vysílač, nebo přijímač a vysílá signál konstantní délky ve stanovených intervalech. Tímto radarem se dá měřit směr, vzdálenost, popřípadě rozměry objektu. Proto je tento radar dobrý například pro statistické účely na silnici, nebo v letecké technice. [3][7]

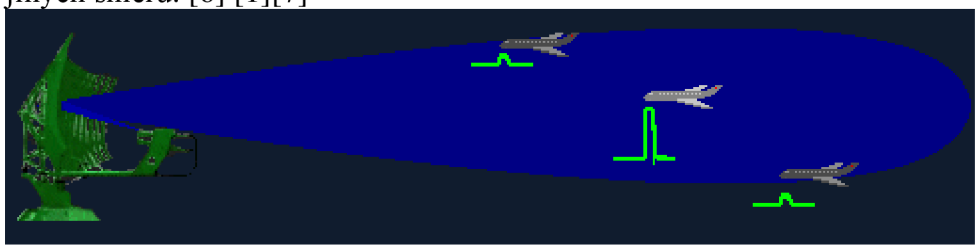
- Radar se spojitou vlnou – tento radar musí mít dvě antény, jednu vysílací, která neustále vysílá signál o konstatní frekvenci i amplitudě a jednu přijímací, která neustále přijímá odražený signál. Používá se především k měření rychlosti, například u policejních radarů. [3][7]

- Radar s frekvenčně modulovanou spojitou vlnou – těmto radarům se v práci budu věnovat nejvíce a mají také vysílací a přijímací anténu, které neustále pracují, ovšem vysílaný signál má proměnnou (lineárně rostoucí) frekvenci a stálou amplitudu. Jedná se o jeden z nejmodernějších typů radarů a jelikož měří vzdálenost, rychost, úhel i např. počet objektů, má velice široké využití, ať už v zabezpečovací technice, požární technice, stastistice, nebo také v automobilovém průmyslu (například senzory pro automní vozidla). [4][7][8]

Pasivní radary jsou už méně časté, velké využití ovšem nacházejí ve vojenské technice. Aktivní radary jsou mnohem jednoduššeji vystopovatelné než radary pasivní, jelikož neustále vysílají signál a dají se tedy lehce zaměřit, zatímco pasivní radar jen přijímá elektromagnetické vlny, které dnes moderní letouny vysílají téměř neustále, například při komunikaci s letištěm či při zjišťování polohy. [5][7]

Další způsob dělení je podle způsobu zjišťování polohy měřeného objektu. Směroměrné radary mají více přijímačů a využívají směrovosti antén. Směrovost je vlastnost antény, která popisuje závislost intenzity přijatého/vyslaného signálu na směru příjmu/vyslání signálu. Číselně se tato vlastnost vyjadřuje činitelem směrovosti, který je dán poměrem intenzity vyzářeného (přijatého) záření do jednoho směru ku intenzitě záření vyzářeného (přijatého) do celého prostoru. Příklad směrové antény je na obrázku

2.3. Je vidět že signál v přímém směru před anténou má vyšší hodnotu intenzity než signál z jiných směrů. [6] [1][7]



Obr. 2.4 Příklad směrové antény [1]

Časoměrné radary také mají více přijímačů a měří dobu letu signálu k jednotlivým přijímačům, z čehož pak určí polohu objektu. Dopplerovské radary poté využívají posun frekvence a pokud mají také více přijímačů, zjistí i polohu objektu. [4] [6]

3. RADARY PRACUJÍCÍ V OBLASTI MM VLN

Obsah této kapitoly, vyjma podkapitoly 3.2 vychází ze zdroje [9]

Radary pracující v oblasti mm vln, stejně jako mnoho dalších radarů, fungují na principu vysílání elektromagnetického signálu, který je odražen od objektu v zorném poli senzoru a přijatý odražený signál slouží ke zjištění vzdálenosti, rychlosti a úhlu objektu, popřípadě objektů a jejich počtu.

Jak z názvu těchto senzorů vyplývá, pracují v oblasti mm vln, tzn. podle vzorce 3.1, že frekvence vysílaného signálu se pohybuje v řádu desítek GHz. Tyto frekvence umožňují použití relativně malých vysílačů (antén), což vede k miniaturizaci celého systému (radaru). Mm vlny nejsou ovlivněny faktory okolí jako počasí, jasnost, kouř a další, které ovlivňují radary například typu Lidar, nebo ultrazvukové radary.

$$\lambda = \frac{c}{f} \tag{3.1}$$

Kde: λ – vlnová délka [mm]
c – rychlost světla (zaokrouhleně 300 000 km/s)
f – frekvence [Hz]

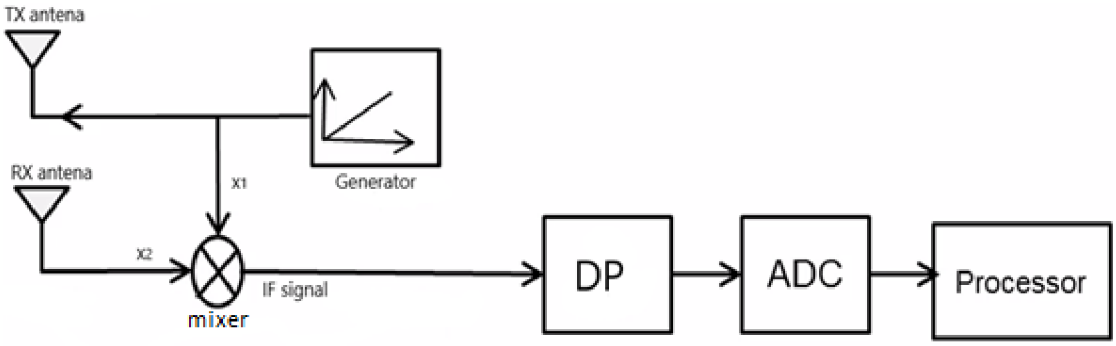
Tyto senzory mají velice široký rozsah použití, především díky jejich robustnosti (rozeznají pohyby ve vzdálenosti v řádu mm, ale až po stovky metrů) a vysoké přesnosti (zlomek milimetru).

Většina mmWave senzorů (= senzory pracující v oblasti milimetrových vln) používá schéma FMCW radaru (viz obrázek 3.1), což znamená, že nevysílá pulsy o konstantní frekvenci jako většina radarů, ale vysílají frekvenčně modulovaný spojitý signál (FMCW).

3.1 Princip FMCW radaru

FMCW radary se skládají ze základních bloků, které jsou znázorněny na obrázku 3.1. Generátor signálu (synthesizer) generuje signál, který je následně vysílán pomocí Tx antény. Signál odražený od objektu je přijat na přijímací anténě Rx. Tyto signály jsou spojeny v bloku směšovače (mixer), na jehož výstupu je tzv. IF signál. Tento IF signál se dále zpracovává a pomocí něj se vypočítávají parametry objektu jako je vzdálenost, úhel, počet a rychlost objektů.

Jelikož označení "signál" pro vyslanou elektromagnetickou vlnu by mohlo být v následujících kapitolách zavádějící, budu pro něj používat anglické označení "chirp".



Obr. 3.1 Základní blokové schéma FMCW radaru [9]

Směšovač je zařízení se dvěma vstupy x_1, x_2 a jedním výstupem IF. Signály x_1 a x_2 jsou v následujícím tvaru:

$$x_1 = \sin(\omega_1 t + \phi_1) \quad (3.2)$$

$$x_2 = \sin(\omega_2 t + \phi_2) \quad (3.3)$$

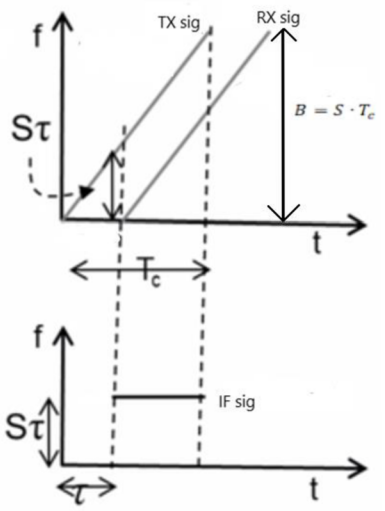
Kde: x_1, x_2 – vstupní signály směšovače (vysílaný a přijímaný)
ω_1, ω_2 – úhlová frekvence signálu [rad/s]
t – čas [s]
ϕ_1, ϕ_2 – fáze signálu [°]

Frekvence IF signálu je rovna rozdílu frekvencí vstupních signálů a fáze IF signálu je rovna rozdílu fází vstupních signálů (vzorec 3.4).

$$IF = \sin[(\omega_1 - \omega_2)t + (\phi_1 - \phi_2)] \quad (3.4)$$

3.1.1 Měření vzdálenosti

Pokud je před radarem jeden objekt, vyslaný signál se odrazí a je zachycen přijímačem s časovým zpožděním τ. Na obrázku 3.2 jsou vidět frekvence vyslaného a přijatého signálu (lineárně rostoucí) a IF signálu, který má mezi dobou τ a T_c konstantní frekvenci, která je přímo úměrná strmosti S a době mezi vysláním a přijetím odraženého signálu τ. Šířka pásma vysílaných frekvencí je určena strmostí nárůstu frekvence a dobou, po kterou je signál vysílán (Obrázek 3.2).



Obr. 3.2 Časový průběh frekvencí – vyslané, přijaté a IF signálu [9]

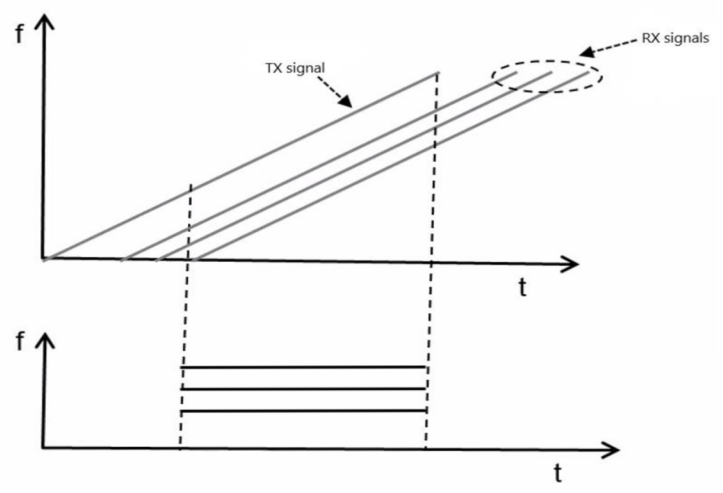
Jelikož známe rychlost šíření elektromagnetické vlny (chirpu), která je rovna rychlost světla c a dobu, za kterou signál urazí vzdálenost k objektu a zpět, můžeme vypočíst vzdálenost, kterou signál urazil a označíme ji 2d, jelikož signál musí dorazit k objektu a zpět. Vzdálenost d tedy označuje vzdálenost objektu od radaru.

Frekvence IF signálu mezi časy τ a T_c je přímo úměrná vzdálenosti objektu a to podle vzorce 3.5.

$$f_{IF} = S\tau = \frac{2dS}{c} \tag{3.5}$$

Kde: S – strmost růstu frekvence [Hz/s]
τ – doba mezi vysláním signálu a jeho přijetím [s]

Hodnoty τ bývají oproti hodnotám T_c velice malé, například pro radar s dosahem 300m a dobou T_c = 40μs je hodnota τ = 2μs. Pokud se před radarem nachází více objektů, přijímací anténa zachytí postupně více signálů a v IF signálu se poté objeví více složek frekvencí (obrázek 3.3), které zjistíme pomocí Fourierovy transformace.



Obr. 3.3 Průběh frekvencí v případě více objektů v zorném poli radaru [9]

Abychom tyto frekvence pomocí Fourierovy transformace rozlišili, musí se lišit o více než 1/T Hz, kde T je doba pozorování signálu. Z tohoto tvrzení můžeme nyní zjistit, jak daleko od sebe mohou minimálně být objekty, abychom rozlišili, zda se nejedná pouze o jeden objekt.

Pokud tedy uvažujeme, že rozdíl frekvencí je úměrný rozdílu vzdáleností (vzorec 3.6. vlevo) a zároveň rozdíl frekvencí musí být větší než $1/T_c$ (vzorec 3.6. vpravo) ($T=T_c$ při zanedbání τ), abychom ho pomocí Fourierovy transformace rozpoznali, pak úpravou těchto výrazů získáme rozlišení rozsahu FMCW radaru, což je jeden z důležitých parametrů. (vzorec 3.7).

$$\Delta f = \frac{2S\Delta d}{c} \quad \wedge \quad \Delta f > \frac{1}{T_c} \tag{3.6}$$

Kde: T_c – doba po kterou je signál vysílán [s]

Úpravou těchto vztahů získáme vztah pro rozlišení rozsahu a to:

$$\Delta d > \frac{c}{2ST_c} \tag{3.7}$$

A jelikož z obrázku 3-2 víme, že strmost násobená dobou vysílání signálu T_c je rovna šířce pásma B, můžeme tento vztah upravit na vztah 3.8, ze kterého je zřejmé, že rozlišitelnost rozsahu můžeme zvyšovat zvyšováním šířky pásma vysílaných frekvencí. [9]

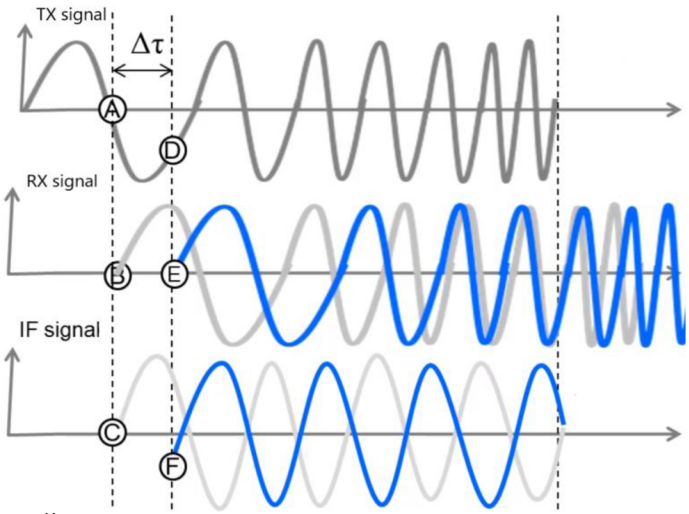
$$\Delta d > \frac{c}{2B} \quad => \quad d_{res} = \frac{c}{2B} \tag{3.8}$$

Kde: B – šířka pásma vysílané fekvence [Hz]

Fáze IF signálu

Pro rozeznání velmi malých změn vzdáleností (zlomek vlnové délky signálu) nemůžeme použít rozpoznání pomocí frekvence, ale musíme se zabývat fází IF signálu. Pomocí fáze můžeme tedy zjišťovat velmi rychle a přesně rychlost objektů.

Fáze IF signálu je dána rozdílem fází vyslaného a přijatého signálu. Na obrázku 3.4 je vidět, jak se změní IF signál, pokud se objekt pohne o velmi krátkou vzdálenost, to znamená, že signál bude přijat o $\Delta\tau$ později. Na frekvenci se to téměř neprojeví (nelze rozeznat Fourierovou transformací), nicméně je vidět změna fáze IF signálu, a to podle vzorce 3.9.



Obr. 3.4 Časový průběh vysланého, přijatého a IF signálu [9]

$$\Delta\phi = 2\pi f_c \Delta\tau = \frac{4\pi\Delta d}{\lambda} \tag{3.9}$$

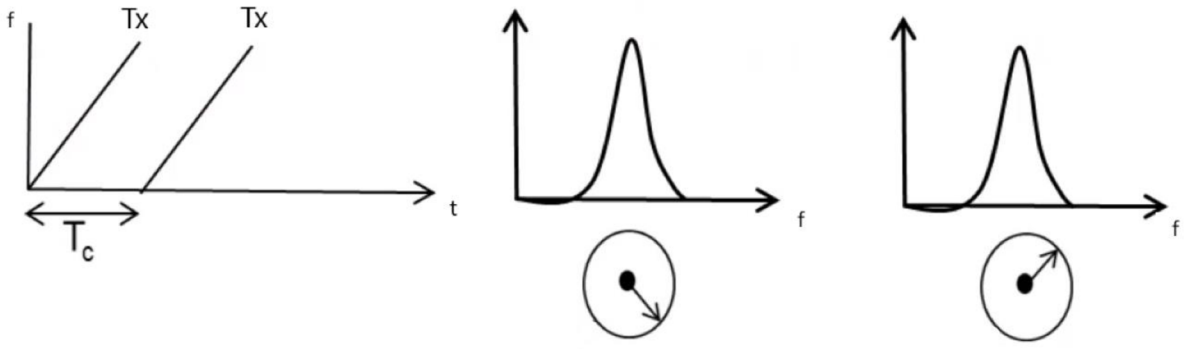
Ze vzorce 3.9 je zřejmé, že fáze IF signálu se mění úměrně s časovým zpožděním zachycení odraženého signálu, který odpovídá vzdálenosti objektu.

Pokud tedy před radarem máme jeden objekt, tak IF signál je sinusoida, kterou můžeme matematicky popsat vztahem 3.10. Frekvence se mění podle vzorce 3.6 se změnami vzdálenosti většími, než je vlnová délka signálu a fáze se mění podle vzorce 3.9 se změnami vzdálenosti menšími ne je vlnová délka signálu.

$$IF = A\sin(2\pi f t + \phi_0) \tag{3.10}$$

3.1.2 Měření rychlosti

Jak je již zmíněno v předchozí kapitole, pro měření rychlosti využijeme změnu fáze IF signálu, a to tím způsobem, že vyšleme dva signály T_x po sobě, přijmeme tedy dva signály R_x s velmi blízkou frekvencí (neboť se objekt během času T_c pohnul o malou, nebo žádnou vzdálenost) ovšem s jinou fází (pokud se objekt pohybuje, pokud se nepohybuje, fáze i frekvence zůstanou stejné a objekt je vyhodnocen jako objekt s nulovou rychlostí). Na obrázku 3.5 jsou vidět vyslané signály Tx a frekvenční spektra IF signálu, která jsou totožná, ovšem mají jinou fázi. [9]



Obr. 3.5 Změna fáze IF signálu [9]

Fáze se tedy změnila podle vzorce 3.9 a jelikož změna fáze v čase odpovídá úhlové rychlosti ω a změnu vzdálenosti můžeme zapsat jako rychlost, kterou se objekt pohybuje vynásobenou časovým úsekem Tc během kterého předmět pozorujeme. Získáváme tedy vzorec 3.11, ze kterého můžeme vyjádřit rychlost a je zřejmé, že rychlost objektu můžeme určit z úhlové rychlosti IF signálu. Tímto způsobem se dají dobře měřit například vibrace, kdy frekvence IF signálu zůstává stejná, ale fázor fáze rotuje úhlovou rychlostí ω.

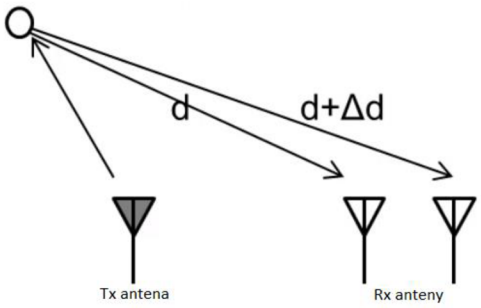
$$\omega = \frac{4\pi v T_c}{\lambda} \quad => \quad v = \frac{\lambda \omega}{4\pi T_c} \tag{3.11}$$

Kde: v – rychlost měřeného objektu [m/s]

3.1.3 Měření úhlu

V předchozích kapitolách je vysvětleno, jakým způsobem lze pomocí FMCW radaru určit vzdálenost, rychlost a popřípadě počet objektů. V této kapitole bude vysvětleno, jak určíme úhel objektu vzhledem k pozici radaru, což je důležité, jelikož bychom bez toho nezjistili nejen přesnou polohu objektu, ale například pokud by se ve stejné vzdálenosti od radaru nacházelo více objektů se stejnou rychlostí, nebyli bychom schopni je rozlišit.

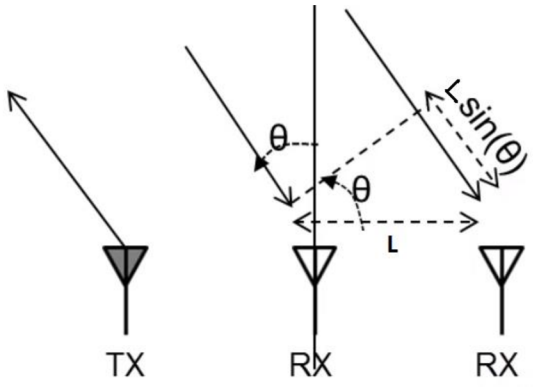
Pro určení úhlu jsou potřeba minimálně dvě přijímací antény. Přidáním druhé antény bude odražený signál přijat dvakrát a pokaždé urazí jinou vzdálenost (znázorněno na obrázku 3.6). Rozdíl těchto vzdáleností je dán vzdáleností objektu od antén a vzdáleností antén od sebe.



Obr. 3.6 Určení úhlu objektu pomocí druhé přijímací antény [9]

Podle vztahu 3.9 z předchozí kapitoly víme, že pokud se vzdálenost objektu mění pouze o malé vzdálenosti, mění se nám úhlová rychlost IF signálu. Podobně je tomu i v tomto případě, kde úhlová rychlost IF signálu bude odpovídat vzdálenosti Δd podle vzorce 3.12.

$$\omega = \frac{2\pi\Delta d}{\lambda} \tag{3.12}$$



Obr. 3.7 Obrázek pro výpočet úhlu pomocí dvou přijímacích antén [9]

Za předpokladu, že objekt je dostatečně daleko (vzhledem ke vzdálenosti přijímacích antén (L)), můžeme považovat oba dva signály za rovnoběžné. Z obrázku 3.7 je zřejmé, že vzdálenost, kterou signál urazí navíc, než dorazí k druhé anténě můžeme zapsat podle vzorce 3.13.

$$\Delta d = L\sin(\theta) \tag{3.13}$$

Kde : θ – úhel pod kterým dopadá signál na přijímací antény (viz obrázek 3-7)

Dosazením do vzorce 3.13 a vyjádřením úhlu θ získáváme vzorec pro výpočet úhlu (3.14).

$$\omega = \frac{2\pi L\sin(\theta)}{\lambda} \Rightarrow \boldsymbol{\theta = \sin^{-1}\left(\frac{\lambda\omega}{2\pi L}\right)} \tag{3.14}$$

Na signál z každé antény aplikujeme 2D-FFT a získáme podobný výsledek jako u měření rychlosti, špička bude v bodě kde je stejná vzdálenost i rychlost, ovšem bude mít jinou fázi, která tentokrát odpovídá úhlu. Změřením rozdílu fází pak můžeme určit podle vzorce 3.14 úhel.

Jelikož závislost mezi úhlem objektu a úhlovou rychlostí je narozdíl od měření předchozích veličin nelineární, je zjišťování úhlu nejpřesnější, pokud je objekt přímo před radarem ($\theta = 0°$) a klesá s rostoucím θ.

Úhel více objektů - pokud je ve stejné vzdálenosti více objektů se stejnou rychlostí, signál bude obsahovat více frekvencí, potřebujeme tedy více antén a provedeme FFT, tím zjistíme, jaké úhlové rychlosti se ve spektru nacházejí a z nich zjistíme příslušné úhly.

3.1.4 Zorné pole senzoru

Úhel objektu se podobně jako rychlost určuje z fáze IF signálu. Fáze se mění od 0° do 360°, pokud se objekt pohybuje na levou stranu od radaru, úhlová rychlost je kladná, pokud na pravou stranu, je úhlová rychlost záporná. Abychom mohli jednoznačně určit pozici objektu, musí mít „omega“ hodnoty od 0° do 180°. (Jinak by se například u hodnoty 10° nedalo určit, zda je objekt na levé straně blízko osy, či na pravé straně vzdálen od osy).

Pro výpočet maximálního měřitelného úhlu tedy vycházíme z toho, že hodnota úhlové rychlosti je pro maximální úhel rovna 180° (π). (rovnice 3.15). Z této rovnice se již dá vyjádřit maximální měřitelný úhel. [9]

$$\frac{2\pi L \sin(\theta_{max})}{\lambda} = \pi \Rightarrow \quad \theta_{max} = \sin^{-1}\left(\frac{\lambda}{2L}\right) \tag{3.15}$$

Největšího zorného pole dosáhneme, pokud vzdálenost L mezi anténami bude odpovídat polovině vlnové délky λ/2 a bude tedy +-90°.

3.2 Frekvenční pásma

V této práci se několikrát zmiňuji o tom, že senzory vysílají do okolí elektromagnetické signály o frekvencích v řádu desítek GHz. Dva typy radarů, kterým se v práci věnuji nejvíce používají pásmo 76-81 GHz. V této kapitole bych chtěl ujasnit, proč jsou to zrovna tato čísla.

Pokud někdo chce vysílat do okolí (především na veřejných místech) elektromagnetické vlny, musí se řídit určitou legislativou, jelikož v dnešní době je kolem nás velké množství zařízení vysílajících různé signály o různých frekvencích (mobily, televize, WiFi, 4G sítě, rádio, vysílačky, letadla atd.). Z těchto důvodů jsou na každém území takzvaná frekvenční pásma a je přesně určené které pásmo může kdo používat, právě proto, aby například doma sestavený vysílač nemohl rušit bezdrátovou komunikaci, nebo třeba televizní a rozhlasové vysílání. V České republice má toto

rozdělení na starost Český telekomunikační úřad a jelikož jsme v Evropské Unii, tak se musí řídit nařízeními evropského institutu pro komunikační standardy (European Institut for telecomunnication standards - EITC). Jelikož je TI americká firma, dodávající produkty do celého světa, musí její produkty vždy vyhovovat zákonům daného území. Pokud tedy někdo poskytuje zařízení vysílající do okolí signál o určité frekvenci, musí se řídit tím, aby byla daná frekvence povolena používat, popřípadě požádat o její užívání. Na webových stránkách českého telekomunikačního úřadu jsou přesně popsána jednotlivá frekvenční pásma, která jsou komu a za jakých podmínek přístupná.

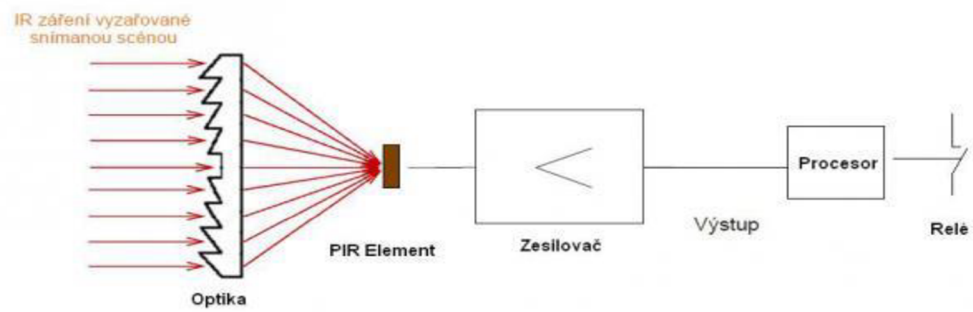
Většina senzorů od společnosti Texas instruments využívá frekvenční pásma 24 GHz (24 – 24,25 GHz, 60 GHz (60 – 64 GHz) a 77 GHz (77-81 GHz). Nicméně podle rozhodnutí EITC a amerického úřadu Federal Communications Comissions se od září 2018 nesmí vyrábět produkty vysílající do okolí signál o frekvenci 24 GHz a do roku 2022 musí být vyřazeny i stávající produkty.[9]

4. DOSAVADNÍ ŘEŠENÍ ELEKTRONICKÝ ZABEZPEČOVACÍCH SYSTÉMŮ

V dnešní době se v elektronické zabezpečovací technice (dále EZS) nejvíce využívá PIR čidel k detekci pohybu, případně v kombinaci s kamerami pro jednodušší identifikaci událostí probíhajících ve střežené zóně. Jednou z největších a nejrozšířenějších firem zabývajících se vývojem a distribucí EZS je kanadská firma Paradox, nabízející kompletní řešení zabezpečení od bytů po velké firmy. Z českých firem je jednou z největších výrobců a dodavatelů EZS firma Jablotron. Detektory se vyrábí v různých variantách a typech, například zmíněna firma Paradox aktuálně nabízí kolem sta typů detektorů rozdělených například podle odolnosti, přesnosti, venkovního nebo vnitřního použití, snímání pohybu, rozbití skla, detekce kouře a podle mnoha dalších parametrů. Tyto detektory jsou spolu propojeny a spojeny s ústřednou, která vše řídí. Do ústředny je připojena například klávesnice s displejem pro ovládání EZS obsluhou (zakódování/odkódování), popřípadě servisním technikem. K ústředně mohou být připojeny i další zařízení jako například čtečka otisku prstů pro vstup, samostatná tlačítka například na zakódování objektu, tablet pro pohodlnější ovládání, nebo sirény. [10] [11]

4.1 Princip PIR čidla

PIR čidlo, zkratka z anglického názvu Pasive Infrared Detector, česky pasivní infračervené čidlo je senzor pohybu založen na vyhodnocení změny dopadajícího infračerveného záření, které vysílá každý objekt s teplotou vyšší, než je absolutní nula. Pasivní je z toho důvodu, že do okolí nevysílá žádný signál, nebo záření, ale přítomnost objektu vyhodnocuje pouze na základě detekce infračerveného záření v určené zóně před detektorem. Princip je založen na pyroelektrickém jevu, který vychází z toho, že při deformaci krystalické mřížky dielektrik vzniká na deformované látce elektrický náboj. Deformaci látek lze provést buďto tlakem (piezoelektrický jev), nebo změnou jejich teploty (pyroelektrický jev). Pyroelektrický jev tedy tvrdí, že je daná látka schopna generovat náboj při změně její teploty. [12]



Obr. 4.1 Blokové schéma PIR čidla [12]

Dopadající infračervené záření je pomocí soustavy čoček, nebo zrcadel soustředěno na PIR element. Počet čoček (zrcadel) v soustavě zároveň rozděluje střeženou zónu na několik segmentů. PIR element je základ celého čidla, je vyroben z polovodičů citlivých na změnu intenzity infračerveného záření, je nastaven tak, aby snímal především takovou vlnovou délku záření, jakou vyzařuje lidské tělo (cca 9,4μm), v tomto elementu je i vestavěný citlivý FET tranzistor, který měří změnu náboje způsobenou právě změnou dopadajícího infračerveného záření. Signál je zesílen, v procesoru zpracován a na výstupu už je nějaký spínací prvek, například relé, nebo tranzistor, který reaguje na pohyb v zóně senzoru a může spustit poplach, nebo přivolat ostrahu. [12]

PIR čidla také bývají téměř vždy vybaveny tzv. „tamper“ ochranou. Pojmem tamper se označuje spínač uvnitř čidla, který čidlo chrání před úmyslným poškozením zvenčí, například před nežádoucím otevřením krytu čidla, nebo jeho zničení. Pokud je kryt otevřen, kontakt sepne (rozepne) a je hlášen poplach.

4.2 Zapojení a komunikace

PIR čidla je možno zapojovat několika způsoby. Nejčastěji se využívá zapojení pomocí sběrnice BUS, což je čtyřvodičová sběrnice – dva vodiče slouží pro napájení a dva se zemí pro přenos dat. Jednotlivá čidla jsou spojena touto sběrnicí s ústřednou, která s jednotlivými prvky oboustranně komunikuje. Čidla většinou bývají NC, to znamená, že při poplachu se rozepnou a v této kapitole budu uvažovat z důvodu zjednodušení pouze tyto čidla.

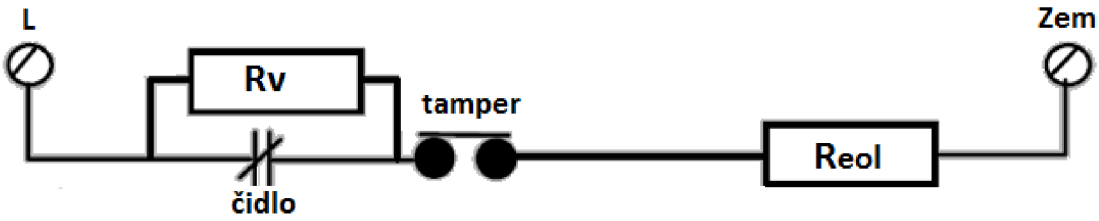
Nejjednodušší způsob zapojení je s jedním čidlem v zóně. Mezi svorku zóny a zem je připojeno jedno čidlo, které při se při poplachu rozepne a ústředna vyhodnotí v jaké zóně (podle toho na kterou je čidlo připojeno) se poplach odehrál.

Obr. 4.2 Nejjednodušší zapojení PIR

Dalším způsobem je přidat sériově k čidlu EOL rezistor (end of line, nebo také vyvažovací), z čehož vznikne tzv. vyvážená smyčka. V klidovém stavu je pak hodnota odporu smyčky rovna hodnotě EOL rezistoru. Pokud by se někdo pokusil obejít bezpečnostní systém například zkratem mezi zónou a zemí, tak to ústředna pozná, jelikož mezi zónou a zemí nebude požadovaný odpor R_{eol}, ale odpor téměř nulový.

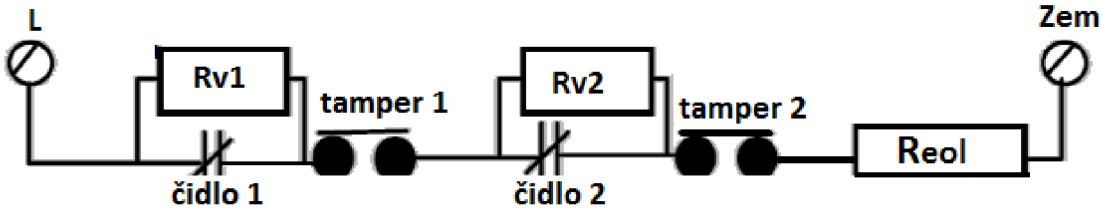
Obr. 4.3 Zapojení PIR s EOL rezistorem

Další možností je k čidlu paralelně připojit odpor, zatímco kontakt tamperu necháme v sérii k tomuto paralelnímu zapojení. Ústředna pak může jednoduše podle hodnoty odporu linky poznat, zda čidlo seplo (výsledný odpor dán součtem R_v a R_{eol}), či bylo narušeno (nekonečný odpor). Opět možnost s EOL odporem či bez.



Obr. 4.4 Zapojení PIR s odděleným tamperem a EOL rezistorem

Pokud chceme na jednu zónu připojit více čidel, tak je to možné, pokud ke každému čidlu paralelně připojíme odpor jiné hodnoty. Ústředna pak podle hodnoty odporu linky pozná, které čidlo seplo (popřípadě obě). Opět můžeme přidat i EOL rezistor, nebo oddělit tamperové kontakty od čidel. Kombinace těchto tři způsobů je na obr. 4-5.

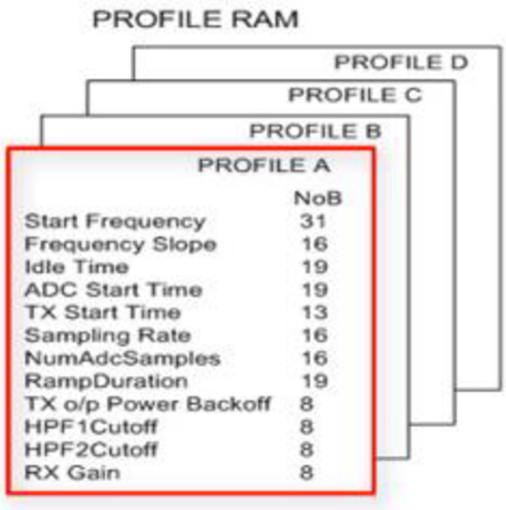


Obr. 4.5 Zapojení dvou PIR s oddělenými tampery a EOL rezistorem

5. KONKRÉTNÍ ŘEŠENÍ OD SPOLEČNOSTI TEXAS INSTRUMENTS

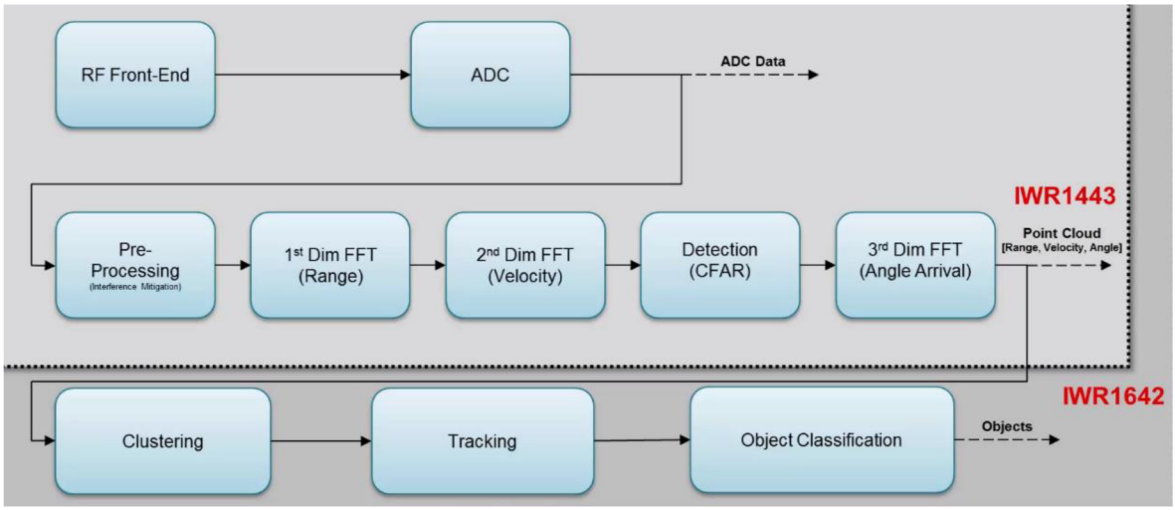
V této práci se budu zabývat radary od společnosti Texas Instruments. Tyto radary mají široké možnosti použití. Základní rozdělení těchto senzorů je na industrial (průmyslové) a automotive (automobilové). Zde se zaměřím především na industrial senzory IWR1443 a IWR1642. Právě senzor IWR1642 budu používat pro experiment v následujících kapitolách.

Tyto dva typy radarů vysílají signál o frekvenci 76-81 GHz se šířkou pásma až 4GHz. Obsahují čtyři vysílací antény a dvě (typ IWR1642), nebo tři (typ IWR1443) přijímací antény. Vysílaný signál (chirp) je možné programovat pomocí profilů (obrázek 5.1), kde je možné vytvořit až čtyři druhy chirpů pro jeden přenášený rámec (frame), což je výhodné, jelikož můžeme například v jednom framu zjišťovat objekty v krátkých i delších vzdálenostech (parametry chirpu ovlivňují maximální dosah radaru). [9]



Obr. 5.1 Profil pro naprogramování parametrů chirpu [13]

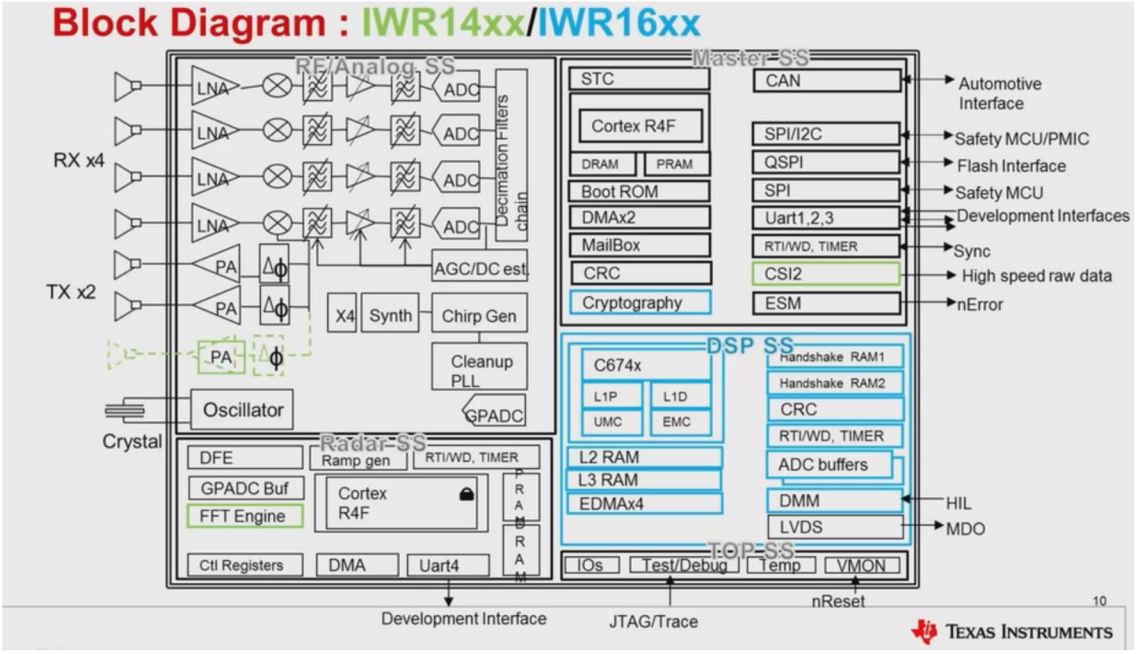
5.1 Základní řetězec úloh senzorů od TI



Obr. 5.2 Základní řetězec úloh senzorů IWR1443 a IWR1642 od TI [9]

Tento řetězec začíná blokem RF Front-End, tento blok obsahuje vysílací a přijímací antény, je v něm tedy přijímán odražený signál. je v něm také vytvořen IF signál, který je v dalším bloku A/D převodníku převeden na digitální (navzorkován). V následujícím bloku jsou vzorky připraveny na digitální zpracování, a to pomocí FFT (Fast Fourier Transform – rychlá Fourierova transformace). Jednoduchou FFT se získá vzdálenost, pomocí 2D FFT se získá rychlost a pomocí 3D FFT úhel jednotlivých odrazových bodů. Radar IWR1443 tyto kroky realizuje pomocí hardwarového urychlovače (hardware accelerator) a na výstup jde tzv. Point Cloud, což je soubor odrazových bodů obsahující jejich vzdálenost, absolutní rychlost a úhel. Radar IWR1642 tyto kroky realizuje pomocí DSP (C674X) a pokračuje dalším zpracováním Point Cloudu (clustering, tracking, object classification). Vytvoří trajektorii a ze shluku bodů a informací o nich vytvoří objekty, také pomocí DSP. Na výstupu už je tedy i informace o jednotlivých objektech. [9]

5.2 Blokové schéma senzoru IWR14xx/IWR16xx



Obr. 5.3 Blokový diagram čidel IWR14xx a IWR16xx od TI [9]

Blokový diagram je rozdělen na pět základních částí, které jsou níže popsány. Zeleně označené bloky jsou pouze v radaru IWR14xx, modře označené bloky jsou pouze v radaru IWR16xx.

- RF/Analog Subsystem
  Tento blok můžeme rozdělit na tři hlavní části a to:

- Hodiny
  Tato část generuje požadovanou frekvenci od 76 do 81 GHZ, celý senzor je řízen krystalem (Crystal), který kmitá na frekvenci 40 MHz, následuje fázový závěs (cleanup PLL), který frekvenci sníží a generátor požadovaného signálu pak pracuje s frekvencemi 19-20,25GHz. Za generátorem (Synth) je násobička frekvence x4 pro získání požadované frekvence. [9]

- Vysílací část
  Podle typu senzoru se vysílací část skládá ze dvou, nebo tří paralelních vysílacích řetězců. Amplituda a fáze jednotlivých řetězců je řízena nezávisle na sobě. Signál vytvořený v hodinové části je zde pomocí jednosměrné antény se zakončovacím odporem 50Ω vysílán do okolí. [9]

- Přijímací část
  Přijímací část se skládá ze čtyř paralelní částí, každá z nich obsahuje nízkošumový zesilovač (LNA – low noise amplifier), směšovač, IF filtr a AD převodník. Všechny čtyři části mohou pracovat paralelně. Funkce těchto bloků je popsána v předchozí kapitole. [9]

- Radarový Subsystém (také BSS – Built-in Self-test Subsystem)

  Obsahuje ARM cortex 4F procesor, běžící na 200 MHz, naprogramovaný pomocí firmwaru dodávaným výrobcem (TI) a je nepřístupný uživateli. Zajišťuje kalibraci, sebetestování (self-test) a monitoring funkcí v běžících v tomto subsystému. Uživatelské aplikace běží v části Master Subsystem a do Radarového subsystému nemají přímý přístup. Master Subsystem komunikuje s radarovým subsystémem pomocí definovaných zpráv, které jsou odesílány pomocí tzv. hardware mailboxes (mm Wave length API obsaženo v mm Wave Software development Kitu – SDK). [9]

- Master Subsystem

  Tato část obsahuje ARM procesor stejného typu jako je v radarovém subsystému, ale je určen pro zpracování uživatelských aplikací a dat, která mu poskytne DSP. Obsahuje také různá průmyslová komunikační rozhraní jako SCAN, I2C, UART, SPI a také podporují vysokorychlostní přenos surových dat pomocí CSI2 a LVDS. [9]

- DSP Subsystem (jen 16XX)

  Obsahuje digitální signálový procesor (DSP) C674X běžící na 400 MHz. Zajišťuje zpracování přijatého odraženého signálu a jeho zpracování pomocí Fourierových transformací a výpočtu vzdálenosti, rychlosti a úhlu jednotlivých odrazových bodů (viz kapitola 3 – radary pracující v oblasti mm vln) a vyhodnocování objektů. [9]

  V senzorech typu 14XX tyto operace zajišťuje tzv. hardware accelerator (hardwarový urychlovač). Jelikož v práci používám pro měření pouze radar 1642, nebudu zde funkci hardware acceleratoru podrobněji popisovat.[9]

5.3 Programování radaru

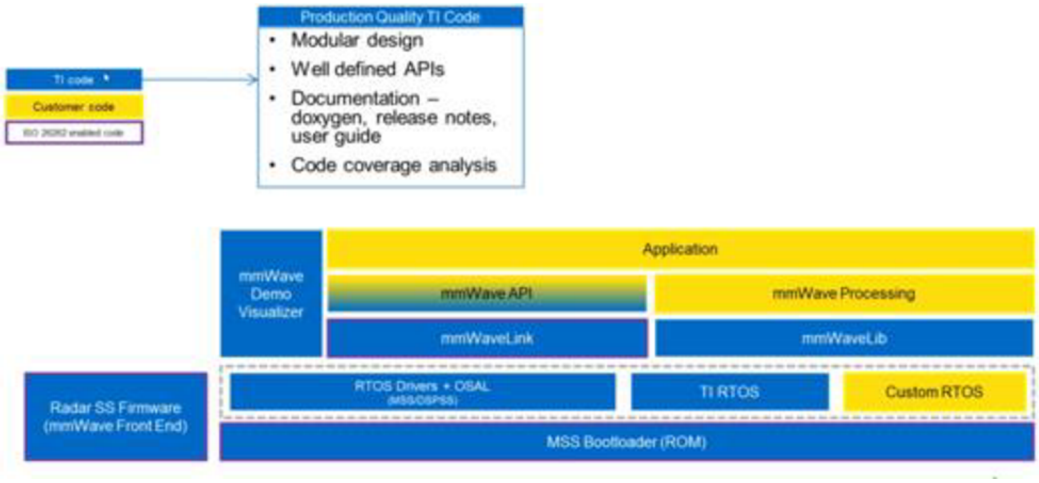
Obsah této podkapitoly vychází ze zdroje [9]

Pro programování radarů od společnosti TI slouží dvě základní platformy a to mmWave SDK (Software Development Kit) a mmWave Studio.

MmWave Studio slouží například k nadefinování parametrů chirpu pomocí abstraktních parametrů jako je maximální a minimální dosah radaru, rozlišitelnost objektů atd. Dále slouží k zachycení surových dat z radaru (z ADC) pro jejich následné zpracování.

MmWave SDK obsahuje RTOS (Real Time Operating System) pro procesory ARM a pro DSP. Dále obsahuje různé drivery a knihovny pro periferie. Také obsahuje mmWave api pro vysokoúrovňové programování.

Na obrázku 5.3 je blokový diagram popisující funkčnost mmWave SDK.



Obr. 5.4 Blokový diagram mmWave SDK [9]

Modré části jsou naprogramované od TI a jsou uživatelem neměnné, žluté části jsou jako vzor od TI a předpokládá se jejich modifikace uživatelem.

MSS Bootloader zajišťuje správné naběhnutí celého zařízení a také načítá a vykonává kód nahraný ze serial flash.

Radar SS firmware – řídí RF hardwarové analogové operace a je zodpovědný za všechny operace s radarem.

MmWave link – driver pro radar subsystém – poskytuje low-level API pro řízení všech hardwarových bloků (především FMCW chirp parameters)

MmWave API je nadstavba nad mmWave link a zajišťuje komunikaci mezi R4F MCU a DSP

SDK obsahuje část s bloky RTOS a to buď přímo od TI, nebo uživatelský RTOS.

MmWaveLib je knihovna obsahující základní funkce a algoritmy pro signalprocessing jako je FFT.

SDK také obsahuje základní aplikace, které ukazují použití těchto výše uvedených komponent pro vytvoření jednoduchých aplikací. Tyto aplikaci může uživatel upravovat pro vlastní použití

MmWave Demo Visualizer je jednoduché grafické uživatelské rozhraní a vykresluje data o objektech jako je vzdálenost rychlost, úhel.

Jelikož mmWave SDK nebudu ve vlastní realizaci používat, tak ani v této části nebudu dopodrobna popisovat jak funguje, nicméně je tu alespoň základní přehled bloků a popis jejich funkcí.

6. USPOŘÁDÁNÍ SENZORŮ A ZAMĚŘENÍ NA CÍLOVOU APLIKACI

Pro účely experimentu jsem si vybral jako objekt, který je potřeba zabezpečit chodbu v prostorách FEKT VUT a to konkrétně v budově SE ve druhém patře. Chodba je ve tvaru "T" a senzor umístěn nad dveřmi tím způsobem, že je čelem namířen na vstupní dveře na chodbu a zároveň snímá i části chodby při rozdvojení (doprava a doleva). Přesnější informace o umístění senzoru poskytují obrázky 6.1 až 6.4.

Toto řešení jsem zvolil především kvůli jednoduchosti. Pro základní zabezpečení objektu tohoto typu stačí jeden radar, s tím že perimetr lze následně rozdělit na zóny. Například zakódovat (zabezpečit) pouze pravé, nebo levé křídlo. Pro splnění požadavků cílové aplikace, která předpokládá zabezpečení tohoto křídla budovy, což znamená zjištění, zda se zde někdo nachází, kolik se tam nachází objektů (lidí), jejich přibližná velikost, rychlost a směr, kterým se pohybují, popřípadě v jaké části chodby zmizely z dosahu radaru (z důvodu nalezení narušitele) předpokládám, že je umístění jednoho radaru na této pozici (viz obrázky 6-1 až 6-3) vhodné. Více v 8. a 9. kapitole této práce, ve kterých se zabývám tím, jak moc je toto řešení spolehlivé a funkční a jak by se popřípadě dalo zdokonalit například přidáním dalšího radaru.

Obr. 6.1 Pohled na radar z pravé části chodby

Obr. 6.2 Pohled na radar z levé části chodby

Obr. 6.3 Pohled na radar zepředu (od vstupu)

Další možností je umístit senzor nad vchodové dveře (obrázek 6.4), to znamená přímo naproti umístění radaru z předchozího řešení. Funkce by byla velice podobná, jelikož by radar opět zabíral celou část chodby od vstupu a částečně i odbočení doleva a doprava. Výhodou by bylo méně nežádoucích odrazných ploch pro signál (kovová futra – porovnání obrázku 6.3 a 6.4), což by znamenalo lehké zpřesnění výsledků především v údajích o narušiteli). Problém by ovšem byl, pokud by narušitel pouze pootevřel dveře a do prostor nevcházel (například z důvodu nahlédnutí do prostor, nebo vpuštění nedetekovatelného média), pak by ho radar nezaregistroval. Z tohoto důvodu a z důvodu jednoduššího technického řešení (ústředna – stolní počítač – umístěna v kanceláři za dveřmi pod radarem) je vhodnější předchozí způsob umístění radaru.

Obr. 6.4 Možné umístění radaru

Třetí možností řešení umístění senzorů je použít více senzorů, například jeden pouze pro vstupní chodbu a jeden pro každé (levé a pravé) křídlo. Toto řešení jsem nerealizoval, jelikož jsem měl k dispozici pouze jeden senzor, byla by podstatně složitější konstrukce, náročnější a pomalejší vyhodnocování vzhledem k většímu množství dat a musela by se také řešit vzájemná interference radarů. V praxi by navíc toto řešení bylo podstatně dražší.

Podobně jako jsou PIR čidla zabezpečena proti otevření a vniknutí zvenčí, měl by být i tento radar zabezpečen podobným způsobem. Aby se k němu nikdo nepřipojil a nenahrával do něj falešná data je ošetřeno softwarově viz kapitola 7 - Návrh komunikačního protokolu. Zajištění radaru proti odejmutí z jeho pozice a například natočení jiným směr, ve kterém nebude žádný pohyb a následného vniknutí narušitele do objektu je možné zajistit například umístěním radaru na spínač, který bude konstrukcí radarů stlačen a sepnutý, při odejmutí radaru se rozepne a spustí poplach (princip podobný jako temperový kontakt u PIR čidel)

7. NÁVRH KOMUNIKAČNÍHO PROTOKOLU

7.1 Základní komunikace radaru

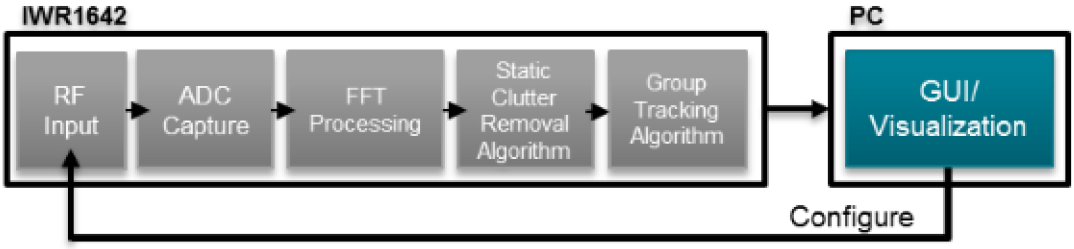
Pro účely experimentu v této bakalářské práci používám typ radaru IWR 1642, který je určen pro použití v průmyslovém prostředí. V čipu tohoto radaru jsou vysílací a přijímací antény, DSP a ARM procesor – podrobněji popsáno v kapitole 5 – Konkrétní řešení od společnosti Texas Instruments. Tento čip je pomocí dvou sériových linek spojen s TI Development Kitem, který zajišťuje převod komunikace ze sériové linky na USB. TI Development Kit je spojen s počítačem právě pomocí USB.

Jedna sériová linka zajišťuje oboustranný pomalejší přenos dat rychlostí 115200 baudů a zajišťuje předávání CLI příkazů radaru, nastavování parametrů jako například parametry chirpu, místnosti, errory. Druhá linka, rychlejší, komunikuje pouze jednostranně rychlostí 1Mboud a přenáší pouze data o objektu, která byla vyhodnocena v čipu radaru pomocí DSP a ARM procesoru, v tzv. framech. Data jsou přenášena po jednotlivých bytech, kde k přenosu jednoho bytu je potřeba 10 baudů (8 bitů dat + start a stop bit)

7.2 Komunikace konkrétního řešení

Pro aplikaci zabezpečení parametru používám v radaru zdrojový kód, který je volně dostupný na stránkách Texas Instruments v nástroji TI Resource Explorer. Konkrétně People Counting Demo pro radary IW16xx.

Na obrázku 7.1 je vidět blokově znázorněný tok dat mezi radarem a počítačem. TI Development Kit není znázorněn, jelikož jeho funkce není podstatná (jen převádí data ze sériové linky na USB)



Obr. 7.1 Blokové znázornění toku dat [13]

Radar odesílá data ve formátu zobrazeném na Obrázku 7.2.

První je hlavička framu o velikosti 52 bytů a obsahuje základní věci pro přenos jako synchronizační pattern, kontrolní součet bytů, verzi a typ platformy.

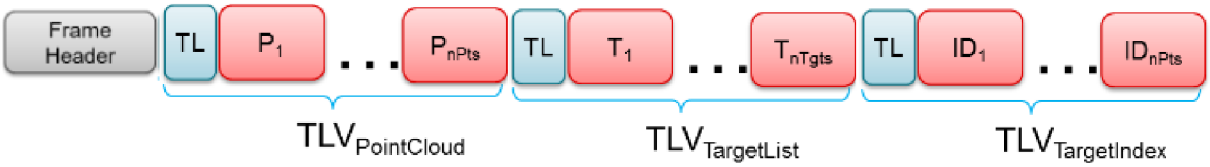
Následují tři druhy odesílaných dat ve formátu TLV (Type-Lenght-Value) Každý z těchto druhů má svou hlavičku, kde je informace o tom, jaká data se budou přenášet a jak budou velká a za hlavičkou následují data. Velikost dat je potřeba kvůli ověření, že chodí správná data.

První druh dat je PointCloud TLV, tyto data obsahují informaci o vzdálenosti, úhlu, absolutní rychlosti a síle signálu (snr) jednotlivých odrazových bodů. Tyto informace jsou získány zpracováním surových dat pomocí DSP v chipu radaru.

Duhý druh dat je TargetObject TLV. Shluk odrazových bodů z PointCloudu je při splnění určitých nastavených podmínek vyhodnocen jako objekt. TargetObject TLV pak obsahuje data o jednotlivých objektech – pozici, rychlost, zrychlení.

Třetí odesílaný druh dat je Target Index TLV, který přiřazuje ID jednotlivým objektům, ovšem z předchozího framu.

V příloze č. 1 je znázorněno, které konkrétní informace jednotlivé části přenášejí, jejich název, datový typ, velikost, stručný popis. Pod každou částí je také výpočet velikosti kvůli ověření správnosti dat a na konci přílohy příklad toho, jak mohou odesílaná data vypadat. [13]



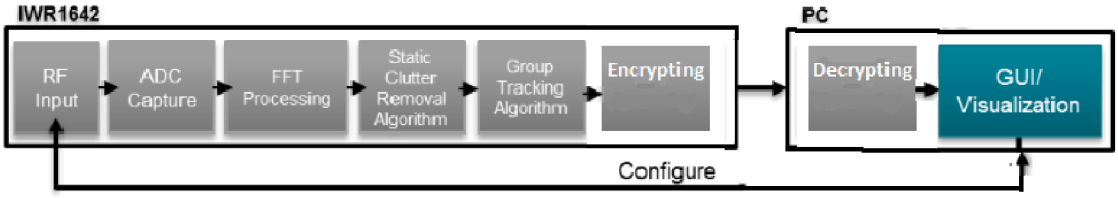
Obr. 7.2 Formát dat odesílaných radarem [13]

7.3 Vlastní návrh

Na stránkách Texas Instruments, konkrétně v TI Resource explorer je množství zdrojových kódu, jak pro radar, tak pro matlab, včetně definovaných komunikačních standardů. Není proto nutné navrhovat tyto kódy a protokoly úplně od začátku, je spíše vhodné buď použít veřejně dostupné přímo od výrobce (TI), popřípadě s drobnými úpravami. Proto v této kapitole navrhuji dvě řešení komunikačního protokolu. První je nechat odesílaná data ve formátu, které nabízí People Counting Demo s přidáním šifrování. Druhou možností je posílat pouze ta data, která nutně potřebuji k vyhodnocení zadaných kritérií.

7.3.1 Upravené stávající řešení

První možností je nechat odesílat data ve formátu, který nabízí People Counting Demo. Veškerá data, která jsou odesílána jsou v Příloze č.1. Jelikož se ovšem jedná o zabezpečovací techniku, je potřeba komunikaci nějakým způsobem zabezpečit, aby se nikdo nemohl připojit na sériovou linku a například posílat ústředně, nebo počítači data, která by simulovala klidový stav v zóně, zatímco by se narušitel mohl do střežené zóny bez problémů dostat. Základní blokové schéma toku dat z obrázku 7.1 by tedy bylo doplněné o blok šifrování tak, jak je zobrazeno na obrázku 7.3. Toto řešení má výhodu v jednoduchosti (není nutné psát nový vlastní protokol) a v robustnosti, pokud by kdokoliv chtěl využívat i další data například k různým analýzám, může je jednoduše získat. Nevýhodou tohoto řešení je větší množství přenášených dat.



Obr. 7.3 Blokové znázornění toku dat se šifrováním [13]

7.3.2 Protokol s odesíláním pouze požadovaných dat

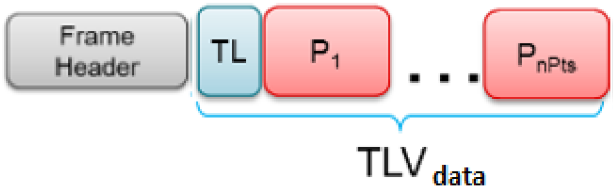
Druhou možností je neodesílat data tak, jak je to defaultně nastavené v používaném People Counting Demu, ale vytvořit si pro ně vlastní protokol. V rámci tohoto protokolu se pak odesílá frame header, který je stejný jako v příloze 1, za ním následují data TLV Data složená z hlavičky obsahující informaci o počtu objektů a velikosti dat včetně hlavičky. Informace o jednotlivých objektech jsou ukládány jako struktura DataStruct, která obsahuje pouze požadovaná data, což pro tuto cílovou aplikaci znamená počet objektů (pokud je roven nule, zóna je v klidu, pokud je vyšší než nula, vyhlásí se poplach), pozice objektu (v x-ové a y-ové ose), rychlost objektu (v x-ové a y-ové ose) a počet bodů ze kterých je objekt vytvořen, což vypovídá o mohutnosti objektu. Struktury hlavičky a dat mohou vypadat například takto:

```
TlvHeadStruct = struct (…
    ‘ObjNum’      {‘uint16’ , 2} … % Number of object
    ‘Length’      {‘uint32’ , 4}); … % TLV object length in bytes including header

DataStruct = struct (…
    ‘posX’ ,      {‘float’ , 4}, …  % Target position in x dimension [m]
    ‘posY’        {‘float’ , 4}, …  % Target position in y dimension [m]
    ‘velX’        {‘float’ , 4}, …  % Target position in x dimension [m/s]
    ‘velY’        {‘float’ , 4}, …  % Target position in y dimension [m/s]
    ‘pntNum’      {‘uint32’, 4}); … % Number of points in target [/]
```

Velikost odesílaných dat se vypočítá jako velikost hlavičky + počet objektů (ObjNum) * velikost DataStruct (v bytech).

Schéma odesílaného framu je na obrázku 7.4



Obr. 7.4 Formát dat vlastního řešení

7.3.3 Šifrování

V předchozích dvou podkapitolách jsem se věnoval pouze tomu, jaká data budou odesílaná, jak jsem se ovšem zmínil v úvodu kapitoly, je potřeba tyto data ještě zabezpečit. Způsobů, jak zabezpečit přenášená data je mnoho, jako nejvhodnější řešení jsem zvolil zabezpečení odesílaných dat pomocí elektronického podpisu.

Radar ke každým odesílaným datům přidá ještě elektronický podpis, který je vytvořen pomocí privátního klíče, který je uložen ve firmwaru radaru a nikdo jiný ho nezná. Pokud by se tedy někdo napojil na přenosovou linku a snažil se napodobit klidová data z radaru, ústředna, nebo počítač rozpozná, že je neposílá radar, jelikož jim bude chybět unikátní elektronický podpis a může například spustit poplach. V počítači, nebo v ústředně je uložen veřejný klíč pomocí něhož se ověří, zda přichází data se správným elektronickým podpisem. Nikdo, kdo nevlastní privátní klíč nemůže napodobit radarová data. Opatření dat elektronickým podpisem je zajištěno v ARM procesoru v čipu radaru.

7.3.3.1 Vytvoření a ověření elektronického podpisu

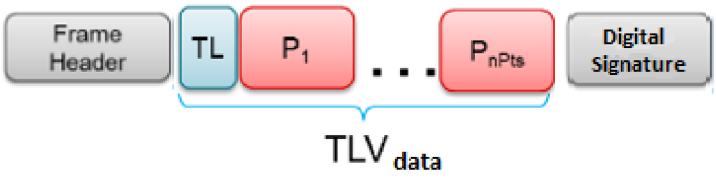
Princip vytvoření digitálního podpisu spočívá v asymetrické kryptografii a je znázorněný na obrázku 7.5. Data (na obrázku 7.5 označené jako Dokument), která chceme předávat z radaru dál na ústřednu, vytvoří pomocí hashovací funkce tzv. otisk (hash dokument). Hashovací funkce je matematický algoritmus, který z dat vytvoří číslo, které je podstatně menší než obsah dat a v praxi je pro danou zprávu v podstatě jedinečné, neboť je velmi nízká pravděpodobnost, že dvěma různým zprávám bude odpovídat jeden otisk. Toto číslo vzniklé hashovací funkcí (otisk) se opět pomocí matematické algoritmu zkombinuje s privátním klíčem, který vlastní pouze odesílatel dat (radar) a vznikne dokument i s digitálním podpisem. [14]

Obr. 7.5 Princip vytvoření elektronického podpisu [14]

V ústředně se data po přijetí ověrují, zda opravdu přišla data z radaru. Ověření probíhá ve dvou krocích. Přijatá data jsou rozdělena na dokument a podpis. Vytvoří se opět otisk dokumentu stejnou hashovací funkcí jako při odeslání. Zatímco podpis se pomocí veřejného klíče dešifruje a tím se získá původní otisk dokumentu. V případě, že jsou tyto dva otisky totožné, tak příjemce ví, že data opravdu odeslal systém (popř. osoba) s odpovídajícím privátním klíčem. [14]

7.3.3.2 Výsledný tvar odesílaných dat

Data odesílaná radarem, která už budou obsahovat elektronický podpis budou tedy mít strukturu stejnou jako je na obrázku 7.2, popřípadě 7.4, jen na konci bude následovat blok s elektronickým podpisem, jak je znázorněno na obrázku 7.5.



Obr. 7.6 Formát odesílaných dat se šifrováním

Lehce pozměněn bude i struktura Frame headeru a to tak, že bude obsahovat navíc položku obsahující délku elektronického podpisu, například takto:

‘SignLength’ {‘uint32’ , 4}); … % Length of digital signature signature in bytes

Velikost elektronického podpisu se pak musí také připočíst k výpočtům celkové velikosti kvůli kontrole přicházejících dat.

V případě reálného řešení, reálného zabezpečení objektů je popsané řešení – připojení čipu radaru přes TI Dev Kit pomocí USB do počítače a následné ovládání přes Matlab a mmWave Studio – velmi nevhodné. Vhodnější řešení je použít pouze radarový čip, jehož obsah je popsán v kapitole 5 – Konkrétní řešení od společnosti TI (hlavní bloky - vysílací a přijímací antény, DSP a ARM), k němu připojit kroucenou dvoulinku včetně nulového vodiče. Komunikace pak probíhá pomocí standardu RS-442 (z důvodu lepšího přenosu dat na větší vzdálenosti než u RS-232) a pomocí převodníku se převede na RS-232 a připojí do vyhodnocovací ústředny, která by vyhlašovala poplachy. Musel by se ovšem navrhnout i jiný vhodný způsob vizualizace, který by neběžel přesprogram Matlab.

8. NAMĚŘENÁ DATA, JEJICH ZPRACOVÁNÍ A VIZUALIZACE

8.1 Nastavení parametrů pro měření

8.1.1 Co je potřeba

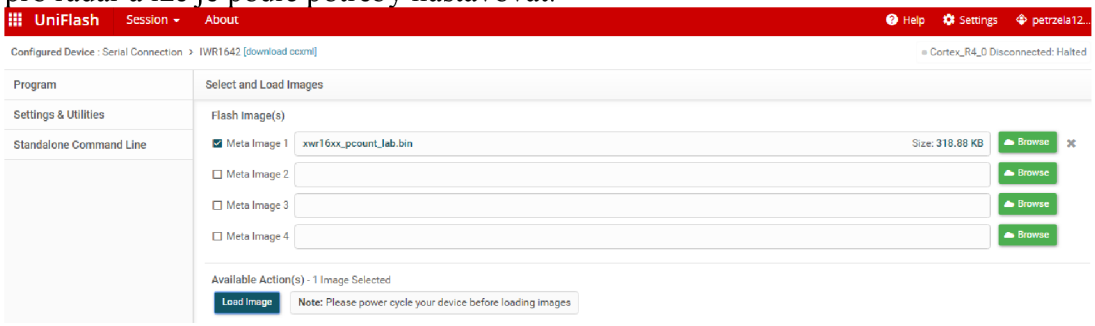
Pro rozchození radaru je potřeba splňovat určité softwarové a hardwarové požadavky. Tyto požadavky se mohou podle aplikace lehce lišit, pro mé měření jsem používal radar IWR 1642, připojený k TI Dev Kitu a přes USB kabel do počítače. Ze stránek společnosti Texas Instruments lze nainstalovat prostředí mmWave studio a mmWave SDK, přes které lze konfigurovat různé vlastnosti a parametry senzoru. Dále je vhodné mít v počítači program Matlab, přes který lze poměrně jednoduše zpracovávat, analyzovat a vizualizovat data získaná z radaru. Dále je vhodné mít účet na stránkách společnosti Texas Instruments.

Na webových stránkách společnosti TI lze získat veškeré informace ohledně jejich senzorů. Přes webové rozhraní TI Cloud Tools se dá dostat ke dvěma užitečným webovým nástrojům.

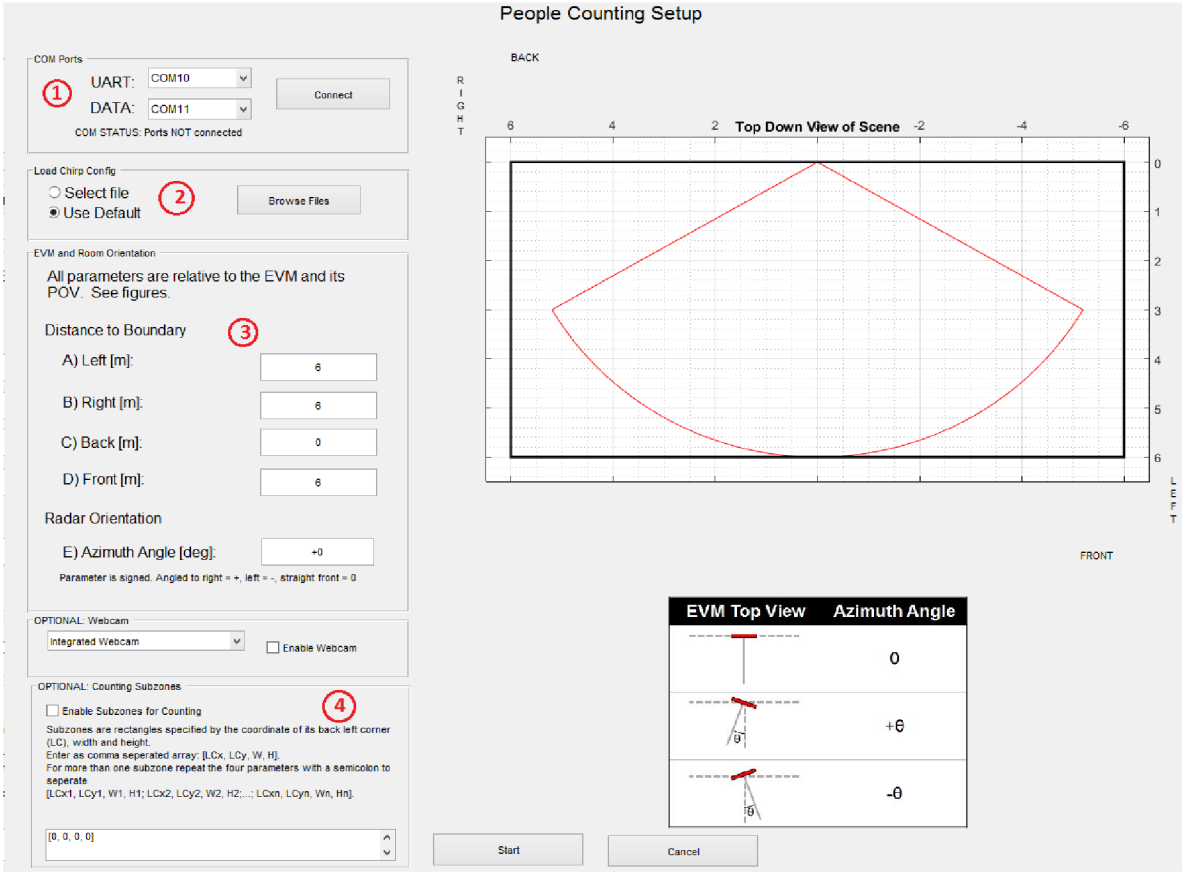
Prvním je TI Resource Explorer, ve kterém jsou na cloudu uložené různé knihovny, příklady, dema (připravené zdrojové kódy MatLabu i mm Wave Studia včetně veškeré dokumentace), dokumenty, zdrojové kódy atd. Druhým nástrojem je TI UniFlash přes který lze nahrávat parametry pomocí zdrojových binárních kódů do senzorů.

8.1.2 Jak nastavit Demo

Pro účely měření je použito Demo stažené z TI Resource Exploreru a to konkrétně 16xx - People Counting Demo. Toto demo je možné použít pro zabezpečení perimetru, jelikož je primárně určené pro počítání lidí v zóně radaru. Lze v něm nastavovat různé zóny, počítat kolik objektů se v jaké chvíli nachází v jaké zóně a podobné. Soubor z tohoto dema lze pomocí prostředí UniFlash nahrát do radaru (viz obrázek 8.1). V demu je také soubor obsahující zdrojové kódy do Matlabu. Po otevření a spuštění souboru v Matlabu se otevře okno s přednastavenými hodnotami některých parametrů pro radar a lze je podle potřeby nastavovat.



Obr. 8.1 Nahrání dat do radaru [13]



Obr. 8.2 Okno po spuštění Matlabového souboru z Dema

Popis obrázku 8.2:

1 – V části COM Ports se nastavují porty počítače ke kterým je radar připojen, po správném nastavení a připojení hardwaru potvrdit tlačítkem connect.

2 – V části Load Chirp Config lze nahrát parametry chirpu (uvedené v kapitole 5). Jedna možnost je nechat nastavené defaultně z Dema, druhá možnost je nahrát vlastní/upravený konfigurační soubor s vlastními parametry.

3 – V části EVM and room orientation se nastavují parametry místnosti, objekty za těmito vzdálenostmi jsou ignorovány. Těmito parametry Matlabu říkáme se kterými daty z radaru má počítat a vyhodnocovat je.

4 – V části Counting subzones lze rozdělit snímaný prostor na určité zóny, defaultně žádné zóny nastaveny nejsou, v podkapitole s vlatním nastavením budou zóny znázorněny. Zóny jsou ve tvaru čtverců/obdélníků a zadávají se jako vektor o čtyřech hodnotách – první x-ová souřadnice výchozího bodu zóny, druhá y-ová souřadnice výchozího bodu zóny (levý zadní roh z pohledu radaru), třetí je šířka zóny a čtvrtá délka . Pokud je potřeba zadat více zón, oddělují se mezi sebou hodnoty pro jednotlivé zóny středníkem.

Tyto zákadní parametry lze tedy nastavovat přes spuštěnou MatLab aplikaci a podle těchto parametrů Matlab vyhodnocuje data přicházející z radaru.

Pro nastavení parametrů radaru je v Demu konfigurační soubor "long_range_people_counting.cfg", jeho obsah je na obrázku 8.3. Tento soubor se nahrává do radaru.

```
dfeDataOutputMode 1
channelCfg 15 3 0
adcCfg 2 1
adcbufCfg 0 1 1 1
profileCfg 0 77 30 7 62 0 0 60 1 128 2500 0 0 30
chirpCfg 0 0 0 0 0 0 0 1
chirpCfg 1 1 0 0 0 0 0 2
frameCfg 0 1 128 0 50 1 0
lowPower 0 1
guiMonitor 1 1 0 0
cfarCfg 6 4 4 4 4 16 16 4 4 50 62 0
doaCfg 600 1875 30 1
SceneryParam -6 6 0.05 6
GatingParam 4 3 2 0
StateParam 10 5 10 100 5
AllocationParam 450 0.01 25 1 2
VariationParam 0.289 0.289 1.0
PointCloudEn 1
trackingCfg 1 2 250 20 200 50 90
sensorStart
```

Obr. 8.3 Defaultní obsah konfiguračního souboru [13]

Veškeré parametry jsou popsány v dokumentaci, která je součástí dema. Pro moji aplikaci jsou zajímavé především parametry SceneryParam, Allocation Param a popřípadě i StateParam.

SceneryParam
První dva parametry určují levou a pravou stěnu.
Druhé dva parametry horní a spodní mez (strop a podlaha).
Hodnoty jsou v metrech.

AllocationParam
První hodnota (SNR treshold) udává minimální hodnotu SNR (v součtu všech bodů z PointCloudu – každý bod má svou hodnotu SNR, která reprezentuje sílu odraženého signálu), aby shluk těchto bodů byl prohlášen za objekt. Změnou této hodnoty lze předcházet například falešným poplachům.

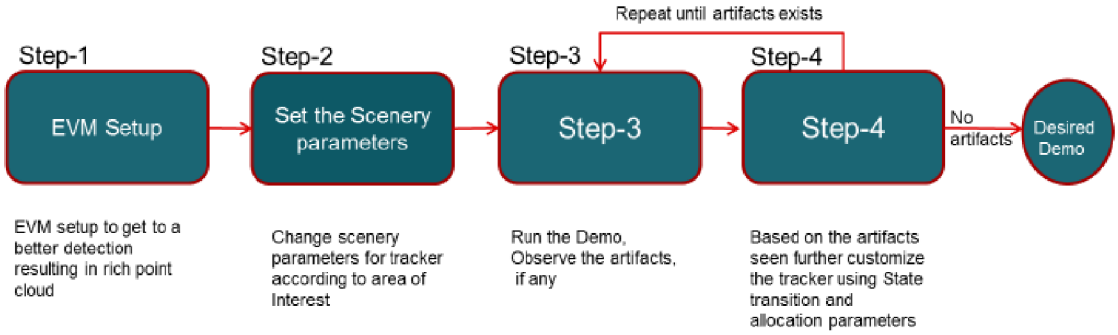
Druhá hodnota udává minimální rychlost, kterou chceme detekovat v m/s.

Třetí hodnota udává minimální počet bodů z PointCloudu, aby mohl být shluk prohlášen za objekt.

Čtvrtá hodnota udává maximální vzdálenost bodu od centru objektu, aby se ještě dal považovat za součást objektu (v m^2) a poslední parametr určuje maximální rozdíl rychlostí bodů, aby mohli být součástí jednoho objektu (v m/s).

StateParam
V tomto parametru se zapisují thresholdové hodnoty, které také určují, kdy se ještě považuje shluk bodů za objekt, nebo kdy se vypisuje jeho trajektorie.
První hodnota udává, kolikrát je potřeba za sebou zaregistrovat událost (odraz) od objektu, aby se začala zapisovat trajektorie objektu.
Druhá hodnota udává kolikrát musí přijít signál bez události (odrazů) od objektu, aby se trajektorie nezapisovala. Všechny hodnoty jsou opět popsány v dokumentaci, která je součástí dema.

Toto jsou základní věci, které je potřeba ve staženém demu nastavovat/upravovat. Na obrázku 8.4 je tento postup znázorněn graficky. Nejprve je nutné v okně People Counting Setup v části EVM and room orientation nastavit správné rozměry místnosti, aby Matlab nevyhodnocoval odrazy od stěn jako objekty. Poté nastavit parametry SceneryParam, aby radar věděl, která data má smysl vyhodnocovat. Následně spustit demo a sledovat co se děje a jak reaguje na objekty, na základě nežádoucích vyhodnocení poté upravovat parametry StateParam a AllocParam, abychom se zbavili například šumových odrazů, odrazů od drobných předmětů, lepší detekci počtu osob atd. Tyto dva kroky opakujeme, dokud nedostaneme žádoucí výsledky.



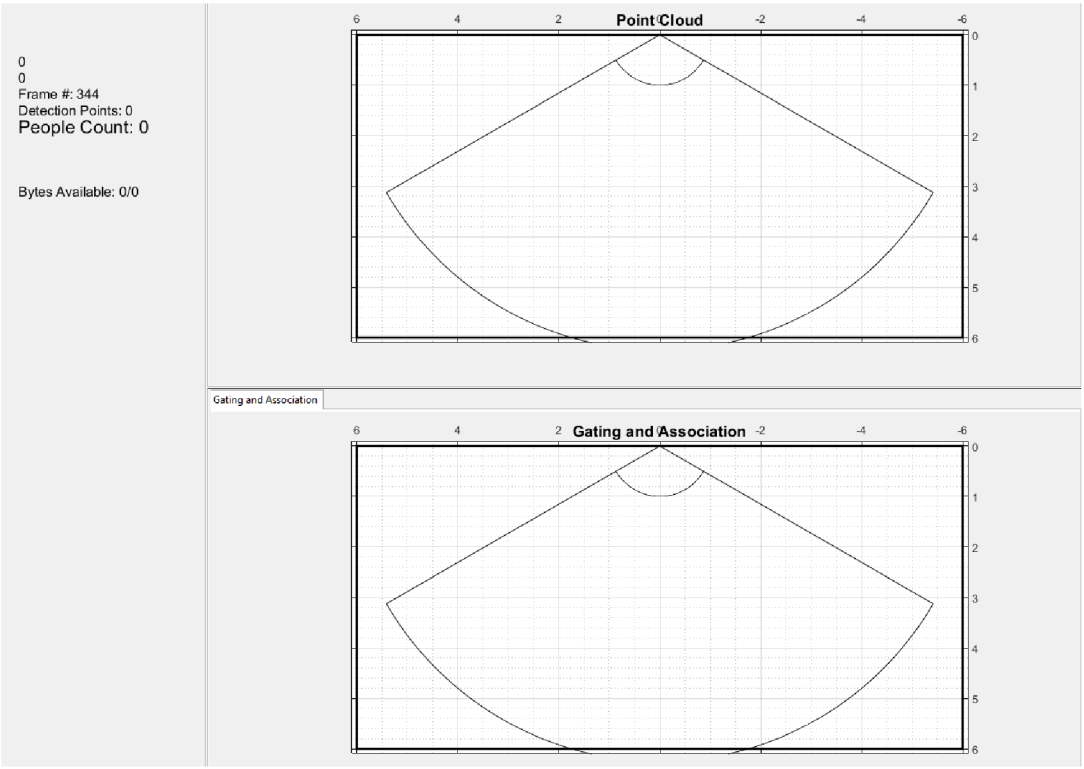
Obr. 8.4 Řetězec úloh při nastavování People Counting Dema [13]

Po spuštění programu pomocí tlačítka Start se otevře okno, které je na obrázku 8.5. Zde jsou dvě hlavní části:

PointCloud – zde se zobrazují jednotlivé odrazové body (jak bylo vysvětleno v kapitole 7 – Návrh komunikačního protokolu) a jejich trajektorie.

Gating and Association – zde se zobrazují objekty vyhodnocené na základě bodů z PointCloudu a jejich trajektorie.

V levé části je vidět počet objektů v zóně, aktuální číslo framu a počet detekovaných bodů.



Obr. 8.5 Okno spuštěného defaultně nastaveného Dema

8.2 Vlastní měření

Při měření jsem nastavoval parametry způsobem uvedeným v předchozích podkapitolách.

Parametry místnosti v People Counting Setup jsou nastaveny následovně a jsou stejné při každém měření :

Left : 2 m
Right : 2 m
Front : 6 m
Back : 0 m
Angle : 0 deg

Toto nastavení je zvoleno na základě parametrů chodby – vchodové dveře jsou přibližně 6 metrů před radarem, levou a pravou stranu jsem zvolil dva metry především kvůli uživatelsky příjemného zobrazení.

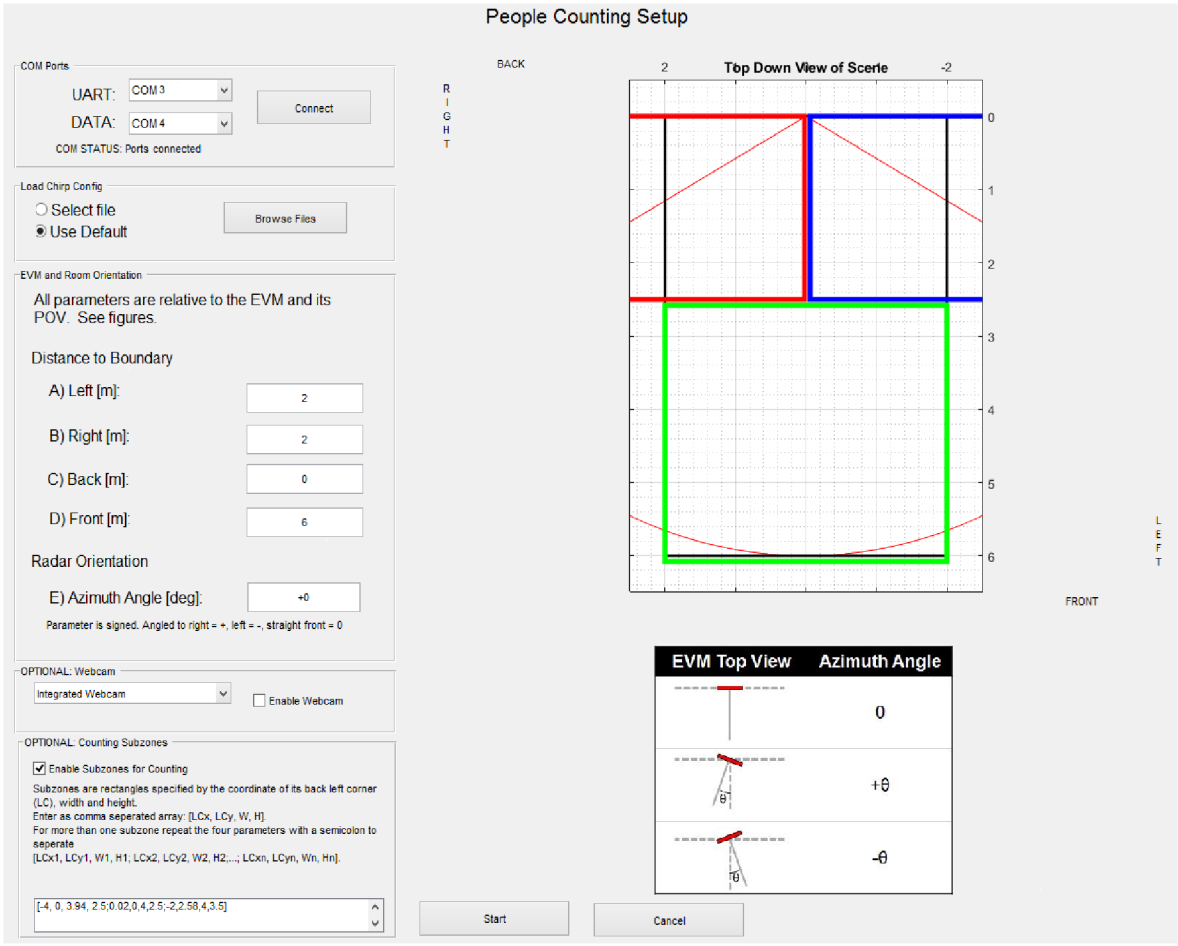
Scenery parameters jsou nastaveny takto:
“ SceneryParam 1.37 1.37 0 6 “
1.37 metru na každou stranu je experimentem zjištěná hodnota a je to dostačující vzdálenost pro určení toho, zda narušitel vstoupil do levého či pravého křídla, nebo nikoliv. Snímání od země je nastaveno na hodnotu 0, aby radar detekoval i například plazícího se narušitele.

Allocation parameters jsou nastaveny takto:
“ AllocationParam 450 0.01 17 1 2 “
Kromě třetí hodnoty zůstali tyto parametry nezměněné. Třetí hodnota určující minimální počet bodů, které budou prohlášeny za objekt jsem snížil na sedmnáct, tím se zvýšila citlivost a radar zachytí každého narušitele.

StateParam a ostatní parametry radaru zůstaly nezměněny tak, jak jsou napsány na obrázku 8.3.

První možnost, jak jsem nastavil zóny je tato:
[-4, 0, 4, 2.5 ; 0, 0, 4, 2.5 ; -2, 2.6, 4, 3.5]
Jsou zvoleny tři zóny a v tomto rozložení je možné detekovat, zda se narušitel nachází jen ve vstupní hale, nebo jestli vešel do dlouhé chodby (viz obrázky v kapitole 6 – Uspořádání senzorů a zaměření na cílovou aplikaci) a do kterého křídla (levé/pravé). Tímto způsobem rozložení zón je možné například zakódovat dlouhou chodbu (modrá a červená zóna) a nechat volně přístupnou jen vstupní část haly, přes kterou je možné jít například na záchody, ovšem pokud by objekt pokračoval dál ke kancelářím, tak se spustí poplach.

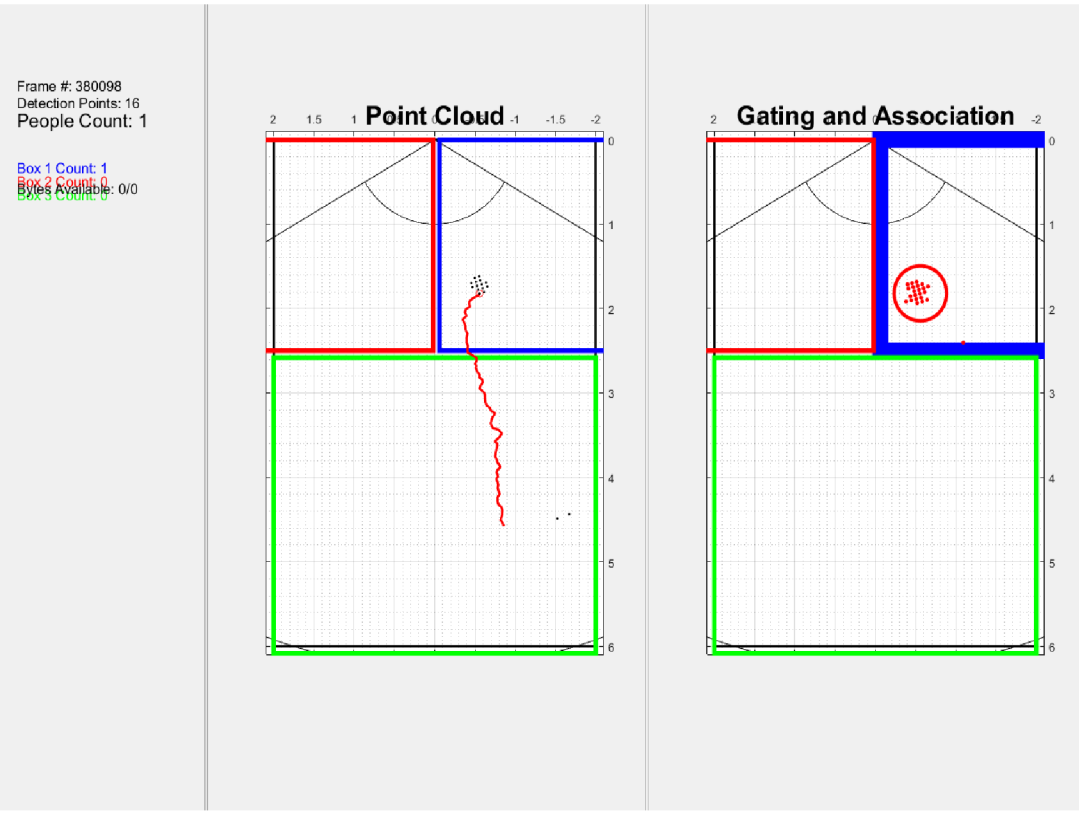
Nastavení těchto parametrů (PeopleCounting Setup a zóny) je vidět na obrázku 8.6.



Obr. 8.6 Okno People counting setupu s nastavenými parametry místnosti a zón

Takto nastavené demo detekuje počet osob v perimetru a rozlišuje kolik osob je v jednotlivých zónách. Toto nastavení zón je vhodné pro zabezpečení celé chodby, jakmile někdo vstoupí, dostaneme informaci o tom, že počet osob není roven nule a vyšle se poplach. Obsluha bezpečnostního systému, například ostraha objektu má i přehled o přesnější pozici narušitele a jeho přibližnou mohutnost (např. zda má s sebou psa, zda běží, nebo je v klidu atd.) a na základě těchto informací se může rozhodnout, zda na střežené místo dojít, jakým způsobem se vybavit, či zda například vyčkat příchodu na policie.

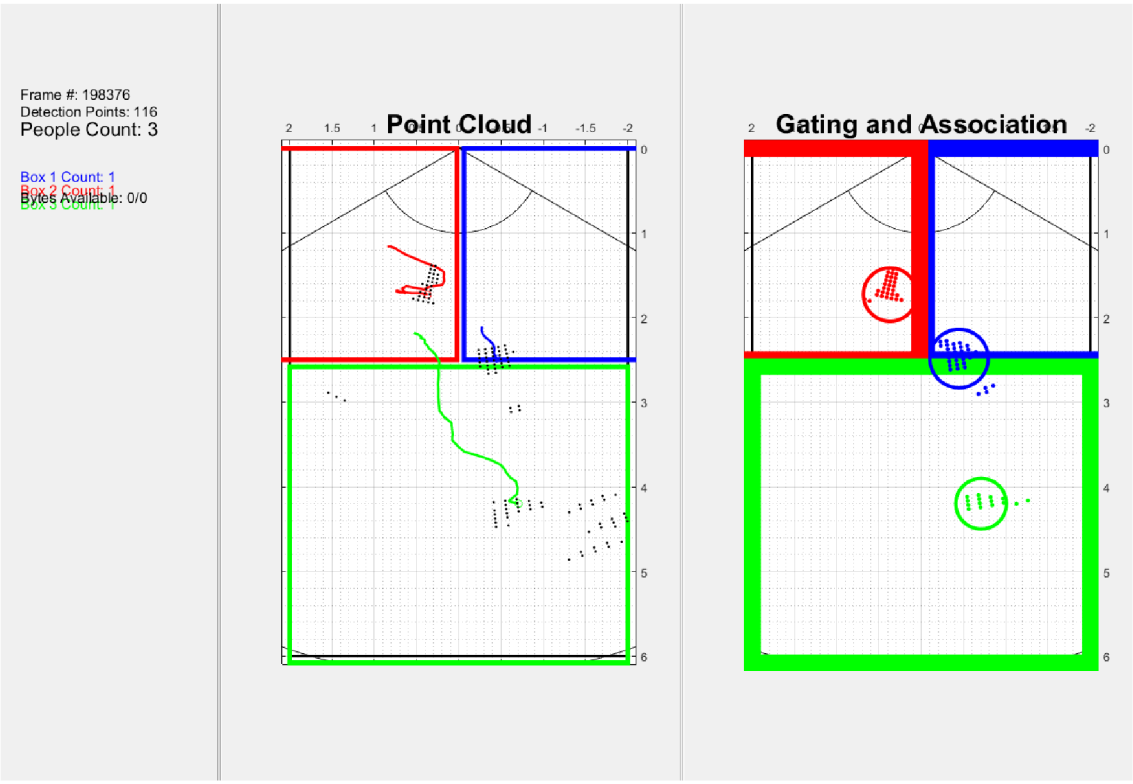
Na obrázku 8.6 je vidět snímek z vizualizace, kterou může obsluha bezpečnostního systému vidět, pokud je v zóně jeden narušitel, který přišel ze vchodových dveří a vydal se do pravého křídla. V levé části je vidět shluk bodů (PointCloud) s jeho trajektorií díky níž pozná odkud narušitel přichází. V pravé části už narušitel prohlášen za objekt, jelikož splňuje podmínky nastavené v konfiguračním souboru na celkovou hodnotu SNR (součet hodnot SNR jednotlivých bodů z Point Cloud) a minimální počet bodů splňujících dané vlastnosti. V levé části vidí v textové podobě celkový počet lidí v perimetru, počet detekovaných bodů a kolik osob se nachází v jednotlivých zónách.



Obr. 8.7 Snímek z vizualizace při jednom narušiteli přecházejícího ze zelené do modré zóny

Na následujícím obrázku 8.8 je snímek z vizualizace, pokud se do zóny dostalo více narušitelů (3). Na snímku se každý z narušitelů nachází v jedné zóně, což je patrné

z vizualizace (zóna v níž se objekt nachází má silnější okraj) i je to v textové formě v levé části, kde obsluha vidí celkový počet tři objektů a pod tím kolik objektů je v jaké zóně. V pravé části zelené zóny si v sekci Point Cloud lze všimnout několika bodů, které ovšem nejsou vyhodnoceny jako objekt. Zdrojem těchto bodů jsou odrazy od kovových předmětů na zdech chodby (především dveře). Body nejsou vyhodnoceny jako objekt především správným nastavením parametrů v konfiguračním souboru (nesplňují alokační parametry allocParam) a tudíž nepošlou nesprávnou informaci obsluze, popřípadě nevyhlásí poplach v jiné zóně, než se narušitel nachází.



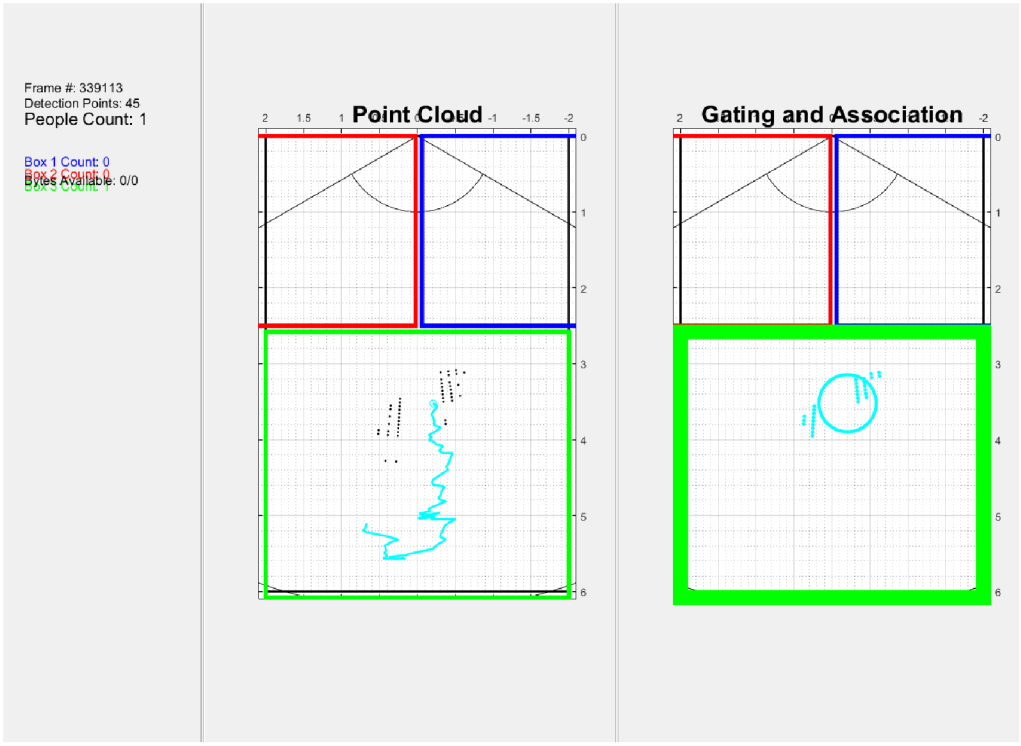
Obr. 8.8 Snímek z vizualizace při třech narušitelích přicházejících z červené zóny do zelené (modrý objekt jde i přes modrou zónu)

9. VYHODNOCENÍ FUNKČNOSTI A SPOLEHLIVOSTI

Navržené experimentální řešení, jehož realizace je popsána v předchozích kapitolách vykazuje 100% spolehlivost v detekci narušitele v zabezpečeném parametru, to znamená, že vždy, když se do perimetru dostala nějaká osoba, radar ji zaregistroval, prohlásil za objekt a následně by tedy byl spuštěn poplach.

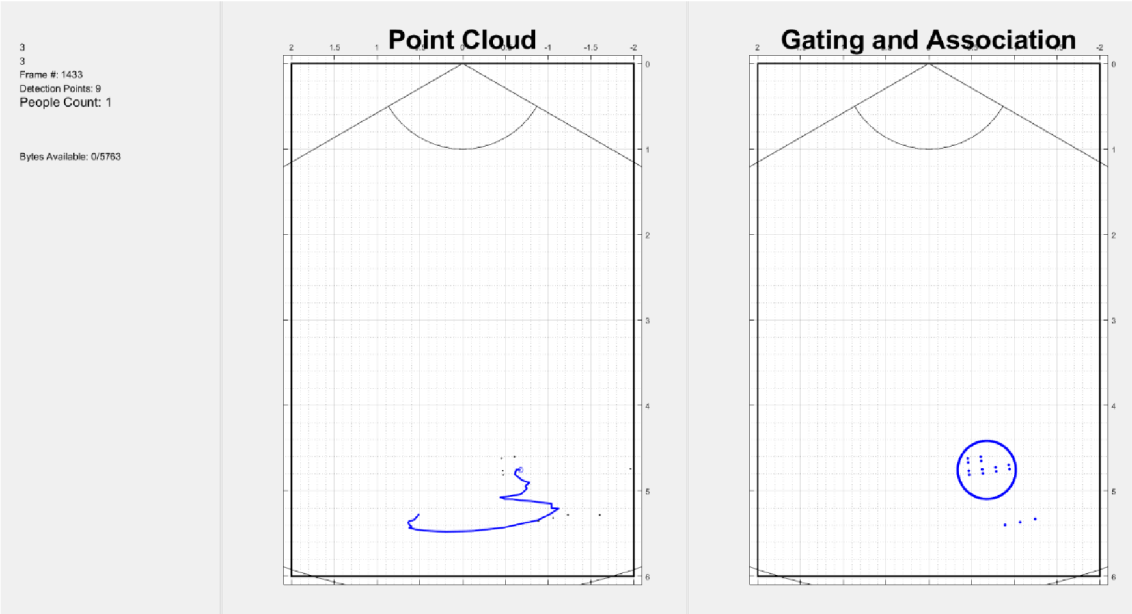
100% spolehlivost také řešení vykazuje z pohledu falešných poplachů. Nikdy se nestalo, že by radar zaregistroval množinu bodů, kterou by prohlásil za objekt, aniž by se objekt reálně nacházel v perimetru. Jiné by to mohlo být například ve venkovních prostorách, kde se před radar za pomoci větru může dostat například shluk listí, v této práci ovšem předpokládám z časových i technických důvodů pouze vnitřní použití.

Horší spolehlivost už je v určení počtu narušitelů. Pokud jdou například dvě osoby blízko sebe, radar je nerozpozná a vyhodnotí je pouze jako jeden objekt. Tento problém by se dal odstranit například nahráním jiných prahových hodnot pro vyhodnocení shluku bodů jako objekt, nicméně by se poté mohlo stávat, že se jako objekt budou považovat i shluky bodů odražené od kovových předmětů (jako na obrázku 8.8) a jelikož se nerozpoznání více objektů děje minimálně a je to podstatně menší chyba než spuštění falešného poplachu, tak jsem nechal toto nastavení jako optimální. Jiná možnost řešení tohoto problému může spočívat například v nahrání jiných parametrů chirpu, úpravou zdrojového kódu v Matlabu, použitím jiného typu detektoru, nebo třeba jiným uspořádáním senzorů. Pokud je ovšem obsluha zabezpečovacího systému všímavá, tak ve většině případů lze rozeznat dva objekty alespoň na vizualizaci Point Cloudu. Na obrázku 9.1 je vidět snímek z vizualizace, kde jsou dvě osoby, v části Gating and association je sice vidět pouze jeden objekt, ovšem v části PointCloud jsou vidět dva shluky bodů a podle jejich pohybu a směru může obsluha odvodit, zda se jedná jen o odraz či dva narušitele.



Obr. 9.1 Snímek z vizualizace, kde jsou dva narušitelé považováni za jeden objekt

Dalším problémem by mohlo být sofistikovanější vniknutí do objektu než příchodem přes vstupné dveře. V rámci experimentu jsem vyzkoušel například plazení a detekce už byla horší, sice radar narušitele detekoval, vyhodnotil ho i jako objekt, především hlavu, která byla výše nad zemí než zbytek těla (obrázek 9.2), pokud by ovšem narušitel byl podstatně menších rozměrů, nemusel by ho radar vyhodnotit jako objekt. Je to dané i zvolením dema pro počítání lidí, které počítám s chodícími osobami, tudíž by se problém dal částečně vyřešit úpravami zdrojových souborů, nicméně stále platí omezení daná konstrukcí radaru (zorný úhel atd.). Dalším řešením může být například větší sklon radaru směrem k zemi, nicméně pak by nastal opačný problém, a to vniknutí například z horní patra a pohyb po stropě pomocí přísavek. Konkrétní řešení by se poté muselo přizpůsobit daným prostorům. Jedno z možných řešení je umístit dva radary pod sebe, jeden by snímal spodní polovinu včetně podlahy, druhý horní polovinu včetně stropu. Pak se nabízí otázka, jak by spolu signály z radarů interferovaly. Toto řešení jsem především z časových, ale i technický důvodů nezkoušel.



Obr. 9.2 Snímek z vizualizace plazícího se narušitele

Pro základní zabezpečení objektu, například bytu, sklepu, chodby lze tento způsobem řešení celkem spolehlivě použít, pokud bychom chtěli zabezpečovat prostory obshující cenné věci, popřípadě komerční objekty, muselo by se dané řešení ještě podstatně vylepšit.

Zabezpečení objektů pomocí těchto radarů místo PIR čidel může mít pro konečného uživatele spoustu výhod. Systém se může propojit se zabezpečovací technikou a zatímco PIR čidla i kamery v případě požáru selhávají, pomocí radaru se dá i ve velmi nepříznivých podmínkách zjistit například počet osob v jednotlivých místnostech (zónách) a tomu přizpůsobit záchranné práce. Dalším využití může být pro statistické účely, například v komerčních objektech jako jsou obchody mohou pomocí radarů sbírat informace o vytíženosti jednotlivých pokladen/poboček a na základě vyhodnocených dat pak přizpůsobovat jejich počet.

Nevýhodou tohoto řešení je především vyšší spotřeba než při použití PIR čidel. Výpočtem spotřeby a porovnáním, ani řešením napájení baterií například při výpadku proudu jsem se z časových důvodů v této práci nevěnoval.

10. ZÁVĚR

Cílem této práce bylo zjistit možnosti využití radarů pracujících v oblasti milimetrových vln od společnosti Texas Instruments v zabezpečovací technice, a tedy navrhnout a pomocí experimentu zjistit možnosti realizace zabezpečení perimetru se zjištěním údajů o narušitelích.

Před začátkem práce bylo potřeba nejprve nastudovat, jak fungují radary obecně, jaké existují druhy radarů, na jakých principech fungují a kde všude mají dané typy využití. Tato rešerše je shrnuta v druhé kapitole – Principy a techniky radarové technologie.

Dále bylo potřeba zjistit, jakým způsobem pracují právě radary pracující v oblasti milimetrových vln – principy vysílání a přijímání signálu, způsob vyhodnocování přijatého signálu a parametry těchto radarů. To je shrnuto ve třetí kapitole – Radary pracující v oblasti mm vln.

Jelikož se jedná o práci, která se zabývá návrhem zabezpečení parametru, je také potřeba zmínit, jakým způsobem se objekty zabezpečují v současné době. Nejběžnější způsob zabezpečení proti vniku narušitelů do objektu je stále zabezpečení pomocí PIR čidel a z toho důvodů se jim věnuji ve čtvrté kapitole – Dosavadní řešení elektronických zabezpečovacích systémů.

Aby bylo možné prakticky pracovat a provádět experiment s radarem od společnosti Texas Instruments, bylo potřeba zjistit, jakým způsobem tyto radary fungují, co v sobě obsahují, jakým způsobem komunikují a jaké operace v jakých posloupnostech vykonávají. To je popsané v páté kapitole – konkrétní řešení od společnosti Texas Instruments.

Od šesté kapitoly již začíná praktická část neboli vlastní řešení. Nejprve bylo potřeba vymyslet kde a jakým způsobem budou senzory rozmístěny, následoval teoretický návrh komunikačního protokolu, poté již oživení senzoru a nastavení správných parametrů a sběr dat pro analýzu.

V poslední kapitole je zhodnocení navrženého řešení a tipy na možné zdokonalení.

Způsobem uvedeným v této práci se podařilo základní zabezpečení perimetru, nicméně pro komerční využití by byla potřeba podstatná zdokonalení (viz kapitola 9). Při případném pokračování v experimentu, nebo zdokonalování této práce je možnost aplikovat navržený komunikační protokol, vyzkoušet zabezpečení perimetru v jiném prostředí, přidání více senzorů a sledování jejich interference.

Literatura

[1] Radar basics [online]. [cit. 2019-05-14]. Dostupné z: http://www.radartutorial.eu/index.en.html

[2] *Radar a jeho využití* [online]. [cit. 2019-05-14]. Dostupné z: http://www.army.cz/images/id_8001_9000/8753/radar/k23.htm

[3] PŘIBYL, Ondřej. Neintrusivní dopravní detektory. Prezentace [online] [Praha] [2016] [cit. 2019-05-14]. Dostupné z: https://zolotarev.fd.cvut.cz/mzd/ctrl.php?act=show,file,23845

[4] POSPÍŠIL, Jaroslav a PLUHÁČEK František. Základní struktura a subsystémy radaru [online]. Olomouc, 2012 [cit. 2019-05-14]. Dostupné z: http://docplayer.cz/20246909-Zakladni-struktura-a-subsystemy-radaru.html

[5] KAIN, Petr. I Češi mají zbraně, kterým patří budoucnost [online]. 13.1.2018 [cit. 2019-05-14]. Dostupné z: http://ceskapozice.lidovky.cz/i-cesi-maji-zbrane-kterym-patri-budoucnost-fjs-/tema.aspx?c=A180112_104131_pozice-tema_houd

[6] MACOUN, Jindra. Směrovost a zisk antén. *Praktická elektronika* [online]. 2012, **2012**(09), 2 [cit. 2019-05-10]. Dostupné z: http://www.crk.cz/FILES/VR-ANT/39.%20Sm%C4%9Brovost%20a%20zisk%20ant%C3%A9n%20(1).pdf

[7] *Different types of radar systems* [online]. [cit. 2019-05-14]. Dostupné z: http://lidarradar.com/definition/different-types-of-radar-systems

[8] *FERGUSON, Robert, CHEVRIER Matthieu a RANKIN Alan. mmWave radar: Enabling greater intelligent autonomy at the edge* [online] Dallas, Texas, 2018 . [cit. 2019-05-14]. Dostupné z: http://www.ti.com/lit/wp/sszy035/sszy035.pdf

[9] *Industrial (IWR) mmWave Sensors | Overview | TI.com* [online]. [cit. 2019-05-14]. Dostupné z: http://www.ti.com/sensors/mmwave/iwr/overview.html

[10] *Paradox.cz - zabezpečení Vašeho majetku* [online]. [cit. 2019-05-14]. Dostupné z: http://www.paradox.cz/index.php

[11] *PZTS (EZS) - Poplachové systémy* [online]. [cit. 2019-05-14]. Dostupné z: https://eshop.eurosat.cz/kategorie/2324

[12] LIBOR, Michalec. *PIR detektor: skvělý sluha, ale zlý pán* [online]. 19.3.2013 [cit. 2019-05-14]. Dostupné z: https://vyvoj.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html

[13] TI Resource Explorer. *Ti.com* [online]. 2019 [cit. 2019-05-14]. Dostupné z: http://dev.ti.com/tirex/explore/

[14] Digitální podpis. *Earchivace.cz* [online]. 2014 [cit. 2019-05-14]. Dostupné z: http://www.earchivace.cz/technologie/digitalni-podpis/

Seznam příloh

Příloha 1 - Data odesílaná do PC

```
frameHeaderStructType = struct(...
    'sync',             {'uint64', 8}, ... % syncPattern in hex is: '02 01 04 03 06 05 08 07'
    'version',          {'uint32', 4}, ... % 0xA1642 or 0xA1443
    'platform',         {'uint32', 4}, ... % See description below
    'timestamp',        {'uint32', 4}, ... % 600MHz free running clocks
    'packetLength',     {'uint32', 4}, ... % In bytes, including header
    'frameNumber',      {'uint32', 4}, ... % Starting from 1
    'subframeNumber',   {'uint32', 4}, ...
    'chirpMargin',      {'uint32', 4}, ... % Chirp Processing margin, in ms
    'frameMargin',      {'uint32', 4}, ... % Frame Processing margin, in ms
    'uartSentTime' ,    {'uint32', 4}, ... % Time spent to send data, in ms
    'trackProcessTime', {'uint32', 4}, ... % Tracking Processing time, in ms
    'numTLVs' ,         {'uint16', 2}, ... % Number of TLVs in thins frame
    'checksum',         {'uint16', 2});    % Header checksum
```

Obr. P1-1 Data přenášená v hlavičce framu (Frame header) [13]

```
% TLV Type: 06 = Point cloud, 07 = Target object list, 08 = Target index
tlvHeaderStruct = struct(...
    'type',             {'uint32', 4}, ... % TLV object
    'length',           {'uint32', 4});    % TLV object Length, in bytes, including TLV header
```

Obr. P1-2 Data přenášená v hlavičce TLV (TLV header) [13]

```
pointStruct2D = struct(...
    'range',            {'float', 4}, ... % Range, in m
    'azimuth',          {'float', 4}, ... % Angle, in rad
    'doppler',          {'float', 4}, ... % Doppler, in m/s
    'snr',              {'float', 4});    % SNR, ratio
```

Obr. P1-3 Data přenášená v Point Cloudu [13]

Velikost trackeru je dána velikostí TLV hlavičky + velikost struktury pintStruct2D * počet bodů

```
targetStruct2D = struct(...
    'tid',              {'uint32', 4}, ... % Track ID
    'posX',             {'float', 4}, ... % Target position in X dimension, m
    'posY',             {'float', 4}, ... % Target position in Y dimension, m
    'velX',             {'float', 4}, ... % Target velocity in X dimension, m/s
    'velY',             {'float', 4}, ... % Target velocity in Y dimension, m/s
    'accX',             {'float', 4}, ... % Target acceleration in X dimension, m/s2
    'accY',             {'float', 4}, ... % Target acceleration in Y dimension, m/s
    'EC',               {'float', 9*4}, ... % Error covariance matrix, [3x3], in range/angle/dopp
ler coordinates
    'G',                {'float', 4});    % Gating function gain
```

Obr. P1-4 Data přenášená v Target Object [13]

Velikost trackeru je dána velikostí TLV hlavičky + velikostí struktury targetStruct2D * počet objektů

```
targetIndex = struct(...
'targetID',         {'uint8', 1});    % Track ID
```

Obr. P1-5 Data přenášená v Target ID [13]

Velikost trackeru je dána velikostí TLV hlavičky + velikostí struktury targetIndex * počet objektů

02 01 04 03 06 05 08 07 02 00 01 01 42 16 0A 00 47 48 31 6B 4A 01 00 00 8D 5E 00 00 00 00 00 00 4E 00 00 00 9D 50 00 00 53 00 00 00 0B 0E 00 00 03 00 00 66 06 00 00 00 38 00 00 00 6C D6 8F 3F DB 0F C9 3D B3 15 A6 3D 1B 30 0A 41 59 99 A2 3F 92 0A 86 3D B3 15 A6 BD 49 6D 18 41 52 DA A8 3F 92 0A 86 3D B3 15 A6 BD 38 26 02 41 07 00 00 00 D4 00 00 00 00 00 00 00 7B BA A3 3D 83 4F 98 3F FE 47 0A BE 00 B0 77 38 1E 9F D9 BE 80 BB B0 3A A7 EE 2F 41 FC C8 3D 3D 25 87 C7 BD FE C8 3D 3D E2 E6 6A 41 77 1C 18 3D 25 87 C7 BD 75 1C 18 3D D7 7E 5A 3F C8 79 A0 40 01 00 00 00 9F 41 11 3E 90 64 08 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A AE 0D 41 50 3B D0 BE 68 BD AC BE 51 3B D0 BE 69 AE E4 41 2A CE 2C 3D 68 BD AC BE 29 CE 2C 3D A3 C0 20 3F 00 00 80 3F 02 00 00 00 D8 6F 90 BF C4 0B 36 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B0 67 2D 41 78 6D 4E BD AD AF 93 BE 7E 6D 4E BD 8C CD 8E 42 92 4F 91 3D AD AF 93 BE 7C 4F 91 3D AA 3F 31 3F 00 00 80 3F 08 00 00 00 0A 00 00 00 00 00 02 01 04 03 06 05 08 07 02 00 01 01 42 16 0A 00 62 11 CA 6B 8B 01 00 00 8E 5E 00 00 00 00 00 00 4E 00 00 00 84 50 00 00 58 00 00 00 7B 0E 00 00 03 00 AE 9B 06 00 00 00 78 00 00 00 6C D6 8F 3F DB 0F C9 3D B3 15 A6 3D 51 FA 0A 41 66 17 96 3F DB 0F C9 3D B3 15 A6 3D A1 F4 D0 41 59 99 A2 3F DB 0F C9 3D B3 15 A6 BD A4 A9 24 41 6C D6 8F 3F 92 0A 86 3D B3 15 A6 3D E7 87 FA 40 66 17 96 3F 92 0A 86 3D B3 15 A6 3D E2 69 0A 42 5F 58 9C 3F 92 0A 86 3D B3 15 A6 3D CA E5 A4 41 59 99 A2 3F 92 0A 86 3D B3 15 A6 BD 58 47 8D 41 07 00 00 00 D4 00 00 00 00 00 00 00 5D 0B A5 3D D1 B1 98 3F 08 27 CA BD 1B 12 8E 3B 4A BC 5B BE 5A FB 82 BC 7D 7F 2E 41 31 D7 2E 3D 55 B0 2C BE 31 D7 2E 3D CC AA 58 41 91 5A 14 3D 55 B0 2C BE 95 5A 14 3D 74 A1 48 3F 14 46 A0 40 01 00 00 00 9F 41 11 3E 90 64 08 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A AE 0D 41 50 3B D0 BE 68 BD AC BE 51 3B D0 BE 69 AE E4 41 2A CE 2C 3D 68 BD AC BE 29 CE 2C 3D A3 C0 20 3F 00 00 80 3F 02 00 00 00 D8 6F 90 BF C4 0B 36 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B0 67 2D 41 78 6D 4E BD AD AF 93 BE 7E 6D 4E BD 8C CD 8E 42 92 4F 91 3D AD AF 93 BE 7C 4F 91 3D AA 3F 31 3F 00 00 80 3F 08 00 00 00 0B 00 00 00 00 00 00

Frame Header
Point Cloud TLV
Target List TLV
Target Index TLV
Type Length Header

Obr. P1-6 Příklad přenesených dat [13]