

UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

System ochrany před krádeží dopravního prostředku

Pavel Hanus

Bakalářská práce

2023

Univerzita Pardubice  
Fakulta elektrotechniky a informatiky  
Akademický rok: 2023/2024

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Pavel Hanus**  
Osobní číslo: **I21026**  
Studijní program: **B0714A060022 Komunikační technika**  
Téma práce: **Systém ochrany před krádeží dopravního prostředku**  
Zadávající katedra: **Katedra elektrotechniky**

## Zásady pro vypracování

Cílem práce je navrhnout a sestavit zařízení, které bude sloužit ke zjištění pokusu o odcizení střeženého dopravního prostředku a bude tento pokus aktivně sabotovat. Navržené zařízení bude provádět dvě základní sady operací. První sadou operací bude zjištění pokusu o odcizení střeženého objektu. Druhou sadou operací bude aktivní obrana proti tomuto odcizení. Zařízení bude primárně řízené pomocí dálkového ovladače. Ukončení střežení bude možné provést pouze správným zadáním identifikačního kódu. Detekce pokusu o odcizení bude prováděna pomocí kombinace více senzorů. Aktivní obrana bude realizována pomocí sady akčních členů, které budou pokus o odcizení cíleně sabotovat.

V teoretické části se bude student zabývat možnostmi detekce pokusu o odcizení střeženého objektu. V praktické části student navrhne a sestaví funkční vzor systému pro ochranu dopravního prostředku před odcizením.

Rozsah pracovní zprávy: **30**  
Rozsah grafických prací:  
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

- [1] MATOUŠEK, David. *Práce s mikrokontroléry ATME<sup>®</sup> AT89C2051: [měření, řízení a regulace pomocí několika jednoduchých přípravků]*. Praha: BEN – technická literatura, 2006. ?C & praxe. ISBN 8073001748.
- [2] ROUBAL, J. a P. HUŠEK. *Regulační technika v příkladech*. BEN, 2011. ISBN 978-80-7300-260-2. [3] ŠEDA, M., I. ŠVARC a M. VÍTEČKOVÁ. *Automatické řízení*. CERM, 2011. ISBN 978-80-214-3491-2.

Vedoucí bakalářské práce: **Ing. Luboš Rejfek, Ph.D.**  
Katedra elektrotechniky

Datum zadání bakalářské práce: **15. prosince 2023**  
Termín odevzdání bakalářské práce: **10. května 2024**

**Ing. Zdeněk Němec, Ph.D.** v.r.  
děkan

L.S.

**doc. Ing. Jan Pidanič, Ph.D.** v.r.  
vedoucí katedry

## **Prohlášení autora**

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 10. 5. 2024

Pavel Hanus

## **Poděkování**

Na tomto místě bych chtěl poděkovat své rodině a přátelům, kteří mě podporovali jak při psaní této práce, ale i při průběhu celého studia. Dále velké poděkování patří panu Ing. Lubošovi Rejfkovi, Ph.D. za jeho cenné rady, trpělivost a veškerý čas, který mi věnoval.

## **Anotace**

Tato bakalářská práce je zaměřena na návrh a realizaci systému pro ochranu dopravních prostředků před zloději. Teoretická část obsahuje studii použitelných systémů pro detekci, kdy byl dopravní prostředek odcizen, a aktivních systémů pro ochranu proti odcizení. Na základě této studie byl vytvořen systém pro ochranu dopravních prostředků. Navržený systém byl testován souborem měření a podle výsledků upraven pro zlepšení kvality systému.

## **Klíčová slova**

GNSS, akcelerometr, GSM, ochrana proti zcizení, zabezpečení

## **Title**

The system of protection against theft of means of transport

## **Annotation**

This bachelor thesis is aimed on a design and realization of the system for the means of transport protection again thieves. A theoretical part contains a study of the applicable systems for detection, when the means of transport was stolen and active systems for the protection against the steeling. Based on the study was created system for protection of the means of transport. The designed system was tested by the set of the measurements and modified according to the results for improving the system quality.

## **Keywords**

GNSS, accelerometer, GSM, protection against steeling, security

# Obsah

<b>Seznam zkratk</b> .....	<b>8</b>
<b>Seznam obrázků</b> .....	<b>9</b>
<b>Seznam tabulek</b> .....	<b>10</b>
<b>Úvod</b> .....	<b>11</b>
<b>1 Možnosti zabránění zcizení dopravního prostředku</b> .....	<b>12</b>
1.1 Detektory pokusů o zcizení .....	13
1.1.1 Tlakový senzor .....	13
1.1.2 Akcelerometr .....	13
1.1.3 Gyroskop .....	14
1.1.4 Otřesový senzor .....	15
1.1.5 Senzor magnetického pole.....	16
1.1.6 Určování polohy za využití GNSS .....	17
1.1.7 PIR čidlo .....	21
1.1.8 Výběr vhodných senzorů .....	22
1.2 Akční členy komplikující pokusy o zcizení .....	22
1.2.1 Audio poplach – piezo aktivní bzučák .....	22
1.2.2 Rádiové varování vlastníka (pager).....	23
1.2.3 Zasílání informace o poloze .....	24
1.2.4 Blokace brzd.....	25
1.2.5 Zhodnocení akčních členů a výběr .....	25
<b>2 Sestavení a princip fungování zabezpečovacího zařízení</b> .....	<b>26</b>
2.1 Použité prvky v projektu .....	26
2.1.1 Mikrokontroler .....	26
2.1.2 Akcelerometr .....	27
2.1.3 Bluetooth modul .....	29
2.1.4 GPS modul.....	30
2.1.5 GSM modul .....	31
2.1.6 Zdroj napájení.....	32
2.2 Konstrukce zařízení .....	32
<b>3 Firmware</b> .....	<b>34</b>
3.1 Úpravy firmwaru proti falešným poplachům .....	36

<b>4</b>	<b>Testovací měření.....</b>	<b>39</b>
4.1	Popis experimentu pro původní nastavení.....	39
4.2	Úpravy systému na základě prvotních měření.....	42
4.3	Výsledky experimentu po úpravách firmware.....	42
4.4	Testování finální verze systému v reálném prostředí .....	43
	<b>Závěr .....</b>	<b>45</b>
	<b>Literatura .....</b>	<b>46</b>
	<b>Příloha A – Tabulky po úpravě kódu, k zamezení poplachů .....</b>	<b>49</b>
	<b>Příloha B – Zdrojový kód .....</b>	<b>51</b>



## **Seznam zkratek**

GPS	Global Positioning System
GNSS	Global Navigation Satellite System
LORAN	LONG RANGE Navigation
PDA	Personal Digital Assistant
NMEA	National Marine Electronics Association
GDOP	Geometric Dilution Of Precision
DOP	Dilution Of Precision

## Seznam obrázků

Obr. 1.1 - Ukázka jednoduchého zámku na volant [9].....	12
Obr. 1.2 - Ukázka tlakového senzoru FSR402 [11] .....	13
Obr. 1.3 - Kapacitní akcelerometr [2].....	14
Obr. 1.4 - Rozložení sil v gyroskopu [3] .....	15
Obr. 1.5 - Hallův senzor [5].....	16
Obr. 1.6 – Rozložení satelitů nad Zemí [18] .....	18
Obr. 1.7 - Vliv atmosférických chyb [8] .....	19
Obr. 1.8 - Vícenásobný příjem signálu [8] .....	20
Obr. 1.9 - Vliv rozložení a viditelnosti satelitů[8].....	20
Obr. 1.10 – Určování polohy statického přijímače signálu GPS modelu NEO-7N .....	21
Obr. 1.11 - Blokové schéma PIR detektoru. [13] .....	22
Obr. 1.12 - Ukázka piezo sirény [15] .....	23
Obr. 1.13 - Ukázka zařízení PAGER [17].....	23
Obr. 1.14 - Mapa pokrytí sítě GSM v ČR (Vodafone) [16] .....	24
Obr. 1.15 - Struktura sítě GSM [21].....	25
Obr. 2.1 - Rozložení pinů, ARDUINO MEGA 2560 [12] .....	27
Obr. 2.2 - Akcelerometr ADXL335 .....	28
Obr. 2.3 - Schéma zapojení akcelerometru k mikrokontroleru .....	28
Obr. 2.4 - Část kódu pro překročení hraniční hodnoty pro vyhlášení poplachu.....	29
Obr. 2.5 - Bluetooth modul HC-06 [10] .....	29
Obr. 2.6 - Část kódu pro uvedení identifikačního kódu .....	30
Obr. 2.7 - GPS modul Neo-7N .....	30
Obr. 2.8 - GSM modul SIM800L .....	31
Obr. 2.9 – Část kódu, s AT příkazy .....	31
Obr. 2.10 - Zdroj napájení .....	32
Obr. 2.11 - Blokové schéma zařízení .....	33
Obr. 2.12 - Zkonstruované bezpečnosti zařízení .....	33
Obr. 3.1 - Ukázka komunikace přes GSM modul .....	34
Obr. 3.2 - Vývojový diagram.....	35
Obr. 3.3 - Vývojový diagram s kontrolním měřením .....	36
Obr. 3.4 - Vývojový diagram, kde je GPS modul spojen s akcelerometrem.....	37
Obr. 3.5 - Vývojový diagram s průměrováním signálu mimo oblast.....	38
Obr. 4.1 - Mobilní platforma .....	39
Obr. 4.2 – Lokace pro experiment v zástavbě (vlevo) a výhled na oblohu z dané lokace (vpravo). .....	40
Obr. 4.3 – Lokace pro experiment s volným výhledem (vlevo) a výhled na oblohu z dané lokace (vpravo). .....	40
Obr. 4.4 – Chyba určené vzdálenosti od nastavené polohy v čase.....	42
Obr. 4.5 - Únik signálu pro úpravu kódu s varováním .....	43

## Seznam tabulek

Tabulka 1 - Tabulka akcelerometrů.....	14
Tabulka 2- Statické měření zástavba (15 minut).....	40
Tabulka 3- Vyhlášení pohybu při pohybu v zástavbě .....	41
Tabulka 4- Statické měření volný prostor (15 minut) .....	41
Tabulka 5- Vyhlášení pohybu při pohybu ve volném prostoru .....	41
Tabulka 6- Výsledky měření v klidovém stavu vozidla (15 minut).....	44
Tabulka 7- Výsledky měření při uvedení do pohybu .....	44
Tabulka 8- Vyhlášení poplachu v zástavbě ( průměrování měření ).....	49
Tabulka 9- Vyhlášení poplachu v zástavbě ( Kontrolní měření po vyhlášení úniku signálu ) .....	49
Tabulka 10- Vyhlášení poplachu v zástavbě ( Synchronní vyhlášení s akcelerometrem ) .	49
Tabulka 11- Vyhlášení poplachu ve volném prostoru ( Kontrolní měření po vyhlášení úniku signálu ).....	49
Tabulka 12- Vyhlášení poplachu ve volném prostoru ( Synchronní vyhlášení s akcelerometrem) .....	49
Tabulka 13- Vyhlášení poplachu ve volném prostoru ( Průměrování měření) .....	50

## Úvod

Zcizování dopravních prostředků je velkým problémem, který je nutné řešit i v současnosti. Je jedno, jestli se jedná o bicykl, motocykl nebo automobil, počet krádeží je úměrný množství používaných dopravních prostředků. Výsledek toho jevu je stejný a nepříjemný, proto jsou navrhovány různá opatření a zařízení, která mají této události zabránit nebo ji alespoň ztížit, aby se četnost zcizování dopravních prostředků omezila.

Cílem této bakalářské práce bylo vytvořit zařízení, které detekuje pokusy o odcizení dopravního prostředku a v případě pokusu, tento pokus o odcizení cíleně sabotuje.

V první části byla provedena rešerše možných a dostupných technik, které by mohly být nápomocny při detekci pokusu o krádež. Dále pak byla provedena rešerše dostupných elektronických systémů pro ochranu před zcizením. Na základě těchto rešerší byly vybrány prvky, které pak byly použity při návrhu zařízení pro ochranu dopravního prostředku

V praktické části je pak popsán koncept navrženého zařízení a jeho jednotlivé části. Dále je zde popsán firmware vytvořený pro ovládání navrženého zařízení a v neposlední řadě jsou zde popsány experimenty, které měli za cíl ověřit funkčnost zařízení. Na základě prvotních měření byly navrženy optimalizace řídicího programu za účelem zlepšení vlastností navrženého systému. Systém byl po aplikaci optimalizačních podprogramů opět otestován sadou měření, která jsou také popsána v praktické části.

## 1 Možnosti zabránění zcizení dopravního prostředku

Na trhu je k dostání celá řada systémů, jež jsou navrženy tak, aby ochránily dopravní prostředky před krádeží, nebo neoprávněným vniknutím. Je ale důležité vybrat takový, který je vhodný pro konkrétní případ, protože každý má své výhody a nevýhody.

Mezi nejjednodušší varianty patří mechanické zábrany, které mají i odrazující efekt. Příklady takových řešení jsou různé zámky, řetězy a západky, které zabraňují odcizení dopravního prostředku. Příklad mechanické zábrany, která se umísťuje na volant dopravního prostředku, je ukázán na obrázku **Chyba! Nenalezen zdroj odkazů.** Při použití specializovaného vybavení, lze však tyto zábrany eliminovat (například přestípnutí bezpečnostního lanka kleštěmi) a proto se uplatňují při zabezpečení dopravních prostředků elektronické systémy, které zvyšují míru ochrany dopravního prostředku před zcizením.



Obr. 1.1 - Ukázka jednoduchého zámku na volant [9]

Současná technologická řešení umožňují vybavit dopravní prostředky ochranou založenou na principu skenování biometrických údajů. V těchto řešeních se využívají k identifikaci biometrická data, což mohou být otisky prstů, nebo i sítnice. Zabezpečení tohoto typu mohou být zabudována například na tlačítko startování motoru nebo do volantu a bez příslušné shody s řidičem, nedovolí aktivaci další činnosti. [9] Tato řešení se implementují do nových dopravních prostředků, ale jejich implementace do starších dopravních prostředků, je finančně nákladná, případně vyžaduje větší úpravy dopravního prostředku.

Jednodušší variantou elektronického zabezpečení dopravních prostředků jsou systémy elektronické ochrany, které nezasahují přímo do řízení dopravního prostředku, ale na základě senzorů zabraňují zcizení pomocí audiovizuálních signálů. Mezi takové se řadí například alarmy, sledovací systémy GPS, imobilizéry a další. Tyto systémy jsou vhodné na implementaci do starších dopravních prostředků. Cílem této práce je navrhnout systém na zabezpečení staršího dopravního prostředku, a proto je toto řešení vhodným kandidátem. Pro realizaci systému je nutné v první řadě provést rozbor, jak dostupných vhodných senzorů, tak dostupných vhodných systémů, které ztíží pokusy o zcizení dopravního prostředku.

## 1.1 Detektory pokusů o zcizení

Vzhledem k tomu, že toto bezpečnostní zařízení bude sloužit pro zabezpečení automobilu, budou se volit pro porovnání takové senzory, aby v co největší míře vyhovovaly právě tomuto účelu. Účelem senzorů je detekovat, zda je dopravní prostředek v pohybu, nebo zdali nedošlo k narušení v důsledku vniknutí. Na základě popsaného byly vybrány pro porovnání níže uvedené senzory.

### 1.1.1 Tlakový senzor

Mezi detektory, které by mohly detekovat pokus o zcizení automobilu, by se mohl zařadit tlakový senzor. V případě, že by byl umístěn někde v prostoru řidiče, tak v momentu, pokud by došlo k neoprávněnému vstupu do vozidla, tento senzor by toto vniknutí zaznamenal.



Obr. 1.2 - Ukázka tlakového senzoru FSR402 [11]

Tyto senzory jsou svým vzhledem podobné fóliovým spínačům, ale rozdíl mezi nimi je v odporu, pokud na ně vyvíjen tlak v normálovém směru. [11]

Zobrazený tlakový senzor FSR402, který je na Obr. 1.2, pracuje na změně odporu při stisknutí. Pokud dojde ke stisknutí o tlaku 10g až 10kg, jeho hodnota se změní z hodnoty  $1\text{M}\Omega$  na přibližně  $3\text{k}\Omega$ . Jako jednu z jeho předností by se dalo považovat jeho životnost, senzor je schopný pracovat až 10 000 000 spouštěcích cyklů.

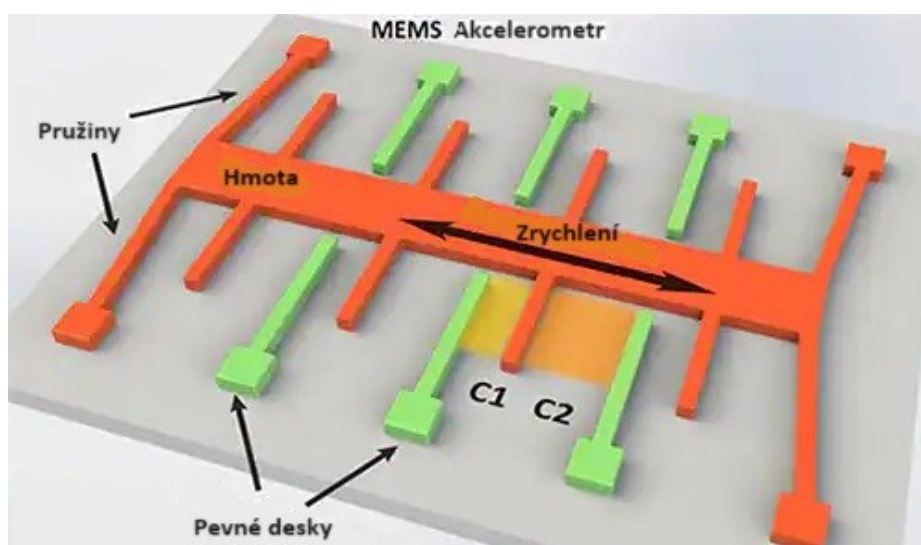
### 1.1.2 Akcelerometr

Další z možností, jak zaznamenat pokus nebo i uskutečněné odcizení prostředku je použití akcelerometru. To je buď součástka nebo přístroj, který měří zrychlení. Toto zrychlení se rozlišuje do dvou skupin, a to dynamické a statické. Funkce akcelerometru využíváme v téměř každé sféře našeho života. Je zakomponovaná jak v domácích zařízeních, která používáme každý den (viz. mobilní telefon), tak se užívá i v průmyslových a výzkumně-vývojových aplikacích. [1]

Samotné fugování akcelerometru není nijak zvlášť složité. Měří sílu zrychlení, která má jednotky g. Jeho měření jako takové může probýhat buď v jedné, nebo ve třech rovinách a to X, Y a Z. Vzhledem k tomu, že to není nijak finančně náročná součástka, tak se v dnešní době převážně používá tříosých akcelerometrů. Existují 3 druhy akcelerometrů, kapacitní, piezorezistivní a piezoelektrické. Porovnání akcelerometrů dle principu je v Tabulka 1 , jako nejlepší řešení pro danou aplikaci se jeví kapacitní akcelerometr (Pod vlivem zrychlení se mění kapacita mezi deskami, která je následně přepočítaná na chtěné zrychlení.), jeho princip je na Obr. 1.3.

**Tabulka 1 - Tabulka akcelerometrů**

	Kapacitní [2]	Piezorezistivní [2]	Piezoelektrické [2]
Výhody	Nejčastěji používané Nejlevnější Nejmenší Možnost implementace přímo na plošný spoj	velké měřicí pásmo používá se například při nárazových testech.	vysoká citlivost a přesnost
Nevýhody	Poměrně malá přesnost	v porovnání s kapacitním dražší	
Princip	Využívají technologii MEMs	Využívají technologii MEMs	Využívají technologii MEMs



**Obr. 1.3 - Kapacitní akcelerometr [2]**

### 1.1.3 Gyroskop

Gyroskop je také zařízení, které by nám mohlo dodat informaci o tom, zda se někdo pokouší náš dopravní prostředek odcizit. Jako nejjednodušší příklad by se dalo požit zařízení, které i při působení vnějších sil udržuje stabilitu ve středu těla, na které je namontováno. Princip funguje ve třech rovinách.[3]

Dělí se do několika typů, ale asi za nejznámější se považuje tzv. setrvačný gyroskop, jinak známý jako setrvačnický. Ten se skládá z rotoru, který když na něho působí cizí síla, tak mění svou orientaci a na tyto změny reaguje. Pokud se objekt, na kterém je gyroskop umístěn dá do pohybu, tak se rotor snaží zůstat ve své původní orientaci a to vede k vytvoření úhlové rychlosti.

Pro účely této bakalářské práce by byl vhodnější ale **gyroskopický senzor**. Uvnitř tohoto senzoru se pohybují dvě hmoty, ale vůči sobě v opačném směru. Pokud se objeví síla působící na toto zařízení, začne se měnit vzdálenost mezi elektrodami uvnitř senzoru, tím se začne měnit kapacita kondenzátoru a v neposlední řadě i napětí na jeho deskách, což můžeme považovat za elektronický signál, ( princip využívání technologie MEMs, jako v akcelerometru viz. Obr. 1.3) který je rozeznáván senzorem.



Obr. 1.4 - Rozložení sil v gyroskopu [3]

Rozdíl mezi akcelerometrem a gyroskopem je v principu funkce a měřených veličinách. Gyroskop určuje úhel sklonu vůči zemi, zatímco akcelerometr je schopen měřit lineární zrychlení. Akcelerometr díky své funkci dokáže vypočítat vzdálenost, po které byl přemístěn, ale gyroskop měří jenom polohu zařízení. Přes všechny výhody a nevýhody ale mohou obě zařízení být vyměňovány nebo se doplňovat a v praxi se často používají současně. [3]

#### 1.1.4 Otřesový senzor

Mezi další z možností, jak detekovat odcizení dopravního prostředku, by se mohl zařadit senzor, který zachytí otřes. Při začátku používání jakéhokoliv prostředku, se tento jev projeví a mohla by to tak být vhodná a účinná volba.

Jedním z takových by se dal použít senzor, který pro svou funkci využívá rtuť, která je zapracována uvnitř čidla samotného. Princip jeho fungování je založen na vlastnosti, kdy při zaznamenání nějakého pohybu, vibrace, nebo náklonu se spojí elektricky-vodivý obsah s vývody a uzavře se elektrický obvod. [4] Nicméně k používání této technologie se poslední dobou upouští, a to zejména z důvodu bezpečnosti. Rtuť je těžký kov a má vážně zdravotní rizika.



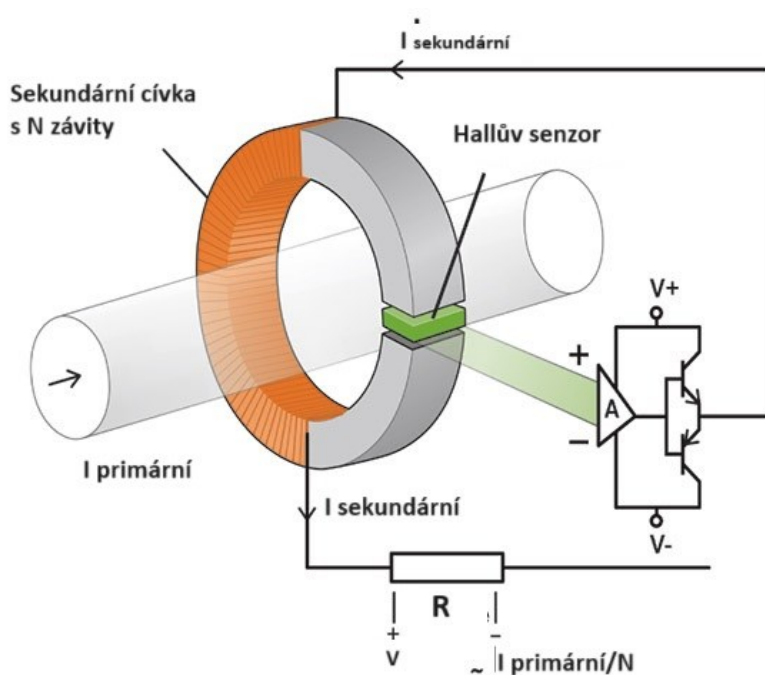
Použit se může i takový, který využívá změnu odporu. Například pokud je senzor ve vodorovné poloze, tak vykazuje nějakou rezistivitu, pokud se ale dostane do jiné polohy, jeho následný odpor je již rozdílný od původního.

Existuje celá řada čidel/senzorů, které se používají k detekci otřesu nebo nárazu. Nicméně všechny fungují na téměř totožném principu. Při zaznamenání děje, se spojí jejich elektrický obvod a senzor následně vyšle data pro další zpracování.

### 1.1.5 Senzor magnetického pole

Pokud jako dopravní prostředek bude použit například automobil, nebo motocykl, nabízí se použití senzoru pro detekci magnetického pole. V dnešní době se již jedná o velice dostupné zařízení o malé velikosti. I navzdory poměrně složitému úkolu, který plní je jejich princip funkce poměrně jednoduchý.

Nejjednodušší senzor tohoto typu je složen z permanentního magnetu nebo cívky, ve které je tvořeno magnetické pole. A druhou částí je Hallův snímač, což je polovodičový prvek, který jakmile je pod vlivem magnetického pole, tak mění své elektrické vlastnosti a poté je možná detekce tohoto pole. [5] Princip, na kterém snímač funguje je znázorněn na Obr. 1.5.



Obr. 1.5 - Hallův senzor [5]

Nejběžnější a zároveň nejjednodušší jsou **Hallovy senzory**. Pracují na principu již zmíněného hallova jevu, kdy při protékání proudu a působení magnetického pole na materiál se vytvoří příčné napětí. Využívají se tam, kde je potřeba detekovat magnetické pole a následně změřit jeho sílu.

**Magnetorezistory** využívají jevu magnetorezistence. Ta vznikne pod působením magnetického pole, kdy se změní elektrický odpor materiálu. Hlavní použití nacházejí ve snímačích polohy, díky změně elektrického odporu vůči poloze umístění magnetu.

**Magnetooptické čidla**, ty se používají méně často a to hlavně v případě, kde dochází pouze k malým změnám magnetického pole. Ke své funkci využívají Faradayův jev, který se dá jednoduše popsat asi tak, že jakmile se materiál pod vlivem magnetického pole, změní se polarizace světla, to je, změní se směr kmitání světla vůči původnímu.

**Indukční senzory**, zde se využívá jev zvaný elektromagnetická indukce. Kde ve chvíli změny magnetického pole se indukuje, tj. vzniká elektrický proud. Tento typ se používá především pro zjištění kovového předmětu v okolí.

### **1.1.6 Určování polohy za využití GNSS**

K určování polohy na Zemi, se používá celá řada různých technologií už neskutečně dlouhou dobu. Jako předchůdce technologie GPS, by se dal uvést systém LORAN. Jednalo se o rádiový navigační systém. Jeho hlavní využití bylo pro leteckou a námořnickou navigaci. Pomocí středovlnných signálů, umožňoval určovat polohu a rychlost dopravního prostředku.

S postupem času, ale vznikaly nové požadavky a předem zmíněné možnosti již nevyhovovali. Bylo třeba vyvinout nové technologie, podle kterých by se dala určovat poloha.

## **GLOBAL POSITIONING SYSTEM (GPS)**

Tato inovace umožňuje komukoli na Zemi určit své zeměpisné souřadnice. Pro svou funkci využívá několik, pro tento účel navržených, družic. Družice na oběžných drahách vysílají elektromagnetické signály k Zemi, díky kterým se určí poloha. Původně systém vznikl pro vojenské účely Spojených států v 70. letech minulého století. Až přibližně po dalších dvaceti letech ho mohla používat veřejnost. Celý systém GPS lze rozdělit na tři hlavní části: kosmickou, řídicí a uživatelskou. Z nichž nejpodstatnější je pro účely této práce část uživatelská. [7]



Obr. 1.6 – Rozložení satelitů nad Zemí [18]

Zde bude pospsána část, která je pro tuto práci klíčová a to je **uživatelská část**. Zde se jedná jak o klasické přijímače, které mají v dnešní době už minimálně i nějaký displej, tak o přijímače, které jsou dále zabudované do nějakého zařízení, jako může být například PDA, telefon a další. Většina těchto zařízení je pouze pasivní, takže lze signál přijímat, nikoliv ale vysílat.

Princip fungování tohoto navigačního systému, by se dal jednoduše vysvětlit asi tak, že každá družice vysílá data o své poloze, přesný čas díky atomovým hodinám a přibližnou polohu dalších družic. Poměrně důležitou podmínkou je, aby přijímač měl přímou viditelnost na oblohu. Pro určení polohy potom využívá rozdílů času od vyslání informace ze satelitu na oběžné dráze a doby přijetí informace v přijímači na Zemi. Rozlišuje se potom z kolika satelitů se data přijímají. V případě, že budou zahrnuty tři satelity, určíme tak zeměpisnou šířku a délku (tzv. 2D poloha), pokud už se určuje ze tří, zjistíme tak i nadmořskou výšku. A pokud se počet satelitů zvyšuje, bude naše poloha přesnější. GPS přijímač komunikuje s počítačem nebo jiným zařízením pomocí protokolu NMEA (National Marine Electronics Association). Díky tomuto protokolu si mezi sebou vyměňují spoustu informací, jako například: čas, poloha, poloha družic, azimut, počet aktivních satelitů. [7]

## Zdroje chyb měření

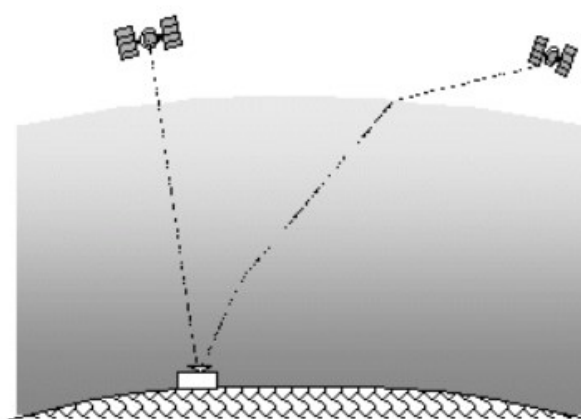
Asi jako každý navigační systém, tak i právě systémy satelitní navigace dosahují určité míry přesnosti. Ta je ovlivňována hlavně chybami měření vzdálenosti násobené hodnotou geometrické odchylky od přesnosti (GDOP – Geometric Dilution Of Precision). [8]

Přesnost satelitních je statická míra chyby tohoto systému a lze ji rozdělit do několika skupin, podle kterých je rozpoznávána.

- **Opakovatelná** – Je taková, se kterou se může uživatel vrátit na danou polohu, která byla již dříve určena stejným systémem.
- **Predikovatelná** – To je přesnost, která se určuje vzhledem k zákresu na mapě.
- **Relativní** – Pokud má uživatel stejný systém s dalším uživatelem a měření probíhá ve stejném čase, může se poloha měřit vzhledem k poloze druhého uživatele.

Při určování polohy pomocí satelitního navigačního systému, se uplatňují chyby, které vznikají vždy minimálně z jedné, nebo i více příčin. Tyto příčiny lze rozdělit do skupin :

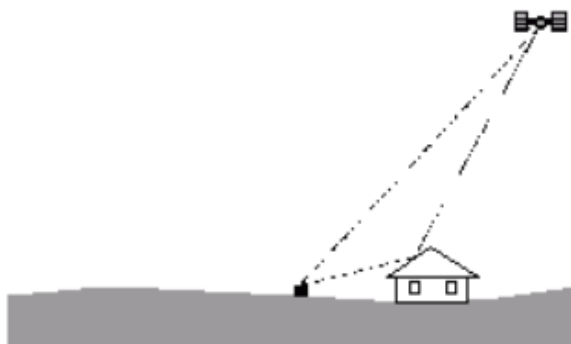
- **Chyba satelitových hodin** – Vznikají chyby v přenášených údajích, které ovlivňují satelitové signály.
- **Chyba efemerid** – Pokud satelitová chyba nepředá správnou pozici satelitu, vzniká chyba s tímto názvem. S časem od poslední opravy této chyby, je zde tendence nárustu chyby, přesto jde ale o pomalé změny
- **Chyby ionosférické a troposférické** – Zde se projevují vlastnosti elektromagnetických vln při průchodu různými vrstvami atmosférou. Průchodnost elektromagnetických vln je ovlivňována množstvím volných elektronů, které se v různých výškách atmosféry mění. Podle situace se signál různě mění, může dojít k jeho ohybu, nebo i úplnému odrazu. (viz. Obr. 1.7)



**Obr. 1.7 - Vliv atmosférických chyb [8]**

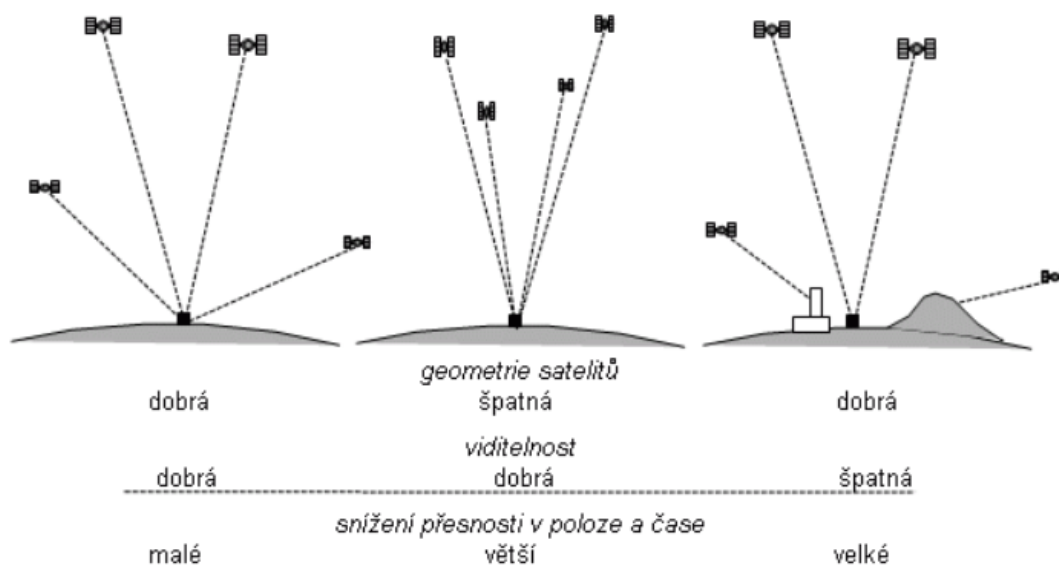
- **Chyby z vícenásobného příjmu signálu** – Může se stát, že signál se nešíří přímo od vysílače k přijímači, ale dochází k odrazu signálu od okolních objektů nebo odrazných ploch, jako jsou například budovy, jezera apod. . V přijímači potom

dochází k takzvanému vícenásobnému příjmu. Většina novějších přijímačů však tuto chybu již eliminuje pomocí anténních filtračních technik. Problematika je znázorněna na Obr. 1.8 .



Obr. 1.8 - Vícenásobný příjem signálu [8]

- Chyby přijímače – Do těchto chyb se počítají jednak chyby v konstrukci přijímače, mohou to být jedno či vícekanálové, rozhoduje i typ použitých mikroprocesorů, tak rozdíl udělá i typ použitého softwaru. Míra vlivu, jak jsou satelity rozloženy nad obzorem v okamžiku měření se nazývá snížení přesnosti určení polohy neboli DOP ( Dilution of Precision )



Obr. 1.9 - Vliv rozložení a viditelnosti satelitů[8]

Mezi hlavní výhody systémů satelitní navigace patří přesnost, globální dosah (systém GPS a jiné satelitní systémy, pokrývají celý svět), dostupnost (systémy bývají obvykle k dispozici nepřetržitě 24/7). Samozřejmě jako vše, i zde lze nalézt nevýhody. Asi největší je zakrytí signálu, pokud se nachází objekt mezi vysokými budovami, nebo

například v hustém lese, může být signál oslaben, nebo dokonce i zcela zablokovan. Dále zde je poměrně velká závislost na infrastruktuře systému. Je vyžadována dostatečně velká infrastruktura satelitů a zemských stanic, což může být finančně nákladné a náchylné k poruchám. [8] Příklad statického měření polohy je ukázán na Obr. 1.10, kdy vlivem šíření signálu v ionosféře a troposféře dochází k chybě určení polohy (v tomto případě jsou nejdlehlší body vzdáleny přes 10 metrů).



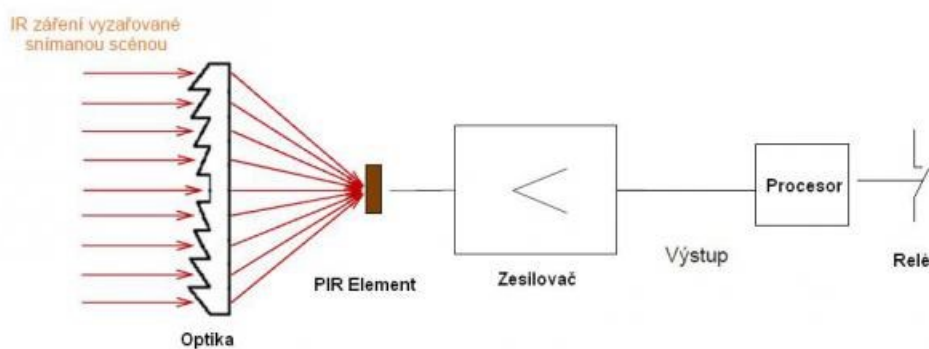
Obr. 1.10 – Určování polohy statického přijímače signálu GPS modelu NEO-7N

### 1.1.7 PIR čidlo

Jednou z možností, jak efektivně detekovat odcizení majetku, je použití PIR čidla. Ať už se snažíme zabránit krádeži pevně umístěného majetku, nebo jako v případě této bakalářské práce, dopravního prostředku, tohle může být správná volba.

PIR neboli pasivní infračervené čidlo, je druh elektromagnetického čidla, jež detekuje infračervené záření a jeho nejběžnější využití je právě v detektorech pohybu. Ve chvíli, kdy má objekt teplotu vyšší, než je absolutní nula, toto zařízení ho detekuje a podle své funkce, kvůli které bylo instalováno, provádí potřebné úkony. Pokud se objekt ( v tomto případě člověk ) nachází v detekčním poli čidla, dochází ke změnám v infračerveném záření. [13]

Na Obr. 1.11 je uvedeno blokové schéma jednoduchého PIR detektoru. Součástky jsou uspořádány z levé strany, jak jsou postupně umístěny v detektoru.



Obr. 1.11 - Blokové schéma PIR detektoru. [13]

Velkou výhodou těchto čidel je, že pracují v pasivním režimu. To znamená, že samy o sobě nevyzařují žádná infračervená záření. Pouze reagují na záření, která detekují ve svém dosahu. Díky pouze pasivnímu provozu, mají nízkou energetickou spotřebu a hodí se pro bateriově napájené zařízení, nebo tam, kde se řeší energetická náročnost.

Prostor, ve kterém čidlo snímá, je rozdělen do tzv. detekčních zón, jejichž počet je dán počtem segmentů zrcadla nebo čoček. Detekční pole může být nastavováno pro konkrétní případy, aby funkce byla co nejkvalitnější. Při správném nastavení mohou poskytovat kvalitní detekci pohybu. I tak ale může docházet k falešným poplachům, které mohou být způsobeny například zvířaty, větrnými pohyby rostlin nebo změnami teploty.

### 1.1.8 Výběr vhodných senzorů

Při výběru vhodné technologie, která slouží pro účely této práce je důležitým faktorem finanční stránka věci a taky, aby nebylo třeba fyzicky zasahovat do dopravního prostředku, z důvodu narušení jeho technického stavu.

V první části se volila taková zařízení, která detekují případný pokus o odcizení. Jako prvotní zaznamenání pokusu, je v projektu umístěn akcelerometr, který pokud zaznamená nějaký pohyb, tak vyvolá příslušnou reakci v podobě alarmu. V případě, že by daný čin probíhal i nadále, je v projektu umístěn druhý prvek, který zajišťuje střežení. Tím je GPS modul, který v aktivním režimu zaznamenává aktuální polohu vozidla.

## 1.2 Akční členy komplikující pokusy o zcizení

Při výběru vhodných akčních členů, které by sabotovali, nebo znepríjemňovali pokusy o odcizení, se v této práci bude volit mezi audiovizuálními členy, formou mechanického zásahu do řízení, nebo informačním způsobu, který by v případě pokusu o zcizení vozidla informoval majitele. Rozhodující faktor bude jednoduchost implementace do vozidla a nenarušení technického stavu vozidla.

### 1.2.1 Audio poplach – piezo aktivní bzučák

Jedna z možností, kterou do projektu zakombinovat za účelem komplikace pokusu o odcizení je použití aktivního bzučáku, který funguje na principu piezoelektrického jevu. Jednalo by se o první akci, která by následovala po detekci pokusu o zcizení vozidla.



**Obr. 1.12 - Ukázka piezo sirény [15]**

Tento bzučák potřebuje pro svůj provoz napětí 5V, což umožňuje napájení přímo z desky Arduino a není třeba přidávání dalšího externího zdroje. Dokáže vyvinout frekvenci až 2300Hz +- 200Hz. [15] Na Obr. 1.12 je ukázan příklad piezo sirény, kterou lze použít pro účely této práce.

### **1.2.2 Rádiové varování vlastníka (pager)**

Za aktivní bránění odcizení vozidla lze považovat i varování vlastníka vozidla. V případě, že se jedná jenom o jednoduchou zprávu, lze využít radiové varování přes pager. Jedná se o spolehlivou volbu, jak rychle někoho informovat. Je to osvědčená a spolehlivá technologie. Lze ji využít pro přenos zvukových, číselných nebo textových zpráv. [17]

Provoz této technologie je zdarma, v případě, že se využije kmitočtů pro tento účel určených. V případě potřeby je možné zprávu rozeslat velké skupině příjemců a pokud by došlo k přetížení sítí pro mobilní sítě, nehrozí zpoždění zprávy poslané přes pager.

Na Obr. 1.13 je uveden příklad zařízení PAGER.



**Obr. 1.13 - Ukázka zařízení PAGER [17]**

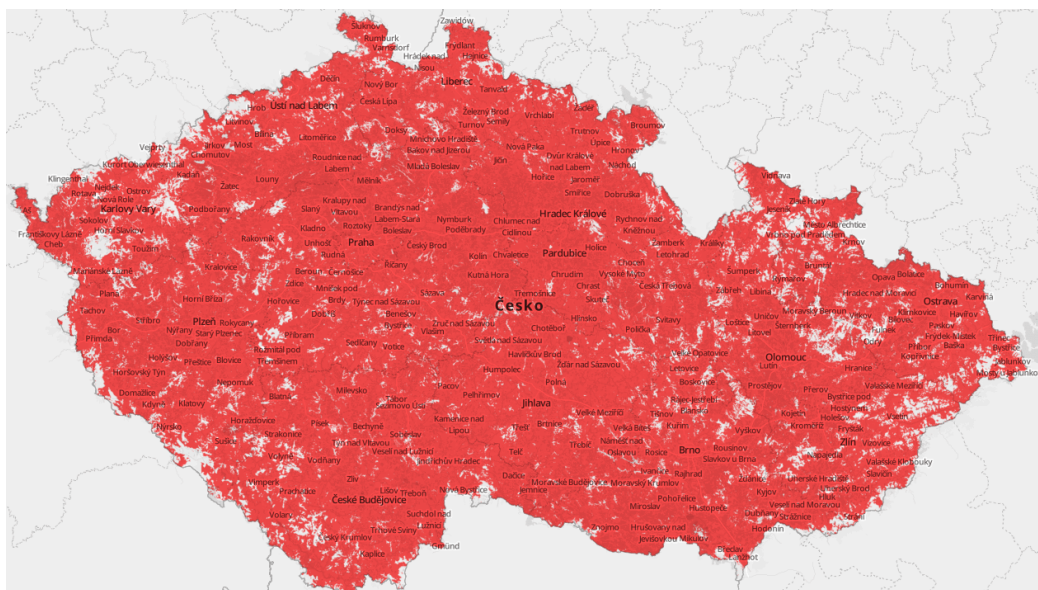
Nicméně, v dnešní době se jedná o poměrně zastaralé zařízení, a ne každý na tuto technologii je zvyklý.



### 1.2.3 Zasilání informace o poloze

Možnost, jakou bránit zcizení dopravního prostředku, je zasilání informace o poloze. Vzhledem k tomu, že se v projektu nachází GPS modul, stává se tato volba výhodnou. Jedná se o možnost, která dovoluje sledovat polohu, v případě, že by k zcizení již došlo a případně poskytnutí informací o poloze vozidla policii.

Posílat tuto informaci lze pomocí technologie Bluetooth, v případě že se budou zařízení nacházet v dostatečné vzdálenosti od sebe. Pokud by vzdálenost byla větší, lze do projektu zakomponovat GSM modul, který nám umožní zaslání informace o poloze na mobilní telefon téměř kamkoliv, pokud budou zařízení mít přístup k signálu. Mapa pokrytí ČR signálem GSM (operátor Vodafone) je ukázána na Obr. 1.14.

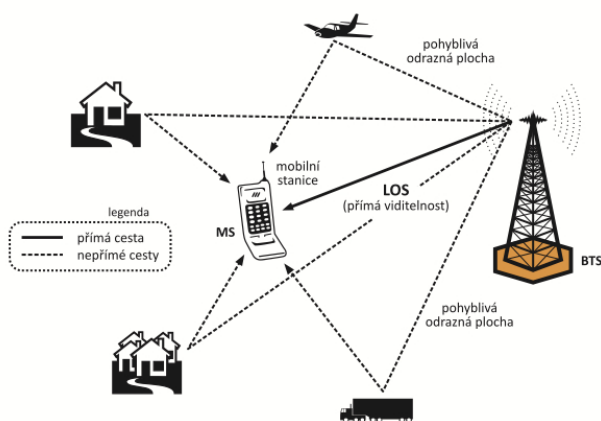


Obr. 1.14 - Mapa pokrytí sítě GSM v ČR (Vodafone) [16]

**Bluetooth** je technologie, která umožňuje propojení dvou a více elektronických zařízení. Může se jednat například o mobilní telefon, osobní počítač, nebo i bezdrátová sluchátka. [19] Umožňuje nám tak vyměňovat data mezi zařízeními bez nutnosti propojení kabelem, tedy bezdrátově.

**GSM**, v telekomunikacích se jedná o celostvětově nejrozšířenější standart pro mobilní sítě. [20] Umožňuje vzájemně komunikovat pomocí rádiových vln. Je v něm zahrnuto několik klíčových prvků. Jsou to mobilní telefony, báze stanic a řídicí centra, které vzjemně spolupracují, k zajištění přenosu.

Na Obr. 1.15 Je znázorněna struktura sítě GSM. A způsob komunikace mezi jednotlivými prvky této sítě.



Obr. 1.15 - Struktura sítě GSM [21]

#### 1.2.4 Blokace brzd

Další možnost, jak aktivně bránit odcizení by mohla být blokace brzd. Pokud by došlo k tomu, že jeden ze senzorů vyhodnotil pokus o odcizení vozidla, tak za použití například elektromagnetu by došlo k sepnutí toho magnetu a brzdový pedál by zůstal v zamknuté poloze, což by znemožnilo zcizení vozidla.

Aby měl elektromagnet dostatečnou sílu, potřebnou pro přidržení pedálu v zamknuté poloze, muselo by se použít vyššího napájení, než je možné použít z desky Arduina. Tím by se ale zvyšovala finanční stránka tohoto projektu. Navíc by při této možnosti bylo třeba manipulovat s brzdovým systémem, což by mohlo ohrozit bezpečnost, v případě, že by došlo k nechtěné aktivaci systému.

#### 1.2.5 Zhodnocení akčních členů a výběr

Při výběru akčních členů rozhodovalo, jako v případě výběru detektorů, finanční stránka a nutnost nenarušení technického stavu vozidla. S ohledem na tyto podmínky bude jako první z těchto členů v projektu zabudována piezo siréna. Jedná se o levné a účinné řešení, které bude plnit daný účel. Jako druhý prvek bude zasílání informace o poloze pomocí GSM GPRS modulu, protože v projektu bude umístěn i GPS modul.

## 2 Sestavení a princip fungování zabezpečovacího zařízení

Prototyp tohoto bezpečnostního zařízení bude založen na platformě Arduino, přesněji to bude model Mega, který funguje na procesoru ATmega2560. Součástí bude bluetooth modul, přes který bude docházet k zadání bezpečnostního kódu, k odjištění/zajištění střežení. Dále budou přítomny aktivní části, což budou akcelerometr a GPS modul. Ty budou kontrolovat konkrétní vozidlo a v případě detekce pokusu o odcizení dojde k akci, která bude pokus o zcizení sabotovat. Tato druhá část projektu bude realizována pomocí alarmu a GSM modulu, přes který dojde k zaslání SMS o narušení střežení vozidla a po vyžádání dojde k zaslání další SMS, kde se bude nacházet aktuální poloha vozidla.

Cílem realizace a testování bude zprovoznit navrhnutý bezpečnostní systém s vybranými součástkami, vytvořit řídicí aplikaci pro Arduino a po splnění bude celý výrobek řádně otestován.

### 2.1 Použité prvky v projektu

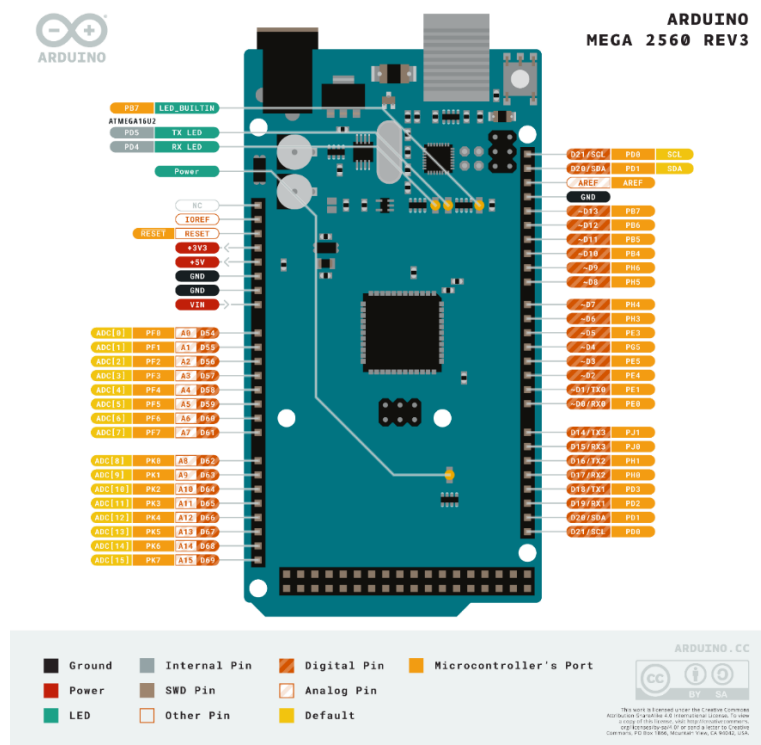
Seznam součástek, které jsou použity pro bezpečnostní zařízení :

- Mikrokontroler
- Bluetooth modul
- GPS modul
- Aktivní bzučák
- Akcelerometr
- GSM modul
- Zdroj napájení

#### 2.1.1 Mikrokontroler

Jako hlavní řídicí část tohoto projektu byla zvolena deska od firmy Arduino. Model má označení MEGA 2560 Rev3. Deska je založena na čipu ATmega2560, má celkem 54 digitálních vstupních/výstupních pinů, z toho jich 15 můžeme využívat jako výstupy pro PWM. Dále je na ní 16 analogových vstupů a pracuje na frekvenci 16MHz.

Čip pracuje s pamětí EEPROM, to zaručuje, že po vypnutí, nebo výpadku napájení nebudou data ztracena. Pracuje na 5V a limitní hodnoty jsou v rozmezí 6-20 V. [12]



Obr. 2.1 - Rozložení pinů, ARDUINO MEGA 2560 [12]

Volba tohoto modelu byla provedena na základě požadavku připojit 3 systémy přes sběrnici UART, nižší řady mají jen jednu a bylo by nutné řešit multiplexování (při výrobě jednoho kusu zabezpečovacího systému bylo vyhodnoceno jako výhodnější použít dražší variantu, ale ušetřit čas potřebný na programování řídicího programu).

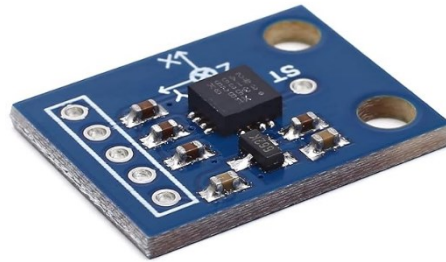
### 2.1.2 Akcelerometr

Po určení, že do projektu bude jako prvek pro detekci zabudován akcelerometr, bylo třeba vybrat ten správný, na trhu jich je nespočet vhodných, které jsou propojitelné se systémem Arduino.

Volilo se mezi několika typy:

- 3-osý modul Yunique GY521 MPU-6050
- 3-Osý modul GY-45 s MMA8452
- 6-Osý modul MPU-6500

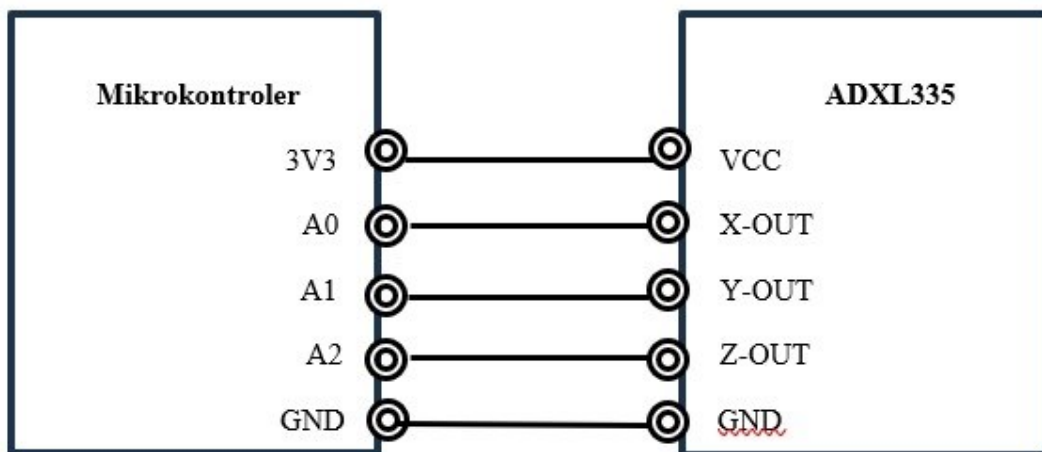
Do tohoto projektu byl zvolen akcelerometr s obvodem ADXL335. V tomto případě nebude použit vyloženě pro jeho prvotní účel, ale zde bude plnit pouze účel detekce pohybu. Z tohoto důvodu byl zvolen tento model. Pro účely této práce je svou funkčností plně dostačující, ostatní zmíněné modely by tuto funkci zastaly také, ale nabízejí i jiné, jako je třeba detekce volného pádu nebo obsahují i gyroskop, což je v této práci nadbytečné.



**Obr. 2.2 - Akcelerometr ADXL335**

Jelikož pro svou funkci využívá analogových hodnot, bude taky pro komunikaci s mikrokontrolerem využívat analogových pinů, což je znázorněno níže.

Na Obr. 2.2 je uveden akcelerometr ADXL335, tento typ akcelerometru je použit i v konstrukci tohoto zařízení.



**Obr. 2.3 - Schéma zapojení akcelerometru k mikrokontroleru**

Sám akcelerometr bude fungovat tak, že bude mít v programu nastavenou prahovou hodnotu, pokud tato hodnota bude překročena, v programu dojde reakci a to sice, že se spustí alarm.

Hodnota 512, kterou je v kódu naznačena, znamená střední pozici rozsahu analogového signálu. Je použita jako referenční hodnota pro nulovou hodnotu akcelerace ve směru x, y, z.

Na Obr. 2.4, je ukázána část kódu, která řeší tuto problematiku.

```
float xAcc = (xValue - 512) * citlivost;
float yAcc = (yValue - 512) * citlivost;
float zAcc = (zValue - 512) * citlivost;

if (strezeni && (abs(xAcc) > prah || abs(yAcc) > prah || abs(zAcc) > prah)) {
    digitalWrite(buzzerPin, HIGH);
    delay(3000);
    digitalWrite(buzzerPin, LOW);
}
```

Obr. 2.4 - Část kódu pro překročení hraniční hodnoty pro vyhlášení poplachu

### 2.1.3 Bluetooth modul

Bluetooth modul bude v práci plnit úlohu zadávání bezpečnostního kódu pro započítí a následné vypnutí střežení. Jedná se o model s označením HC-06, tento model je uveden na Obr. 2.5. Jedná se o komunikační modul pro Arduino. Umožňuje bezdrátové propojení s dalšími zařízeními, které podporují Bluetooth. Pro komunikaci využívá funkce UART, omezení, které se týče tohoto modulu je jeho anténa, která je za účelem dodržení malých rozměrů poměrně malá a dosah je omezen na vzdálenost přibližně 10 metrů. Pro tyto účely je to však dostačující a nebude to působit potíže při používání.



Obr. 2.5 - Bluetooth modul HC-06 [10]

Zařízení umožňuje celou řadu funkcí, kterou dokáže zpracovat, v této práci však bude plnit funkci, kde po vzájemném spárování s dalším zařízením ( Je nutné použít zařízení s operačním systémem android ), bude přijímat pouze znaky, díky kterým bude buď zapnuta funkce střežení, nebo po zadání druhého, odlišného znaku bude vypnuto.

V kódu je přidán i třetí znak, který v případě, že jsem v dosahu zařízení a jeho následného odeslání, pošle pomocí GSM modulu zprávu na mobilní telefon s aktuální polohou střeženého vozidla. Typově lze tuto variantu využít například Při ladění řídicího softwaru, aby se neposílaly placené SMS pro každou změnu v softwaru.

Na Obr. 2.6 je uvedeno řešení, pro zadání správného identifikačního kódu, pro zapnutí a vypnutí střežení.

```
if (BLUETOOTH_SERIAL.available()) {
  char receivedChar = (char)BLUETOOTH_SERIAL.read();
  if (receivedChar == 's') {
    strezeni = true;
    Serial.println("Střežení zapnuto");
  } else if (receivedChar == 't') {
    strezeni = false;
    Serial.println("Střežení vypnuto");
  } else if (receivedChar == 'p') {
    sendSMS_poloha();
  }
  bluetoothSpojeni = true;
}
```

Obr. 2.6 - Část kódu pro uvedení identifikačního kódu

#### 2.1.4 GPS modul

Jako druhý akční člen v tomto projektu je požit GPS modul, který zajišťuje druhou sadu opatření, které fungují jako zajištění detekce střežení. Zde byl zvolen modul Neo-7N od firmy U-Blox, modul je znázorněn na Obr. 2.7. Na modulu jako takovém se nachází pasivní anténa, nicméně pro lepší a spolehlivější vlastnosti je zde použita externí anténa, která je připojena přes SMA konektor.



Obr. 2.7 - GPS modul Neo-7N

Funkce modulu zde spočívá v tom, že pokud je projekt v režimu „střežení“, tak model v prvním okamžiku zapíše polohu zastřeženého vozidla do paměti kódu a nadále aktivně zaznamenává polohu. V případě, že dojde k změně polohy větší, než je odchylka modulu, zašle pokyn pro GSM modul, přes který je odeslána SMS zpráva s oznámením o pokusu odcizení vozidla.

### 2.1.5 GSM modul

Tento modul zde bude používán, jako aktivní prvek proti sabotování krádeže. Jedná se o modul GSM GPRS SIM800L v2.0 (viz. Obr. 2.8). Lze pomocí něho posílat zprávu, uskutečnit hovor, nebo i přenést data přes GPRS. Je schopen pracovat v sítích 2G a 3G, což je v současné době dostačující.



Obr. 2.8 - GSM modul SIM800L

V této části byl problém s napájením modulu. Přesněji s jeho odběrem proudu. Při používání modul totiž špičkově odebírá až přes 2A. To je problém, protože takový proud deska Arduino není schopna dodat, proto bylo třeba speciálně pro tento modul zajistit externí napájení pro jeho správnou a bezchybnou funkčnost.

Ovládání modulu je zajištěno pomocí AT příkazů. To jsou příkazy, které se používají k ovládní modemu nebo mobilního telefonu. Nejjednodušším z nich je samotná dvojice znaků AT. Pokud je příkaz zadán správně, odpovědí telefonu je „OK“. V případě, že jsou zadány chybně, jsou ignorovány a z telefonu přijde odpověď „ERROR“.

Níže je na Obr. 2.9 uvedena část kódu, kde se používají AT příkazy pro správné nastavení GSM modelu, aby plnil funkci, která je po něm žádaná v této práci.

```
GSM_SERIAL.println("AT+CMGF=1");  
delay(100);  
GSM_SERIAL.print("AT+CMGS=\"");  
GSM_SERIAL.print(123456789);  
}
```

Obr. 2.9 – Část kódu, s AT příkazy



### 2.1.6 Zdroj napájení

Zdroj elektrické energie bude pro účely této bakalářské práce využita powerbanka. Jedná se o model PPBD30, který je uveden na Obr. 2.10. Akumulátor je vyroben polymer-lithiovou technologií. Právě tento typ baterií se hojně využívá pro různá přenosná zařízení, která vyžadují bezdrátové napájení bez přidané kabeláže, jako jsou například různá čidla, senzory nebo i drony.

Powerbanka má kapacitu 30000mAh s výkonem 15W, to je pro tento projekt plně dostačující. Zároveň se jedná o poměrně kompaktní model, a to je žádoucí vlastnost, při napájení tohoto projektu.



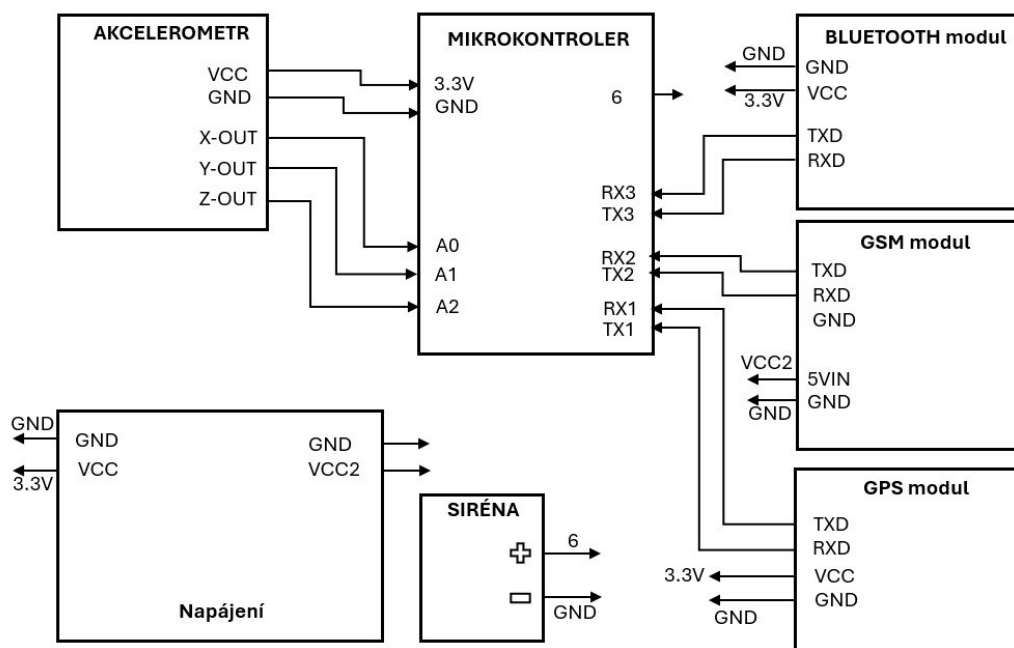
Obr. 2.10 - Zdroj napájení

Jak již bylo zmíněno dříve, projekt vyžaduje zajistit externí zdroj napájení pro GSM modul. To tento typ akumulátoru nabízí, protože je vybaven dvěma USB výstupy. Navíc je třeba zajistit výstup, který bude dodávat dostatečný proud, který je nezbytný pro spolehlivou funkci GSM modulu. USB výstupy akumulátoru nabízí 5V/3A.

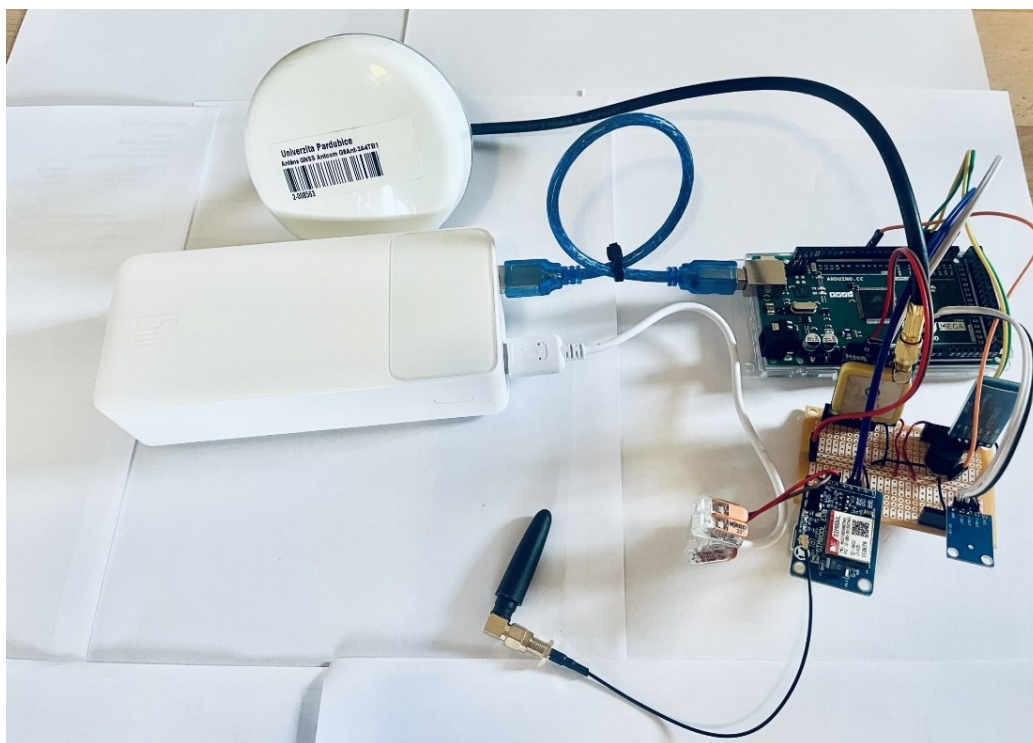
## 2.2 Konstrukce zařízení

Na Obr. 2.11 je zpracované blokové schéma zařízení. Jsou zahrnuty všechny části bezpečnostního zařízení a jsou popsány všechny piny pro korektní zapojení. Jako řídicí část celého zařízení je zde mikrokontroler, který zpracovává všechny příkazy a řídí projekt. Bluetooth modul, který zajišťuje dálkové ovládání střežení a zadávání identifikačního kódu. Akcelerometr s GPS modulem zde pracují jako detektory pro zjištění pokusu o zcizení. GSM modul se sirénu jsou aktivní prvky zařízení, které mají za úkol sabotovat daný pokus o odcizení vozidla. Celý projekt je vybaven napájením, které umožňuje dva výstupy, což je

nezbytná vlastnost (z důvodu samostatného napájení GSM modulu), pro korektní funkci zařízení.



Obr. 2.11 - Blokové schéma zařízení

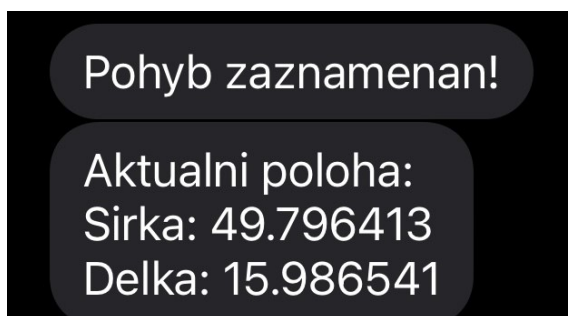


Obr. 2.12 - Zkonstruované bezpečnosti zařízení

Na Obr. 2.12 je zobrazené kompletně zkonstruované zařízení se všemi prvky projektu.

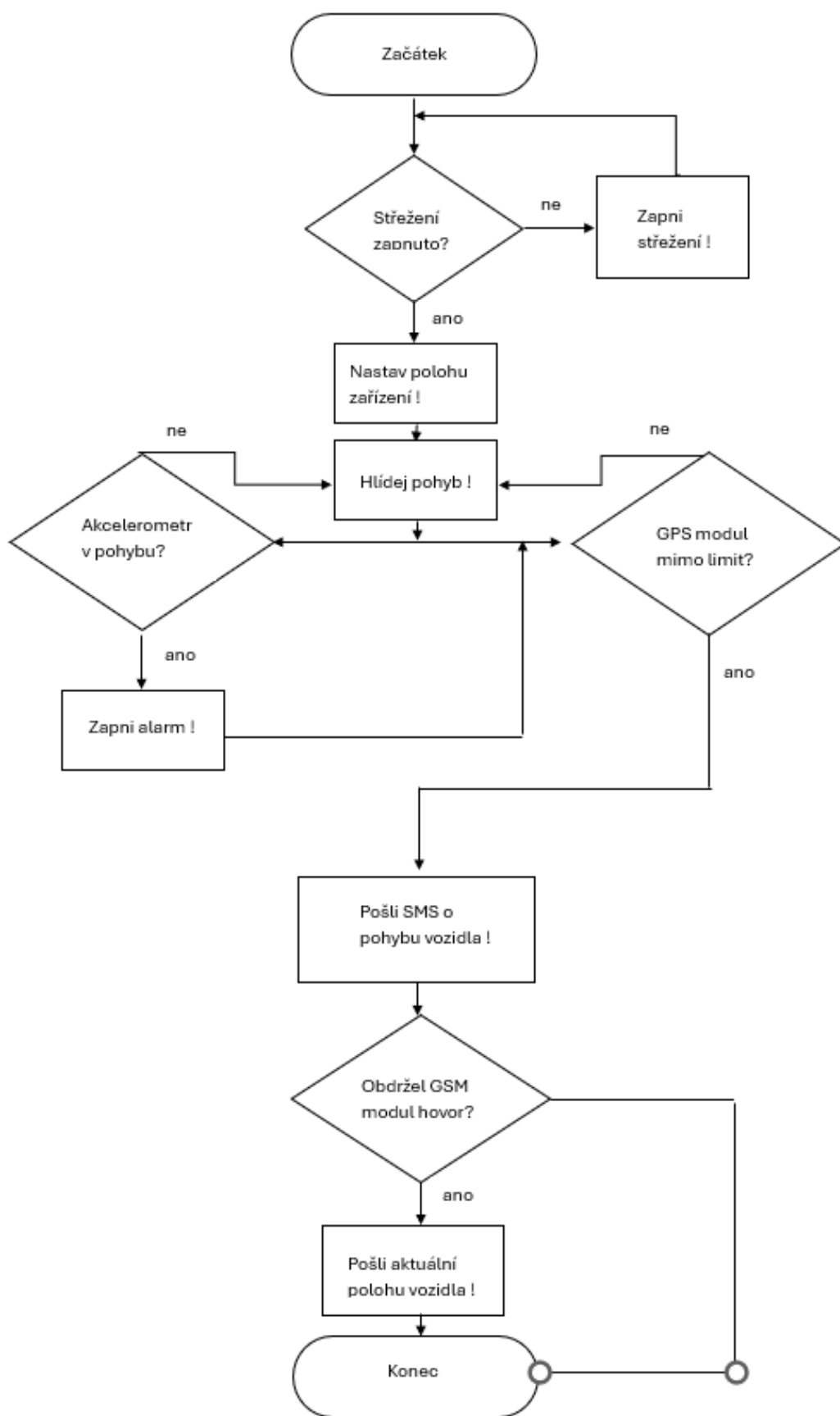
### 3 Firmware

Na Obr. 3.2 je uveden vývojový diagram pro toto zařízení. Pro zapnutí střežení, je třeba zadat identifikační kód pomocí Bluetooth modulu. Pro zapnutí střežení je třeba poslat přes modul znak „s“ a pro vypnutí se jedná o znak „t“, v kódu je ještě přidán znak „p“, který slouží pro zaslání aktuální polohy zařízení pomocí GSM modulu. Ve chvíli, kdy je kód zadán, zařízení je ve stavu aktivního střežení. GPS modul si nastaví jako výchozí polohu takovou, kde se nachází po zapnutí zařízení. Potom oba členy hlídají pohyb. V případě, že se vozidlo uvede do pohybu (dojde k pokusu o odcizení), tak jeden nebo oba členy začnou reagovat, akcelerometr spustí alarm a GPS modul, pokud vyhodnotí pohyb vozidla i přes vymezené pásmo, tak pošle SMS zprávu, pomocí GSM modulu o pokusu o zcizení vozidla. GPS modul i nadále zaznamenává aktuální polohu a v případě, že GSM modul obdrží hovor, tak pošle další SMS s aktuální polohou (zeměpisná délka a šířka). Aby se zamezilo odesílání SMS v případě, že by na GSM modul zavolalo neautorizované číslo, je v kódu přidána část, kde probíhá kontrola telefonního čísla a v případě, že kontrolou neprojde, systém na něj nereaguje.



Obr. 3.1 - Ukázka komunikace přes GSM modul

Na Obr. 3.1, je ukázán formát zpráv, které jsou posílány přes GSM modul na mobilní telefon, který je nastavený ve firmwaru tohoto zařízení.

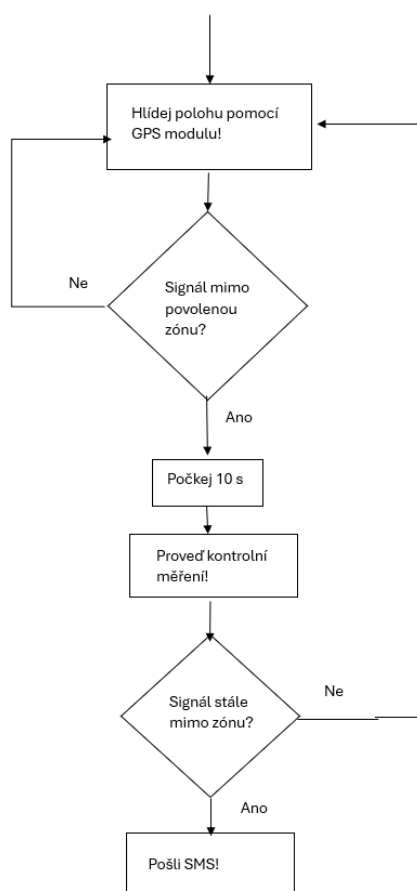


Obr. 3.2 - Vývojový diagram

### 3.1 Úpravy firmwaru proti falešným poplachům

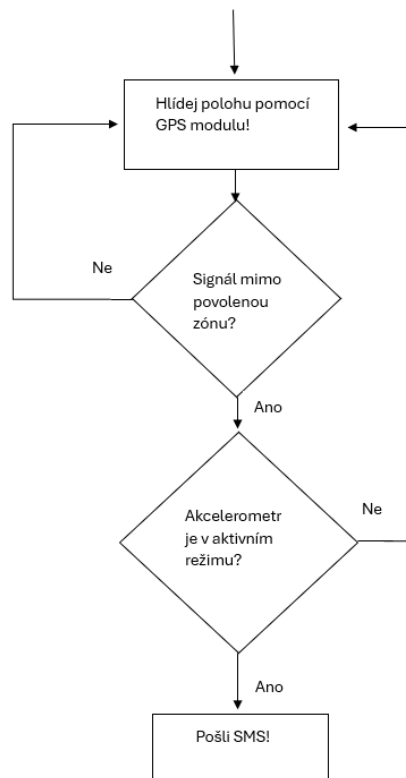
V této části budou uvedeny části vývojových diagramů, které bylo nutné vytvořit, za účelem zamezení vyvolávání falešných poplachů.

Na Obr. 3.3 je vidět princip, jakým je upravený firmware, aby nedocházelo k falešnému vyvolání poplachu. V Případě, že GPS modul vyhodnotí poplach, dojde pouze k varování a po 10 sekundách dojde ke kontrolnímu měření. Po tomto měření, pokud je poloha pořád mimo povolenou zónu, tak je odeslána SMS s oznámením o pohybu vozidla, v opačném případě se program vrátí do stavu střežení.



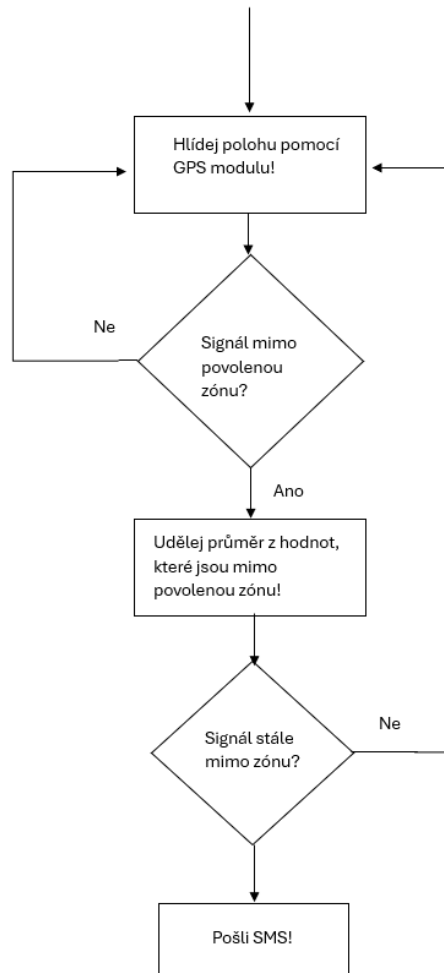
**Obr. 3.3 - Vývojový diagram s kontrolním měřením**

Níže je uveden Obr. 3.4, zde je kód upraven způsobem, že k poplachu dojde pouze v případě, kde musí dojít k vyhodnocení alarmu jak u akcelerometru, tak i u GPS modulu. Takže k odeslání SMS zprávy dojde jenom v případě, dojde ke změně polohy mimo vymezenou oblast, ale zároveň musí být aktivován i akcelerometr.



**Obr. 3.4 - Vývojový diagram, kde je GPS modul spojen s akcelerometrem**

Třetí varianta, která byla použita při měření je uvedena na Obr. 3.5. Zde, aby bylo zamezeno falešným poplachům, je po zaznamenání úniku signálu mimo danou oblast, prováděno průměrování vzdáleností vůči statické poloze zařízení, která je nastavena po zapnutí střežení. V Případě, že je i po vypočítání tohoto průměru je vyhodnocena poloha mimo povolenou oblast, teprve potom je vyhlášen poplach a odeslána SMS.



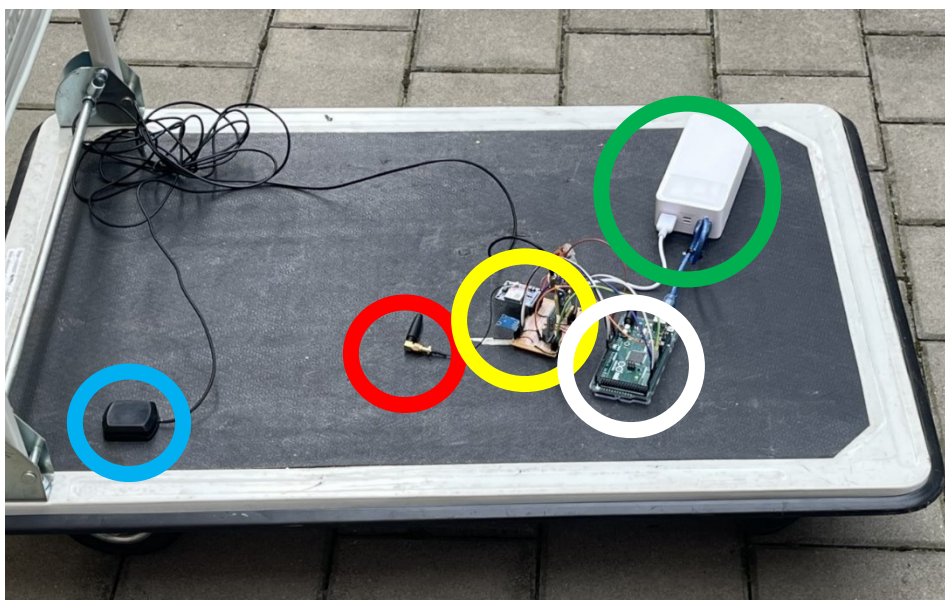
Obr. 3.5 - Vývojový diagram s průměrováním signálu mimo oblast

## 4 Testovací měření

Ověření funkčnosti navrženého systému bylo provedeno sadou měření. V této kapitole jsou popsána tato měření a shrnuty poznatky z těchto měření. Jsou zde popsány jak výsledky prvotních měření, tak měření systému po úpravách, které byly realizovány na základě poznatků z prvotních měření.

### 4.1 Popis experimentu pro původní nastavení

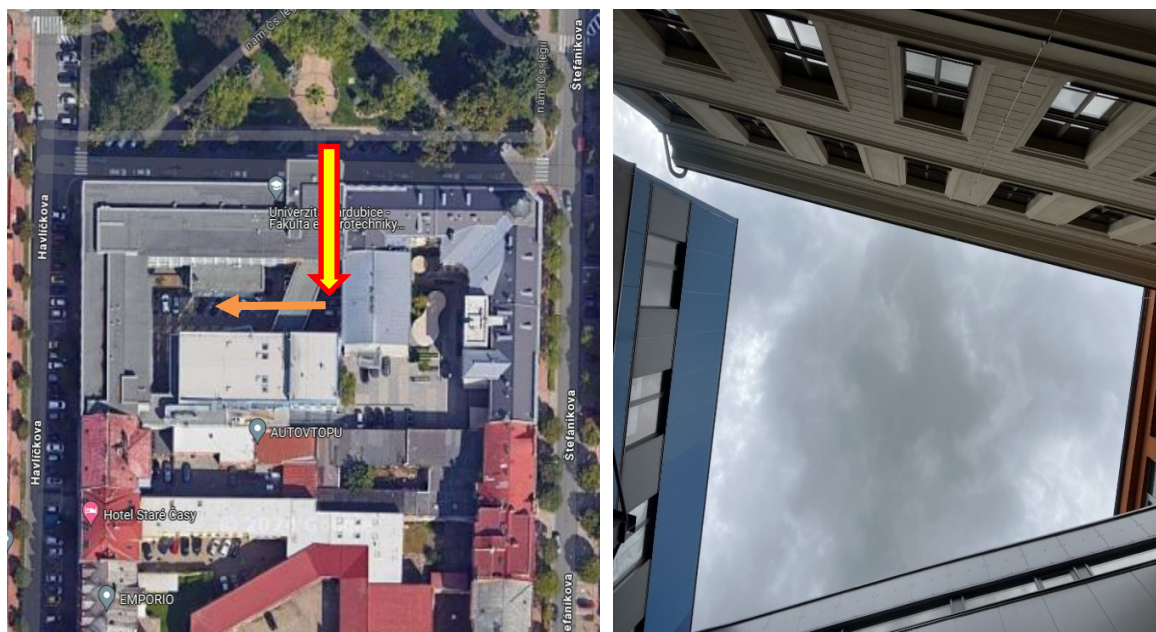
Pro provedení testovacího zařízení bylo třeba nasimulovat situace, které by mohli nastat při pokusu o odcizení vozidla. Pro tento účel byla použita mobilní platforma, jak je vidět na Obr. 4.1. V obrázku jsou zvýrazněné jednotlivé části zařízení. Modře označená je anténa pro GPS modul, červeně pro GSM modul. Ve žlutém kruhu jsou všechny senzory a čidla na nepájivém poli. V zeleném se nachází zdroj napájení a v bílém je mikrokontroler Arduino.



Obr. 4.1 - Mobilní platforma

Pro první měření byly vybrány místa, kde signál z antény byl blokován budovami, jak je vidět na Obr. 4.2. Druhé místo bylo zvoleno bez budov v dohledu antény, aby byl vidět co největší rozdíl ve funkčnosti, viz. Obr. 4.3. Jak lze vidět na přiložených obrázcích, místa, kde byla provedena měření jsou vyznačena žlutou šipkou s červeným označením a směr, ve kterém se následně začalo se zařízením pohybovat je vyznačen oranžovou šipkou.





Obr. 4.2 – Lokace pro experiment v zástavbě (vlevo) a výhled na oblohu z dané lokace (vpravo).



Obr. 4.3 – Lokace pro experiment s volným výhledem (vlevo) a výhled na oblohu z dané lokace (vpravo).

Měření probíhalo v patnácti minutových intervalech, kde zůstalo zařízení nehybné a vyhodnocovali se případné falešné poplachu, vyvolané únikem signálu z GPS modulu mimo povolený rozsah nebo nechtěná aktivace akcelerometru. Po patnácti minutách se mobilní platforma dala do pohybu a byly zapsány délky, kde se v první řadě rozezněl alarm a potom přišla SMS přes GSM modul.

Tabulka 2- Statické měření zástavba (15 minut)

Pokus	GPS zabezpečení	AKCELEROMETR zabezpečení
1	Poplach za 4 minuty	Bez poplachu
2	Bez poplachu	Bez poplachu
3	Poplach za 6 minut	Bez poplachu

**Tabulka 3- Vyhlášení pohybu při pohybu v zástavbě**

Pokus	GPS zabezpečení	AKCELEROMETR zabezpečení
1	NA	2 metry
2	15,5 metru	0,5 metru
3	NA	2,6 metru

Z Tabulka 2 a

Tabulka 3 lze vidět, že pokud je zařízení umístěno v místě, kde je z více stran krytý dosah signálu, dochází k falešnému poplachu v části GPS zabezpečení, což vede k nesprávné funkci zabezpečování. Část s akcelerometrem funguje správně, nedochází k nechtěnému vyvolání alarmu a v případě uvedení platformy do pohybu je alarm vyvolán v řádu několika metrů.

**Tabulka 4- Statické měření volný prostor (15 minut)**

Pokus	GPS zabezpečení	AKCELEROMETR zabezpečení
1	Bez poplachu	Bez poplachu
2	Bez poplachu	Bez poplachu
3	Bez poplachu	Bez poplachu

**Tabulka 5- Vyhlášení pohybu při pohybu ve volném prostoru**

Pokus	GPS zabezpečení	AKCELEROMETR zabezpečení
1	7,4 metru	1,25 metry
2	4,7 metru	4,7 metru
3	5,10 metru	5,1 metru

Z Tabulka 4 a Tabulka 5, pokud je zařízení ve volném prostoru a jsou vhodně nastaveny meze pro poplach, tak zařízení funguje bez poplachů jak v části GPS, tak i akcelerometru. Při uvedení do pohybu, se oba poplarchy spustí do několika metrů.

Po provedeném měření lze dojít k závěru, že část s akcelerometrem funguje tak, jak se od ní očekávalo, nedochází k falešnému vyvolání poplachu v důsledku nějakého otřesu a při uvedení do pohybu se aktivuje alarm v jednotkách metrů. Část s GPS modulem, ale v případě, že bylo zařízení umístěno v zástavbě, 2x ze tří pokusů vyvolalo poplach a odeslalo SMS. To je nechtěný výsledek a tuto část je třeba upravit, aby se zamezilo takovým situacím.

Chyba ve vzdálenosti vůči nastavené poloze v průběhu měření, která vzniká chybami měření, je znázorněna na Obr. 4.4.



Obr. 4.4 – Chyba určené vzdálenosti od nastavené polohy v čase.

## 4.2 Úpravy systému na základě prvotních měření

Je třeba navrhnout takové řešení, aby k odeslání SMS došlo jen v případě, že se vozidlo dá opravdu do pohybu a nebude to vyvolané jenom únikem signálu. Níže jsou uvedeny možná řešení :

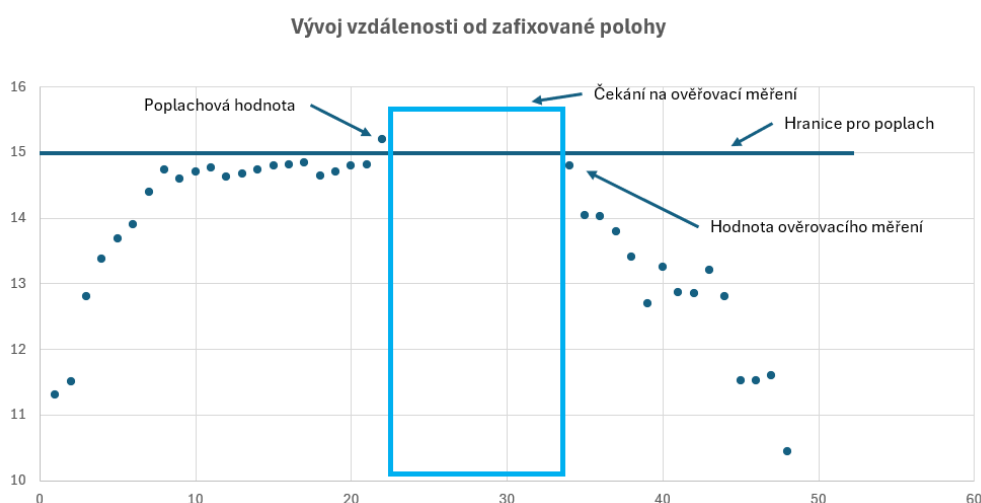
- Provedení rozšíření zóny, kterou je třeba přesáhnout, aby došlo k vyvolání poplachu. Toto řešení bude asi nejjednodušší ze všech, ale dojde tím k navýšení vzdálenosti, kdy GPS modul vyhodnotí poplach.
- Přidat ověřovací měření, kde dojde po uběhnuté době k opětovnému měření a v případě, že zařízení bude pořád mimo povolené území, potom dojde k vyvolání detekce pohybu,
- Synchronizovat fungování obou senzorů, aby k poplachu došlo pouze v případě aktivace obou zároveň. To znamená, že k aktivaci GPS modelu nemůže dojít v případě, že zároveň s ním není aktivní i akcelerometr.
- Dalo by se průměrovat měření, kde například z každých 10 by se vyhodnotilo, zda došlo k pokusu o odcizení. Tato možnost by sice zamezila falešnému poplachu, kdyby došlo k úniku GPS signálu mimo povolené území, ale v případě, že by vozidlo bylo skutečně v pohybu, tak by pouze docházelo k oddalování zaslání oznámení o krádeži

## 4.3 Výsledky experimentu po úpravách firmware

V příloze A jsou uvedeny výsledky měření, v případech s různými úpravami kódu, za účelem zamezení falešných poplachů. Varianta, kde bylo měření polohy GPS

průměřované, se ukázala jako nepřilíř vhodná, protože k falešnému poplachu docházelo i nadále a vzdálenost, kterou zařízení urazilo než, systém zareagoval, se podstatně zvýřila.

Při měření, kde po úniku signálu dořlo k pouze k varování v podobě spuštění sirény a po uplynulém čase 10ti sekund se provedlo kontrolní měření znovu (modrý rámeček), již nedocházelo k nežádoucímu odeslání SMS zprávy. Ale vzdálenost, kterou zcizované vozidlo urazilo, se navýřila jeřtě více než v případě, kdy se měnila velikost povolené oblasti. Na **Chyba! Nenalezen zdroj odkazů.** je ukázán vývoj vzdálenosti od zafixované polohy v důsledku chyby měření. Z obrázku je patrné, že v určitém okamžiku byla tato hranice překročena, ale jelikož se za 10 sekund provedlo kontrolní měření, poplach nebyl aktivován, jelikož se poloha vrátila zpět do požadované oblasti.



Obr. 4.5 - Únik signálu pro úpravu kódu s varováním

Jako třetí varianta této úpravy, se použila možnost synchronizace s akcelerometrem. Poplach bude vyvolán pouze v případě, že při pokusu o odcizení, bude aktivován jak akcelerometr, tak i GPS signál bude mimo nastavenou hodnotu. Při měření s touto možností nedošlo k falešnému poplachu a vzdálenost aktivace poplachu při pokusu o odcizení je podstatně menří než v předchozích případech. Rizikem tohoto případu je, že při výpadku akcelerometru je zablokován i systém GPS a dopravní prostředek zůstane nestřežen.

Jako nejlepší varianta se ze zmíněných možností jeví část úpravy kódu, kde se oba členy pro detekci pohybu synchronizují. Při této možnosti nedochází k falešným poplachům a rychlost vyhlášení poplachu je znatelně efektivnější než v ostatních případech.

#### 4.4 Testování finální verze systému v reálném prostředí

Při finálním řešení byla vybrána varianta synchronizace akcelerometru a GPS, pro zasílání SMS, pro zvukový poplach byl systém ponechán v režimu využívající pouze akcelerometr. V tomto případě bylo již zařízení umístěno v osobním automobilu. Automobil nejdříve byl ponechán v nepohyblivém stavu přibližně 15 minut, za účelem zjištění případných falešných poplachů. Po uplynutí této doby se vozidlo plynule dostávalo do

pohybu a byla měřena vzdálenost, při které zareagují senzory a bude následovat příslušná reakce.

**Tabulka 6- Výsledky měření v klidovém stavu vozidla (15 minut)**

Pokus	GPS zabezpečení	AKCELEROMETR zabezpečení
1	Bez poplachu	Bez poplachu
2	Bez poplachu	Bez poplachu
3	Bez poplachu	Bez poplachu

**Tabulka 7- Výsledky měření při uvedení do pohybu**

Pokus	GPS zabezpečení	AKCELEROMETR zabezpečení
1	34.5 metrů	5 metrů
2	41 metrů	7 metrů
3	46 metrů	6,5 metrů

V Tabulka 7 a Tabulka 7 jsou výsledky pro takové měření. Měření probíhalo s již upraveným firmwarem. Lze vidět, že v případě ponechání vozidla v klidu, nedošlo ani jednou k falešnému vyvolání poplachu. Pokud se vozidlo dalo do pohybu, zabezpečení alarmem začalo fungovat do několik metrů. Část s GPS signálem vyhodnotila pokus o krádež ve vzdálenosti v rozmezí 30 až 50 metrů.

Je důležité ale zdůraznit, že pokud budou oba detektory fungovat společně, jako v tomto měření, potom ve chvíli, kdy by na akcelerometru vznikla chyba, že by například přestal fungovat, nedojde ani k vyhlášení poplachu z GPS modulu.

## Závěr

Cílem této práce bylo navrhnout a sestavit zařízení, jež bude sloužit ke zjištění pokusu o zcizení zastřeženého dopravního prostředku a v případě pokusu o odcizení, bude této činnosti aktivně bránit. Podmínkou pro navržené zařízení bylo, aby provádělo dvě základní sady operací, a to v první řadě zjištění daného pokusu a pokud k takové situaci dojde, potom aby jí aktivně sabotovala. Bezpečnostní zařízení se také musí primárně ovládat pomocí dálkově řízeného ovladače. Všechny zmíněné body jsou v této práci úspěšně implementovány a funkčně otestovány. Lze tedy říci, že zadání práce bylo splněno v celém rozsahu

V teoretické části byl proveden rozbor dostupných možností pro detekci pokusu o odcizení vozidla a možnostech sabotáže těchto pokusů. Byly porovnány výhody a nevýhody jednotlivých prvků a na základě této rešerše byly vybrány vhodné prvky a zařízení, které jsou v práci použity.

Výsledné zařízení, pokud je pomocí Bluetooth modulu zadán příslušný identifikační kód, tak je uvedeno do stavu aktivního střežení. Prvky detekce pokusu o odcizení, což jsou akcelerometr a GPS modul, jsou aktivní a v klidovém stavu vozidla jsou nečinné. V případě pokusu o zcizení, kdy tyto detektory zaznamenají pohyb, dají pokyn pro akční členy systému. Zde se jedná o sirénu a GSM modul, pomocí kterého je vyslána SMS zpráva o pohybu vozidla. GPS modul nadále zaznamenává aktuální polohu střeženého vozidla a na vyžádání odesílá další SMS zprávu s aktuální pozicí dopravního prostředku.

Do budoucna by se dalo do projektu přidat vlastnost, aby se údaje o poloze vozidla mohl vyžádat kdokoliv, kdo má o zařízení potřebné informace. Například pokud by již došlo k odcizení, aby se tyto informace dali předat policii a oni mohli nezávisle vozidlo sledovat, za účelem úspěšného nalezení dopravního prostředku.

## Literatura

- [1] *JAK FUNGUJE A K ČEMU SLOUŽÍ AKCELEROMETR?* [online]. [cit. 2023-11-21]. Dostupné z: <https://www.tme.eu/cz/news/library-articles/page/22568/jak-funguje-a-k-cemu-slouzi-akcelerometr/>
- [2] *Použití technologie fúze senzorů na akcelerometry a gyroskopy* [online]. In: . [cit. 2023-11-21]. Dostupné z: <https://www.digikey.tw/zh/articles/apply-sensor-fusion-to-accelerometers-and-gyroscopes>
- [3] *Gyroskop v telefonu: co to je a princip zařízení, ve kterém jsou nainstalovány modely smartphonů* [online]. In: PORADCE, Agatha. 2020 [cit. 2023-11-24]. Dostupné z: <https://povedet-cz.eu/smieny/gyroskop-v-telefonu-co-to-je-a-princip-zaizeni-ve.html>
- [4] *Rtuťový spínač polohy* [online]. 1 [cit. 2023-12-01]. Dostupné z: [https://www.hwpro.cz/oc/index.php?route=product/product&product\\_d=267](https://www.hwpro.cz/oc/index.php?route=product/product&product_d=267)
- [5] MARCINKOWSKA, Sandra. *Magnetický senzor – co to je a k čemu se používá?* [online]. 2023, 1 [cit. 2023-12-01]. Dostupné z: <https://botland.cz/blog/magneticky-senzor-co-to-je-a-k-cemu-se-pouziva/>
- [6] HARTING S.R.O. *Proudové senzory využívající Hallův jev* [online]. 2019, 1 [cit. 2023-12-01]. Dostupné z: <https://www.elektroprumysl.cz/merici-technika/proudove-senzory-vyuzivajici-halluv-jev>
- [7] MLČOCH, Zbyněk. *Princip GPS navigace, jak funguje GPS - vysvětlení* [online]. 2009, 2009, 1 [cit. 2024-01-22]. Dostupné z: <https://www.zbynekmlcoch.cz/texty/technika/princip-gps-navigace-jak-funguje-gps-vysvetleni>
- [8] *Globální polohovací a navigační satelitní systémy. Geoinformatika* [online]. 1 [cit. 2024-03-04]. Dostupné z: <http://geologie.vsb.cz/geoinformatika/kap09.htm>

- [9] Jaké moderní systémy proti krádeži existují pro automobily? *Auto* [online]. 2024, 1 [cit. 2024-04-05]. Dostupné z: <https://levnepneu-online.cz/jake-moderni-systemy-proti-kradezi-existuji-pro-automobily/>
- [10] *Bluetooth modul HC-06* [online]. In: . s. 1 [cit. 2024-04-12]. Dostupné z: <https://navody.drateg.cz/navody-k-produktum/bluetooth-modul-hc-06.html>
- [11] HADEC. *Tlakový senzor FSR402 /váhový senzor Arduino/* [online]. [cit. 2024-04-16]. Dostupné z: <https://www.hadex.cz/m529-tlakovy-senzor-fsr402--vahovy-senzor-arduino/>
- [12] *Arduino Mega 2560 Rev3* [online]. In: . [cit. 2024-04-03]. Dostupné z: <https://store.arduino.cc/products/arduino-mega-2560-rev3>
- [13] *Co je PIR čidlo a jak funguje?* [online]. 1 [cit. 2024-03-01]. Dostupné z: <https://www.kvelektro.cz/blog/clanek/pir-cidlo>
- [14] DESERTCART. *Sensors* [online]. DESERTCART. [cit. 2024-04-17]. Dostupné z: <https://czech.desertcart.com/products/174426869-adxl335-3-axis-accelerometer-angular-transducer-sensor-gy-61-module-analog-output-3-5v-for-arduino>
- [15] PÁJENÍČKO.CZ. *Piezo Sirénka* [online]. [cit. 2024-04-17]. Dostupné z: <https://pajenicko.cz/piezo-sirenka-aktivni-bzucak-buzzer-5v>
- [16] CZECH MOBILE. Pokrytí sítě Czech mobile. *CZECH MOBILE* [online]. 2016 [cit. 2024-04-17]. Dostupné z: <https://czech-mobile.cz/mapa-pokryti/>
- [17] RADIOSTANICE. Pagery. *Radiostanice.cz* [online]. [cit. 2024-04-17]. Dostupné z: <https://www.radiostanice.cz/pagery>
- [18] Navigační systém Galileo začal nabízet služby. Pro jediný model telefonu. *Technet* [online]. 2016, 1 [cit. 2024-04-27]. Dostupné z: [https://www.idnes.cz/technet/vesmir/galileo.A161215\\_132601\\_tec\\_vesmir\\_kuz](https://www.idnes.cz/technet/vesmir/galileo.A161215_132601_tec_vesmir_kuz)
- [19] WIKIPEDIE. Bluetooth. *Wikipedie* [online]. [cit. 2024-05-06]. Dostupné z: <https://cs.wikipedia.org/wiki/Bluetooth>



- [20] WIKIPEDIE. GSM. *Wikipedie* [online]. [cit. 2024-05-06]. Dostupné z: <https://cs.wikipedia.org/wiki/GSM>
- [21] PUBLI.CZ. Mobilní telekomunikační sítě. PUBLI. *Publi.cz* [online]. [cit. 2024-05-06]. Dostupné z: <https://publi.cz/books/236/02.html>

## Příloha A – Tabulky po úpravě kódu, k zamezení poplachů

**Tabulka 8- Vyhlášení poplachu v zástavbě ( průměrování měření )**

Pokus	GPS zabezpečení (statické měření)	GPS zabezpečení (Při pohybu)
1	Poplach za 4 minuty	NA
2	Bez poplachu	21 metrů
3	Poplach za 3 minuty	NA

**Tabulka 9- Vyhlášení poplachu v zástavbě ( Kontrolní měření po vyhlášení úniku signálu )**

Pokus	GPS zabezpečení (statické měření)	GPS zabezpečení (Při pohybu)
1	Bez poplachu	31,2 metrů
2	Bez poplachu	36,3 metrů
3	Varování za 8 minut, potom následné vrácení signálu do vymezené oblasti	NA

**Tabulka 10- Vyhlášení poplachu v zástavbě ( Synchronní vyhlášení s akcelerometrem )**

Pokus	GPS zabezpečení (statické měření)	GPS zabezpečení (Při pohybu)
1	Bez poplachu	14,2 metrů
2	Bez poplachu	11,8 metrů
3	Bez poplachu	13

**Tabulka 11- Vyhlášení poplachu ve volném prostoru ( Kontrolní měření po vyhlášení úniku signálu )**

Pokus	GPS zabezpečení (statické měření)	GPS zabezpečení (Při pohybu)
1	Bez poplachu	23,4 metrů
2	Bez poplachu	18,7 metrů
3	Bez poplachu	25,6 metrů

**Tabulka 12- Vyhlášení poplachu ve volném prostoru ( Synchronní vyhlášení s akcelerometrem )**

Pokus	GPS zabezpečení (statické měření)	GPS zabezpečení (Při pohybu)
1	Bez poplachu	8,7 metrů
2	Bez poplachu	10,3 metrů
3	Bez poplachu	9,6 metrů

**Tabulka 13- Vyhlášení poplachu ve volném prostoru ( Průměrování měření)**

Pokus	GPS zabezpečení (statické měření)	GPS zabezpečení (Při pohybu)
1	Poplach za 7 minut	NA
2	Bez poplachu	18,3
3	Bez poplachu	23,9 metrů

## Příloha B – Zdrojový kód

```
#include <TinyGPS.h>
#define GPS_SERIAL Serial1
#define GSM_SERIAL Serial2
#define BLUETOOTH_SERIAL Serial3
TinyGPS gps;
const int xPin = A0;
const int yPin = A1;
const int zPin = A2;
const int buzzerPin = 6;
float citlivost = 0.1;
int prah = 25;
int chyba_prumer = 0;
bool strezeni = false;
bool varovani = false;
bool bluetoothSpojeni = false;
bool smsOdeslana = false;
bool poloha = false;
bool pohybDetekovan = false;
float initialLat = 0.0;
float initialLon = 0.0;
const float minALARM = 15.0;

void setup() {
  Serial.begin(9600);
  GPS_SERIAL.begin(9600);
  GSM_SERIAL.begin(9600);
  BLUETOOTH_SERIAL.begin(9600);
  pinMode(buzzerPin, OUTPUT);
}

void loop() {
  if (BLUETOOTH_SERIAL.available()) {
    char receivedChar = (char)BLUETOOTH_SERIAL.read();
    if (receivedChar == 's') {
      strezeni = true;
      Serial.println("Střežení zapnuto");
    } else if (receivedChar == 't') {
      strezeni = false;
      Serial.println("Střežení vypnuto");
    } else if (receivedChar == 'p') {
      sendSMS_poloha();
    }
    bluetoothSpojeni = true;
  }
  if (bluetoothSpojeni) {
    int xValue = analogRead(xPin);
    int yValue = analogRead(yPin);
    int zValue = analogRead(zPin);
    float xAcc = (xValue - 512) * citlivost;
    float yAcc = (yValue - 512) * citlivost;
    float zAcc = (zValue - 512) * citlivost;
    if (strezeni && (abs(xAcc) > prah || abs(yAcc) > prah || abs(zAcc) >
    prah)) {
      digitalWrite(buzzerPin, HIGH);
      delay(3000);
      digitalWrite(buzzerPin, LOW);
      smsOdeslana = false;
      pohybDetekovan = true;
    } else {
```

```

    pohybDetekovan = false;
}
}
if (strezeni && !smsOdeslana) {
    bool newData = false;
    for (unsigned long start = millis(); millis() - start < 1000;) {
        while (GPS_SERIAL.available()) {
            char c = GPS_SERIAL.read();
            if (gps.encode(c)) {
                newData = true;
            }
        }
    }

    if (newData) {
        float sirka, delka;
        gps.f_get_position(&sirka, &delka);
        Serial.println("GPS udaje:");
        Serial.print("Zemepisna sirka: ");
        Serial.print(sirka == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : sirka, 6);
        Serial.print(" delka: ");
        Serial.print(delka == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : delka, 6);
        if (!poloha) {
            initialLat = sirka;
            initialLon = delka;
            poloha = true;
        }
        float vzdalenost = TinyGPS::distance_between(initialLat, initialLon,
sirka, delka);
        String poslat = "vzdalenost" + String(vzdalenost);
        Serial.print(poslat);
        if (vzdalenost >= minALARM && pohybDetekovan) { //varianta 1 start
            sendSMS("Pohyb zaznamenan!");
            smsOdeslana = true;
        } //varianta 1 stop
        if (GSM_SERIAL.available()) {
            // Pokud je k dispozici data na sériovém portu GSM modulu
            String c = "a";
            c=GSM_SERIAL.readString(); // Přečtení příchozího znaku
            //c = "a";
            //Serial.print(c.substring(2,6));
            delay(1000);
            //Serial.print(c[1]);

            if (c.substring(2,6) == 'RING'){
                sendSMS_poloha();
                delay(4000);
                while(GSM_SERIAL.available()) char t = GSM_SERIAL.read();
            }
        }
        /*
        if (vzdalenost >= minALARM ) { //Varianta 2 start
            if(varovani){
                sendSMS("Pohyb zaznamenan!");
                smsOdeslana = true;
                digitalWrite(buzzerPin, HIGH);
                delay(1000);
                digitalWrite(buzzerPin, LOW);
                delay(1000);
                digitalWrite(buzzerPin, HIGH);
            }
        }
    }
}
}

```

```

        delay(1000);
        digitalWrite(buzzerPin, LOW);
    }else{
        varovani = true;
        digitalWrite(buzzerPin, HIGH);
        delay(1000);
        delay(1000);
        digitalWrite(buzzerPin, LOW);
        delay(7000);
    }
    }else{
        varovani = false;
    } //Varianta 2 stop
    */
    /*
    if ((vzdalenost+chyba_prumer)/2 >= minALARM ) {           //Varianta 3
start
        digitalWrite(buzzerPin, HIGH);
        delay(1000);
        digitalWrite(buzzerPin, LOW);
        delay(1000);
        digitalWrite(buzzerPin, HIGH);
        delay(1000);
        digitalWrite(buzzerPin, LOW);
        smsOdeslana = true;
    }
    chyba_prumer = vzdalenost;
    //Varianta 3 stop
    */
    }
    }
    delay(500);
}
void sendSMS(String message) {
    GSM_SERIAL.println("AT+CMGF=1");
    delay(100);
    GSM_SERIAL.print("AT+CMGS=\"");
    GSM_SERIAL.print(733715035);
    GSM_SERIAL.println("\");
    delay(100);
    GSM_SERIAL.print(message);
    delay(100);
    GSM_SERIAL.println((char)26);
    delay(1000);
}
void sendSMS_poloha() {
    if (!poloha) {
        Serial.println("Pozor: Poloha není k dispozici!");
        return;
    }
    float sirka, delka;
    gps.f_get_position(&sirka, &delka);

    String message = "Aktualni poloha:\nSirka: " + String(sirka, 6) +
"\nDelka: " + String(delka, 6);
    sendSMS(message);
}

```