Automatický tester dosahu RFID čteček

Alexandr Hrach

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Alexandr Hrach**
Osobní číslo:	**A20480**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Automatický tester dosahu RFID čteček**
Téma práce anglicky:	**Automatic Tester of Range for RFID Readers**

Zásady pro vypracování

1. Proveďte rešerši RFID technologií.
2. Vysvětlete princip použití RFID v přístupových systémech.
3. Popište vliv rozměrů RFID antén na dosah čtení.
4. Vyberte vhodný mechanismus pro automatizovaný tester RFID čteček.
5. Proveďte měření čtecích vzdáleností dvou čtecích hlav.
6. Navrhněte vlastní vizualizaci měření.
7. Porovnejte výsledky měření.
8. Odhadněte další vývoj RFID technologií.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management I. Zlín: VeRBuM, 2011. ISBN 978-80-87500--05.
2. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management II. Zlín: VeRBuM, 2012. ISBN 978-80-87500--19-4.
3. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management III. Zlín: VeRBuM, 2013. ISBN 978-80--87500-35-4.
4. Security and Privacy in RFID Systems [online]. UNIVERSITY OF WOLLONGONG, 2015 [cit. 2022-12-02]. Dostupné z: https://ro.uow.edu.au/theses/4481/. Disertační práce. UNIVERSITY OF WOLLONGONG.
5. Contributions to RFID security [online]. UNIVERSITY OF WOLLONGONG, 2012 [cit. 2022-12-02]. Dostupné z: https://ro.uow.edu.au/theses/3549/. Disertační práce. UNIVERSITY OF WOLLONGONG.

Vedoucí bakalářské práce: **Ing. Rudolf Drga, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **13. prosince 2022**
Termín odevzdání bakalářské práce: **5. června 2023**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 13. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 5.6. 2023 Alexandr Hrach v. r.

ABSTRAKT

Tato práce se zaměřuje na testování dosahu hlav RFID čteček při vývoji a čtecích vzdálenostech hlav, zmenšování čitelnosti RFID nosičů. V dnešní době, kdy spousta firem, škol, rodinných domů či jiných míst využívá přístupových systémů, se zvyšuje počet karet, které u sebe každý člověk nosí. Tímto dochází ke kolizi signálů karet, a protose snažíme zmenšovat čitelnost tagu za pomocí různých flexibilních odlišně propustných materiálů nebo stínění za pomocí kovů. V teoretické části jsou popisovány prvky RFID, jejich vývoj a vznik, možnosti zmenšení dosahu čitelnosti a vlivu velikosti na dosah čtení,dále metody šifrování a zabezpečení jejich prvků a samotné komunikace. Poslední část teorie se zabývá odhadem budoucího vývoje RFID a NFC v bezpečnosti. V praktické části bude popsán výběr ideálního zařízení pro testování prvků RFID a jeho dokumentace. Následně postup měření a jeho grafické vyhodnocení a porovnání výsledků.

Klíčová slova: RFID, NFC, Automatický tester dosahu RFID čteček, Arduino, Python

ABSTRACT

This work focuses on testing the range of the heads of RFID readers during the development and reading distances of the heads, reducing the readability of RFID carriers. Nowadays, when many companies, schools, family homes and other places use access systems, the number of cards that everyone carries is increasing. This creates a collision and we try to reduce the readability of the tag using different flexible materials with different permeability or shielding using metals. In the theoretical part, it describes RFID elements, their development and creation, the possibilities of reducing the readability range and the effect of size on the reading range. Furthermore, methods of encryption and security of their elements and the communication itself. The last part of the theory deals with estimating the future development of RFID and NFC in security. In the practical part, the selection of the ideal device for testing RFID elements and its documentation will be described. Subsequently, the measurement procedure and its graphic evaluation and comparison of results.

Keywords:RFID, NFC, Automatic Tester ofRangefor RFID Readers, Arduino, Python

OBSAH

ÚVOD

Automatický tester dosahu RFID čteček je zařízení navržené pro efektivní a přesné testování dosahu RFID čteček. RFID (RadioFrequencyIdentification) je technologie, která umožňuje bezkontaktní identifikaci objektů pomocí rádiových vln. Čtečky RFID jsou klíčovými komponenty této technologie, které přijímají a vysílají signály pro komunikaci s RFID tagy.Správná funkčnost čteček RFID je zásadní pro úspěšné provádění různých aplikací, jako je řízení přístupu, sledování zásob, logistika a mnoho dalších. Pro zajištění spolehlivého a konzistentního provozu je důležité pravidelně testovat dosah a výkon čteček.Automatický tester dosahu RFID čteček přinese výhody oproti ručnímu testování. Tento tester umožňuje automatické měření a vyhodnocování dosahu čteček. Díky automatizovanému procesu je dosaženo zvýšené efektivity a přesnosti testování.Tester bude schopen provádět sérii testů na dosah čteček RFID za různých podmínek jako je například zapouzdřená karta, karta v peněžence, rušení a jiné. Výsledky testů jsou analyzovány a prezentovány ve formě 3D modelu a souboru se seznamem naměřených bodů, které umožňují identifikovat případné problémy nebo nedostatky.Díky použití automatického testovacího zařízení se zkracuje doba potřebná k testování a zvyšuje se spolehlivost výsledků. Tester umožňuje opakované testování a monitorování výkonu čteček v pravidelných intervalech, což přispívá k prevenci a odhalování případných poruch a nedostatků.Tato práce se bude podrobněji zabývat konstrukcí, funkcemi, výhodami a použitím automatického testovacího zařízení pro dosah RFID čteček.

Práce je rozdělena celkem do dvou hlavních částí. První část se soustředí na teoretické poznatky o RFID technologii, její parametry, funkce zabezpečení komunikace, aplikace, formy a odhadovaný vývoj ve formě NFC. Druhá praktická část se již věnuje výběru a konstrukci zařízení na automatické testování, komponentům zařízení s popisem jejich využití,zvoleným postupům a programům pro řízení automatizace, jejich detailním rozborem azpracováním naměřených dat a jejich vyhodnocením.

I. TEORETICKÁ ČÁST

1 RFID TECHNOLOGIE

RFID (RadioFrequencyIdentification) je technologie umožňující bezdotykovou identifikaci objektů pomocí rádiových vln. Sestává z dvou hlavních komponentů. RFID čteček a RFID tagů, známých také jako transpondéry. RFID čtečka vysílá rádiový signál, který je detekován RFID tagem. Následně tag reaguje na čtečku posíláním informací uložených v jeho paměti.[1]

1.1.1 Počátky RFID

První koncepty bezkontaktní identifikace se začaly objevovat již v 20. letech 20. století. V roce 1945 publikoval Vannevar Bush článek nazvaný "As We May Think" v časopise TheAtlanticMonthly, ve kterém diskutoval o možnostech automatického zaznamenávání informací. Tento článek je často považován za jedno z prvních záznamů myšlenek, které vedly k rozvoji technologie RFID.V roce 1973 profesor Mario Cardullo získal první patent na aktivní RFID zařízení. Patent popisoval zařízení, které využívalo rádiové vlny k bezkontaktní identifikaci objektů. V průběhu let se technologie RFID dále rozvíjela a zdokonalovala se.[2]

1.2 Užití RFID

Technologie RFIDmá široké spektrum využití v různých odvětvích. Zde je několik příkladů:

- Logistika a dodavatelský řetězec: RFID se často používá k sledování a správě zásob, sledování pohybu zboží v reálném čase a zefektivňování procesů v dodavatelském řetězci.[3]
- Průmysl: RFID se používá v průmyslovém prostředí pro sledování a správu inventáře, sledování výrobního postupu, identifikaci a údržbu zařízení. To může pomoci zvýšit efektivitu výroby, minimalizovat chyby a optimalizovat plánování a údržbu zařízení.[3]
- Doprava: V dopravním sektoru se RFID používá pro automatické vybírání mýtného, sledování a správu nákladních vozidel a kontejnerů, zajištění bezpečnosti při přepravě a sledování veřejné dopravy. RFID umožňuje rychlé a přesné identifikace vozidel a sledování jejich pohybu.[3]

- Osobní identifikace: RFID se používá pro identifikaci a sledování osob v různých prostředích, jako jsou přístupové systémy do budov, identifikační karty a bezpečnostní opatření. RFID může umožnit rychlý a pohodlný přístup do prostor a zvýšit úroveň bezpečí.[3]

1.3 Vlastnosti

Výhodou je, že obsah tagu lze snadno přečíst. Není třeba mít přímý viditelný kontakt a není tedy nutná specifická manipulace při čtení jako je například otáčení prvku RFID nebo vyndávání z pouzdra a další na rozdíl od čárových kódů nebo magnetických pásků. Ve srovnání s biometrickou identifikací osoby jsou eliminovány problémy související s používáním biometrických systémů, jako je například fyzické poškození, zvukový šum nebo špatná viditelnost či jiné.[4]

Další výhody a nevýhody Tabulka 1 Vlastnosti RFID, kde můžeme vidět stručný souhrn pozitivních a negativních vlastností RFID. Za neutrální vlastnosti by se dal považovat dosah čtení na větší vzdálenost a nečitelnost dat z prvku pro člověka. S rostoucím dosahem čtení se zvedá i šum a také je náchylnější k útokům na obsah tagu nebo na přenos komunikace. Nečitelnost je dobrá ve chvíli, kdy dojde k odcizení tagu RFID.[4]

Tabulka 1 Vlastnosti RFID [vlastní]

Výhody	Nevýhody
Velká kapacita uložených dat	Dražší než jiné alternativy
Unikátnost	Možnost
Dosah čtení na větší vzdálenost	Dosah čtení na větší vzdálenost
Nečitelnost dat pro člověka	Nečitelnost dat pro člověka
Rychlost čtení a zpracování dat	
Odolnost prvku RFID	

1.4 RFID systémy

RFID tagy mohou být rozděleny na základě několika kritérií. Zde jsou hlavní kritéria, která se používají k jejich kategorizaci:

Napájení:

- Aktivní tagy.
- Pasivní tagy.
- Semi pasivní tagy

Dosah:

- Dlouhý dosah
- Krátký dosah

Frekvence:

- Nízká frekvence (LF)
- Vysoká frekvence (HF)
- Duální frekvence (DF)
- ultravysoká frekvence (UHF)[5]

2 RFID NOSIČE

RFID tag je malé zařízení, které obsahuje čip a anténu, a slouží k bezkontaktní identifikaci objektů. Tag je přiřazen k objektu, který chceme sledovat nebo identifikovat, a obsahuje unikátní identifikační kód.[7]

2.1 RFID dle napájení

Existuje několik kategorií RFID systémů, které se liší způsobem napájení RFID tagů. Hlavními typy RFID dle napájení jsou pasivní, aktivní a semi pasivní tagy.[7]

2.1.1 Pasivní tagy

Pasivní RFID tag je specifický typ RFID tagu, který nepotřebuje vlastní napájení a využívá energii z rádiových signálů čteče. Pasivní tagy jsou obvykle menší a levnější než aktivní tagy, ale mají omezený dosah a funkční možnosti.Pasivní RFID tagy jsou snadno použitelné a mají dlouhou životnost díky absenci baterií nebo vlastního napájení. Jejich dosah je obvykle omezen na několik centimetrů a přenosová rychlost je nižší než u aktivních tagů. Nicméně díky své nízké ceně a kompaktním rozměrům jsou pasivní tagy široce využívány v mnoha oblastech pro sledování, správu a identifikaci objektů.[7]

2.1.2 Aktivní tagy

Aktivní RFID tagy jsou druhem tagů, které disponují vlastním napájením a aktivně vysílají signály. Na rozdíl od pasivních tagů, které získávají energii z rádiových signálů čtečky, aktivní tagy mají vlastní zdroje energie, nejčastěji baterie.Aktivní RFID tagy se vyznačují větším dosahem a vyšším výkonem ve srovnání s pasivními tagy. Díky vlastnímu napájení mohou aktivní tagy komunikovat na větší vzdálenosti, často v rozsahu desítek až stovek metrů. To je velmi užitečné pro aplikace, které vyžadují sledování objektů na rozlehlých plochách nebo ve velkých prostorách.Aktivní RFID tagy se často využívají v oblastech, kde je potřeba přesné sledování a monitorování objektů, například v logistice, dopravě, přepravě zboží a v oblasti bezpečnosti. Mohou být připevněny k cenným předmětům, vozidlům, kontejnerům nebo zvířatům a umožňují jejich sledování v reálném čase.[7]

2.1.3 Semi pasivní tagy

Semi-pasivní RFID tagy, také známé jako pasivní tagy s bateriovou podporou (BAP), představují speciální typ RFID tagů, které kombinují vlastnosti pasivních a aktivních tagů. Tyto tagy nejsou vybaveny vlastním zdrojem napájení, ale obsahují integrovanou baterii, která slouží k napájení interních komponent.Fungování semipasivních tagů je podobné jako u pasivních tagů, které získávají energii z rádiových signálů čtečky. Nicméně, na rozdíl od pasivních tagů, které využívají tuto energii pouze pro přenos svého identifikačního kódu, semipasivní tagy využívají baterii ke zvýšení svých funkčních možností.[7][8]

2.2 RFID dle tvaru a rozměrů antény

RFID tagy mohou být klasifikovány podle tvaru a rozměrů jejich antény, což ovlivňuje jejich vlastnosti a výkon. Zde je několik způsobů, jak rozdělit RFID tagy na základě tvaru a rozměrů antény:

- Lineární anténa: Nejběžnější typ antény, který má rovný tvar. Jeho délka je obvykle volena tak, aby odpovídala frekvenci RFID systému. Lineární antény mohou být umístěny na různých materiálech, jako je papír, plast nebo kov.[5]
- Spirálová anténa: Anténa ve tvaru spirály, která se často používá na menších RFID tagy. Spirálová anténa poskytuje lepší stabilitu signálu při rotaci tagu, což je užitečné v aplikacích, kde se tag často pohybuje.[5]
- Meandrová anténa: Anténa s charakteristickým zalamováním linie. Meandrové antény jsou vhodné pro tagy s omezeným prostorem, protože umožňují dosažení dostatečného dosahu a výkonu při zachování kompaktních rozměrů.[5]
- Plošná anténa: Anténa umístěná na ploché nebo tištěné desce. Plošné antény se často používají v identifikačních systémech, jako jsou přístupové karty, výrobní štítky nebo značky pro sledování zásob. Jejich plochý tvar umožňuje snadnou integraci do různých zařízení.[5]

2.2.1 Vliv velikosti antény na dosah RFID komunikace

Velikost antény hraje klíčovou roli v dosahu RFID komunikace. Velká anténa umožňuje dosáhnout větší vzdálenosti přenosu signálu mezi RFID čtečkou a tagem. Toto je způsobeno tím, že větší anténa generuje silnější elektromagnetické pole, které je schopné

být přijímáno tagem na větší vzdálenost. Díky tomu může být dosaženo komunikace i přes delší vzdálenost mezi čtečkou a tagem.Na druhou stranu, použití menší antény omezuje dosah komunikace. Menší anténa generuje slabší elektromagnetické pole, které není tak efektivní při přenosu signálu na větší vzdálenost. To znamená, že tag musí být umístěn blíže k čtečce, aby byla zajištěna úspěšná komunikace.Při navrhování RFID systému je důležité pečlivě vybrat anténu, která odpovídá požadovanému dosahu komunikace. Je třeba zohlednit specifické potřeby a omezení prostoru, abychom vybrali optimální velikost antény, která umožní dosažení požadovaného dosahu přenosu signálu. Správná volba antény je klíčová pro zajištění spolehlivé a efektivní RFID komunikace ve specifickém prostředí.[9][10]

2.3 RFID dle paměťové funkce

Kapacita paměti tagů se obvykle pohybuje od několika bajtů do několika kilobajtů. Výjimkou jsou systémy proti krádeži (EAS - ElectronicArticleSurveillance) nacházející se v obchodech, které vyžadují 1 bit paměti, což je dostačující pro uložení informace o tom, zda byla položka zaplacena či nikoli. Tyto tagy však ukládají informace na fyzické bázi bez řadiče a paměti.

Typy trvalých pamětí používaných v RFID:

- ROM (Read-OnlyMemory): ROM paměť je určena pro jednosměrný zápis dat. Data jsou v této paměti předem programovaná výrobcem tagu a nelze je následně změnit. ROM paměť se často používá pro ukládání unikátního identifikačního kódu tagu.[7]
- PROM (ProgrammableRead-OnlyMemory): PROM paměť umožňuje jednorázový zápis dat. Data jsou do paměti programována a nelze je následně přepisovat. PROM se často používá pro ukládání fixních informací, které jsou specifické pro každý tag.[7]
- EEPROM (ElectricallyErasableProgrammableRead-OnlyMemory): EEPROM je paměť, která umožňuje elektricky vymazatelné zápisy dat. Data lze zapisovat a mazat pomocí elektrických signálů, což umožňuje opakované programování. EEPROM se často používá pro ukládání konfiguračních a uživatelských dat.[7]

- Flash paměť: Flash paměť je podobná EEPROM, ale umožňuje hromadné mazání dat. Je používána pro ukládání většího množství dat, jako jsou firmware aktualizace, logovací informace nebo uživatelská nastavení.[11]

Tag dále obsahuje pracovní paměť pro různé operace (inkrementace hodnot v paměti, kryptografické funkce atd.), jejichž obsah se při přerušení napájení ztratí.[5][7]

2.4 Příkazy RFID nosiče

V RFID nosiči se nacházejí zabudované příkazy, které umožňují čtení, zápis a další operace s daty. Zde jsou některé z těchto funkcí:

- Čtení (Read): Umožňuje čtečce přístup k datům uloženým v tagu. Čtečka může přečíst informace, jako je identifikační kód, sériové číslo, uložené parametry nebo další uživatelská data.[7]
- Zápis (Write): Schopnost zapsat nebo aktualizovat data v tagu. Čtečka může přenášet informace na nosič, čímž umožňuje změnu obsahu paměti nebo nastavení parametrů.[7]

3 ČTEČKY RFID

Čtečky RFID existují v různých formátech a provedeních, jako jsou ruční čtečky, pevně umístěné čtečky, vestavěné čtečky v zařízeních apod. Výběr vhodné čtečky závisí na konkrétním využití a prostředí, ve kterém bude používána. Čtečka vytváří pole, které nabije RFID tag a ten díky tomu může odpovědět. Čtečka zprostředkovává komunikaci s ústřednou nebo s přístupovým systémem. Má přístup do databází kde porovnává načtené tagy.[3]

4 RFID V PŘÍSTUPOVÝCH SYSTÉMECH

Technologie RFID se často využívá v přístupových systémech k zajištění bezpečného a pohodlného vstupu do různých prostorů. Tyto systémy využívají RFID čtečky a RFID tagy také nazývané RFID karty nebo klíčenky, které umožňují identifikaci uživatelů a autorizaci jejich přístupu.Fungování RFID v přístupových systémech je následující: Každý uživatel je vybaven RFID tagem, který obsahuje unikátní identifikační číslo nebo jiné relevantní informace. Tento tag může mít podobu karty, klíčenky nebo jiného nosiče. Při přiblížení RFID tagu k RFID čtečce umístěné poblíž vstupu do prostoru, čtečka aktivuje bezdrátový signál a navazuje komunikaci s RFID tagem.[12]

4.1 Přístupové systémy

Přístupové systémy jsou technologie navržené k řízení přístupu do určitých prostorů nebo oblastí. Tyto systémy slouží k autorizaci a správě přístupu uživatelů na základě různých kritérií a parametrů. Jejich hlavním cílem je ochrana majetku, zajištění bezpečnosti a omezení neoprávněného vstupu do určitých oblastí.Přístupové systémy se využívají ve všech možných prostředích, od firem a kanceláří po průmyslové areály, bytové komplexy, zdravotnická zařízení a veřejné instituce. Mohou být implementovány pomocí různých technologií, jako jsou RFID biometrie (například otisk prstu nebo rozpoznávání obličeje), kódy (například PIN) nebo kombinací různých metod.

Využívá se velká škála přístupových systémů, které se liší v závislosti na použité technologii a způsobu autentizace uživatelů. Mezi nejčastěji používané přístupové systémy patří:

- Klíčové přístupové systémy: Tyto systémy využívají fyzických klíčů nebo karet pro autorizaci přístupu. Uživatelé mají při sobě klíč nebo kartu, kterou používají k odemknutí dveří nebo přístupového bodu.
- Kódy a hesla: Přístupové systémy mohou vyžadovat zadání správného kódu nebo hesla pro autorizaci přístupu. Uživatel musí znát přesný kód nebo heslo, které slouží jako autentizační prvek.
- Biometrické přístupové systémy: Tyto systémy využívají biometrických charakteristik jednotlivce, jako je otisk prstu, duhovka oka nebo rozpoznání obličeje, k identifikaci a autorizaci přístupu. Biometrické údaje jsou uloženy v databázi a porovnávány s živým biometrickým vzorkem uživatele.

- RFID přístupové systémy: RFID technologie se používá k identifikaci a autorizaci přístupu. Uživatelé mají RFID tagy, které komunikují s RFID čtečkami. Tyto systémy umožňují bezkontaktní přístup a rychlou identifikaci.[12]

4.2 Princip RFID v přístupových systémech

Při využití RFID čtečky se odesílá signál směrem k RFID tagu, který následně odpovídá svým vlastním signálem. Tímto způsobem dochází k identifikaci tagu a navazuje se komunikace s přístupovým systémem. Na základě identifikace tagu a předem stanovených autorizačních pravidel systém posuzuje, zda má daný uživatel dostatečné oprávnění ke vstupu do daného prostoru. V případě splnění všech potřebných podmínek přístupový systém aktivuje otevření dveří či umožní uživateli vstup do daného prostoru.[13]

4.3 Výhody použití

Použití RFID v přístupových systémech přináší řadu výhod. Mezi ně patří rychlá identifikace uživatelů, provoz bez nutnosti fyzického kontaktu, dlouhá životnost RFID tagů, možnost centralizovaného řízení a správy oprávnění uživatelů, a také schopnost sledování a zaznamenávání vstupů a výstupů. RFID přístupové systémy se hojně využívají v kancelářích, veřejných budovách, průmyslových areálech, nemocnicích, školách a dalších prostředích, kde je nezbytné zajistit bezpečný a řízený přístup.[13]

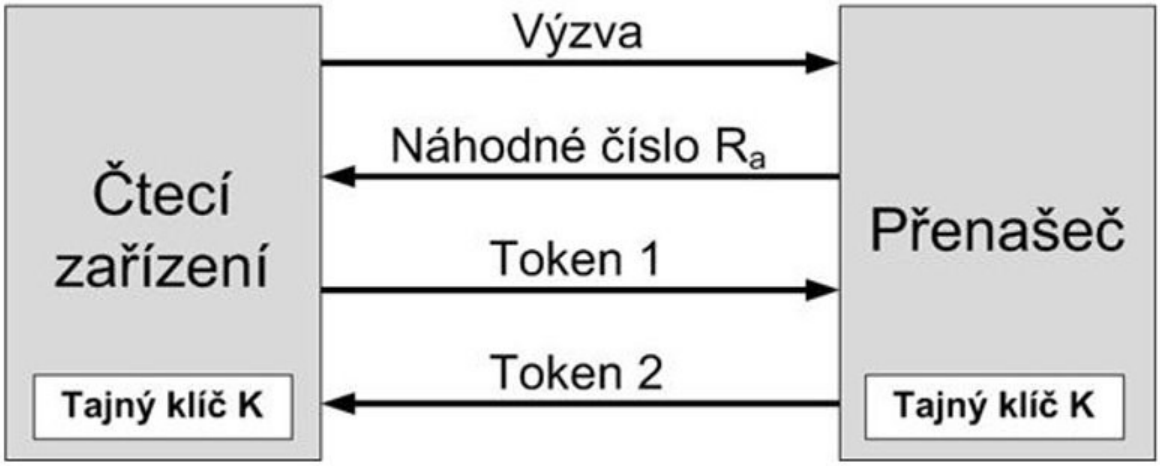
5 ZABEZPEČENÍ RFID

Bezpečnost RFID (RadioFrequencyIdentification) je klíčovým aspektem technologie RFID, který se zabývá ochranou dat, soukromí a zabezpečením proti neoprávněnému přístupu a útokům. Existuje několik postupů, metod a standardů používaných k zajištění bezpečnosti RFID, a to jak v normách, tak v řešeních průmyslových výrobců. [14]

5.1 Bezpečnostní metody

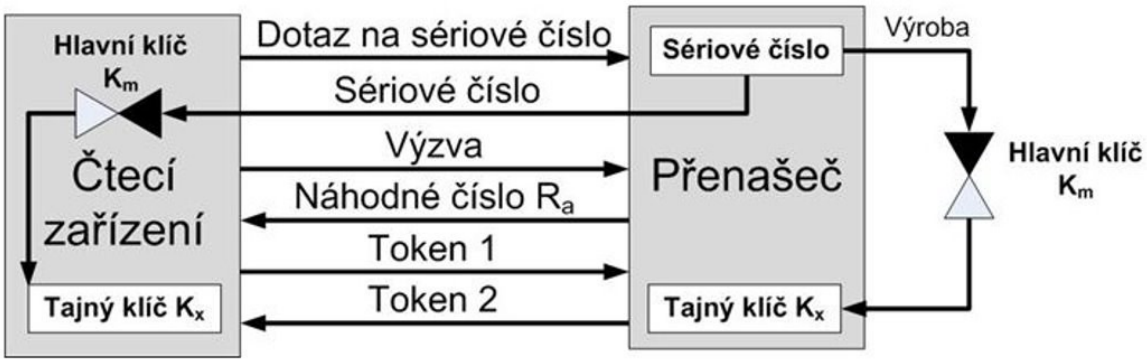
Tato část představuje technické metody pro zvýšení bezpečnosti technologie RFID, které jsou implementovány v populárních standardech. Kromě toho existuje mnoho netechnických metod, které jsou velmi důležité pro praktické aplikace.

Jako ty nejzákladnější formy komunikace mezi prvky RFID řadíme vzájemné symetrické ověřování viz **Chyba! Nenalezen zdroj odkazů.**, kde se pro celý systém využívá jednoho klíče. Tento systém je levný a rychlý, ale může nastat velký problém při úniku komunikačního hesla. Únikem hesla dojde k naprostému prolomení systému a kdokoliv se pak může přihlásit nebo prokázat tagem, na který si nahraje ukradené heslo.[14]



Obrázek 1 vzájemné symetrické ověřování [15]

Druhý základní a velice rozšířený je princip ověřování pomocí odvozených klíčů viz Obrázek 2, který se používá v EKV vždy s kombinaci šifrováním a dalšími způsoby ochrany. Zde má každý nosič již od výroby dané své unikátní heslo, a to je zašifrováno často pomocí SHA-256 a tudíž zná jen svůj otisk. Čtečka pak zná heslo, to zašifruje a porovná výsledek s otiskem na kartě.[14][15]



Obrázek 2 ověřování pomocí odvozených klíčů [15]

5.2 Autentizace a integrita dat

Autentizace a integrita FAT (FileAllocation Table) v rámci RFID se týkají zabezpečení a integrity dat, která jsou uložena na paměťových nosičích. FAT je souborový systém používaný k organizaci a správě dat na RFID nosičích a autentizace a integrita FAT se zaměřují na zajištění, že tato data zůstávají neporušená a důvěryhodná.Autentizace FAT v RFID se zabývá ověřováním pravosti a platnosti dat uložených na RFID nosičích. Proces autentizace může zahrnovat použití kryptografických technik, jako je asymetrické nebo symetrické šifrování, s cílem zajistit, že pouze oprávněné osoby nebo systémy mají přístup k datům na nosiči. Autentizace může vyžadovat výměnu klíčů nebo ověřování digitálních podpisů, aby byla zaručena pravost dat a zabránilo se neoprávněnému přístupu nebo manipulaci s nimi.[16]

5.3 Digitální podpis

Digitální podpis v kontextu RFID je kryptografický mechanismus, který slouží k ověření autenticity a integrity dat na RFID nosičích, tj. tagy. Jeho účelem je potvrdit, že data byla odeslána od oprávněného odesílatele a zůstala nedotčena po celou dobu přenosu.Digitální podpis využívá asymetrického šifrování. Odesílatel používá svůj soukromý klíč ke generování digitálního podpisu, který je vytvořen kombinací hash hodnoty dat a šifrovacího algoritmu. Tento digitální podpis je připojen k datům a slouží jako důkaz o jejich původu a neporušenosti.Příjemce dat může ověřit digitální podpis pomocí veřejného klíče odesílatele. Proces zahrnuje dešifrování digitálního podpisu a porovnání získané hash hodnoty s nově vypočítanou hash hodnotou přijatých dat. Shodují-li se obě hodnoty, znamená to, že data jsou autentická a neporušená.Použití digitálního podpisu v RFID přináší vyšší úroveň bezpečnosti a důvěryhodnosti komunikace. Pomáhá chránit data před

neoprávněnými změnami, falšováním nebo napadením. Digitální podpis je důležitým nástrojem pro zabezpečení komunikace mezi čtečkami RFID a tagy, a to při identifikaci, sledování a správě objektů v různých aplikacích RFID technologie.[17]

5.4 Cover-Coding

Covercoding (kódování krycími kódy) v je technika, která se využívá k optimalizaci spolehlivosti a přesnosti přenosu dat mezi čtečkou atagem. Jeho hlavním cílem je minimalizovat vliv rušení, šumu a chyb při komunikaci.Covercoding dosahuje svého účinku tím, že kódování dat pomocí redundantních bitů, které slouží k detekci a opravě přenosových chyb. Těmito redundantními bity jsou do přenášených dat zahrnuty dodatečné informace, které umožňují detekovat a opravit případné chyby v přenosu. Tím se zajišťuje, že původní data jsou správně přenesena a zachována jejich integrita.Covercoding je zejména užitečný v prostředí s výskytem rušení a šumu, které mohou negativně ovlivnit přenos dat. Tato technika významně zvyšuje spolehlivost a robustnost RFID systémů, což přispívá ke zlepšení přesnosti a spolehlivosti identifikace, sledování a správy objektů v různých aplikacích RFID technologie.[18]

5.5 Šifrování přenášených dat

Používá se, když techniky krycího kódování nejsou dostatečné (když útočník může odposlouchávat komunikaci uplinkového kanálu). Data jsou před odesláním přes rádiové rozhraní zašifrována. Nosič lze použít k uložení zašifrovaných dat pouze v případě, že nemá schopnost se sám dešifrovat (běžné pasivní tagy). Nebo můžete zahrnout dekódovací obvod. To samozřejmě vede ke složitější a dražší spotřebě tagů a zpožděním. Proto tento způsob není vhodný pro systémy s vysokými nároky na rychlost komunikace s tagy.[19]

5.6 Omezení šíření signálu

Omezení šíření signálu je důležitým faktorem při návrhu a implementaci systémů RFID. Cílem je minimalizovat nežádoucí rozptyl signálu a zajistit přesné a spolehlivé fungování technologie RFID. Zde je několik způsobů, jak lze omezit šíření signálu:

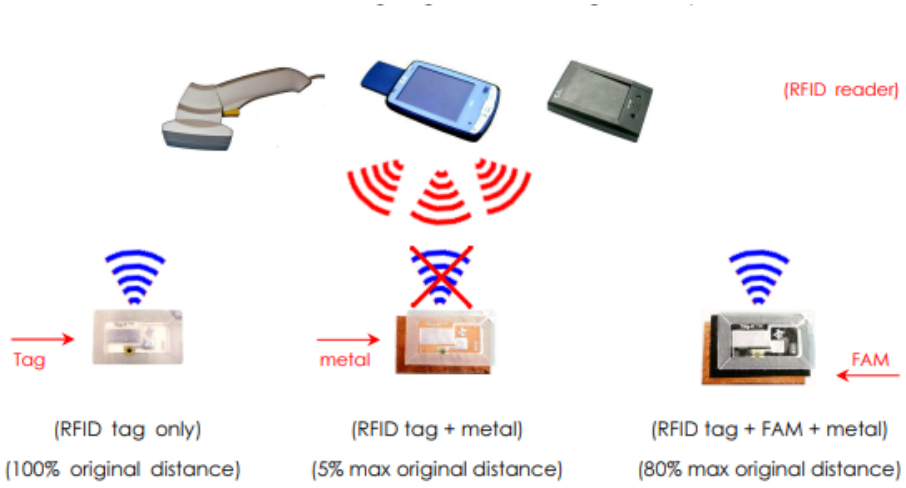
- Anténní design: Správný design antény je klíčový pro optimální šíření signálu. Antény by měly být navrženy tak, aby minimalizovaly odrazy a interference, a zároveň maximalizovaly dosah a citlivost signálu.

- Řízení výkonu: Správné řízení výkonu čtečky je důležité pro minimalizaci rušení a šíření signálu. Příliš vysoký výkon může způsobit interferenci s jinými zařízeními a ovlivnit výkon celého RFID systému.
- Upravení frekvence: V případě, že se v daném prostředí vyskytují jiná zařízení pracující na podobných frekvencích, je vhodné zvolit frekvenci, která minimalizuje interferenci. V některých případech lze použít i antikolizní protokoly, které umožňují řízení komunikace více tagů současně.
- Absorpce a odraz signálu: Různé materiály mohou mít různé vlastnosti absorpce a odrazu signálu. Pokud je potřeba omezit šíření signálu do určité oblasti, mohou se použít materiály s vysokou absorpční schopností, které minimalizují odraz a šíření signálu mimo zamýšlenou oblast.[5][10]

5.6.1 Elektromagnetické stínění

Elektromagnetické stínění je technika, která se používá k omezení nebo eliminaci rušivých elektromagnetických polí v určitém prostoru. Cílem elektromagnetického stínění je chránit elektronická zařízení před vnějšími rušivými signály a zajišťovat jejich správnou funkci.Existuje několik způsobů, jak provést elektromagnetické stínění:

- Použití kovových obalů: Elektronická zařízení mohou být umístěna do kovových obalů, které působí jako bariéra proti vnějším elektromagnetickým polím. Kovový obal odráží nebo absorbuje rušivé signály a zabraňuje jejich pronikání do zařízení.
- Použití stínících materiálů: Speciální materiály, nazývané stínící materiály, mohou být použity k pokrytí elektronických zařízení nebo kabelů. Tyto materiály obsahují vodiče nebo feromagnetické částice, které pohlcují nebo odrážejí elektromagnetické signály.
- Zemní pásy a stínící vrstvy: Při návrhu elektronických desekse mohou použít zemní pásy a stínící vrstvy. Tyto vrstvy slouží k oddělení citlivých částí desky od rušivých signálů. Zemní pásy a stínící vrstvy vytvářejí bariéru, která minimalizuje rušení.
- Správné umístění a uspořádání komponent: Správné umístění a uspořádání komponent v elektronickém zařízení může také přispět k elektromagnetickému stínění. Například umístění citlivých komponent blíže ke stínícím vrstvám nebo vnitřním částem kovového obalu může minimalizovat jejich expoziční plochu vůči rušivým signálům.[20]



Obrázek 3 elektromagnetické stínění [20]

5.6.1.1 Stínění za pomocí FAM

Jedná se o různé nemagnetické flexibilní materiály, které mají specifické vlastnosti v rámci ELM propustnosti. Mají širokou škálu využití a existuje mnoho druhů. Často bývají využívány v kombinaci se kovovým stíněním, ale lze je použít samostatně. Jsou odolné vůči nepříznivým podmínkám a využívají se pro velké RFID média.[20]

- Poskytuje účinné potlačení EMI v širokém frekvenčním rozsahu (1 MHz až 18 GHz)
- Změňte dráhu magnetického toku, abyste zabránili rušení jiných součástí
- Snižte vířivý proud, když magnetický tok uzavírá kov
- Ultra tenký a extrémně flexibilní, lze jej volně rozmístit v prostoru
- K dispozici je nevodivý adhezivní podklad (Uznáno UL).
- Účinné při prevenci rezonance a potlačení vazby
- Vysoký povrchový odpor (106 ohmů)
- Snadné a rychlé zpracování
- Lze snadno řezat jakýkoli tvar

Tabulka 2 Vlastnosti FAM [20]

Property	Unit	FAM1	FAM3	FAM7
Operating Temperature	°C	-40 ~ +85		-30 ~ +120
Applicable Frequency	GHz	1MHz ~ 18GHz		1MHz ~ 3GHz
Permeability (μ'@1MHz)	-	25	50	140
Material	-	Magnetic Powder + Rubber		Sintered Ferrite Sheet
Thickness Range	mm	0.12 ~ 2.50	0.25 / 0.50 / 0.75	0.12 / 0.22
Max. Dimension	mm	600 x 400		130 x 130
Surface Resistance	ohm	10^6		10^9
Density	g/cm³	3.6	4.8	3.8
RoHS 2.0 Compliance	-	2011/65/EU		2011/65/EU
Halogen-Free	-	No		Yes

Property	Unit	FAM6	FAM6B	FAM9
Operating Temperature	°C	-40 ~ +155		-30 ~ +120
Applicable Frequency	GHz	1MHz ~ 9GHz		1MHz ~ 3GHz
Permeability (μ'@1MHz)	-	170	250	600
Material	-	Magnetic Powder + Rubber		Sintered Ferrite Sheet
Thickness Range	mm	0.05 ~ 0.50		0.22
Max. Dimension	mm	210x297 (A4 size)		130 x 130
Surface Resistance	ohm	10^6		10^9
Density	g/cm³	3.8		3.8
RoHS 2.0 Compliance	-	2011/65/EU		2011/65/EU
Halogen-Free	-	Yes		Yes

5.6.2 Snížení vysílacího výkonu

Snížení vysílacího výkonu je jednou z technik používaných k omezení dosahu vysílaného signálu v bezdrátových systémech, včetně RFID. Cílem snížení vysílacího výkonu je minimalizovat interferenci s ostatními zařízeními a omezit nežádoucí šíření signálu na větší vzdálenosti.Existuje několik přístupů, jak dosáhnout snížení vysílacího výkonu:

- Úprava výkonu vysílače: Vysílače v RFID systémech často umožňují nastavení výstupního výkonu. Snížení výkonu vysílače na nižší úroveň pomáhá omezit dosah signálu a zabránit nežádoucímu rušení.
- Použití nižší frekvence: V RFID systémech lze použít nižší frekvenci, což obvykle znamená menší dosah signálu. Nižší frekvence mají tendenci rychleji slábnout při šíření vzduchem, což přispívá ke snížení dosahu vysílaného signálu.[5][10]

5.7 Manuální aktivace tagu

Manuální aktivace tagu je postup, při kterém je RFID tag aktivován a připraven k přenosu dat pouze na základě manuálního zásahu uživatele. Tento způsob aktivace se liší od

standardního pasivního RFID provozu, kde je tag aktivován pomocí rádiového signálu z RFID čtečky.Existuje několik způsobů, jak provést manuální aktivaci RFID tagu:

- Stisknutí tlačítka: Tag může být vybaven tlačítkem, které uživatel stiskne pro aktivaci. Po stisknutí tlačítka se tag připraví k přenosu dat.
- Dotykem: Některé RFID tagy mohou být aktivovány dotykem nebo přiblížením ke specifickému čtecímu zařízení. Při dotyku nebo přiblížení tagu k čtečce se aktivuje a připraví k přenosu dat.
- Magnetickým polem: Tag může být aktivován pomocí magnetického pole generovaného speciálním magnetem nebo čtecím zařízením. Přiložením magnetu nebo přiblížením tagu k magnetickému pole se aktivuje a je připraven k přenosu dat.[7]

5.8 Zabezpečení dat v tagu

Bezpečnost dat v RFID tagu je klíčovým prvkem, který chrání data na něm uložené před neoprávněným čtením, přepisováním a manipulací s nimi. [19]

5.8.1 Šifrování dat

Šifrování dat je důležitou metodou zabezpečení v RFID technologii, která se používá k ochraně přenášených informací před neoprávněným přístupem a dešifrováním. Šifrování zajišťuje, že data uložená v RFID tagu nebo přenášená mezi tagem a čtečkou jsou zabezpečena a mohou být čtena a dešifrována pouze s platným klíčem.Existuje několik algoritmů a protokolů používaných pro šifrování dat v RFID systémech, zahrnující například:

- AdvancedEncryption Standard (AES): AES je jedním z nejčastěji používaných symetrických šifrovacích algoritmů. Používá klíče s délkou 128, 192 nebo 256 bitů a zajišťuje vysokou úroveň zabezpečení dat.
- Data Encryption Standard (DES): DES je starší symetrický šifrovací algoritmus, který se používá ke šifrování a dešifrování dat. Má klíče o délce 56 bitů a byl nahrazen pokročilejšími algoritmy jako je AES.
- RSA: RSA je asymetrický šifrovací algoritmus, který využívá dva klíče: veřejný klíč pro šifrování a soukromý klíč pro dešifrování. RSA se často používá pro zabezpečení komunikace mezi čtečkou a tagem.

- SecureHashAlgorithm (SHA): SHA je rodina kryptografických hashovacích funkcí, které se používají pro zajištění integrity dat. SHA funkce generují jedinečný hash (otisk) z vstupních dat, který slouží k ověření jejich integrity.[19]

5.8.2 Deaktivace tagu - KILL

Deaktivace tagu pomocí příkazu "KILL" je jednou z metod pro zabezpečení RFID technologie. Příkaz "KILL" slouží k trvalému zneplatnění tagu a zabraňuje jeho dalšímu použití.Provedení deaktivace tagu přes příkaz "KILL" vyžaduje speciální oprávnění a potvrzení, aby se zabránilo neoprávněnému zneužití. Tento příkaz se musí provést pomocí speciálního zařízení nebo softwaru, který má přístup k danému RFID tagu.[7]

5.9 Přehled standardů

Zde v Tabulka 3 Přehled standardů můžeme vidět stručný přehled vysoce používaných standardů

Tabulka 3 Přehled standardů [7]

Standard	Použití	Pásmo	Velikost paměti	Důvěrnost	Integrita
ISO 11784/11785	Identifikace zvířat	LF	64bitové ID	Žádná.	CRC kontrola.
ISO/IEC 14443	Přístupové karty, jízdenky apod.)	HF	32, 56 nebo 80bitové ID	Žádná.	CRC kontrola.
ISO/IEC 15693	Přístupové karty s větším dosahem (1m)	HF	64bitové ID a až 8 kB Read/Write paměti	Žádná	Permanentní LOCK, CRC kontrola.
ISO 18000-3	Evidence zboží a zavazadel	HF	64bitové ID a Read/Write paměť dat	Čtení chráněné 48bitovým heslem (Mode 2)	Permanentní LOCK, CRC kontrola. V případě Mode 2 navíc zápis chráněný
EPCglobal Class-1 Generation-2 (ISO/IEC 18000-6C)	Zásobování	UHF	až 496bitové ID, WORM a Read-Write paměť pro data	Cover-Coding (šifrování downlink kanálu), adresace tagů čtečkou pomocí 16bitových	Části paměti lze uzamknout proti zápisu nebo trvale uzamknout, CRC kontrola

6 TECHNOLOGIE NFC A BUDOUCÍ VÝVOJ RFID V BEZPEČNOSTI

Technologie NFC (NearFieldCommunication) je nyní velmi rozšířená a aplikací na ní založených je stále více. Jelikož se jedná o rozšíření technologie RFID, má s technologií RFID mnoho společného. Navíc jde kromě jednoduché identifikace také o přenos dat obecně. Je implementován v mobilních telefonech, takže je pro běžného uživatele dostupnější a snadno použitelný. Uživatel tak nemusí kupovat další položku. Celé hardwarové vybavení již vlastní a nosí ho stále s sebou. Technologie NFC se jeví jako směr, kterým se bude RFID uvíjet a kam bude směřovat jejich budoucnost.[21][22]

6.1 NFC základní parametry

NFC (NearFieldCommunication) je bezkontaktní komunikační technologie, která umožňuje bezdrátový přenos dat mezi zařízeními na krátkou vzdálenost, obvykle do 4 centimetrů. NFC využívá radiových vln pro komunikaci a je založena na standardu RFID.Zde jsou základní parametry NFC:

- Frekvence: NFC pracuje převážně na frekvencích 13,56 MHz, což je univerzální frekvence pro bezkontaktní komunikaci.
- Dosah: Dosah NFC je omezený na krátkou vzdálenost do 4 centimetrů. Tento krátký dosah je intentional, aby se minimalizovalo riziko nechtěného přenosu dat.
- Rychlost přenosu dat: Rychlost přenosu dat u NFC je relativně nízká, obvykle do 424 kbps (kilobitů za sekundu). Tato rychlost je dostačující pro přenos menších objemů dat, jako jsou například kontaktní informace, URL adresy, malé soubory a další.
- Režimy komunikace: NFC podporuje dva základní režimy komunikace - aktivní režim (Active Mode) a pasivní režim (Passive Mode). V aktivním režimu oba zařízení (např. smartphone a NFC tag) mají aktivní roli při komunikaci. V pasivním režimu je jedno zařízení (např. NFC tag) pasivní a pouze přijímá signál od druhého aktivního zařízení (např. smartphone).
- Podpora bezpečnosti: NFC poskytuje integrované bezpečnostní mechanismy pro zabezpečení přenosu dat, jako je šifrování a autentizace. To umožňuje bezpečnou komunikaci mezi zařízeními a prevenci neoprávněného přístupu k datům.[21][22]

6.2 NFC druhy komunikaca

Komunikace přes NFC se v mobilních telefonech často používá k navázání spojení s jinou technologií (jako je Bluetooth nebo WiFi), která umožňuje vyšší přenosové rychlosti nebo delší vzdálenosti. Komunikační režimy a aplikace zařízení účastnících se komunikace jsou iniciátory (čtečka NFC nebo mobilní telefon s NFC), kteréiniciující spojení a řídí komunikaci a cíl (tag nebo mobilní telefon), který odpovídá na požadavky. NFC definuje dva komunikační režimy, a to aktivní a pasivní.[22]

6.2.1 Aktivní

Aktivní NFC (Active NFC) je rozšířená forma NFC technologie, která umožňuje zařízení aktivně komunikovat mezi sebou na větší vzdálenost a dosahovat vyšších rychlostí přenosu dat než pasivní NFC. V aktivním režimu jsou oba komunikující prvky (zařízení) vybaveny vlastními napájecími zdroji a aktivně generují a přijímají signály pro komunikaci.[22]

6.2.2 Pasivní

Pasivní NFC (Passive NFC) je technologie, která umožňuje bezkontaktní komunikaci a výměnu dat mezi dvěma zařízeními, z nichž jedno je pasivní a druhé je aktivní. Pasivní NFC zařízení nemají vlastní napájení a získávají energii potřebnou pro komunikaci z aktivního zařízení pomocí elektromagnetického pole.[22]

6.3 NFC způsoby komunikace a využití

Rozlišují se tři režimy provozu v závislosti na zařízení, se kterým NFC mobilní telefon komunikuje. Každý používá jiné standardy a komunikační protokoly a jsou na nich založeny různé aplikace. Díky progresivnímu vývoji je také možno využívat NFC k bezdrátovému nabíjení.[22]

6.3.1 Reader/Writer

Tato funkce umožňuje zařízení, jako je chytrý telefon nebo tablet, číst a zapisovat data na NFC tagy nebo zařízení. Používá se například při čtení informací z produktů v obchodech, při připojení ke zabezpečovacím systémům nebo při aktualizaci informací na NFC štítcích.[22]

6.3.2 Peer-to-Peer

Peer to peer (přenos mezi zařízeními): Tato funkce umožňuje dvoum NFC zařízením vzájemně komunikovat a vyměňovat si data. To umožňuje rychlé sdílení souborů, kontaktů, multimediálního obsahu a dalších informací mezi dvěma NFC zařízeními. P2P komunikace se využívá například při sdílení fotografií mezi dvěma chytrými telefony nebo při propojení dvou NFC zařízení pro multiplayerové hry.[21][22]

6.3.3 Emulace tagu

Emulace tagu: Tato funkce umožňuje NFC zařízení simulovat NFC tag a přijímat příchozí signály od jiných NFC zařízení, jako je čtečka. To umožňuje například použití chytrého telefonu jako náhrady za NFC tag pro vstup do budovy nebo jako elektronickou vstupenku na akce.[22]

6.4 Další využití NFC

- Mobilní platby: NFC se často používá pro bezkontaktní platební transakce, které umožňují uživatelům platit prostřednictvím svých chytrých telefonů nebo NFC platebních karet.
- Propojení zařízení: NFC může sloužit k jednoduchému propojení různých zařízení, například ke spárování sluchátek s chytrým telefonem.
- Přenos souborů: NFC umožňuje rychlý a jednoduchý přenos souborů mezi dvěma NFC zařízeními, například obrázky, kontakty nebo webové odkazy.
- Identifikace a ověřování: NFC se používá pro identifikaci a ověřování prostřednictvím NFC karet nebo štítků. Například přiblíž[22]

6.5 Bezpečnost NFC

Bezpečnost při používání technologie NFC (NearFieldCommunication) je zásadním hlediskem, neboť se jedná o bezkontaktní komunikaci, která může obsahovat citlivá data. Pro zajištění bezpečnosti NFC se využívají různá opatření a techniky:

- Šifrování dat: Při NFC komunikaci je klíčové používat šifrování dat. To znamená, že informace jsou přenášeny ve formě zakódovaného kódu, který lze dešifrovat pouze s příslušným klíčem. Tím se chrání citlivá data před neoprávněným přístupem.

- Autentizace: Pro zajištění důvěryhodnosti komunikujících zařízení je nutné provést autentizaci. Tím se ověřuje, zda jsou zapojená zařízení oprávněná a důvěryhodná. Autentizace může zahrnovat využití certifikátů, klíčů nebo jiných identifikačních mechanismů.
- Omezení dosahu: NFC je technologie s omezeným dosahem, což znamená, že komunikace mezi zařízeními musí probíhat na velmi krátkou vzdálenost (několik centimetrů). To automaticky snižuje riziko neoprávněného přístupu a odposlechu dat.
- Ochrana proti útokům: NFC musí být chráněno před různými typy útoků, jako jsou odposlechy, manipulace s daty nebo padělání zařízení. K tomu slouží různé techniky, jako je kryptografie, použití unikátních identifikátorů, kontrolní součty a další.
- Aktualizace firmware: Pravidelná aktualizace firmware zařízení na nejnovější verzi je důležitým bezpečnostním opatřením. Výrobci pravidelně vydávají aktualizace, které řeší známé bezpečnostní zranitelnosti a zlepšují ochranu NFC zařízení.[21][23]

6.5.1 NFC-SEC

NFC-SEC (NFC Security) je standardizovaný bezpečnostní protokol pro technologii NFC (NearFieldCommunication). Jeho hlavním cílem je poskytnout zabezpečenou komunikaci a ochranu dat při používání NFC zařízení.NFC-SEC zahrnuje několik bezpečnostních funkcí a mechanismů, které pomáhají chránit komunikaci a data v prostředí NFC:

- Kryptografie: NFC-SEC využívá pokročilé kryptografické algoritmy k šifrování dat při jejich přenosu mezi zařízeními. Tím je zajištěna důvěrnost a integrita dat.
- Autentizace: Protokol NFC-SEC umožňuje vzájemnou autentizaci mezi komunikujícími zařízeními. To znamená, že se ověřuje pravost a důvěryhodnost zařízení a komunikačního partnera.
- Ochrana proti útokům: NFC-SEC se zaměřuje na ochranu před různými typy útoků, jako jsou odposlechy, padělání dat, opakované přehrávání a další. Implementuje bezpečnostní mechanismy, které minimalizují riziko úspěšného útoku.

- Ochrana soukromí: NFC-SEC zohledňuje také ochranu soukromí uživatelů. Poskytuje možnosti pro anonymní komunikaci a ochranu citlivých osobních dat.[21][23]

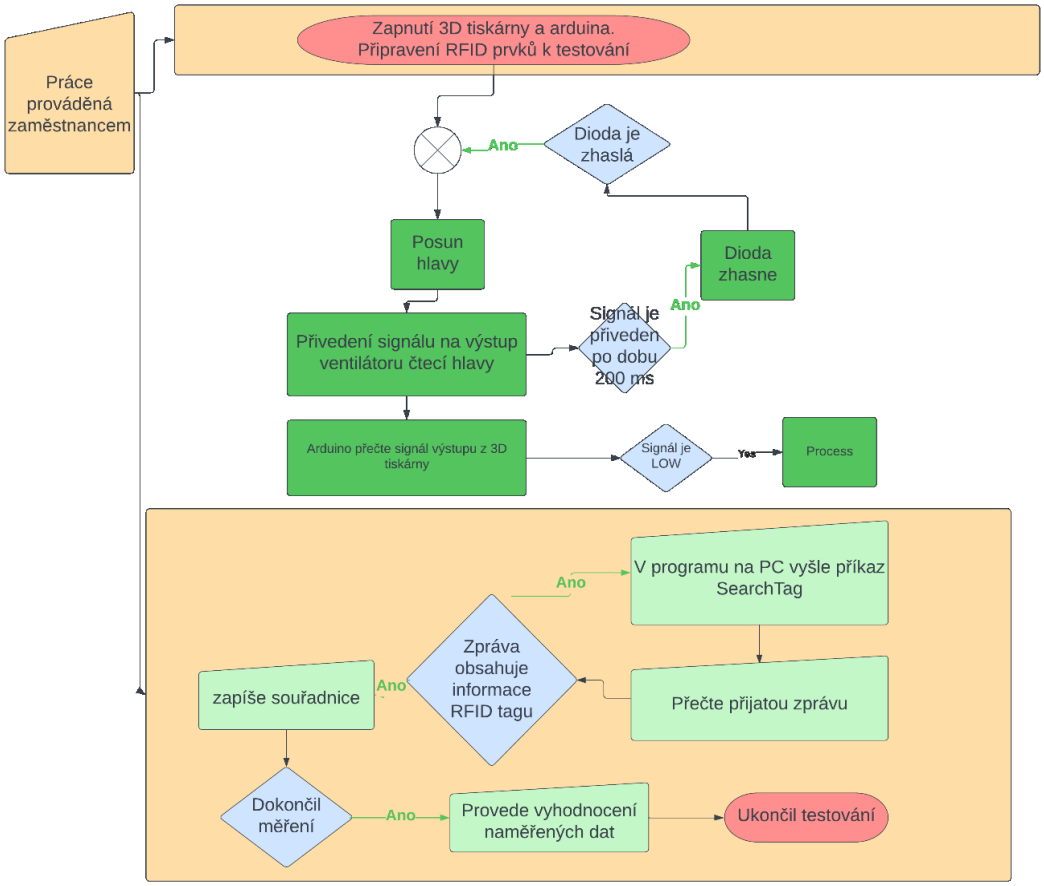
6.5.2 Secure Element (SE)

Secure Element (SE) je bezpečnostní prvek používaný v technologii NFC (NearFieldCommunication) pro ochranu citlivých dat a provádění bezpečných transakcí. Jedná se o dedikovaný hardwarový čip, který slouží k ukládání a správě šifrovaných klíčů, certifikátů a dalších důvěrných informací.SE je fyzicky oddělený od hlavního procesoru zařízení a má vlastní zabezpečený prostor, do kterého nemají neoprávněné aplikace nebo procesy přístup. To zajišťuje vyšší úroveň ochrany proti různým útokům, jako je odposlech, podvrhnutí dat nebo krádež identifikátorů.SE se často používá pro realizaci bezpečných platebních aplikací, například pro bezkontaktní platby pomocí mobilních telefonů. Díky tomu je možné provádět bezpečné transakce s vysokou úrovní ochrany dat a soukromí uživatele.[23]

II. PRAKTICKÁ ČÁST

7 ROZBOR PROBLEMATIKY

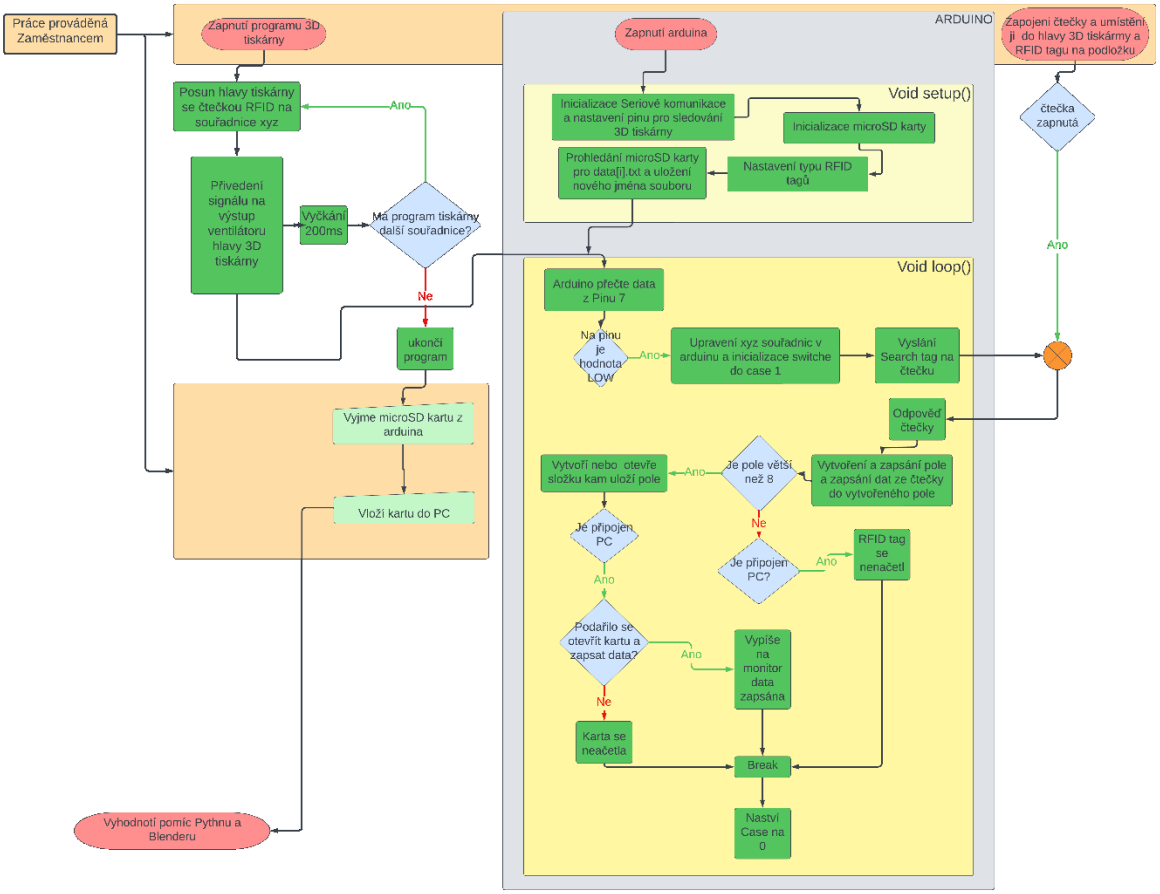
Společnost Trade FIDES, a. s. tak jako další společnosti, které se zabývají zabezpečováním objektů nebo vývojem RFID zařízení, testují čtečky RFID prvků a jednotlivé prvky na jejich dosah přenosu, sílu elektro magnetického pole, možné rušení nebo možnost zachycení komunikace. Doposud RFID prvky musel testovat zaměstnanec, kterému otestovat jednu kartu s jednou čtečkou trvalo hodinu času, během které se musel aktivně zapojovat do měření ve formě zapisování naměřených hodnot a manuálního spínání čtení, když 3D tiskárna dorazila na pozici a rozsvítila se led dioda připojená na výstup ventilátoru. Při implementaci nových čteček pak musí projít čtečku se všemi RFID tagy. To může trvat podle počtu karet klidně i desítky hodin. Návrhem automatizované čtečky RFID prvků výrazně zrychlíme proces měření a snížíme účast zaměstnance na samotném procesu. Bude potřeba pouze usadit čtečku do hlavy 3D tiskárny. Kartu, klíčenku nebo jiný prvek na podložku, zapnout arduino a spustit program v terminálu tiskárny. Po 15 minutách bude plně doměřeno a může jít data zpracovat nebo začít další měření. Tímto se také eliminuje lidská chyba a měření bude přesnější.



Obrázek 4 popis práce před automatizací [Vlastní]

8 NÁVRH ŘEŠENÍ

V rámci praktické části je úkolem vytvořit zařízení pro automatické testování dosahů RFID prvků, které bude následně firma využívat při zavádění a testování nových čteček a karet. Toto zařízení by mělo značně urychlit měření detekčních vzdáleností. Navrhované zařízení bude využívat již funkční konstrukce 3D tiskárny doplněné o nový gcode, arduino, zprostředkovávající řízení celého procesu a přídavné moduly arduina pro komunikaci se čtečkami a ukládání dat. Data budou přímo ukládána na microSD kartu a budou určena pro pozdější zpracování v Pythnu nebo jiném programu na práci s daty a vyhodnocení ve formě 3D modelu v Blendru, Meshlabu a dalších softwarech.



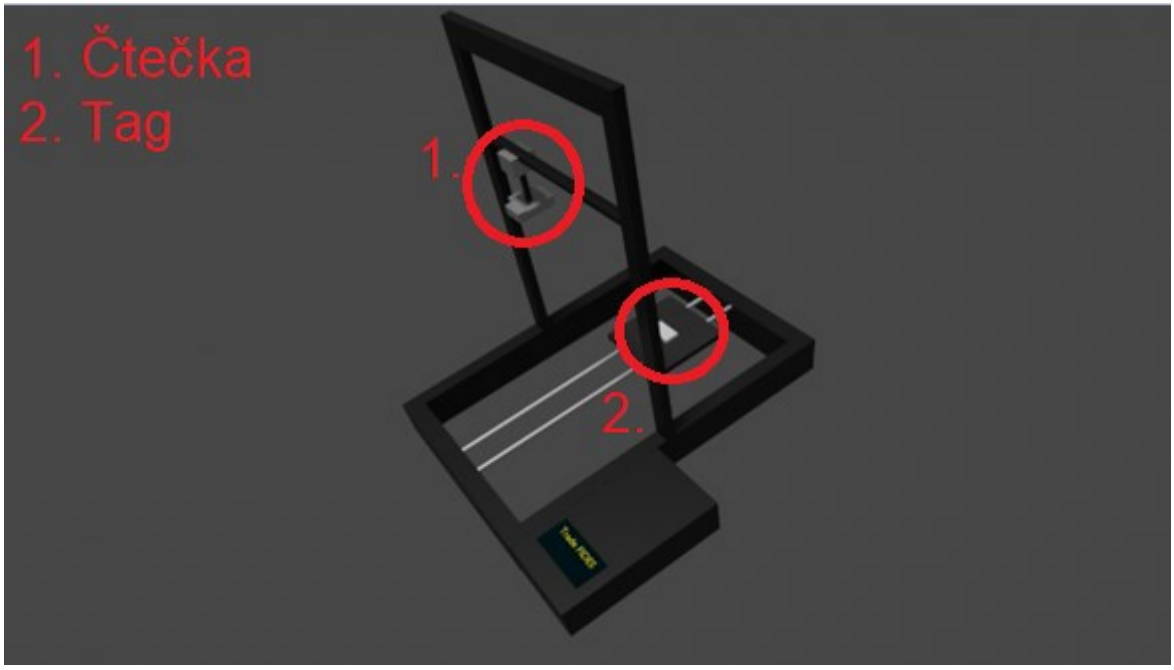
Obrázek 5 popis práce s automatizací [Vlastní]

9 REALIZACE

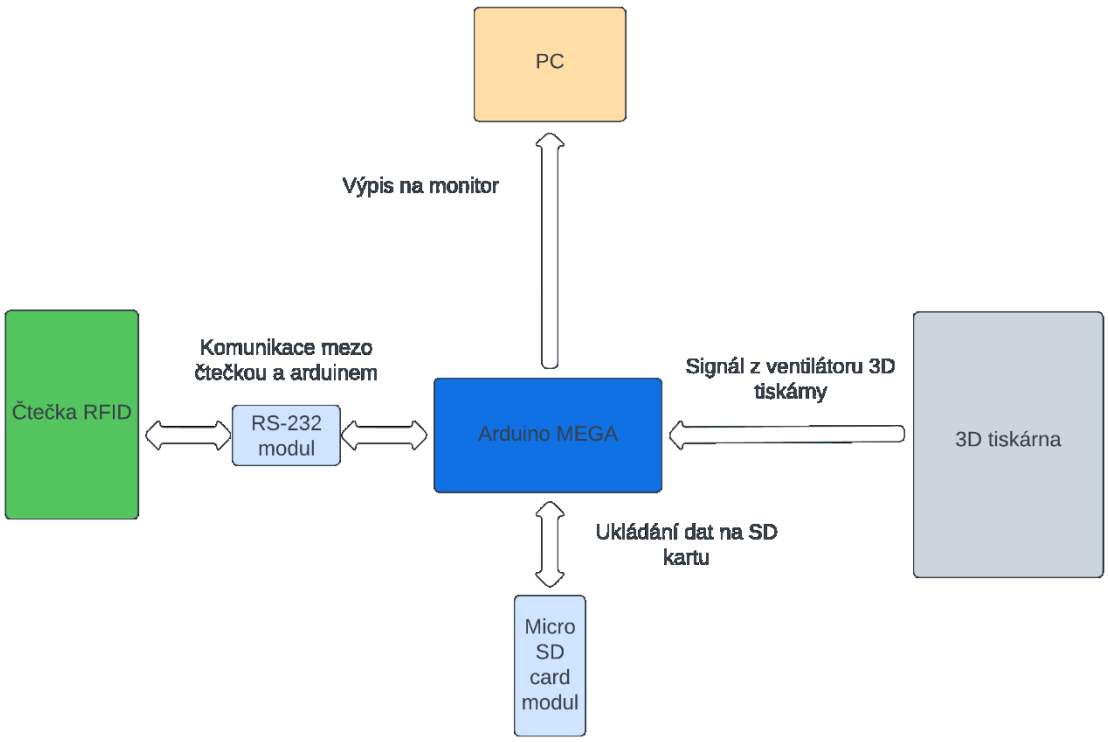
Samotný návrh a realizace zařízení pro automatické testování dosahů RFID prvků se skládá z softwarové (SW) a hardwarové (HW) části. Zde je rozdělení na obě části. Hardwarová část se bude skládat z konstrukce 3D tiskárny, zahrnuje využití stávající konstrukce a případné úpravy pro přidání dalších součástí a funkcionalit. Arduinodesky jako centrální jednotky pro řízení celého zařízení. Arduino by mělo být vybráno tak, aby mělo dostatek pinů a výkonu pro komunikaci s přídavnými moduly a zpracování dat. Přídavné moduly arduino pro komunikaci se čtečkami RFID pomocí rs-232 a ukládání dat na microSD kartu. Softwarová část s arduinem napsaná pomocí Arduino IDE. Implementace komunikačního protokolu pro přenos dat mezi Arduino a čtečkami RFID. To zahrnuje použití sériové komunikace nebo jiných přenosových protokolů. Ukládání naměřených dat na microSD kartu. Vytvoření souborového systému na microSD kartě a zápis naměřených dat do souborů. Vyhodnocení po přenosu dat z microSD karty do počítače pomocí programovacího jazyka jako je Python. Data mohou být zpracována pro vytvoření 3D modelu.

9.1 HW část

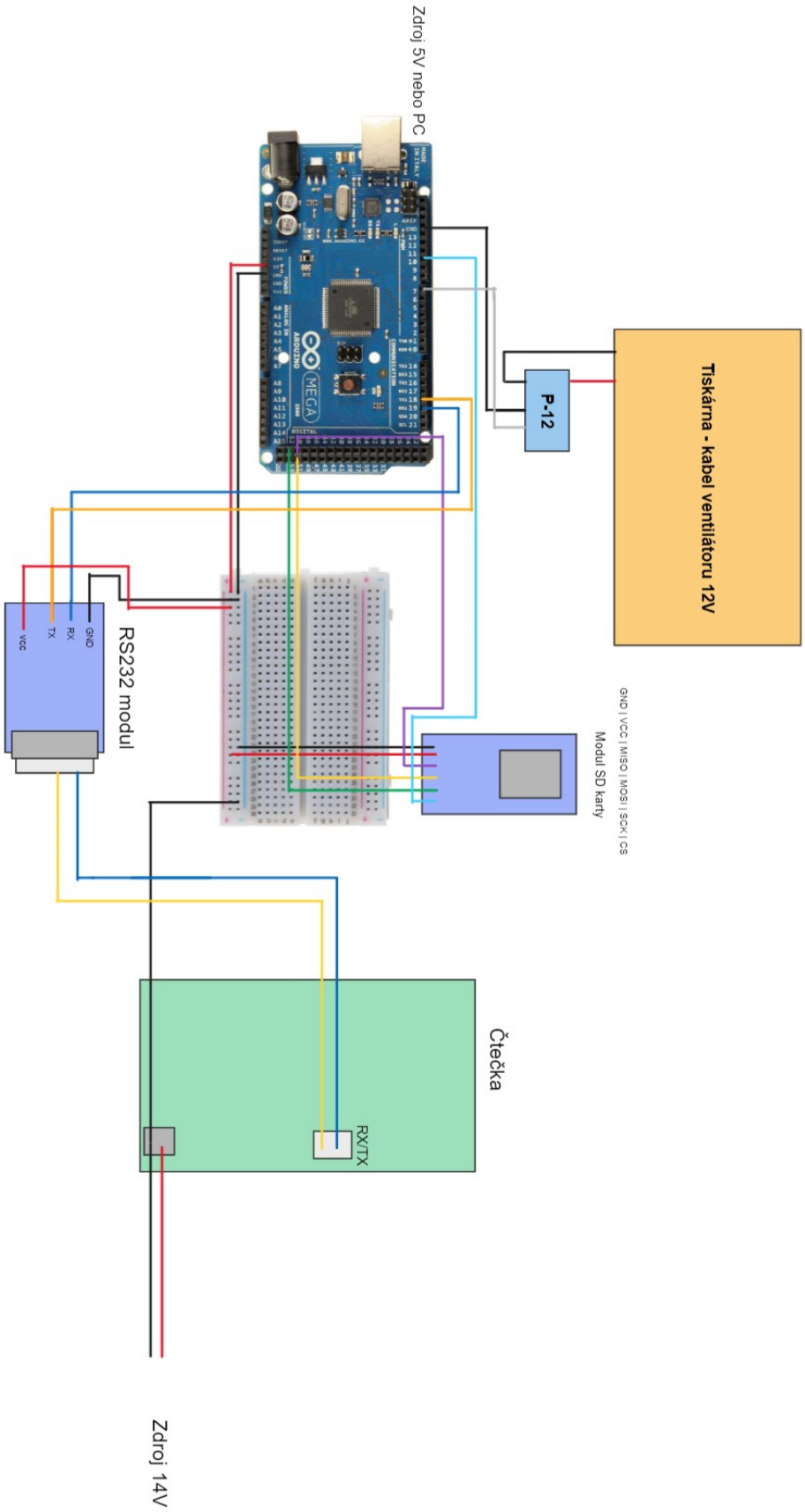
Kompletní konstrukce a zapojení navrhovaného zařízení na automatizovaný tester RFID čteček. Celkové zařízení se skládá z konstrukce 3D tiskárny, 3DPrinter Mega Zero 220* 220*250. Arduina mega 2560 jako hlavního řídícího prvku. Modulu rs-232 M438B pro sériovou komunikaci mezi čtečkami a arduinem. MicroSD card modulu pro možnost ukládání naměřených dat bez nutnosti arduina být připojeného k PC. Relé P-12, které muselo být doplněno pro funkční možnost komunikace mezi 3D tiskárnou a arduinem. Výstup ventilátoru běží na 12 V a celé arduino na 5 V. Díky relé můžeme vyřešit tento problém a mít funkční komunikaci bez nutnosti převádění napětí. Dále jako součást navrhovaného zařízení jsou propojovací kabely, vodivé kontaktní pole a trafo pro napájeni čteček. Testování probíhalo na čtečkách ASSET 602 a ASSET 603 s RFID prvky ve formě karty a klíčenky MIFARE DESfire.



Obrázek 6 konstrukce tiskárny z RFID prvky [Vlastní]



Obrázek 7 HW komunikace [Vlastní]



Obrázek 8 HW zapojení [Vlastní]

9.1.1 Arduino Mega 2560

Arduino Mega 2560 je jednou z nejvyhledávanějších desek z rodiny Arduino. Je založena na mikrokontroleru ATmega2560 a disponuje širokou škálou pinů, včetně digitálních, PWM a analogových vstupů, což umožňuje připojení různých periférií. Má také dostatečnou paměťovou kapacitu pro ukládání kódu a dat, což je výhodné pro složitější projekty.

Arduino Mega 2560 se vyznačuje svou rozšiřitelností a vyšším výkonem ve srovnání s jinými deskami Arduino. Je ideální pro projekty, které vyžadují připojení většího množství senzorů a rozšiřujících modulů. Díky svému výkonu a možnostem je vhodný pro vývoj rozsáhlejších systémů.

Existují však i jiné alternativy k Arduino Mega 2560, jako například ArduinoUno, Leonardo nebo Due. ArduinoUno je základní deskou s omezenějšími možnostmi, zatímco Arduino Leonardo nabízí integrovanou podporu pro klávesnice a myš. ArduinoDue zase poskytuje vyšší výkon a rychlost díky svému 32bitovému mikrokontroleru.

Arduino Mega 2560 přináší výhody ve formě většího počtu pinů a paměťové kapacity, což umožňuje připojení a ukládání většího množství dat. Nabízí také více sériových portů pro snadné připojení zařízení. Nicméně je fyzicky větší a má vyšší spotřebu energie než některé menší desky Arduino, a také je o něco dražší.

Závěrem lze říci, že Arduino Mega 2560 je skvělou volbou pro projekty, které vyžadují rozsáhlejší možnosti rozšíření. Je schopná řešit komplexní úlohy a poskytuje dostatečný výkon pro většinu aplikací. Pro jednodušší a méně náročné projekty však mohou být vhodnější varianty s nižšími náklady a menší velikostí, jako například ArduinoUno. [24]

Obrázek 9 Arduino Mega 2560[24]

Arduino Mega díky velkému počtu digitálních pinů, PWM výstupů a analogových vstupů umožňuje připojení různých periférií a senzorů Arduino Mega je vybavena 4 sériovými porty, což usnadňuje komunikaci s dalšími zařízeními. Také obsahuje USB rozhraní pro jednoduché napájení a připojení k počítači nebo powerbance. Arduino Mega je ideální pro pokročilé i drobné projekty v oblasti automatizace, robotiky, chytrých domácností a IoT. Lze vytvářet sofistikované interaktivní projekty, které jsou snadno programovatelné pomocí Arduino IDE a dostupných knihoven.Celkově Arduino Mega je výkonná a rozšiřitelná deska, která nabízí více pinů, větší paměťovou kapacitu a vyšší výkon než ostatní varianty Arduino. Deska byla zvolena až jako druhá volba. První pokusy probíhali na Arduinu UNO, kde byla využívána SW sériová sběrnice. Ta však nebyla dostatečně rychlá a spolehlivá, a tak bylo nutno najít alternativu. [24]

9.1.2 RS-232 modul M438B pro arduimo

Modul M438B je zařízení, které umožňuje komunikaci pomocí sériového rozhraní RS-232. RS-232 rozhraní se často využívá pro přenos dat mezi různými zařízeními, jako jsou počítače, senzory a další elektronická zařízení. M438B modul poskytuje jednoduché řešení pro připojení zařízení s RS-232 rozhraním k jiným zařízením, která podporují toto rozhraní. Obvykle obsahuje desku plošných spojů s RS-232 konektorem nebo pinovou lištou pro připojení.

Modul M438B obsahuje převodníky úrovní, které slouží k přizpůsobení signálních úrovní RS-232 standardu. To je důležité, protože moderní zařízení často používají nižší úrovně signálů než RS-232. Převodníky úrovní umožňují kompatibilitu mezi různými úrovněmi signálů. Kromě převodníků úrovní může modul M438B obsahovat další komponenty pro ochranu před elektrostatickým vybíjením nebo pro regulaci napětí a proudových hodnot. Této funkce je využito pro komunikaci se čtečkou, která operuje na 14 V. Připojení modulu M438B je obvykle jednoduché. Je třeba správně připojit signály TX (vysílací), RX (přijímací), GND (zem) a případně další signály, které jsou potřebné v daném použití.[24]

9.1.3 microSD Card modul

Modul microSD karty pro Arduino je zařízení, které umožňuje snadné připojení a používání microSD karet s Arduino deskami. Jeho hlavním účelem je umožnit ukládání a čtení datz externí paměťové karty, což je zvlášť užitečné pro projekty s vyššími paměťovými nároky. Tento modul se obvykle skládá z desky plošných spojů a slotu pro microSD kartu. Připojuje se k Arduino desce prostřednictvím digitálních vstupně-výstupních pinů. Existuje několik variant modulů s různými rozložením pinů nebo doplňkovými funkcemi, jako je vestavěný level shifter pro přizpůsobení signálních úrovní. Připojení modulu pro microSD kartu k Arduino je obvykle jednoduché. Modul se připojuje přes piny pro komunikaci a napájení v případě našeho modulu 5V a GND. Arduino pak komunikuje s microSD kartou přes tyto piny a umožňuje zápis a čtení dat. Pro programování a použití modulu pro microSD kartu vArduinu existují knihovny, které zjednodušují práci s microSD kartami. Tyto knihovny poskytují funkce pro inicializaci karty, čtení a zápis dat a další operace. Modul microSD karty je užitečným přídavkem pro projekty, které vyžadují rozšířenou paměťovou kapacitu. SD karta je využívána na ukládání dat ve formě txt souboru se souřadnicemi xyz a kódu obdrženého ze čtečky. Tento modul je často využíván v oblastech robotiky, dataloggingu, sledování senzorů a dalších aplikacích, které vyžadují ukládání a manipulaci s daty na externí paměťové kartě.[24]

9.1.4 Relé P-12

Relé P-12 je elektromagnetické relé, které se často používá pro spínání větších zátěží pomocí nízkého signálu, jako například z Arduino nebo jiných mikrokontrolerů. Zde je však využíván pro spínání větší zátěží, jako alternativu převádění napětí z výstupu ventilátoru 3D tiskárny. Je určeno pro spínání střídavého proudu s maximálním proudem

10 A a napětím 250 V. Relé P-12 je složeno z elektromagnetu a mechanického spínače. Elektromagnet je řízen elektrickým signálem nízké úrovně, který způsobuje magnetické přitahování cívky. Tím se pohybují mechanické kontakty relé, které otevírají nebo uzavírají spojení mezi dvěma elektrickými obvody. Relé P-12 několik kontaktů, včetně hlavního kontaktu a pomocných kontaktů. Hlavní kontakt slouží k připojení napájení zátěže, kterou chceme spínat. Pomocné kontakty se mohou využít pro signalizaci stavu relé nebo připojení dalších zařízení. Připojení relé P-12 k externímu zařízení se provádí pomocí svorek, které umožňují připojení vodičů nebo konektorů. Je důležité správně zapojit napájecí napětí a zátěž. Relé P-12 se často využívá v různých aplikacích, jako je ovládání osvětlení, řízení motorů, spínání elektrických spotřebičů, bezpečnostní systémy a další. Jeho použití umožňuje snadné a spolehlivé ovládání elektrických zařízení pomocí signálů z mikrokontrolerů nebo jiných digitálních zařízení. [27]

9.1.5 Čtečka karet ASSET 602

ASSET 602 je RFID čtečka karet, která sloužící k čtení a zpracování dat z různých typů RFID tagů a čipových karet a dalších. Nachází široké uplatnění v oblasti řízení přístupu, identifikace a dalších aplikací, které vyžadují spolehlivé a bezpečné čtení karet. Čtečka ASSET 602 byla navržena s cílem poskytovat rychlé a přesné čtení dat z karet. Podporuje různá komunikační rozhraní, jako je RS-232, RS-422 nebo Wiegand, což umožňuje snadné připojení k počítačům, terminálům nebo jiným zařízením. Toto zařízení je schopno číst informace z RFID nosičů, který dekóduje magnetické pole zaznamenané na kartě. To umožňuje získávání dat uložených na kartě, jako jsou údaje o účtu, jméno uživatele, číslo karty atd. ASSET 602 čtečka karet také podporuje čtení čipových karet, které obsahují integrované obvody s daty. Tyto karty poskytují vyšší úroveň bezpečnosti a funkcionality, jako je kódování, šifrování a ověřování. Čtečka karet umožňuje komunikaci s čipovými kartami pomocí různých protokolů, jako je EMV, ISO/IEC 14443 a další. Pro správné použití čtečky ASSET 602 je obvykle potřeba vhodný software, který umožňuje zpracování a interpretaci dat z karet. Tento software může poskytovat rozhraní pro získávání informací, ověřování platnosti karet a další operace. ASSET 602 čtečka karet je využívána v různých oblastech, jako jsou hotely, obchodní centra, dopravní systémy, jaderné elektrárny, muniční sklady a další, kde je zapotřebí spolehlivé a bezpečné čtení karet. Díky svým funkcím a podpoře různých typů karet představuje flexibilní řešení pro různé aplikace, které pracují s kartami.

9.1.6 Čtečka karet ASSET 603

ASSET 603 je vysoce výkonná čtečka karet, která nabízí rychlé a spolehlivé čtení a zpracování dat z různých typů karet. Je navržena s důrazem na bezpečnost, kompatibilitu a vysokou přesnost. Tato čtečka podporuje širokou škálu karet jak HF tak LF. Mezi podporované standardy patří například ISO 14443 nebo ISO 15693. ASSET 603 disponuje pokročilými funkcemi, jako je vysoká rychlost čtení a zpracování dat, podpora šifrování a autentizace a také možnost přizpůsobení a konfigurace dle potřeb uživatele. Čtečka je vybavena různými komunikačními rozhraními tak jako ASSET 602, což umožňuje snadné připojení k různým zařízením, včetně počítačů, terminálů a platebních systémů. Pro účely měření je důležitá komunikace po RS-232. Díky vysoké přesnosti a spolehlivosti čtení je ASSET 603 ideální pro aplikace, které vyžadují rychlé a bezchybné zpracování dat z karet. Aplikace jsou tedy poměrně široké, a to v řízení přístupu, identifikaci, časové a docházkové systémy a dalších oblastech, kde je klíčové získávání a zpracování dat z karet. Díky své flexibilitě a podpoře různých typů karet je čtečka ASSET 603 vhodnou volbou pro profesionální a komerční aplikace, kde spolehlivost, bezpečnost a výkonnost jsou nezbytné.

9.1.7 Čipová karta a klíčenka MIFARE DESFire

MIFARE DESFire je bezkontaktní inteligentní karta, která se široce využívá v různých aplikacích, včetně bezpečnostních systémů, platebních systémů, identifikace a řízení přístupu. Tato karta je založena na technologii RFID a je součástí rodiny karet MIFARE vyvinutých společností NXP Semiconductors. MIFARE DESFire je známá pro svou vysokou úroveň bezpečnosti a integrované šifrování dat. Obsahuje čip s paměťovými sektory a algoritmy pro šifrování a autentizaci, což zajišťuje ochranu dat před neoprávněným přístupem a snižuje riziko krádeže identifikátorů.

Přednosti a výhody karty MIFARE DESFire:

- Bezpečnost: Karta disponuje pokročilými bezpečnostními funkcemi, jako je 3DES a AES šifrování, které chrání data a brání proti podvržení.
- Rychlost a výkon: Karta nabízí vysokou rychlost přenosu dat a efektivní zpracování, což umožňuje rychlé a spolehlivé operace, jako je ověřování a přístup k datům.

- Flexibilita: MIFARE DESFire podporuje různé formáty dat a lze ji využít v různých aplikacích, včetně plateb, řízení přístupu, docházkových záznamů a dalších.
- Kompatibilita: Karty MIFARE DESFire jsou kompatibilní se stávajícími infrastrukturami a zařízeními používanými v RFID aplikacích.
- Odolnost: Fyzická karta je navržena tak, aby byla odolná proti opotřebení a vnějším vlivům, což zajišťuje dlouhou životnost a spolehlivost.

Karta MIFARE DESFire je často využívána v bezpečnostních systémech, jako jsou přístupové karty do budov, veřejné dopravy a další. Je ideální pro aplikace, které vyžadují vysokou úroveň bezpečnosti a rychlosti, a poskytuje spolehlivý a efektivní způsob identifikace a řízení přístupu.

9.1.8 3DPrinter Mega Zero 220* 220*250

3D tiskárna Mega Zero 220*220*250 je kompaktní a cenově dostupná 3D tiskárna, která umožňuje vytvářet objekty ve třech rozměrech. Je navržena s ohledem na jednoduchost použití. Tiskárna disponuje tiskovou plochou o rozměrech 220 mm x 220 mm x 250 mm, což poskytuje dostatečný prostor pro testování komunikace různých tagů a čteček. Tiskárna je kompatibilní s různými softwary pro přípravu tiskových souborů, jako je například Cura.MegaZero 220*220*250, nabízí také několik funkcí, které zvyšují uživatelskou přívětivost. Patří sem například automatické vyrovnání podložky,možnost pokračovánív tisku po výpadku napájení a další.Tato tiskárna je vhodná pro domácí použití, hobby projekty, vzdělávací účely a další aplikace, které vyžadují tisk vlastních 3D objektů. Je snadno ovladatelná a poskytuje dostatečnou přesnost a kvalitu tisku pro běžné potřeby.[28]

9.2 SW část

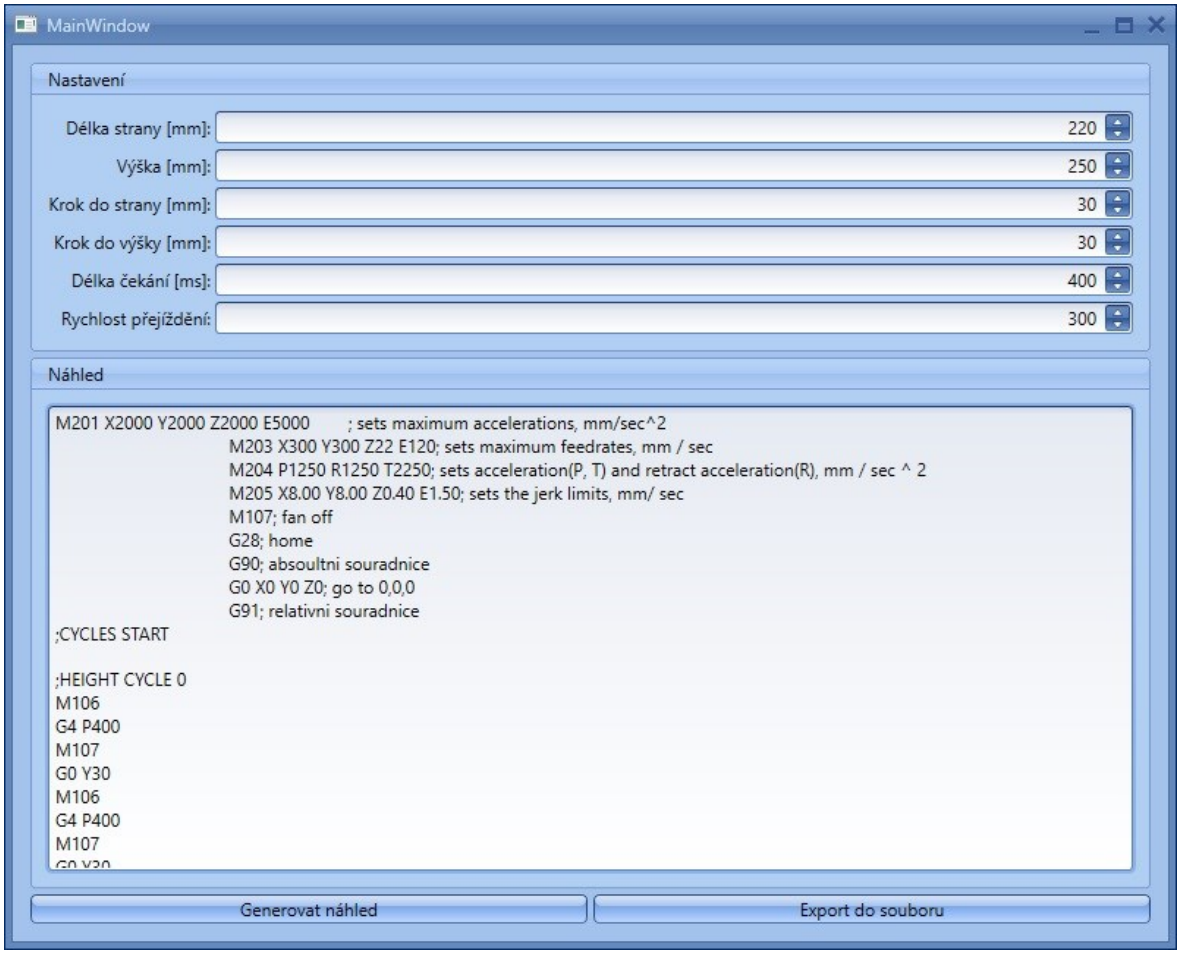
Programová část, která zpracovává chod konstrukce 3D tiskárny, komunikaci se čtečkou a arduinem, přijímání signálu z tiskárny do arduina, ukládání dat na microSD kartu a úpravu dat a její finální zpracování s vyhodnocením. Jako SW pro ovládání 3D tiskárny je vybrán gcode. Výhodou je jednoduchá úprava v generátoru kódu, kde můžeme nastavit jak rychlost, tak velikost posunu, což nám umožní vybrat hustotu bodů, které chceme měřit a díky tomu udělat detailní měření. Menší posun znamená více bodů a díky tomu dostaneme přesnější 3D model. Arduino využívá knihovny na práci s SD kartou, Sériové linky pro

komunikaci. Seriál pro komunikaci s monitorem a Serial1 pro komunikaci se čtečkou. Vysílané data na čtečku musí být vždy zakončena /r pro vytvoření platné zprávy, kterou čtečka přijme a zpracuje.

9.2.1 SW měření

G-kód je normalizovaný programovací jazyk, který se používá pro řízení 3D tiskáren a CNC strojů. Obsahuje instrukce a příkazy, které ovládají pohyb nástroje, rychlosti, teploty a další parametry během procesu tisku nebo obrábění. G-kód se zapisuje ve formě textového souboru, který obsahuje sérii příkazů a jejich parametrů. Každý příkaz začíná písmenem "G" následovaným číslem a případně dalšími parametry. Například příkaz "G1 X100 Y50" by stroji řekl, aby se přesunul na pozici X=100 a Y=50. Existuje široká škála standardních G-kódů, které se často používají v průmyslu. Tyto kódy poskytují společný jazyk pro ovládání různých funkcí stroje a umožňují přesné a efektivní operace. [29]

Pro vytvoření kódu viz bp_hrach_200s15m.gcode byl použit generátor kód Obrázek 10 generátor gcodu [Vlastní], kde byly nastaveny všechny důležité parametry jako jsou posun, délka čekání, rychlost přejíždění a další. Absolutní souřadnice se následně nastaví samy podle posunutí zarážky na konstrukci 3D tiskárny.



Obrázek 10 generátor gcodu [Vlastní]

9.2.1.1 Účelprogramu

Cílem toho program je vytyčit konstrukci z 3D tiskárny, doplněné o RFID čtečku na místo běžné tiskové hlavy, body po kterých se bude pohybovat, jakou rychlostí, dále také jak dlouho se zdrží na daných souřadnicích a příkazy pro spuštění ventilátoru čtecí hlavy. Ventilátor stejně jako čtecí hlava je nahrazen, a tak je výstup ventilátoru používán pro přivádění dat do arduina jakožto signalizace o posunu na další souřadnice.

9.2.1.2 Využívané příkazy:

Tiskárna operuje na FW Marlin. Marlin je open-source firmwarový projekt navržený speciálně pro 3D tiskárny. Je vyvinut jako platforma pro ovládání pohybu a dalších funkcí 3D tiskáren, poskytující uživatelům široké možnosti nastavení a rozšíření. Marlin je jedním z nejpoužívanějších a nejpopulárnějších firmwarů pro 3D tiskárny díky své robustnosti, flexibilitě a aktivnímu vývojářskému společenství.[29]

M106 – V G-kódu pro ovládání 3D tiskáren, příkaz M106 se používá pro ovládání chlazení tiskárny. Slouží k zapnutí a regulaci ventilátorů nebo jiných chladicích zařízení připojených k tiskárně.

M107 – Příkaz M107 slouží k vypnutí chlazení tiskárny. Používá se pro vypnutí ventilátorů nebo jiných chladicích zařízení připojených k tiskárně.

M201 – Používá se k definování maximálních hodnot zrychlení pro jednotlivé osy tiskárny. Tento příkaz ovlivňuje, jak rychle se tiskárna zrychluje a zpomaluje během pohybu po jednotlivých osách. Jeho účelem je nastavit limity pro zrychlení, což umožňuje jemnější a přesnější kontrolu nad pohybem tiskárny. Volbou vhodných hodnot zrychlení je možné minimalizovat vibracea ochránit tiskárnu před přetížením motorů. Doporučuje se provádět experimenty a postupně optimalizovat nastavení maximálních hodnot zrychlení pro dosažení nejlepších výsledků.

M203 – Příkaz M203 v G-kódu nastavuje maximálních rychlost pohybu pro osy tiskárny. Tím lze omezit, jak rychle se tiskárna pohybuje. Každá osa může mít svou vlastní maximální rychlost. Tímto příkazem lze upravit rychlosti tak, aby odpovídaly schopnostem tiskárny. Díky tomu je zamezeno problému s přetížením motorů a možné nepřesnosti měření.

M204 – Stanovuje zrychlení a zpomalení pro pohyb tiskárny. Tyto faktory ovlivňují, jak rychle se tiskárna zrychluje a zpomaluje při pohybu po osách.

M205 – Slouží k nastavování dalších parametrů. Může se lišit napříč jednotlivými verzemi FW Marlin. Zde je využíván pro nastavení rychlosti zrychlení, která ovlivňuje rychlost pohybu a změny směru.

G4 – Příkaz pro zpoždění nebo čekání. Používá se k zastavení pohybu tiskárny na určitou dobu, což může být užitečné pro různé účely, jako je čekání na ustálení tiskového podkladu nebo pro vytvoření umělého zpoždění mezi příkazy. Zde je využíván pro vyčkání před vypnutím signálu pro arduino.

G0 – G0 v G-kódu pro ovládání 3D tiskáren je příkaz pro rychlý pohyb na danou pozici. Také se nazývá příkaz "Rapid Move" nebo "Fast Move". Používá se k přesunu tiskárny na určenou pozici rychle a bez tisku.

G28 – Příkaz pro nulování polohy os tiskárny. Také se nazývá příkaz "Home". Používá se k přesunu tiskárny na předem nastavenou referenční polohu na každé ose.

G90 – Nastavení absolutního polohování. Také se nazývá příkaz "Absolute Positioning". Při použití tohoto příkazu se polohy os tiskárny určují relativně k absolutním souřadnicím.

G91 – Slouží k nastavení relativního polohování. Také se nazývá příkaz "Relative Positioning". Při použití tohoto příkazu se polohy os tiskárny určují relativně k předchozím polohám.

9.2.2 SW pro automatizaci – Arduino

Jazyk Arduino je specifický programovací jazyk, který je používán pro programování mikropočítačů z rodiny Arduino. Tento jazyk je založen na jazyce Wiring a používá se pro vývoj různých projektů a aplikací, včetně automatizace, robotiky, senzorických systémů, interaktivních objektů a dalších elektronických zařízení. Jazyk Arduino je podobný jazyku C/C++ a obsahuje mnoho knihoven a funkcí, které usnadňují programování mikropočítače. Jednoduchá syntaxe a intuitivní přístup umožňují i začátečníkům rychle se naučit programování s Arduino. Programy napsané v jazyce Arduino se nazývají "sketches" a jsou tvořeny dvěma základními funkcemi - "setup()" a "loop()". Funkce "setup()" se spustí pouze jednou na začátku programu a slouží k inicializaci různých parametrů a nastavení. Funkce "loop()" se opakovaně provádí po inicializaci a obsahuje hlavní část programu, která běží neustále v nekonečné smyčce. Kromě toho Arduino nabízí také sadu knihoven, které usnadňují přístup k různým periferním zařízením, jako jsou senzory, displeje, motorové řízení a komunikační rozhraní. Tyto knihovny poskytují předem definované funkce a metody, které usnadňují práci s konkrétními zařízeními a snižují složitost programování. Jazyk Arduino je široce používán komunitou vývojářů a makerů díky své jednoduchosti, přístupnosti a podpoře rozsáhlého hardwarového a softwarového ekosystému Arduino. Díky tomu lze snadno vytvářet a sdílet projekty, najít dostupné zdrojové kódy a získat podporu od ostatních uživatelů.

Kompletní program arduina viz BP_Hrach_v4\BP_Hrach_v4.ino

9.2.2.1 Účel programu:

Tento program má za úkol komunikovat s RFID čtečku a provádět vyhledávání RFID tagů. Pokud čtečka detekuje RFID tag, program zaznamená souřadnice a zprávu z tagu a uloží je na SD kartu.

Inicializace a konfigurace:

- Připojení SD karty k Arduinu a inicializace knihovny pro práci se SD kartou.
- Konfigurace pinů pro komunikaci s RFID čtečkou a SD kartou.

Inicializace souboru na SD kartě:

- Vytvoření souboru na SD kartě, do kterého budou zaznamenávány souřadnice a zprávy z RFID tagů.
- Otevření souboru pro zápis dat.

Smyčka programu:

- Čtení dat z RFID čtečky.
- Pokud byl detekován RFID tag:
- Získání souřadnic a zprávy z tagu.
- Zápis souřadnic a zprávy do souboru na SD kartě.
- Čekání na další detekci RFID tagu.

Program při přivedení signálu na pin pro detekci chodu 3D tiskárny kontroluje RFID čtečku a zaznamenávat data, jakmile je detekován RFID tag, tak dojde k porovnání délky jeho řetězce znaků, který obsahuje identifikátor, typ karty a další atributy. Pokud je řetězec delší než 8 znaků, tak byla karta detekována a obdržená zpráva je zapsána na microSD kartu společně s xyz souřadnicemi. Výsledkem programu je soubor na SD kartě, který obsahuje zaznamenané souřadnice a zprávy z detekovaných RFID tagů. Tento soubor je následně určen pro další zpracování a vyhodnocení dat.

9.2.2.2 Využité knihovny:

Arduino nabízí rozsáhlou knihovnu, která zahrnuje mnoho předdefinovaných funkcí a metod pro usnadnění programování s různými periferními zařízeními a funkcionalitami. V této práci jsou využity knihovny SD.h a SPI.h, během vývoje kódu však byly využity i

další jako například SoftwareSerial.h, která se však do finální verze nedostala kvůli omezené komunikační rychlosti a byla nahrazena druhou hw sériovou linkou arduina mega 2560. Existuje mnoho dalších, které podporují různá zařízení, senzory a funkcionality. Knihovny lze snadno nainstalovat a použít přímo v Arduino IDE, což usnadňuje vývoj a programování různých projektů.

SPI je sériový komunikační protokol, který umožňuje komunikaci mezi mikropočítačem a dalšími zařízeními, jako jsou senzory, displeje, paměťové karty a další. Tento protokol využívá čtyři vodiče pro komunikaci - MOSI (Master Out Slave In), MISO (Master In Slave Out), SCK (SerialClock) a SS (Slave Select). Zahrnutí knihovny SPI do vašeho programu vám umožní používat funkce a metody, které usnadňují komunikaci s periferními zařízeními pomocí protokolu SPI. Například, můžete inicializovat SPI rozhraní, nastavit rychlost komunikace, odesílat a přijímat data a další operace spojené s komunikací přes SPI.[24]

Knihovna SD využívá standardní rozhraní SPI (SerialPeripheral Interface) pro komunikaci s microSD kartou. Proto je také často používána společně s knihovnou SPI, kterou jsme zmínili dříve. Pomocí knihovny SD můžete provádět operace jako otevírání a uzavírání souborů na microSD kartě, čtení a zápis dat do souborů, vytváření adresářů a další operace související s práci s paměťovými kartami.[24]

9.2.2.3 Využití příkazy a funkce

Serial.begin() - Funkce Serial.begin() je funkce v jazyce Arduino, která inicializuje sériovou komunikaci přes sériový port (UART) na desce Arduino. Tato funkce se obvykle volá v bloku setup(), který se spustí při startu programu. Do () se udává baudRate, což je rychlost komunikace. V programu je také využit switch o 3 casech pro možné přepínání a předejitím loopování. [24]

Seriál.avaiable() - Funkce Serial.available() je funkce v jazyce Arduino, která slouží k zjištění počtu dostupných dat k přečtení ze sériového portu. Tato funkce je často používána v kombinaci s funkcí Serial.read() pro asynchronní příjem dat ze sériového portu. [24]

Serial.print() - Funkce Serial.print() je funkce v jazyce Arduino, která slouží k odeslání dat přes sériový port (UART) na desce Arduino. Tato funkce umožňuje zasílat různé datové typy, jako jsou čísla, znaky, řetězce nebo hodnoty proměnných, do sériového monitoru v Arduino vývojovém prostředí (IDE) nebo do jiného zařízení připojeného k sériovému portu.[24]

Serial.println() - Funkce Serial.println() je podobná funkci Serial.print() v jazyce Arduino, ale s jedním rozdílem - automaticky vkládá znak nového řádku (CR-LF) na konec odeslaného textu. Tento znak nového řádku způsobí, že další výpis bude na novém řádku.[24]

Serial.write() - Funkce Serial.write() v jazyce Arduinoslouží k odeslání dat přes sériový port jako binární hodnoty. Tato funkce umožňuje přímo odesílat jednotlivé bajty dat bez konverze na textový řetězec.[24]

pinMode(, INPUT_PULLUP) - Funkce pinMode() v jazyce Arduino slouží k nastavení režimu pinu na vstupní nebo výstupní. Může být také použita ke konfiguraci interních pull-up rezistorů pinů. Kde argument INPUT_PULLUP stanovuje daný pin jako vstupní a s hodnotou HIGH v klidovém stavu.[24]

digitalRead() - Funkce digitalRead() v jazyce Arduino slouží k čtení hodnoty digitálního signálu z daného pinu. Tato funkce umožňuje získat stav pinu, zda je na něm přítomná logická nula (LOW) nebo logická jednička (HIGH).[24]

SD.begin - Funkce SD.begin() je metoda v knihovně SD pro jazyk Arduino, která inicializuje komunikaci s SD kartou a připraví ji pro čtení a zápis dat. Do () se zadává číslo pinu pro SDkartu.[24]

SD.exist - Funkce SD.exists() je metoda v knihovně SD pro jazyk Arduino, která slouží k ověření existence souboru nebo složky na SD kartě.[24]

SD.open - Funkce SD.open() je metoda v knihovně SD pro jazyk Arduino, která slouží k otevření souboru na SD kartě a umožňuje čtení nebo zápis dat do tohoto souboru.[24]

dataFile.println - FunkcedataFile.println() je metoda objektu třídy File v knihovně SD pro jazyk Arduino. Slouží k zápisu řetězce nebo dat na nový řádek v otevřeném souboru.[24]

datafile.close - Funkce dataFile.close() je metoda objektu třídy File v knihovně SD pro jazyk Arduino. Slouží k uzavření otevřeného souboru a uvolnění zdrojů, které byly používány pro práci se souborem.[24]

Break - Klíčové slovo break je součástí jazyka programování, včetně jazyka Arduino, a slouží k ukončení smyčky (for, while, do-while) nebo příkazu switch.[24]

Return - V jazyce Arduino je klíčové slovo return používáno stejným způsobem jako v jazyce C/C++. Slouží k vrácení hodnoty z funkce nebo procedury zpět do volající části programu.[24]

File - V jazyce Arduino, knihovna SD obsahuje třídu File, která poskytuje funkce pro práci se soubory na SD kartě. Třída File umožňuje otevírat, číst, zapisovat a manipulovat se soubory uloženými na SD kartě.[24]

String - V jazyce Arduino se pro práci s textovými řetězci (řetězcovými daty) často používá třída string. Třída string umožňuje jednoduchou manipulaci s textem, včetně vytváření, spojování, porovnávání a dalších operací. Použití třídy string je velmi podobné použití řetězců v jiných programovacích jazycích. Můžete vytvářet objekty typu string, přiřazovat jim hodnoty, manipulovat s nimi a získávat informace o jejich délce. [24]

Switch - V jazyce Arduino a v jazyce C/C++ je klíčové slovo switch používáno pro implementaci přepínačů (switch/case struktury), které umožňují vykonávat různé akce na základě hodnoty proměnné.Struktura přepínače (switch/case) umožňuje vyhodnotit výraz

nebo hodnotu proměnné a vykonat příslušný blok kódu pro odpovídající hodnotu. Struktura switch je často používána pro jednoduché větvení programu, kdy je potřeba provést různé akce v závislosti na různých hodnotách proměnné.[24]

If - V jazyce Arduino a v jazyce C/C++ je konstrukce if používána pro implementaci podmíněného rozhodování. Pomocí if můžete provádět různé části kódu na základě hodnoty nebo stavu určité podmínky.[24]

Else - V jazyce Arduino a v jazyce C/C++ klíčové slovo else je používáno v rámci konstrukce if-else pro definování bloku kódu, který se vykoná, pokud podmínka ve vyjádření if není splněna (hodnota je false).[24]

While - V jazyce Arduino a v jazyce C/C++ klíčové slovo while je používáno pro implementaci cyklu, který opakovaně provádí určitý blok kódu, dokud je splněna určitá podmínka.[24]

For - V jazyce Arduino a v jazyce C/C++ klíčové slovo for se používá pro implementaci cyklu, který opakovaně provádí určitý blok kódu s přesně určeným počtem opakování.[24]

9.2.2.4 Deklarování globálních proměnných a aktivace knihoven

Přidání knihoven pro správnou funkčnost SD karty a komunikaci s microSD card modulem. Přiřazení pinu komunikaci s microSD kartou a jeho pojmenování chipSelect. Deklarování globálních proměnných.

```
#include<SPI.h>
#include<SD.h>

constintchipSelect = 10;

intN;
intopakovani;

intxcord = 0;
intycord = 0;
intzcord = 0;
```

```
intxswitch = 0;
intyswitch = 0;

String currentFileName;
```

9.2.2.5 *Inicializace sériové komunikace a nastavení pinu na vstup*

Aktivace sériových linek (RX/TX) o rychlosti 9600 baudů jakožto doporučenou rychlost pro práci s arduinem, vyšší rychlosti nemusí zvládat. Přiřazení pinu 7 jako vstupní a PULLUP. Celá tato část programu je v void setup, tudíž proběhne pouze jednou a to při zapínání nebo restartování arduina.

```
Serial.begin(9600);
Serial1.begin(9600);

pinMode(7, INPUT_PULLUP);
```

9.2.2.6 *Kontrola funkční microSD karty*

Za pomocí ifa !Sd.begin se vyzkouší zda je karta načtená. ! zde slouží jako negace. Pokud by byla podmínka splněna, tak na monitor vypíše chybová zpráva, pokud není tak se vypíše zpráva o funkčnosti karty. Taktéž je částí voidloop.

```
if(!SD.begin(chipSelect)){
  Serial.println(" SD karta se nenacetla");
  return;
}
Serial.println(" SD kartanactena");
```

9.2.2.7 *Výběr jednotlivého typu karty MIFARE*

Pomocí Serial1.write je zaslán kód do čtečky, který vybere pouze typ karty, který chceme sledovat. Tímto krokem zrychlíme práci čtečky a můžeme nastavit menší prodlevu mezi posuny tiskárny bez chyb způsobených rychlostí čtení a tím udělat celé měření rychlejší. Celý zasílaný kód je 0502000000000001000000. Tento příkaz nastaví čtečku tak, aby sledovala pouze karty MIFARE. Bez tohoto kroku bude čtečka po resetu sledovat všechny typy. Nastavení jiných karet musí být provedeno přepsáním kódu, jenž si najdeme v

TWN4 SimpleProtocol DocRev25.pdf. Po dokončení zápisu je na monitor vypsána zpráva o nastavení typu RFID komunikace. Stejně jako předchozí části spadá do voidloop.

```
Serial1.write('0');
Serial1.write('5');
Serial1.write('0');
Serial1.write('2');

Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');

Serial1.write('0');
Serial1.write('1');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('0');
Serial1.write('\r');
Serial.println(" Typ RFID komunikacenastaven");
```

9.2.2.8 Výběr jména názvu souboru pro uložení dat

Díky for, if a příkazu SD.exist je prohledávána SD karta na soubory s názvem data[i], kde i znázorňuje číslo. Aktuální část programu prohledá kartu a vypíše jaký soubor na kartě není a nastaví ho jako fileName, který je následně v následujících krocích využit pro vytvoření souboru s daným jménem. Program spadá do voidloop.

```
for(inti = 1; i<= 99; i++){
    String fileName = "data" + String(i) + ".txt";

    if(SD.exists(fileName)){
      currentFileName = fileName;
      Serial.println(currentFileName + " Existujena SD karte");
    }else{
```

```
      Serial.println(fileName + " Neexistujena SD karte");
      currentFileName = fileName;
      break;
    }
  }

}
```

9.2.2.9 *Čtení vstupu z 3D tiskárny*

Do SesorVal si za pomocí digitalRead ukládáme hodnotu z pinu 7, který byl již nastaven jako vstupní. Zde je využit datový typ bool, jelikož stačí hodnoty 0,1 nebo LOW, HIGH a také protože digitalRead umí zpracovat pouze tyto hodnoty. Díky tomu, že se na SensorValpřivede hodnotu LOW program rozpozná, že byla čtečka posunuta na další souřadnice a mělo by dojít k pokusu o vyhledání a sečtení RFID tagu. Tato část a celý zbytek programu je již v voidloop, takže pracuje pořád, dokud nedojde k vypnutí nebo restartování arduina.

```
boolSensorVal = digitalRead(7);
```

9.2.2.10 *Přiřazování xyz souřadnic a inicializace switche*

Za pomocí if jsou zde přiřazovány xyz souřadnice pro každý posun a následné přepnutí do switche. Dojde-li k plnému naplnění hodnot a dokončení měření na všech bodech, tak se souřadnice vynulují. Následné měření může probíhat na stejné kartě pro možnou eliminaci chyb a nemusí se tedy vytvářet nový soubor, pokud ale chceme měřit jiný RFID prvek, ať už čtečku nebo tag, tak je nutno restartovat arduino tlačítkem restart na jeho desce.

```
if(SensorVal == LOW){
  if(zcord<= 195){
    if(xswitch<= 13){
      if(yswitch<1){
        if(ycord<195){
        ycord = ycord + 15;
        if(xswitch>=14){
        xswitch = 0;
        xcord = 0;
        ycord = 0;
        yswitch = 0;
        zcord = zcord + 15;
        }
        }
```

```
        elseif(ycord>=195){
          xcord = xcord + 15;
          ycord = ycord + 15;
          yswitch = 2;
          xswitch++;
        };
      };

      if(yswitch>1){
      if(ycord>0){
      ycord = ycord - 15;
      if(xswitch>=14){
        xswitch = 0;
        xcord = 0;
        ycord = 0;
        yswitch = 0;
        zcord = zcord + 15;
      }
      }
      elseif(ycord<=0){
        xcord = xcord + 15;
        yswitch = 0;
        xswitch++;
        if(xswitch>=13){
        xswitch = 0;
        xcord = 0;
        ycord = 0;
        yswitch = 0;
        zcord = zcord + 15;
      }
        }
      }
      }

  }
  elseif(zcord>=180){
      xcord = 0;
      ycord = 0;
      zcord = 0;
      xswitch = 0;
      yswitch = 0;
    }


   N = 1;
}
```

9.2.2.11 Zaslání příkazu na vyhledání RFID tagu

Case 1 switche zasílá kód na čtečku prostřednictvím Serial1. Jedná se o kód pro příkaz SearchTag, který dá příkaz čtečce, aby se pokusila vyhledat RFID tag a následně ho sečíst. Kód je složen ze samotného příkazu 0500 a následného parametru očekávané délky odezvy. Následně dojde k přepnutí do case 2

```
Serial1.write('0');
Serial1.write('5');
Serial1.write('0');
Serial1.write('0');
Serial1.write('f');
Serial1.write('f');
Serial1.write('\r');


N = 2;
```

9.2.2.12 Zapsání příchozích dat do pole

Definuje se pole o délce 32. Následně je skrze while zkontrolováno, zda je čtečka pořád na svém místě nebo se již výstup z tiskárny vypnul a máme přejít k dalšímu měření. Uvnitř tohoto while je vnořený další. Ten kontroluje, zda je komunikace aktivní a jestli něco přichází. Data, které přijdou jsou následně uloženy do pole a místo v poli označeném [i] se zvedne o jedna. Přepne do case 3.

```
charpole[32];
inti = 0;
while(SensorVal == LOW){
  while(Serial1.available()){
    pole[i] = Serial1.read();
    i++;
  }
}
N = 3;
```

9.2.2.13 Zapsání dat na microSD pokud byl RFID tag detekován a odezva

Využitím if podmínky, kde i je hodnota pole z předchozího kroku, která musí být větší než 8. Osm je délka zprávy od čtečky o tom, že žádná karta nebyla zjištěna a načtena. Následně

uzavře pole a dochází ke složení xyz souřadnic a obdržené zprávy z čtečky, která je uložena v poli. Za pomocí SD.open je otevřen nebo při prvním otevření vytvořen txt soubor s fileName, který byl naplněn v void setup části programu a je do něj zapsán náš výsledek. Součástí je také odpověď o úspěšném nebo neúspěšném zapsání a případném nenačtením dat z chybějícího RFID prvku. Ukončení switche pomocí break a následné nulování N, které udává polohu switche. Tímto dojdeme na konec voidloop a program začíná znovu.

```
if(i>8){
        pole[i] = 0;
        String vysledek = String(xcord) + " " + String(ycord) + " " +
String(zcord) + " " + pole;
        File dataFile = SD.open(fileName, FILE_WRITE);
        if(dataFile){
          dataFile.println(vysledek);
          dataFile.close();
          Serial.println(" Data zapsanana SD kartu");
        }else{
          Serial.println(" SD kartaneslaotevrit");
        }
      }else{
        Serial.println(" Data se nenacetlty");
      }
      break;
  }
  N = 0;
```

9.2.3 SW pro zpracování dat Python

Python je vysokoúrovňový programovací jazyk, který je oblíbený pro svou jednoduchou syntaxi, čitelnost a rozsáhlou knihovnu. Jeho syntaxe je přirozená a snadno srozumitelná, což usnadňuje psaní kódu a jeho čtení. Python je také dynamicky typovaný, což znamená, že nemusíte explicitně uvádět typy proměnných. Díky své rozsáhlé knihovně má Python bohaté možnosti v různých oblastech. Můžete využít moduly pro práci se soubory, síťovou komunikaci, databázemi, grafikou, strojovým učením a mnoho dalšího. Tato knihovna usnadňuje vývoj aplikací v Pythonu a umožňuje efektivní využití již hotových funkcionalit. Python je také multiplatformní, což znamená, že můžete psát kód na jednom operačním systému a spouštět ho na jiném. Tímto způsobem je Python velmi flexibilní a snadno použitelný na různých platformách. Další výhodou Pythonu je jeho podpora objektově orientovaného programování, která umožňuje strukturovat kód pomocí objektů a tříd. To

zlepšuje organizaci kódu a usnadňuje jeho správu. Python také umožňuje integraci s jinými jazyky, jako je C/C++, což umožňuje optimalizovat části kódu, které vyžadují vyšší výkon. Díky těmto vlastnostem se Python stal populárním jazykem mezi programátory různých oblastí, včetně webového vývoje, analýzy dat, vědeckých výpočtů a umělé inteligence.[30]

9.2.3.1 Import a aktivace knihoven

Importace knihoven pro práci s numerickými výpočty, vizualizaci dat a manipulaci s geometrickými objekty.[30]

- Numpy je knihovna pro práci s vektorovými a matematickými operacemi v Pythonu.
- matplotlib.pyplot je modul pro vykreslování grafů a vizualizaci dat.
- mpl_toolkits.mplot3d je modul, který rozšiřuje matplotlib o možnost vykreslování 3D grafů.
- scipy.spatial je modul z knihovny scipy, který obsahuje funkce pro práci s prostorovými daty a geometrickými algoritmy, včetně výpočtu konvexní obálky.

```
import numpy as np
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D
fromscipy.spatial import ConvexHull
```

9.2.3.2 Otevření a souboru a uložení souřadnic

Tento kód otevírá soubor, který jsme vytvořili měření v Arduinu pro čtení a postupně načítá řádky ze souboru. Celkově kód čte textový soubor řádek po řádku, zpracovává každý řádek a ukládá jeho souřadnice jako trojice čísel do seznamu points_tmp.[30]

```
file = open("DATA1.TXT")
points_tmp = []
whileTrue:
   point = file.readline()
if point == "\n":
continue
elif len(point) <= 1:
break
coords = point.split(" ")
```

```
points_tmp.append([float(coords[0]), float(coords[1]), float(coords[2])])
```

9.2.3.3 Vykreslení konvexního obalu 3D modelu

Za pomocí použitých knihoven a extrahovaných dat z txt souboru je vytvořen 3D model, který má viditelné body a hrany. Model je možný otáčet, přibližovat, uložit pohled nebo najetím kurzoru myši vypsat přesný bod. [30]

```
points = np.array(points_tmp)


hull = ConvexHull(points)

fig = plt.figure()
ax = fig.add_subplot(111, projection="3d")

# Plot definingcornerpoints
ax.plot(points.T[0], points.T[1], points.T[2], "ko")

for s in hull.simplices:
    s = np.append(s, s[0])  # Herewecycleback to thefirstcoordinate
ax.plot(points[s, 0], points[s, 1], points[s, 2], "r-")
```

9.2.3.4 Popis 3D modelu a příprava zápisu do .obj souboru

Vytvoří popisy os pro konvexní 3D model. Dále zde dojde k přípravě na vytvoření .obj souboru, který nám umožní následně v Blenderu udělat plný 3D model. [30]

```
# Make axis label
for i in ["x", "y", "z"]:
eval("ax.set_{:s}label('{:s}')".format(i, i))

obj = open("model.obj", "w")
obj.write("o Model\n")

vertices = {}
```

9.2.3.5 Zápis vrcholů

Tento kód slouží k zápisu vrcholů 3D modelu do souboru "model.obj" a jejich přiřazení k indexům. Celkově kód zapisuje vrcholy 3D modelu do souboru "model.obj" a přiřazuje jim indexy pro pozdější použití. [30]

```
for i, v in enumerate(hull.vertices):
vertices[v] = i
   vertex = points[v]
obj.write("v {x:.6f} {y:.6f} {z:.6f}\n".format(x=vertex[0], y=vertex[1], z=vertex[2]))
```

9.2.3.6 Kompletace .obj souboru

Kód Zápisu informací o normálách a texturovacích souřadnicích vrcholů a plošek 3D modelu do souboru "model.obj".Celkově kód zapisuje informace o normálách, texturovacích souřadnicích a ploškách 3D modelu do souboru "model.obj". Poté zobrazuje grafické zobrazení modelu pomocí plt.show(). [30]

```
obj.write("vn 0.0000 1.0000 0.0000\n")
obj.write("vt 0.000000 0.000000\n")

for f in hull.simplices:
obj.write("f {x}/1/1 {y}/1/1 {z}/1/1\n".format(x=vertices[f[0]]+1, y=vertices[f[1]]+1,
z=vertices[f[2]]+1))
plt.show()
```

9.2.4 SW pro grafické vyhodnocení datBlender

Blender je software pro tvorbu 3D grafiky, který je zdarma dostupný a nabízí široké možnosti vytváření a renderování 3D modelů, animací, vizuálních efektů a virtuální reality. Tento program je kompatibilní s různými operačními systémy a poskytuje uživatelům různé nástroje pro tvorbu a úpravu 3D modelů.Blender má mnoho funkcí, mezi které patří modelování, kde lze vytvářet a upravovat geometrické tvary a používat různé nástroje pro editaci. Dále poskytuje možnosti nastavení materiálů a textur pro objekty, aby vypadaly přirozeně. Blender také umožňuje animovat objekty a provádět pokročilé animace pomocí klíčových snímků a pohybových drah.Blender je také rozšiřitelný a podporuje skriptování pomocí jazyka Python. To umožňuje uživatelům vytvářet vlastní nástroje, automatizovat úkoly a rozšířit funkcionality programu.Blender je využíván ve filmovém průmyslu, herním vývoji, reklamě, designu a mnoha dalších oblastech, díky svému výkonnému a rozsáhlému souboru funkcí pro tvorbu 3D grafiky.

10 DOSAŽENÉ PARAMETRY VÝSLEDKY

Výhodou použití Pythonu a Blenderu v našem projektu bylo, že jsme byli schopni efektivně zpracovat naměřená data uložená na microSD kartě a vizualizovat je graficky.

Díky programovacímu jazyku Python jsme mohli snadno načíst data z microSD karty a provést potřebné výpočty a analýzy. Python je mocný a flexibilní jazyk, který nám umožnil efektivně zpracovat velké množství dat a provádět různé statistické výpočty, filtraci nebo úpravy dat podle potřeb.

Blender, jako 3D grafický software, nám poskytl možnost vizualizovat naměřená data ve formě 3D modelů. S pomocí Blenderu jsme byli schopni vytvořit detailní a realistické vizualizace na základě dat. Měli jsme možnost vytvořit 3D modely na základě naměřených hodnot. Díky tomu jsme mohli získat vizuální přehled o výsledcích měření a identifikovat případné vzorce nebo anomálie.

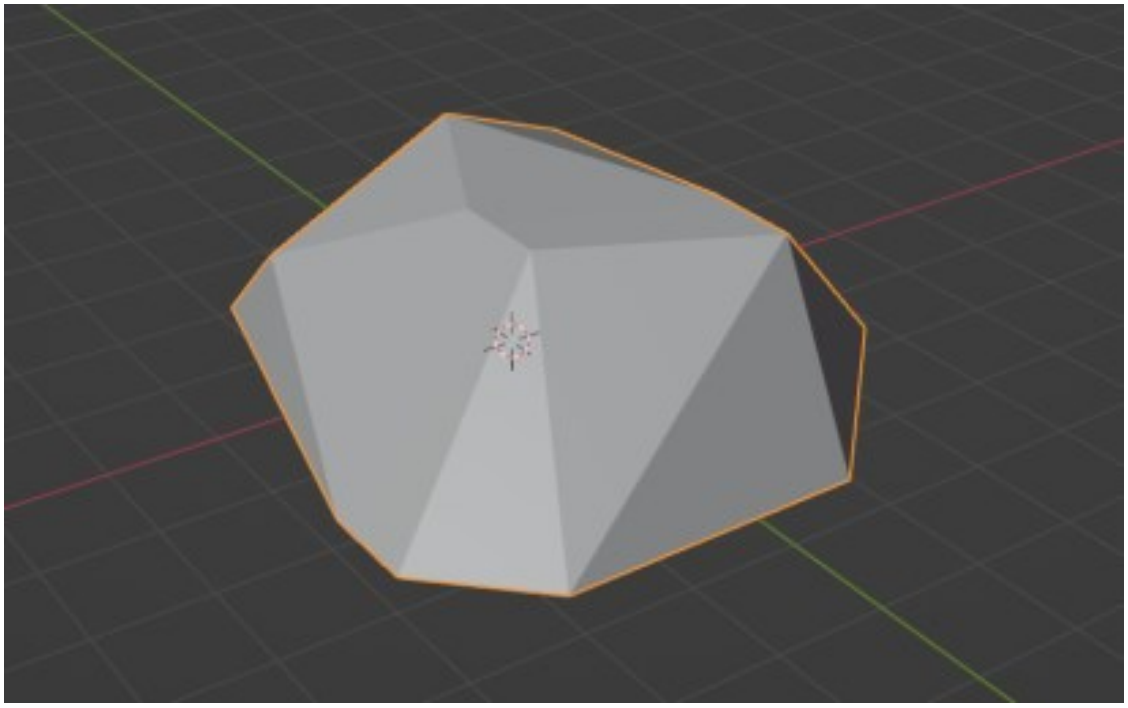
10.1 Průběh měření

Měření bylo prováděno se čtečkami ASSET602, ASSET603 a RFID tagy MIFARE DESFire ve formě karty a klíčenky. Postup měření:

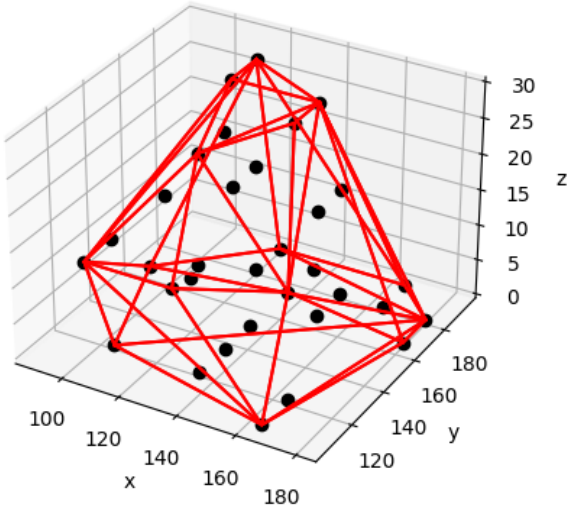
- Zapojení Arduina se všemi přídavnými moduly
- Umístění čtečky RFID prvků na hlavu tiskárny
- Zapojení čtečky a tiskárny do sítě
- Připojení arduina k PC pro napájení
- Propojení rs-232 modulu se čtečkou
- Připojení výstupu tiskárny na relé
- Umístění tagu na vyhrazené místo na podložce pro možnost replikace měření
- Spuštění programu tiskárny
- Počkání na doběhnutí programu
- Výměna RFID prvku nebo čtečky
- Restart arduina
- Zapnutí programu tiskárny.

10.2 ASSET603 karta

Naměřená data viz 603karta.TXT, viz 603karta.obj . Z naměřených dat vyplývá mnohostěn protáhlý po délce směrem, kterým vede kartou anténa. Jde vidět, že na vrcholu je zploštělý, a tudíž snížením posunu kroku tiskárny by šlo dosáhnout detailnějšího měření a objekt by se poté přibližoval protáhlé polokouli.



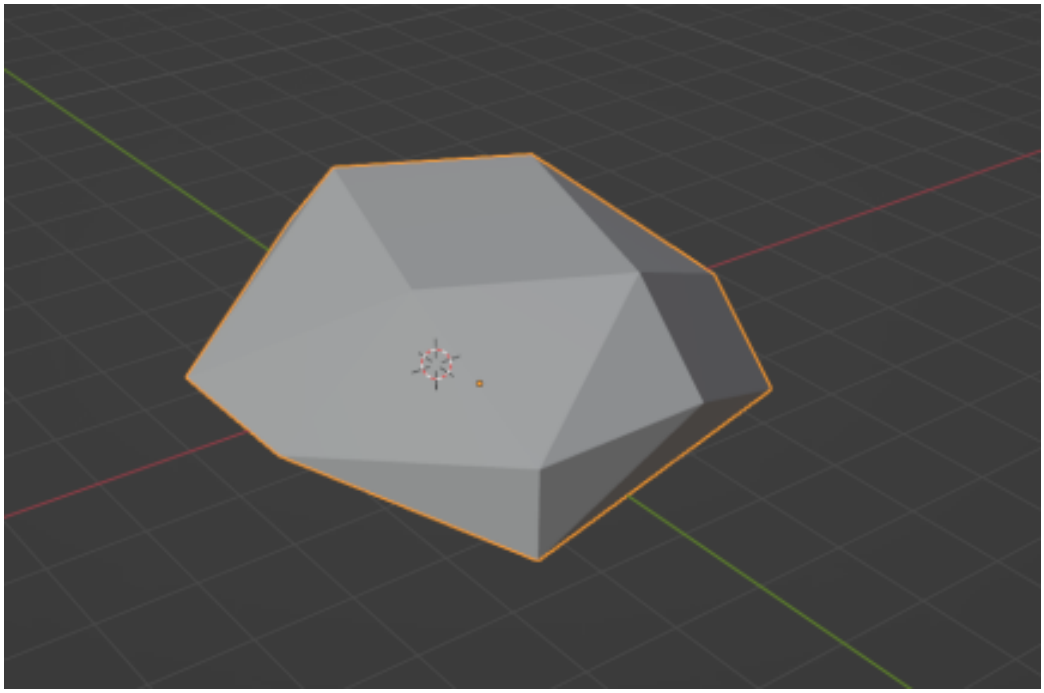
Obrázek 11 3D model ASSET603 karta [Vlastní]



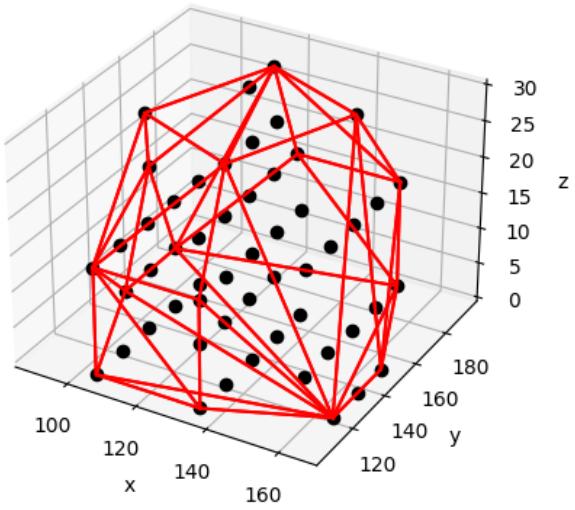
Obrázek 12 kostra 3D modelu ASSET603 karta [Vlastní]

10.3 ASSET602 karta

Naměřená data viz602karta.TXT, 602karta.obj.Z naměřených dat lze vypozorovat objekt tvarem připomínajícím protáhlou polokouli po délce antény RFID karty. Stejně jako u měření ASSET603 karty jde vidět zploštělý vrchol, tudíž by měření opět mohlo být přesnější. Měření čtečkou ASSET602 dosáhlo detekce na více bodech dle očekávání. Čtečka je větší, tudíž má lepší detekční vlastnosti.



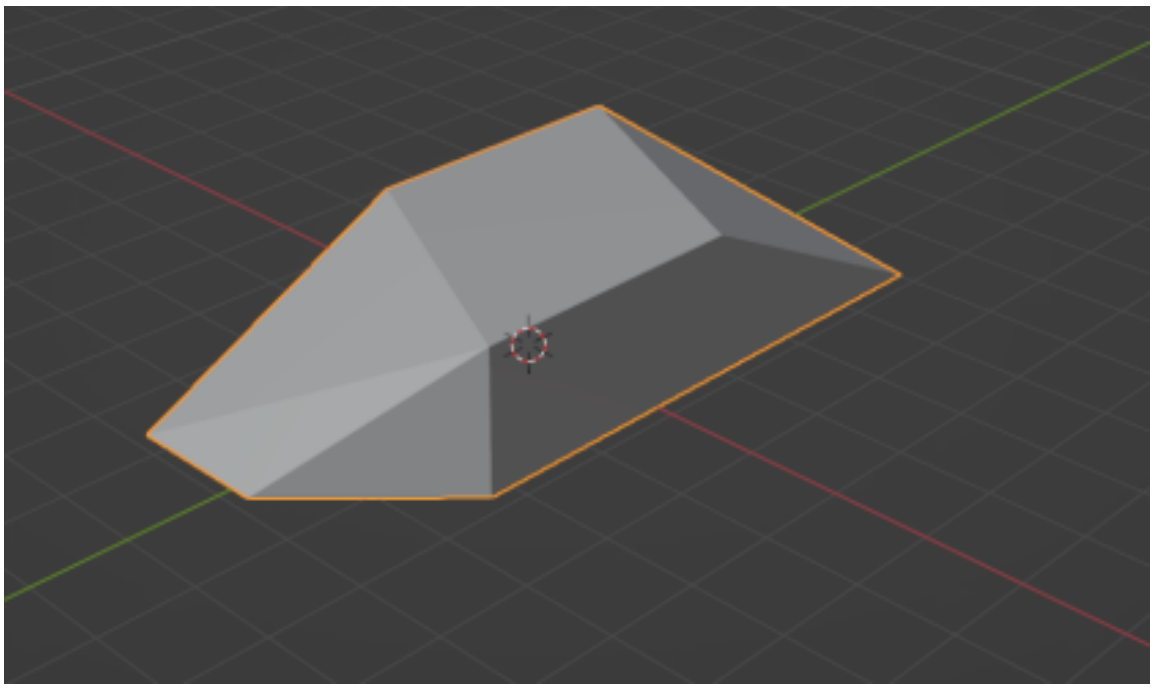
Obrázek 13 3D model ASSET602 karta [Vlastní]



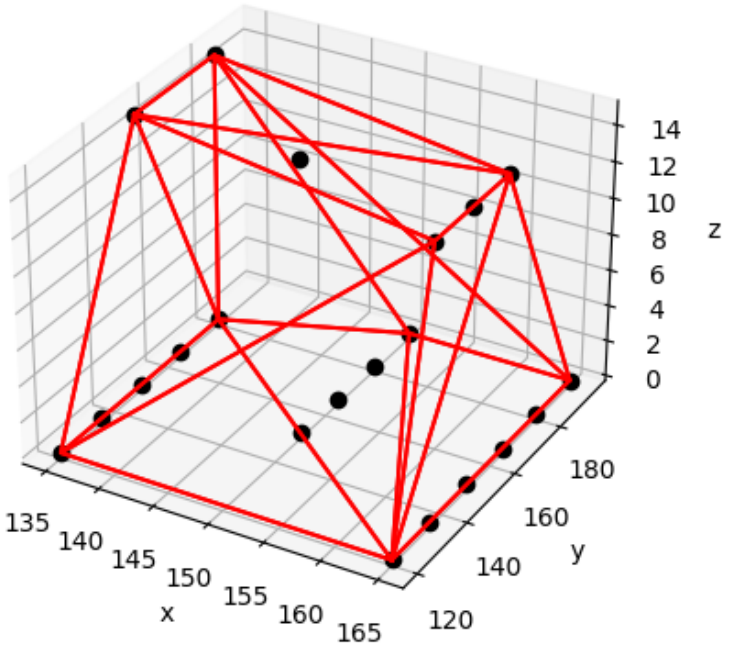
Obrázek 14 kostra 3D modelu ASSET602 karta [Vlastní]

10.4 ASSET603 klíčenka

Naměřená data viz 603klíčenka.TXT, viz 603klíčenka.obj. Naměřená a vyhodnocená data zobrazují protáhlý mnohostran, který svými rozměry odpovídá očekávanému výsledku oproti kartě.



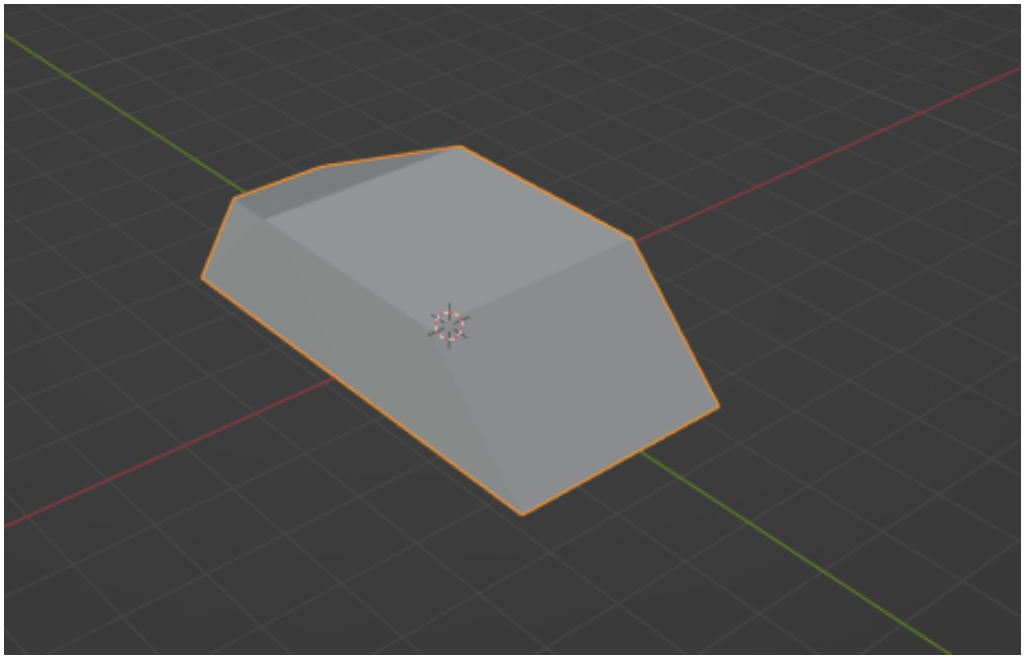
Obrázek 15 3D model ASSET603 klíčenka [Vlastní]



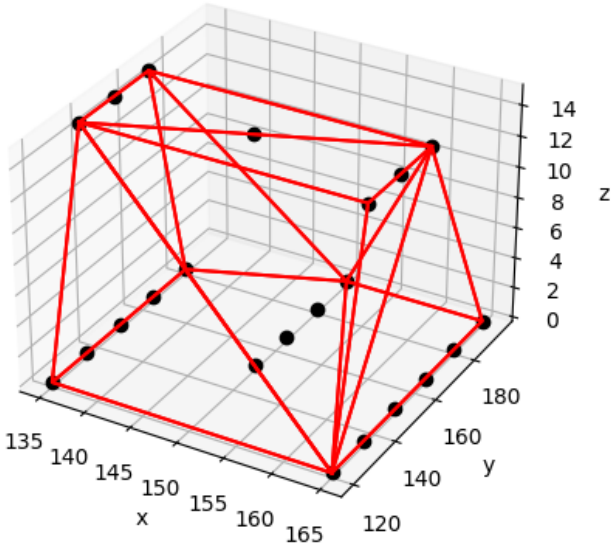
Obrázek 16 kostra 3D modelu ASSET603 klíčenka [Vlastní]

10.5 ASSET602 klíčenka

Naměřená data 602klíčenka.TXT, 602klíčenka.obj Vyobrazený model je podobný jako u měření klíčenky čtečkou ASSET603, ale opět dle očekávání je o pár bodů větší. Čtečka detekovala RFID tag v bodech, kde předchozí čtečkajiž nebyla detekce schopná.



Obrázek 17 3D model ASSET602 klíčenka [Vlastní]



Obrázek 18 kostra 3D modelu ASSET602 klíčenka [Vlastní]

10.6 Vyhodnocení a porovnání výsledků

Z naměřených a vizuálně vyobrazených hodnot je možné provést vyhodnocení a porovnání výsledků. Porovnáním obrázku Obrázek 14 s Obrázek 18 a také obrázky Obrázek 12

s Obrázek 15. Můžeme říci že klíčenka má podstatně menší detekční pole a musí být přítomna mnohem blíže středu čtečky RFID prvků. Zde můžeme vidět vliv velikosti antény RFID tagu, kde kartas větší anténou má daleko větší pole kde je možné kartu detekovat oproti klíčence. Také lze vypozorovat z obrázků že měřená klíčenka má střed pole detekovaných bodů posunutý oproti kartě, ačkoliv byli oba tagy usazeny na stejnou pozici.

Porovnáním Obrázek 14 a Obrázek 16vidíme menší počet bodů detekovaných čtečkou ASSET603 Také zde jde vidět že vykreslený drátový 3D objekt ze čtečky ASSET602 je větší a a více připomíná polokouli.

Z porovnání Obrázek 18 a Obrázek 16můžem vypozorovat že u měření z ASSET603 nám detekční pole na jedné straně klesá dříve než u druhé čtečky.

ZÁVĚR

Cílem této práce bylo vytvořit automatizovaný tester RFID čteček. Práce byla rozdělena na teoretickou a praktickou část. Teoretická část obsahuje rešerši RFID technologií, vysvětlení pojmů a prvků využívaných v této technologii. Popisuje aplikaci RFID v přístupových systémech a vliv rozměru antény v RFID prvcích na jejich dosah čtení. Poslední kapitola teoretické části se zabývá technologií NFC, která je budoucností vývoje RFID. Druhá praktická část obsahuje výběr vhodného mechanismu pro automatizovaný tester RFID čteček. Provedení měření čtecích vzdáleností, návrh a realizace vizualizace a porovnání výsledků a jejich zhodnocení. Tímto byly pokryty zásady pro vypracování.

Vývoj automatického testeru začínal výběrem ideálního mikropočítače pro sledování celé operace. Zpočátku byl vybrán mikropočítač Arduino UNO, který splňoval minimální potřebné parametry pro realizaci plánu automatizace. Využil jsem znalosti arduina, se kterým jsem již dříve pracoval. Po měsíci práce jsem však narazil na problém SW komunikace skrze umělou sběrnici arduina. Ačkoliv podle dokumentace měla zvládat komunikaci se čtečkou, jelikož nedocházelo k přímému současnému přenášení dat ve formě zápisu a čtení, tak arduino nebylo schopné fungovat spolehlivě během předávání dat. Z toho důvodu jsem byl nucenvyměnit mikropočítačArduino UNO za alternativní a výkonnější model Arduina Mega 2560. Na tomto mikropočítači jsem již práci dokončil, vyladil kód i zapojení a provedl všechny měření. Výsledky poté musely být zpracovány a jako ideální program byl zvolen Python, ve kterém byl z txt souboru s xyz souřadnicemi vytvořen obj soubor. Obj soubor byl následně nahrán do Blenderu, kde z něj byl vygenerován 3D model, který byl následně porovnán a analyzován.

SEZNAM POUŽITÉ LITERATURY

[1] WANT, Roy. An introduction to RFID technology. IEEE pervasivecomputing, 2006, 5.1: 25-33.(hned první)

[2] LANDT, Jeremy. Thehistoryof RFID. IEEE potentials, 2005, 24.4: 8-11. (historie)

[3] NATH, Badri; REYNOLDS, Franklin; WANT, Roy. RFID technology and applications. IEEE Pervasivecomputing, 2006, 5.1: 22-24. (užitíú

[4] RADIOM, Soheil; VANDENBOSCH, Guy; GIELEN, Georges. Impactofantenna type and scaling on scavengedvoltage in passive RFID tags. In: 2008 International Workshop on Antenna Technology: SmallAntennas and Novel Metamaterials. IEEE, 2008. p. 442-445.

[5] WĘGLARSKI, Mariusz, et al. DesigningAntennasfor RFID Sensors in Monitoring ParametersofPhotovoltaicPanels. Micromachines, 2020, 11.4: 420.

[6] Thornton, F.; Haines, B.; M.Das, A.; aj.: RFID Security. SyngressPublishing, 2006, ISBN 1-59749-047-4.

[7] BEZPEČNOST TECHNOLOGIE RFID [online]. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, 2013 [cit. 2022-12-16]. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/52700/final-thesis.pdf?sequence=-1&isAllowed=y. Diplomová práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ.

[8] Finkenzeller, K.: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. Wiley, 2003, ISBN 0-470-84402-7.

[9] RADIOM, Soheil; VANDENBOSCH, Guy; GIELEN, Georges. Impactofantenna type and scaling on scavengedvoltage in passive RFID tags. In: 2008 International Workshop on Antenna Technology: SmallAntennas and Novel Metamaterials. IEEE, 2008. p. 442-445.

[10] MARROCCO, Gaetano. The art of UHF RFID antenna design: Impedance-matching and size-reductiontechniques. IEEE antennas and propagationmagazine, 2008, 50.1: 66-79.

[11] DAGAN, Hadar, et al. A low-cost low-power non-volatilememoryfor RFID applications. In: 2012 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2012. p. 1827-1830.

[12] FAROOQ, Umar, et al. RFID basedsecurity and accesscontrolsystem. International JournalofEngineering and Technology, 2014, 6.4: 309.

[13] RAVI, K. Srinivasa, et al. RFID basedsecuritysystem. internationaljournalofinnovative technology and exploringengineering (IJITEE), 2013, 2.5: 132-134.

[14] KNOSPE, Heiko; POHL, Hartmut. RFID security. Informationsecuritytechnical report, 2004, 9.4: 39-50.

[15] HOLENDA, M.; VANĚK, T.; ROHLÍK, M. Klonování RFID čipů na přístupových kartách.

[16] FELDHOFER, Martin; DOMINIKUS, Sandra; WOLKERSTORFER, Johannes. Strongauthenticationfor RFID systemsusingthe AES algorithm. In: Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6. SpringerBerlin Heidelberg, 2004. p. 357-370.

[17] VAVERKA, Aleš; ZEMAN, DOC ING VÁCLAV. Digitální podpis. 2008.

[18] IVANKOVIĆ, Marko, et al. Codecoverageat Google. In: Proceedingsofthe 2019 27th ACM Joint Meeting on European Software EngineeringConference and Symposium on theFoundationsof Software Engineering. 2019. p. 955-963.

[19] Security and Privacy in RFID Systems [online]. UNIVERSITY OF WOLLONGONG, 2015 [cit. 2022-12-02]. Dostupné z: https://ro.uow.edu.au/theses/4481/. Disertační práce. UNIVERSITY OF WOLLONGONG.

[20] Flexible Absorbent Material (FAM). Https://www.cfe.com.tw/2-absorber/crown-ferrite-absorber-flexible-absorbent-material-fam.pdf [online]. [cit. 2022-11-21]. Dostupné z: https://www.cfe.com.tw/2-bsorber/crown-ferrite-absorber-flexible-absorbent-material-fam.pdf

[21] MADLMAYR, Gerald, et al. NFC devices: Security and privacy. In: 2008 Third International Conference on Availability, Reliability and Security. IEEE, 2008. p. 642-647.

[22] COSKUN, Vedat; OZDENIZCI, Busra; OK, Kerem. A survey on nearfieldcommunication (NFC) technology. Wirelesspersonalcommunications, 2013, 71: 2259-2294.

[23] CHEN, ChengHao; LIN, IuonChang; YANG, ChouChen. NFC attacksanalysis and survey. In: 2014 eighthinternationalconference on innovative mobile and internet services in ubiquitouscomputing. IEEE, 2014. p. 458-462.

[24] Arduino.cc [online]. Italy: © 2023 Arduino, 2023 [cit. 2023-05-06]. Dostupné z: https://www.arduino.cc

[25] MAX3232 3-V to 5.5-V Multichannel RS-232 Line Driver/ReceiverWith ±15-kV ESD Protection. Https://www.hadex.cz [online]. Kosmova 1090/11, 702 00 Ostrava, Přívoz: H A D E X , spol. s r.o., 2017 [cit. 2023-06-05]. Dostupné z: https://www.hadex.cz/spec/m438b.pdf

[26] Copyright 2023 LaskaKit. Laskakit.cz [online]. Rychnov nad Kněžnou 144, 516 01: Laskit, 2023, 2023 [cit. 2023-04-24]. Dostupné z: https://www.laskakit.cz/prevodnik-ttl-na-rs232--max3232/

[27] PANASONIC CORP. (TQ2SA-12V) RELAY. Https://octopart.com [online]. Kadoma, 571-8501, Japonsko: © COPYRIGHT Matsushita Electric Works, 2022 [cit. 2023-06-05]. Dostupné z: https://datasheet.octopart.com/TQ2SA-12V-Panasonic-datasheet-10392044.pdf

[28] 3D Printer Mega Zero 220* 220*250. Botland.cz [online]. ul. Vratimovská 681/80 71900 Ostrava – Kunčice Česká republika: © Copyright 2023 botland, 2021 [cit. 2023-06-05]. Dostupné z: https://botland.cz/stazene-produkty/18365-3d-tiskarna-anycubic-mega-zero-0715235125113.html

[29] Marlinfw [online]. Pool Cottage Hengoed, Oswestry, Shropshire, SY10 7EU, United Kingdom: Marlinfw, 2023 [cit. 2023-06-05]. Dostupné z: https://marlinfw.org/meta/gcode/

[30] Python [online]. 512 LafayetteBoulevard, Suite 2, Fredericksburg, Virginia 22401.: Copyright ©2001-2023 Python Software Foundation, 2023 [cit. 2023-05-06]. Dostupné z: https://www.python.org

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

RFID RadioFrequencyIdentification

NFC Nearfieldcommunication

FAM Flexible Absorbent Material

IoT Internet ofThings

HW hardware

FW firmware

SW software

LF lowfrequency

HF highfrequency

PWM Pulse WidthModulation

DF Duální frekvence

UHF Ultra vysoká frekvence

SE SecureElements

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOHY