

Факултет инжењерских наука Универзитета у Крагујевцу



Назив студијског програма: Рачунарска техника и софтверско инжењерство

Ниво студија: Основне академске студије

Модул: /

Предмет: Аутоматско управљање

Број индекса: 575/2016

Марко Н. Милорадовић

Реализација сигурносног система на Ардуино платформи

Дипломски рад

Комисија за преглед и одбрану:

1. Др Маријана Гавриловић Божовић, доцент- ментор

2. _____

Датум одбране: _____

3. _____

Оцена: _____

У оквиру овог завршног рада кандидат треба да:

- размотри постојеће сигурносне системе са аспекта сензора и контролера,
- креира сигурносни систем коришћењем одговарајућих сензора,
- реализује контролер на Ардуино платформи,
- анализира креирани сигурносни систем и прикаже критички осврт на предности и мане реализованог уређаја.

Препоручена литература:

- [1] Благојевић, М. *Алармни системи*. Факултет заштите на раду у Нишу, 2015.
- [2] T. Rustige, *Home Security Projects for Arduino*, TR Computers Limited, 2015
- [3] International electrotechnical commission (IEC). *IEC 62642-1:2010 Alarm systems - Intrusion and hold-up systems - Part 1: System requirements*. IEC, Geneva, 2010.
- [4] Smyth N. *Android Studio 3.0 Development Essentials – Android 8 Edition*. Payload Media, Inc., 2017

Крагујевац, 11.03.2020. год.

Ментор:

др Маријана Гавриловић Божовић, доцент

РЕЗИМЕ

У оквиру дипломског рада реализован је сигурносни систем на Ардуино платформи. Најпре су размотрени постојећи сигурносни системи са аспекта сензора и контролера. Затим је креиран сигурносни систем на Ардуино платформи, уз коришћење ултразвучног сензора покрета и капацитивног сензора додира. За управљање је коришћена мобилна апликација са преносом информација ка кориснику преко *Bluetooth* технологије. На крају је извршена анализа креираног сигурносног система са аспекта потенцијалних предности и мана.

Кључне речи: сигурносни систем, Ардуино, сензор, контролер, *Bluetooth*

ABSTRACT

As part of the thesis, a security system was implemented on the Arduino platform. First, the existing security systems were considered from the aspect of implemented sensors and controllers. A security system was then created on the Arduino platform, using an ultrasonic motion sensor and a capacitive touch sensor. A mobile application with information transfer to the user via Bluetooth technology was used for management. Finally, an analysis of the created security system from the aspect of potential advantages and disadvantages was performed.

Keywords: security system, Arduino, sensor, controller, *Bluetooth*

САДРЖАЈ

1. УВОД.....	1
2. СИГУРНОСНИ СИСТЕМИ.....	3
2.1 ВРСТЕ СИГУРНОСНИХ СИСТЕМА	4
2.2 СТРУКТУРА СИГУРНОСНИХ СИСТЕМА.....	6
2.3 СЕНЗОРИ У СИГУРНОСНИМ СИСТЕМИМА	10
2.3.1 Детектори провале.....	11
2.3.2 Алармни контакти	12
2.3.3 Детекција лома стакла	14
2.3.4 Детекција покрета	15
2.3.5 Заштита периметра.....	17
2.3.6 Видео надзор.....	21
3. КРЕИРАЊЕ СИГУРНОСНОГ СИСТЕМА.....	23
3.1 ANDROID STUDIO.....	24
3.2 ARDUINO SOFTWARE (IDE)	27
3.3 ARDUINO UNO R3 ПЛОЧА	28
3.4 BLUETOOTH МОДУЛ HC-05.....	32
3.5 PIEZZO BUZZER	35
3.6 УЛТРАЗВУЧНИ СЕНЗОР РАСТОЈАЊА HC-SR04	36
3.7 СЕНЗОР ДОДИРА ТТР223В	38
3.8 ПРОТОТИПСКА ПЛОЧА.....	40
3.9 ЖИЦЕ ЗА ВЕЗУ	40
4. РЕАЛИЗАЦИЈА КОНТРОЛЕРА СИГУРНОСНОГ СИСТЕМА ЗА АРДУИНО ПЛАТФОРМУ .	41
4.1 КРИТИЧКИ ОСВРТ НА ПРЕДНОСТИ И МАНЕ РЕАЛИЗОВАНОГ УРЕЂАЈА	54
5. ЗАКЉУЧАК.....	55
6. ЛИТЕРАТУРА.....	56

1. УВОД

Сигурносни системи су системи који раде у реалном времену и припадају групи мерно-информационих система. Као мреже електронских уређаја са централним процесором, они садрже средства или методе за заштиту против оштећења (рецимо, системи за дојаву пожара) и крађе (системи за дојаву провале).

Кућни сигурносни системи појавили су се пре много година. Људи су, прво, користили гране, камење, оружја као што су праћке и лукови да би се заштитили од дивљих животиња. Касније су се појавили пси чувари, као наследници спасених младунчади вукова које су одгајили људи. У старом Египту су грађени ровови око градова и тврђава испуњени водом ради заштите од уљеза.

После завршетка Првог светског рата, порасла је стопа криминала, па су људи тражили начине да заштите себе и своју имовину. Многи власници кућа су се претплатили на услуге групе ноћних чувара који су проверавали сваке ноћи да ли су врата на кућама закључана [1]. Богатији људи су купили алармне системе који су се састојали од електромагнетних контаката постављених на врата и прозоре. Док је алармни систем био укључен, свако отварање врата или прозора изазивало би укључење аларма, а централна станица за надгледање ових система би слала чувара до куће где се аларм укључио.

Технологија видео надзора је развијена још 1940-их година, али се за кућне потребе употребљавала тек од 1970-их година. Први кућни сигурносни систем са даљински контролисаним вратима откривен је 1966. године [1] и састојао се од четири рупице на улазним вратима и моторизоване камере која је могла да се креће горе-доле и гледа кроз рупице. Контролни панел се налазио у соби у којој није била камера и имао је интерком за контакт са посетиоцима, прекидач за закључавање врата и дугме за активацију аларма. Иако је овај систем био превасходно намењен за кућну употребу, његова ефикасност је привукла и пословне кориснике.

Значај употребе сигурносних система може се сагледати и преко неких статистичких показатеља које је обрадио амерички FBI 2018. године. Годишње се у САД деси скоро 1,6 милиона провала (једна сваких 20 s). Око 72% свих провала пријављених 2015. године у САД биле се извршене у становима. Око 58% свих провала су укључивале насилан упад на посед. Најчешће коришћен метод уласка у стан је путем оштећења, уклањања или уништавања врата. Провалници улазе преко отворених или откључаних врата или прозора у више од половине свих провала у празним становима [2].

Статистички подаци подвлаче важност поседовања одговарајућег сигурносног система. Зато се кућни сигурносни системи непрестано развијају са развојем технологије и представљају потенцијални фокус будућих система аутоматизације. Њихове нове електронске технологије се интегришу са традиционалним технологијама грађевинарства, тако да тзв. „паметне куће“ убрзано постају реалност. То се постиже укључивањем бројних подсистема у сигурносни систем са јединственом контролном

јединицом, као што су подсистеми за надгледање, заштиту од провале, контролу приступа, итд. Кућни сигурносни систем заснован на Интернету или *Bluetooth* конекцији, фокусира се на управљање и контролу сигурносних уређаја, било да је власник у кући, или изван ње.

Немогућност приступа и управљања сигурносним системом са удаљене локације један је од главних разлога недостатка сигурности против провалника и незгодних инцидената као што су појава пожара, као и нелагодности при напуштању стана. Ови проблеми често воде до губитка материјалних ствари, имовине, па чак и губитка људских живота. То се може зауставити применом технологија које боље управљају сигурносним уређајима. Један од начина је коришћење електронске платформе отвореног кода као што је Ардуино [3].

У овом дипломском раду, после разматрања постојећих сигурносних система са аспекта сензора и контролера, креиран је сигурносни систем са контролером за Ардуино платформу. Креирани сигурносни систем је критички анализиран и дат је осврт на његове предности и мане.

2. СИГУРНОСНИ СИСТЕМИ

Сигурносни системи подразумевају коришћење различитих средстава, уређаја и, понекад, људске силе, да би се заштитили појединци и имовина од различитих ризика, као што су пожар, криминал и губитак.

Системи за заштиту од провале спадају у класу мерно-информационих система који раде у реалном времену. Они такође спадају у системе за прикупљање података који се срећу у свакодневном животу, почев од малих система у продавницама, до система у великим комплексима, где чине само један сегмент у комплексном сигурносном окружењу. Важећи стандарди у нашој земљи који се баве овом врстом сигурносних система су SRPS стандарди серије:

- **SRPS EN 50130**, који се баве проблематиком електромагнетне компатибилности алармних система и методама испитивања утицаја на животну средину,
- **SRPS EN 50131**, који се баве противпровалним и противпрепадним системима са аспеката:
 - ✓ захтева за систем,
 - ✓ захтева за противпровалне детекторе,
 - ✓ контаката за детекцију отварања (магнетских),
 - ✓ опреме за контролу и индикацију,
 - ✓ уређаја за упозорење,
 - ✓ напајања,
 - ✓ сигурносних уређаја/система за маглу,
 - ✓ смерница за примену,
 - ✓ противпрепадних уређаја,
 - ✓ испитивања компатибилности система у надгледаним просторијама за опрему у противпровалним и противпрепадним алармним системима,
 - ✓ верификације аларма - метода и принципа,
 - ✓ примене специфичних захтева за надгледање простора примопредајника,
 - ✓ метода и захтева за активирање и деактивирање противпровалних алармних система и
 - ✓ противпровалних система - ALDDR,
- **SRPS EN 50134**, који се баве друштвеним алармним системима и алармним системима за социјалне потребе и
- **SRPS EN 50136**, који се баве системима и опремом за пренос алармних сигнала.

Главна тема овог дипломског рада су сигурносни системи за заштиту од провале (противпровални алармни системи), који се могу применити у заштити станова, предузећа, банака, аутомобила и многих других објеката код којих је потребно заштити људство и имовину од уништавања и крађе. Основни захтеви према сигурносним системима за заштиту од провале су следећи [4]:

- откривање покушаја неовлашћеног улаза и генерисање информација о неовлашћеном приступу,
- предаја информације о неисправности и отказу компонената система,
- очување исправног рада система у односу на утицај окружења и успостављање нормалног стања рада после дејства фактора окружења,
- задржавање нивоа поузданости у односу на покушаје диверзије било ког дела система, без могућности настајања индиректне опасности ван система,
- очување функционалног стања система у случају губитка мрежног напајања, или другог основног извора напајања,
- систем не сме да генерише лажне аларме при пребацивању напајања са мрежног на резервно напајање, или са било ког облика напајања на други и
- аутоматски системи за заштиту од провале морају да обезбеде идентификацију лица или њихових лозинки при уласку у штићени објект.

2.1 Врсте сигурносних система

Расположиви сигурносни системи могу се класификовати на различите начине који се често међусобно преклапају. Међутим, пошто је већина расположивих сигурносних система фокусирана на заштиту од специфичног ризика, веома је битно направити разлику између разних типова сигурносних система. Неки од уобичајених сигурносних система су:

- **Кућни сигурносни системи.** Покривају различите аспекте кућне безбедности. Међу најједноставнијим, а у исто време ефикасним кућним сигурносним системима су браве, прозори са решеткама, браве и др. Задњих година, ови системи су удружени са технолошки напредном и софистицираном опремом, као што су, на пример: системи за дојаву пожара, детектори угљен-диоксида, детектори покрета и спољно светло. Апартмански комплекси често користе видео надзор улаза, ходника и лифтова, као и службу обезбеђења. Суседства већих градова могу запослити патролне службе, или организовати добровољне стамбене патроле.
- **Комерцијални сигурносни системи.** Фирме су осетљиве на исте ризике као и приватни станови, али су у ризику и од индустријске шпијунаже, унутрашње крађе, незгода и повреда на раду, итд. Њихови сигурносни системи укључују коришћење софистицираније технологије и опреме, као што су аутоматски системи контроле приступа, аларми „на дугме“, читачи картица, као и тренирано обезбеђење из поузданих фирми. Специјална категорија су сигурносни системи намењени мањим предузећима која не могу да приуште софистицирану технологију - неки од тих система су на нивоу кућних сигурносних система, што међутим не значи да су инфериорнији у односу на системе великих компанија.

- **Сигурносни системи рачунара.** Баве се обезбеђењем информација које се налазе у рачунарима. Главни циљ им је спречавање крађе и губитка информација уз омогућавање лаког приступа информацијама. Већина сигурносних система рачунара користе специјално дизајниране програме који нуде заштиту од физичких и виртуалних упада у систем рачунара. Пошто је сваки сигурносни систем типично дизајниран да пружи заштиту од специфичне претње, често се користи више сигурносних система на рачунару.
- **Системи за дојаву пожара.** И у стамбеним и у комерцијалним окружењима користе се уређаји који детектују дим и упозоравају људе у згради на претњу од пожара. Неки уређаји укључују системе за гашење пожара који даље смањују ризик од оштећења од пожара и људских жртава.
- **Системи за личну заштиту.** Намењени су повећању личне безбедности тако што помажу појединцима да избегну потенцијално опасне ситуације и да се одбране уколико буду физички нападнути. Примери укључују личне аларме, спрејеве за самоодбрану, локаторе за децу и др. Појединце који имају профил високог ризика са вероватноћом да постану жртве киднаповања, напада, атентата, или других криминалних радњи, обично су штићени од стране више телохранитеља.

Према начину преноса информација постоје три врсте сигурносних система за заштиту од провале [5]:

- аутономни системи типа „паметна кућа“,
- жичани системи и
- бежични системи.

Сигурносни систем типа „паметна кућа“ има интегрисану инсталацију која не укључује само примитивни алармни систем за приватну кућу. У овом случају, више система је комбиновано у један, односно сигурносна функција је у комбинацији са аутономном контролом свих уређаја у кући. Зависно од сложености, ови системи могу имати видео камере, сензоре покрета и контроле за уређаје за гас и воду и користити различите методе упозорења када се догоди одређена неугодна ситуација. Ови системи су потпуно аутономни. Једини недостатак су превисоки трошкови самог система и трошкови плаћања услуга фирме за сигурносне системе.

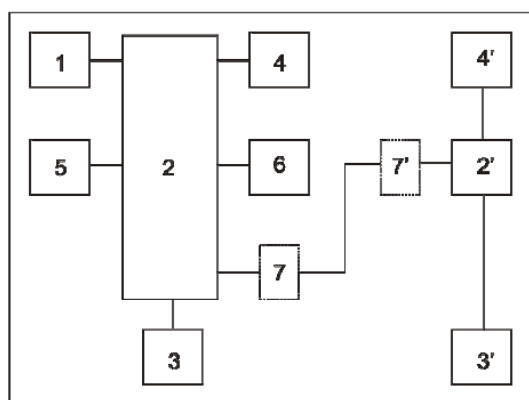
Жичани сигурносни системи за приватну кућу су најлакши и најјефтинији. Њихове предности су што се сензори који се користе у систему не морају стално мењати или пунити батерије. У случају нестанка струје, мора се осигурати уградња посебне јединице за непрекидно напајање. Сви сензори и камере се могу комбиновати у један систем, али све зависи од потреба власника куће.

Коришћење жица за повезивање елемената сигурносних система може да проузрокује тешкоће у смислу додатних трошкова за санацију зидова услед уградње каблова. Зато многи власници кућа користе **бежичне сигурносне системе** за приватне куће и канцеларије. Сви сензори или камере су спојени на управљачку јединицу преко *Wi-Fi* везе, или на одређеној радио фреквенцији. У случају хитне ситуације, или за

емитовање слике, шаље се SMS порука на унапред регистровани број, или неколико бројева мобилних телефона.

2.2 Структура сигурносних система

Глобална структура сигурносних система је дефинисана међународним стандардом IEC 62642-1:2010 и домаћим стандардом SRPS IEC 60839-1-1:1994. Компоненте (блокови) структуре сигурносног система према IEC 60839-1-1 са слике 2.1 су следеће [6]:



Слика 2.1 Структура сигурносног система према IEC 60839-1-1 [6]

- 1 - детектор,
- 2 - контролна опрема (централна јединица),
- 2' - јединица за централни надзор
- 3, 3' - напајање,
- 4, 4' - опрема за визуелну и/или звучну сигнализацију,
- 5 - извршни уређаји које активира централа,
- 6 - програмабилни улазни уређај,
- 7, 7' - уређај или интерфејс за даљинску сигнализацију (модем и слично).

Минимални сигурносни систем може да се састоји од само компоненте - детектора (блок 1) и уређаја за даљински сигнализацију (блок 7), са минимумом следећих захтева [4]:

- систем треба да генерише сигнал аларма у било које време, у складу са националним стандардима,
- систем треба да има минималну стопу генерисања лажних аларма,
- систем треба да има контролу неисправности и
- поступци тестирања и одржавања треба да се обављају у најкраћем могућем року.

Типични кућни сигурносни систем за заштиту од провале укључује:

- контролни панел који је примарни контролер система,
- сензоре за врата и прозоре,
- сензоре покрета, унутрашње и спољашње,
- жичане или бежичне сигурносне камере,
- гласну сирену или аларм,
- ознаке у дворишту и налепнице за прозоре са називом фирме која врши обезбеђење објекта.

Контролни панел, слика 2.2, је основни, али веома важан део сигурносног система. Као центар сигурносног система, контролни панел је ефикасан алат за

комплетну контролу сигурности од стране корисника. Неки контролни панели имају могућност командовања гласом, или даљинског управљања.



Слика 2.2 Контролни панел сигурносног система против провале

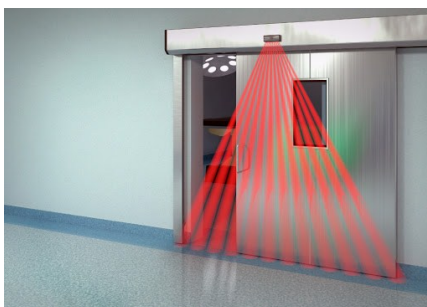
Сврха контролног панела, као уређаја који служи за комуникацију између корисника и система, је да обезбеди:

- укључивање и искључивање система,
- управљање радом светлосног и звучног аларма,
- укључивање и искључивање аларма,
- комуникацију са компанијом која је задужена за праћење аларма,
- тестирање система у циљу откривања отказа у систему.

Сензори у сигурносним системима имају улогу да детектују улазе из физичког окружења као што су: светло, топлота, покрет, притисак и влажност и генеришу одзиве на њих. Користећи читавања на улазу, сензори производе сигнале који могу да се користе за даљу обраду и контролу система. У сигурносним системима се користе бројне врсте сензора (детектора), а најчешће коришћени су: сензори за прозоре и врата, сензори покрета и сензори гасова, слика 2.3.



а)



б)



в)

Слика 2.3 Примери сензора у сигурносним системима: а) сензор за врата, б) сензор покрета за аутоматска врата и в) сензор гасова

Сигурносне камере имају задатак да сниме све што се дешава у њиховом видном пољу, слика 2.4.



Слика 2.4 Сигурносна камера

Ефикасна сигурносна камера има следеће особине:

- могућност детекције покрета (камера шаље власнику куће обавештење да је детектовала кретање у свом пољу),
- могућност флексибилног кретања (могућност заокретања повећава поље које покрива камера и смањује број потребних сигурносних камера),
- могућност остварења бежичне везе (власници могу међусобно да комуницирају са камером),
- могућност „ноћног вида“ (неопходно због чињенице да се многе криминалне активности одвијају ноћу) и
- отпорност на утицај окружења (важан захтев код спољашњих камера у екстремним временским условима).

У случају појаве провале, најбољи начин упозорења власника некретнине и одбијања провалника је употреба изненадног и јаког звука који генеришу сирене, слика 2.5. Сирена производи звук велике јачине и гласности који се далеко чује. Принцип рада је једноставан - уколико се активира сигурносни систем, укључује се сирена.



Слика 2.5 Сирена сигурносног система

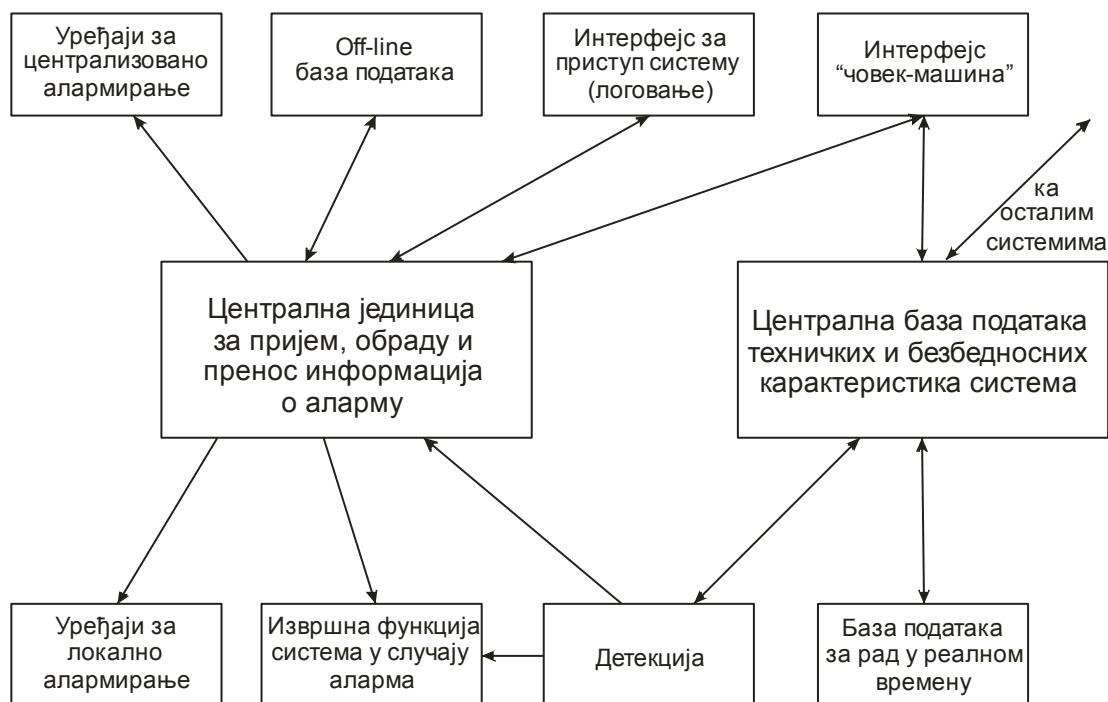
Уз остале елементе сигурносних система, купци добијају и знаке, слика 2.6, и налепнице које светlucaју ноћу, од компаније за обезбеђење. Иако ово личи на маркетиншки потез, има своју улогу у заштити некретнине. Знаци и налепнице показују

да су врата и прозори заштићени од стране компаније за обезбеђење. Овај метод помаже да се смањи шанса да власништво постане мета лопова.



Слика 2.6 Постављање знака компаније за обезбеђење

Савремени системи за заштиту од провале имају структуру са високим нивоом обраде и размене информација која се са мањим или већим модификацијама може применити на било који технички систем заштите, слика 2.7 [4].



Слика 2.7 Глобална структура савременог система за заштиту од провале [4]

Основни облици заштите од провале коришћењем механичких и електронских средстава су [4]:

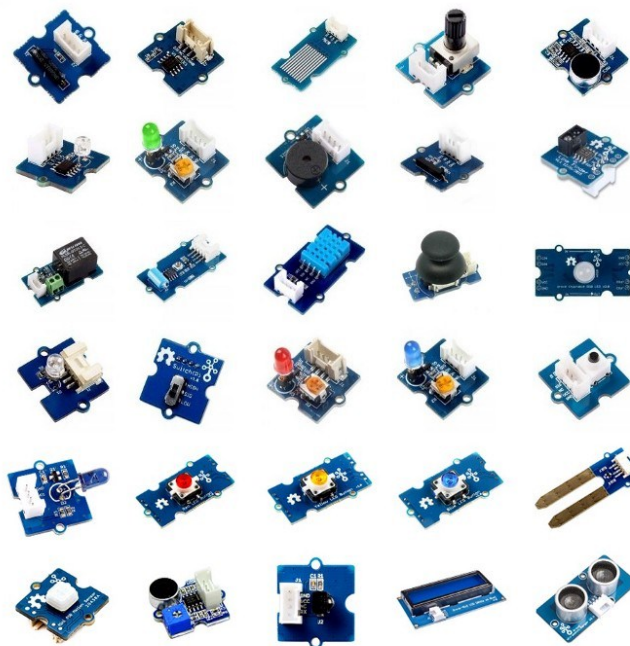
- препреке - природне и вештачке баријере за спречавање нежељеног уласка,
- механичка заштита - катанци, браве, сигурносна врата, сефови,
- електронска заштита - камере за видео надзор, уређаји за контролу приступа, електрични и електромагнетни контакти, детектори за откривање уласка, покрета или присуства, „паник“ тастери, итд.

2.3 Сензори у сигурносним системима

Сензор (детектор, пикап, рецептор) је физички елемент (уређај) који детектује (мери) физичку величину и формира излазни сигнал који зависи од мерене величине и углавном је електрична величина (напон, струја, отпорност, капацитет, индуктивност). Примарни сензорски елемент детектује мерену величину, после чега се формира излазни сигнал који зависи од вредности мерене величине. Излазни сигнал може бити електрична или нека друга физичка величина (напон, струја, померај). Дакле, сензор је уређај који је у директном контакту са објектом мерења, непосредно прима мерену физичку величину и претвара је у величину погодну за мерење.

Детектор у ширем смислу је мерни уређај или супстанца (врста сензора) која указује на присуство одређене појаве, објекта, стања, или процеса. Он даје информацију о квалитативним карактеристикама мерене величине, док квантитативне информације нису обавезне.

Велики број различитих врста сензора развијен у данашње време, слика 2.8, уз савремени развој технологије микроконтролера, омогућава да много различитих објеката, стања или процеса могу да буду предмет мерења и управљања.



Слика 2.8 Различите врсте сензора

Сензори и детектори у сигурносним системима за заштиту од провале су уређаји који откривају упад. Они откривају провалнике различитим методама, као што су: праћење отварања врата и прозора, праћење појаве покрета, звука, лома стакла, вибрације или других поремећаја. Код провале постоји, дакле, само једна појава која треба да се надгледа, а то је неовлашћени улазак у простор који се штити, али је број параметара помоћу којих може да се реализује функција надгледања - практично неограничен.

2.3.1 Детектори провале

Детектори провале могу се поделити према [7]:

- месту постављања/намени (детектори за отворени или затворени простор),
- области покривања (тачка, линија, површина, запремина),
- принципу дејства (на бази електричног отпора, магнетно-контактни, пиезоелектрични, ултразвучни, оптичко-електронски),
- зони дејства (на малом, средњем, или великом растојању),
- принципу конструкције (све компоненте у једном кућишту, или две или више одвојених целина) и
- начину напајања (пасивни, или активни).

Најчешћа подела детектора је према месту примене, односно да ли штите границу простора под заштитом (периметар), сам простор, границу објекта који се налазе у штићеном простору, или унутрашњост објекта. У складу са тим, детектори могу бити:

- унутрашњи детектори провале који штите од неовлашћеног улаза у објект и
- спољашњи детектори провале који надгледају периметар и простор у оквиру периметра.

Спољашњи детектори провале се постављају на отвореном простору, у окружењу објекта, или дуж оgrade, или линије која се штити. Морају да буду робусни и неосетљиви на услове околине (температура, киша, снег, магла), али и довољно осетљиви да детектују неовлашћени улазак. Карактерише их мања поузданост детекције и већа стопа лажног алармирања него код унутрашњих детектора провале. Најчешћи спољашњи детектори провале су приказани у Табели 2.1.

Табела 2.1 Спољашњи детектори провале [7]

Детектори за надзор у околини објекта (спољашњи)		
Надзор на граници простора		Надзор унутар граници простора
Детектори на граници периметра	Детектори испод границе периметра	Запреминска детекција (детектори покрета)
• Детекција вибрација • Затегнута жица • Оптички кабл - Непрекидност - Сметње • Деформација кабла - Коаксијални каблови - Магнетски полимери • Електрично поље • Капацитивност	• Линија осетљива на притисак • Подземни коаксијални кабл • Подземни оптички кабл • Подземна геофона линија (сеизмичка детекција)	• Активни ИС детектори • Микроталасни детектори • Пасивни ИС детектори • Пасивни ИС и микроталасни детектори • Радарски системи • Акустички сензори

Унутрашњи детектори провале штите улазак у објект, или у неки део, или просторију објекта. Обично су пројектовани само за коришћење у затвореном простору

и не могу да се користе у спољашњој средини. Они извршавају једну од следеће три функције:

- детекцију приближавања или преласка линије објекта који се штити (врата, прозори, кровови, зидови),
- детекцију кретања објекта у штићеном простору (просторија, ходник, хол) или
- детекцију померања, подизања или додиривања.

И ови детектори су склони лажном алармирању, али у много мањој мери него спољашњи. Најчешће врсте унутрашњих детектора провале дати су у Табели 2.2.

Табела 2.2 Унутрашњи детектори провале [7]

Детектори за надзор у објекту (унутрашњи)					
Прозори		Врата	Зид	Просторија	
Оквир (рам) прозора	Стакло прозора	Оквир (рам) врата	Површина зида	Запреминска детекција (детектори покрета)	Линијска детекција
• Механички контакти • Магнетни контакти • Балансирани магнетни контакти	• Акустична • Лом • Ударац	• Механички контакти • Магнетни контакти • Балансирани магнетни контакти	• Вибрације • Оптички кабл	• Микроталасни детектори • Пасивни ИС детектори • Пасивни ИС и микроталасни детектори • Активни ултразвучни детектори • Пасивни ултразвучни детектори	• Активни ИС детектори

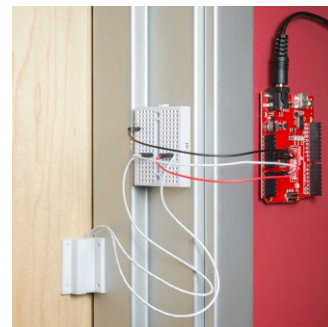
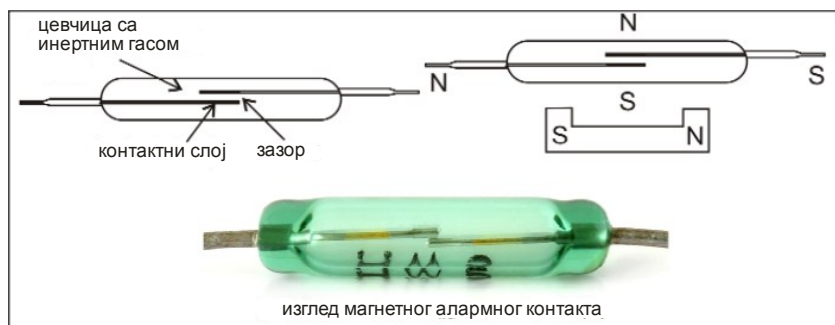
2.3.2 Алармни контакти

Алармни контакти су најстарији алармни уређаји за откривање уласка у објекат. Ови уређаји промену стања контакта насталу под утицајем спољне силе прослеђују преко алармне линије централном уређају за надзор. Могу се класификовати на следећи начин:

- према начину сигнализације у електричном колу (нормално отворено или нормално затворено електрично коло) и
- према начину реализације (магнетни контакти са мембраном, флуидима, живом, итд.).

У алармним системима се највише користи „нормално отворени“ или „нормално затворени“ **магнетни контакт** (стандардни, мали, мини-контакти и микро-контакти). Основна конструкција се састоји од магнетних контаката који се преклапају и који су херметички затворени у стакленој цевчици, слика 2.9. Када се примени спољашња

магнетна сила, крајеви контаката заузимају супротни поларитет и при довољној сили долази до привлачења и спајања контаката.

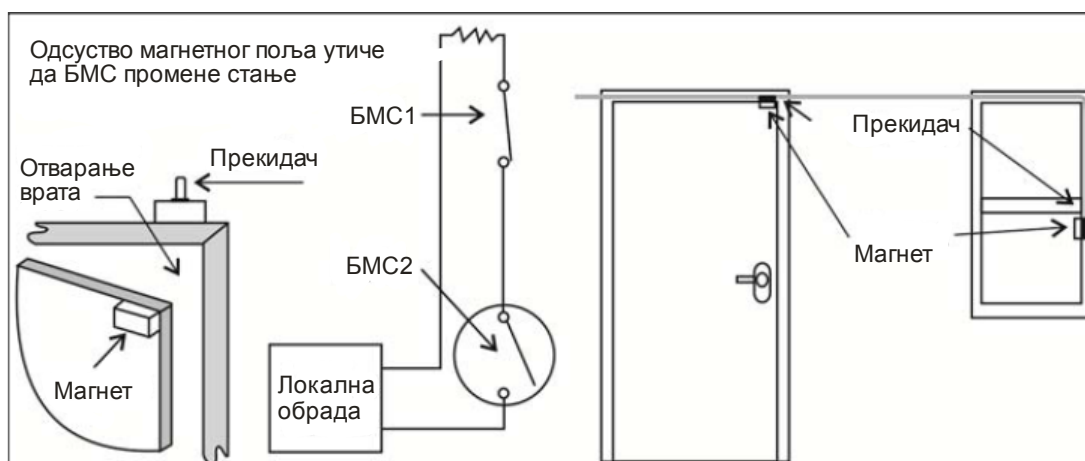


а)

б)

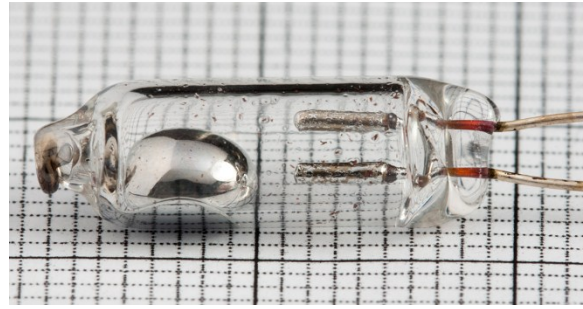
Слика 2.9 Магнетни алармни контакт: а) изглед [7], б) монтажа

Балансирани магнетни контакти (БМС) са састоје од унутрашњег магнета, који се монтира на оквир врата/прозора и спољашњег магнета (балансираног) који се монтира на покретни део врата/прозора, слика 2.10. Ако дође до промене у магнетном пољу због померања спољашњег магнета, прекидач заузима положај „затворено“. Отварањем врата или прозора прекидач заузима положај ближе неком контакту и генерише аларм.



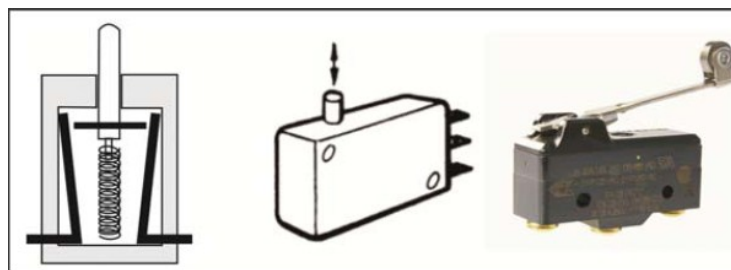
Слика 2.10 Балансирани магнетни контакти [7]

Микропрекидачки контакти са живом, слика 2.11, се користе код прозора. Састоје се од стаклене цевчице у којој су контакти који су везани за алармно коло и мале количине живе која се креће под утицајем гравитације и служи за успостављање везе између алармних контаката. Померањем прозора, жива „бежи“ од контаката, прекида се алармно коло, чиме се укључује аларм.



Слика 2.11 Микропрекидачки контакт са живом

Микропрекидачи представљају основу већине електромеханичких алармних уређаја, слика 2.12. За њихово активирање је потребан притисак на тастер који је повезан са опругом. По завршетку притиска, микропрекидач се враћа у нормалан положај.



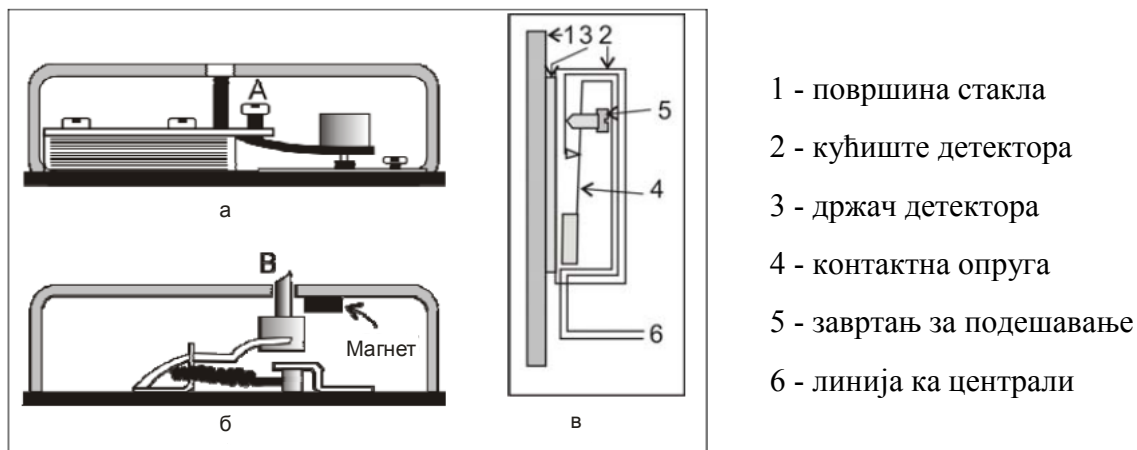
Слика 2.12 Микропрекидачи - конструктивно решење и изглед [7]

2.3.3 Детекција лома стакла

Детектори лома стакла могу бити:

- вибрациони,
- акустички (звучни, аудио) и
- комбиновани (дуал).

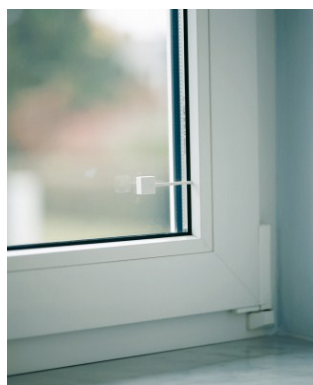
Вибрациони детектори лома стакла (виброконтакти) се највише користе у техници детекције лома стакла. Осетљивост виброконтакта на слици 2.13 а) зависи од величине зазора, који се регулише заокретањем завртња А. Основни недостатак овакве врсте виброконтакта је то што не разликују изворе вибрација, па су мање поуздани у срединама где има буке. Други тип виброконтакта, приказан на слици 2.13 б), ресетује се притиском на тастер В. Под утицајем вибрација, опруга ће приближити контакт довољно близу сталном магнету који привлачи контакт, долази до контакта и укључује се аларм. На слици 2.13 в) је приказан један начин постављања виброконтакта на стаклену површину или зид.



Слика 2.13 Механички вибрациони детектори лома стакла: а) виброконтакт са аутоматским ресетом, б) виброконтакт са ручним ресетом, в) могући начин постављања [4]

Акустички детектори лома стакла реагују на вибрације које се преносе кроз ваздух у једном или више фреквентних опсега, у области чујности човечјег уха (од 20 Hz до 20 kHz), или изван ње. Обично се користе у близини стаклених врата, излога, или прозора. Постоје две врсте ових детектора:

- пиезоелектрични детектори лома стакла који детектују вибрације које се преносе кроз стакло и који се постављају или на само стакло (заштита појединачног прозора), или на оквир прозора (истовремена заштита више прозора) и
- аудио детектори са пиезоелектричним микрофонима, који детектују звук који се произведе при лому стакла.



а)



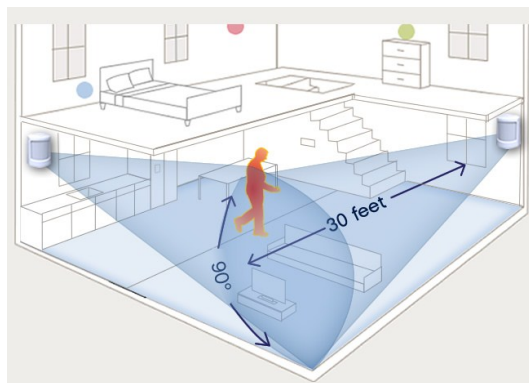
б)

Слика 2.14 Детектори лома стакла: а) пиезоелектрични детектор, б) аудио детектор

Када је неопходна велика сигурност система заштите од провале, користе се **акустички детектори у двострукој („дуал“) технологији**, који садрже комбинацију аудио и вибрационог детектора у истом кућишту.

2.3.4 Детекција покрета

Детектори покрета детектују кретање у објекту, слика 2.15.



Слика 2.15 Детекција покрета у објекту

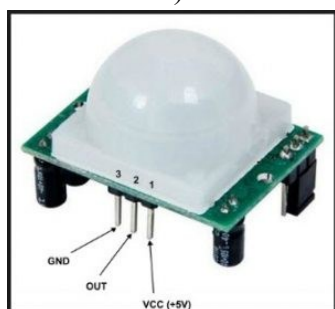
Постоје четири основна типа детектора покрета: ултразвучни, микроталасни, инфрацрвени и томографски, слика 2.16.



а)



б)



в)



г)

Слика 2.16 Детектори покрета: а) ултразвучни, б) микроталасни, в) инфрацрвени и г) томографски

Ултразвучни детектори могу бити активни и пасивни. Пасивни „слушају“ специфичне звуке, као што је лом стакла или кретање метала по металу. Веома су осетљиви, али су често скупи и склони лажном алармирању. Активни ултразвучни сензори емитују импулсе ултразвучних таласа и мере одбијање таласа од покретног објекта. Пошто пси, маčke и неке рибе могу да чују ултразвучне фреквенције, овакав ултразвучни аларм може да их узнемири.

Микроталасни сензори емитују микроталасне пулсеве и мере њихово одбијање од објеката, да би се видело да ли се објекти крећу. И ови сензори су веома осетљиви, али, понекад, могу да „виде“ кроз неметалне објекте и тако детектују покретне објекте изван циљаног опсега. Такође, користе доста енергије, па се често праве тако да се

циклично укључују и искључују, што значи да је могуће да се „заобиђу“ уколико се зна њихов циклус укључивања и искључивања.

Инфрацрвени сензори садрже танак филм пироелектричног материјала који реагује на инфрацрвено зрачење које емитују сва топлоткрвна створења тако што генерише електричну струју. Овај сензор укључује сигурносни аларм када се појави прилив електричне струје. Нису скуп, не користе много енергије и дуго трају, па су веома чести код алармних система унутар објекта.

Томографски сензори емитују радио таласе и осећају када су таласи нарушени. Могу да „виде“ кроз зидове/објекте и постављају се тако да праве мрежу радио таласа која покрива широку област. Веома су скуп, па се обично користе у складиштима, професионалним јединицама за складиштење и другим ситуацијама које захтевају комерцијални ниво заштите.

2.3.5 Заштита периметра

Периметар је затворена линија - граница унутар које се налазе објекти под заштитом, после које почиње деловање техничких система заштите.

Најједноставнији начин заштите периметра су **жичане ограде** које чине једна или више затегнутих жица, које уједно формирају петљу аларма која региструје напрезање, прекидање, или било који други облик деформације, слика 2.17.



Слика 2.17 Заштита периметра помоћу затегнуте жице

Детектори вибрација се примењују на исти начин као и у објекту, али се налазе на стубовима у кућиштима која су заштићена од атмосферских утицаја. Могу да се поставе на ограду или зид који ограђују периметар, слика 2.18. Жице на огради морају да буду затегнуте да би се вибрације пренеле преко кућишта на сам детектор вибрација. Ако је штићени простор ограђен зидом, детектори вибрација се уграђују у зид, при чему се води рачуна у којој мери материјал зида преноси вибрације.

За детекцију вибрација се користе детектори са пиезоелектричним елементом као сензором, или детектори са електро-механичким или магнетним контактима.



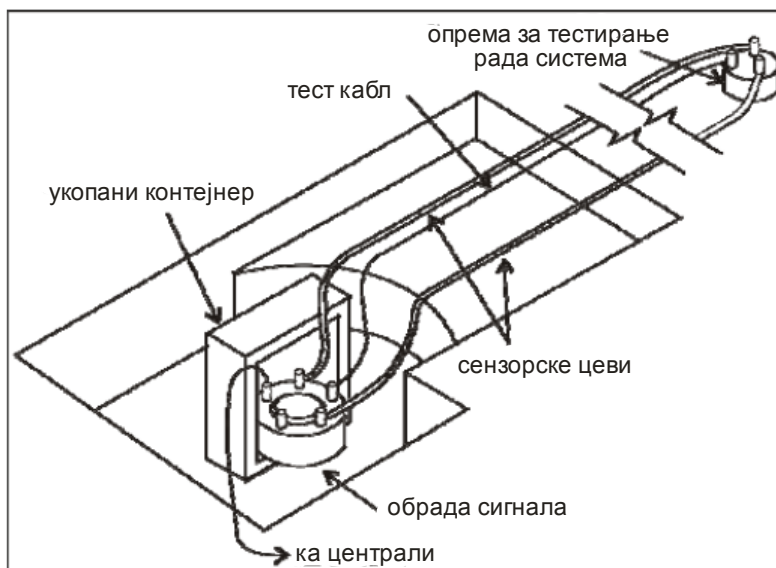
а)



б)

Слика 2.18 *Заштита периметра детектором вибрација: а) на огради, б) на зиду*

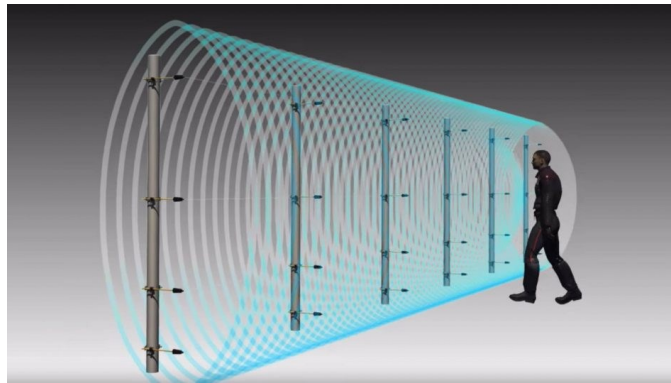
Заштита периметра **подземним цевима са сензорима притиска** је пасивни подземни систем који детектује нискофреквентне вибрације и притисак на тло. Таласе притиска обично изазивају провалник или возило који се крећу преко области испод којих су закопани сензори, слика 2.19. Рад је заснован на детекцији диференцијалног притиска. Сензори притиска су две или више мекане паралелне цеви закопане дуж периметра, напуњене течномшћу и система за регулацију и праћење разлике притисака између њих. Покушај преласка преко заштићене области прави разлику у притиску између цеви. Јединица за мерење притиска детектује разлику притисака у цевима и генерише електрични излаз пропорционалан примењеном притиску на тло. Када разлика притисака пређе дозвољени ниво, анализатор генерише алармни сигнал.



Слика 2.19 *Заштита периметра подземним цевима са сензорима притиска [7]*

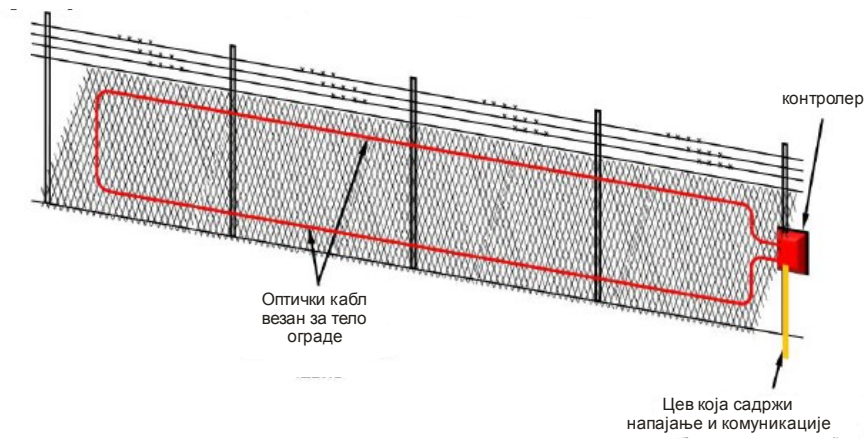
Сензори електричног поља генеришу електростатичко поље око низа паралелних жичаних проводника. Жице сензора постављене паралелно жицама оgrade детектују било који поремећај електростатичког поља изазван приласком оgrade или допицањем оgrade. Сензор се састоји од генератора наизменичне струје који прави електростатичко поље на низу жица које иду паралелно са тлом. Неке жице се користе да направе поље, а неке као елементи детектора. Када провалник уђе у поље,

капацитативност његовог тела ствара неравнотежу у електростатичком пољу. Процесор детектује ову промену сигнала и генерише алармни сигнал.



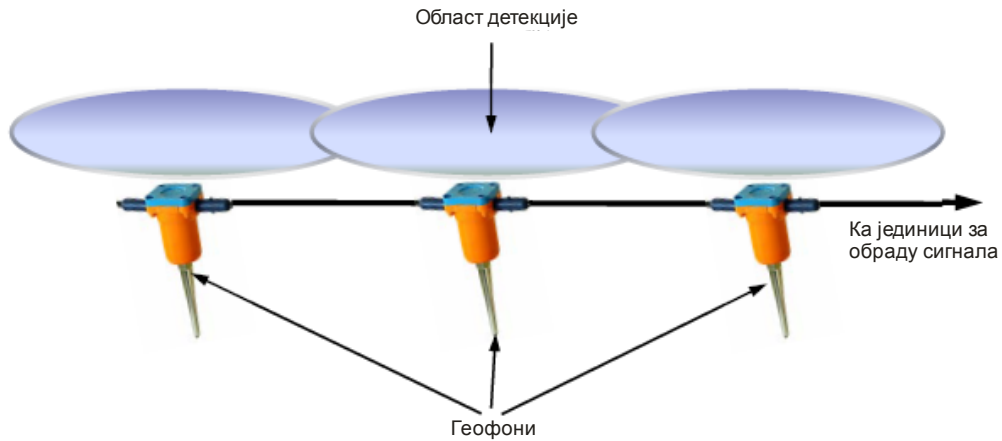
Слика 2.20 Заштита периметра коришћењем електричног поља

Сензори са оптичким влакнима, за пренос и детекцију користе светлосни сигнал који путује дуж стакленог влакна. Оптичко влакно је савитљива стаклена цев која води светлосни сигнал од извора светлости са једне стране до детектора или огледала са друге стране влакна. Када се влакно савије, или креће, карактеристике светлости која путује дуж влакна се мењају. Код система за заштиту периметра, светлосни сигнал се шаље дуж влакна које је везано за ограду и враћа на контролер да би се успоставило стање без аларма. Када неко проба да се попење на ограду, оптички кабл се минимално покрене и образац светлосног сигнала се мења. Детектује се ова промена у светлосном сигналу, и ако она превазиђе претходно утврђену границу, укључује се аларм.



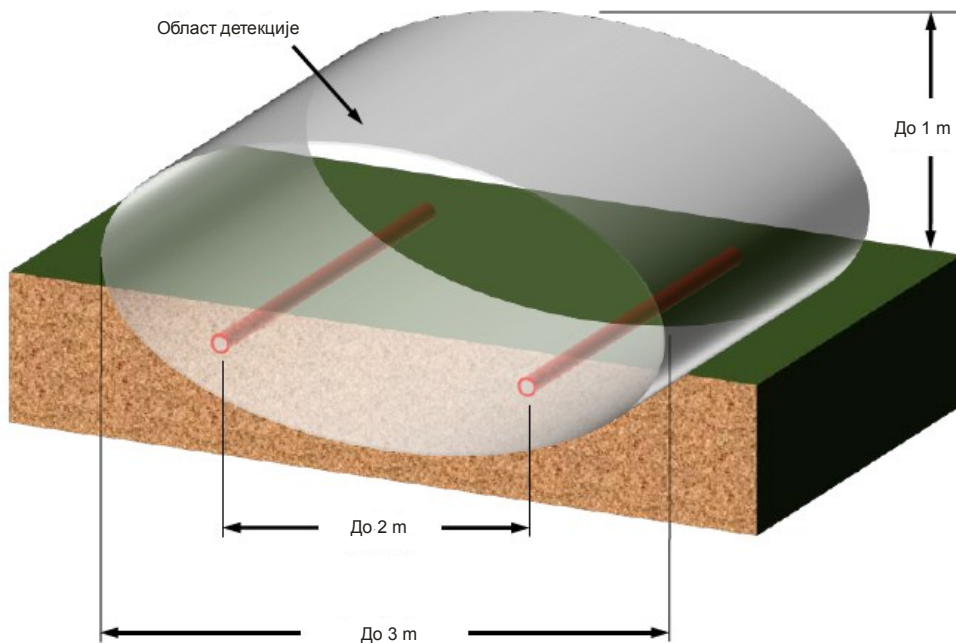
Слика 2.21 Заштита периметра оптичким кабловима на огради [8]

Геофон се састоји од сталног магнета ослобођеног на опругу у проводном калему. Било која вибрација, или покрет, изазива релативно кретање магнета у односу на намотај и генерише електрични напон пропорционалан брзини магнета. Закопани **геофон** претвара покрете земље изнад њега или вибрације ниских фреквенција у електрични напон. Мерење промена електричне струје одређује интензитет вибрација. Свако одступање од измереног напона у нормалном стању је сеизмички одзив који настаје када неко или нешто прелази кроз област детекције изнад сензора. Када карактеристике напона задовоље одговарајући критеријум, оглашава се аларм.



Слика 2.22 *Заштита периметра геофоним системом [8]*

За заштиту периметра се могу користити и коаксијални каблови посебног типа са малим отворима блиско распоређеним на спољном омотачу који омогућавају простирање електромагнетног зрачења око проводника. Тиме се формира електрично поље у непосредној близини проводника. Коаксијални каблови се постављају паралелно испод нивоа земље. Димензије зоне детекције зависе од растојања између каблова и дубине постављања. Када провалник уђе у електрично поље око проводника, оно се мења. Предајник се налази на почетку једног кабла, а пријемник на крају другог кабла надгледа промене које настају у електромагнетном пољу



Слика 2.22 *Заштита периметра укопаним коаксијалним кабловима [8]*

2.3.6 Видео надзор

Коришћење видео надзора је веома актуелно и регулисано је прописима. Опрему за видео надзор уграђује само овлашћена фирма. За постављање видео надзора унутар објекта није потребна посебна дозвола, док је за постављање видео надзора ван објекта потребна специјална дозвола, према Закону о приватном обезбеђењу.

Најновији концепти система видео надзора су изузетно поуздани када је реч о пружању сигурности и заштите. Савремене камере за видео надзор могу да буду мање од стандардног мобилног уређаја. Повезане су на Интернет, имају снажне објективе који могу да снимају или емитују видео снимке високе резолуције. Власници система за видео надзор могу да програмирају системе да шаљу снимке у реалном времену [9].

При избору камере за видео надзор треба водити рачуна о следећем:

- резолуција - број пиксела на екрану при приказу слике,
- ноћни режим рада - да ли камера може да прави добре снимке ноћу и на којој удаљености,
- водоотпорност - да ли је камера отпорна на воду (код спољашње употребе),
- материјал израде - који је материјал кућишта камере (зависи издржљивост камере) и
- димензије - зависно од расположивог простора и жеље да камера (не)буде дискретна.

Најсавременије методе видео надзора подразумевају коришћење: аналогних камера, IP видео надзора и HD-CVI и HD-TVI камера [10].

Најзаступљенији облик видео надзора код нас су **аналогне камере**, слика 2.23, јер имају приступачну цену, а употреба је једноставна. Међутим, резолуција видео снимака није задовољавајућа и то је њихов највећи недостатак. Зато се више препоручује употреба AHD (*Analog High Definition*) камера у односу на CCTV (*Closed Circuit TV*) јер дају бољи квалитет снимака за исту цену.



Слика 2.23 Аналогна камера за видео надзор

IP видео надзор је савремена врста видео надзора са мрежним IP камерама високе резолуције и високим квалитетом снимљеног материјала. То је систем видео надзора код којег је могуће прегледати снимке или гледати снимак уживо, преко мреже (LAN или Интернет), са удаљене локације. Систем мора имати: бар једну IP камеру, слика 2.24, каблове којима је камера везана са снимачем, каблове за напајање, снимач са

одговарајућим хард диском и монитор или телевизор за репродукцију снимљеног садржаја.



Слика 2.24 Мрежна IP камера

HDCVI (*High Definition Composite Video Interface*) је технологија видео надзора нове генерације. Омогућава пренос сигнала у FULL HD резолуцији преко коаксијалних каблова. Због коришћења коаксијалних каблова, обезбеђен је поуздан пренос на већим раздаљинама без употребе појачавача. HDCVI сигнал се може преносити и путем UTP кабла, али на краћим растојањима. Ова технологија подразумева да се једним каблом преносе три сигнала - видео, аудио и PTZ (*point, tilt, zoom*) контрола.



Слика 2.25 HDCVI камера фирме Dahua

HDTVI (*High Definition Transport Video Interface*) видео надзор, слика 2.26, је готово идентичан HDCVI технологији. Подржава пренос видео сигнала путем стандардног коаксијалног кабла, пренос звука и двосмерни пренос података, велике дужине каблова, као и повезивање у хибридне системе за видео надзор. Не захтева изградњу и конфигурацију у мрежном окружењу.



Слика 2.26 HDTVI камера фирме Hikvision

3. КРЕИРАЊЕ СИГУРНОСНОГ СИСТЕМА НА АРДУИНО ПЛАТФОРМИ

Мобилне апликације су софтверски програми за мобилне уређаје као што су паметни телефони (енг. *smartphone*) и таблети. Оне покривају широк спектар примена од индустрије и навигације, до забаве, спорта, и других.

Многе мобилне апликације имају одговарајуће програме који су намењени да раде на десктоп рачунарима. Међутим, оне морају да раде са другачијим ограничењима од еквивалентних десктоп апликација. Са аспекта функционалности, развој мобилних апликација за мобилне платформе је тежи, због различитости мобилних уређаја. Мобилни уређаји имају широк опсег величина екрана, капацитета меморије, могућности процесора, графичких интерфејса, дугмади и *touch* функција, о којима морају да воде рачуна дизајнери софтвера за мобилне апликације. Зато мобилне апликације нуде више интерактивности и дају специфичне информације у формату који је лак за употребу на мобилном уређају.

Најпопуларнији мобилни оперативни системи који су заступљени код већине корисника су:

- *Android (Google)* - најпопуларнији “*open source*” оперативни систем који дозвољава могућност мењање системског кода и прављења апликација по жељи,
- *iOS (Apple)* – оперативни систем који није могуће користити на уређајима које није произвела компанија *Apple* и
- *Windows Phone (Microsoft)* – сличан *Windows* оперативном систему за рачунаре.

На светском тржишту постоје стотине уређаја са *Android* оперативним системом различитих произвођача, укључујући: телефоне, таблете, телевизоре, стерео уређаје у аутомобилима, опрему за вежбање и додатну опрему. Различитост уређаја и лака прилагодљивост помогле су да *Android* оперативни систем повећа базу корисника, али такав раст може да донесе потенцијалне изазове: апликације морају да подржавају велики број: величина екрана, резолуција екрана, тастатура, хардверских сензора, верзија оперативних система, брзина бежичног преноса података и конфигурација система. Све то може да доведе до различитог и непредвидљивог понашања, али тестирање апликација у свим окружењима је немогућ задатак. Ипак, *Android* апликације се могу успешно програмирати на *Windows*, *Linux* или *Mac* оперативним системима, што их сврстава у ред најпопуларнијих.

Најзаступљенији програмски језици за креирање мобилних апликација су: *Java*, *Objective-C* и *Swift*.

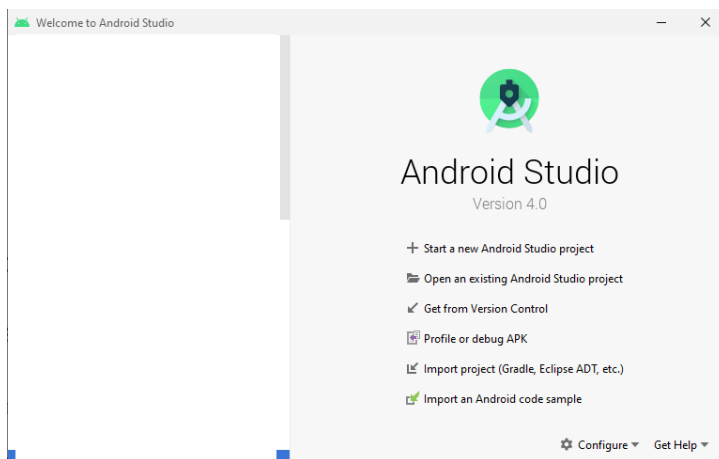
Android платформа дозвољава програмерима да пишу програме користећи језик *Java*, за управљање и контролу рада *Android* уређаја. *Android* апликације могу да се развију

користећи програмски језик *Java* и *Android SDK*. Програмски језик *Java* се појавио средином 1990-их година и био је веома популаран у светским оквирима, у првом реду због великог броја функција које нуди. Обећани концепт *Java* језика „Напиши једном и изврши било где“ један је од главних фактора успеха овог језика у претходним деценијама.

Java Mobile Edition (Java ME) је направљен за креирање апликација које могу да раде на мобилним уређајима. Зато је и овај програмски језик усвојен као примарни језик за развој апликација које раде на *Android* платформи. *Java ME* језик подржава већина паметних телефона и таблета. Апликације написане користећи овај језик су преносиве, сигурне и користе природне способности уређаја.

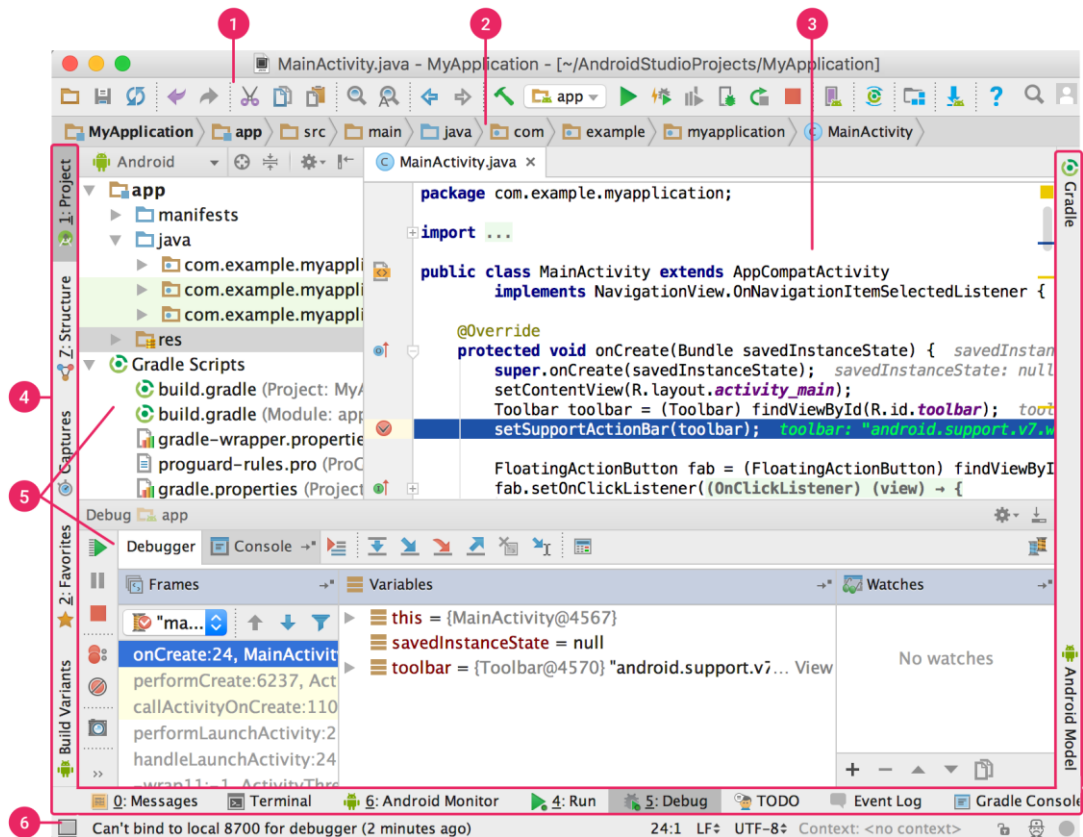
3.1 Android Studio

При покретању програма *Android Studio* приказује се екран са поруком добродошлице, након чега је могуће приступити жељеном радном пројекту (слика 3.1).



Слика 3.1 *Android Studio* - почетни екран

При креирању новог, или при отварању постојећег пројекта, појављује се изглед главног прозора *Android Studio* који се састоји од неколико логичких целина које су приказане на слици 3.2.



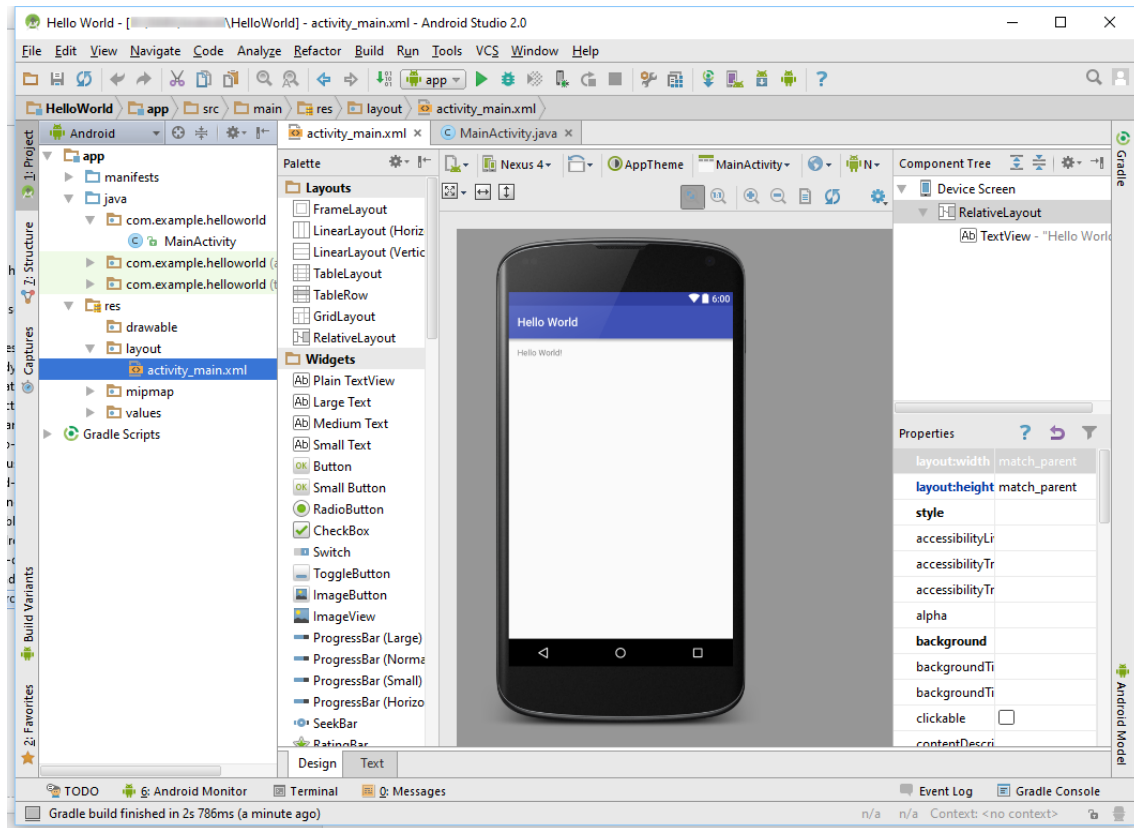
Слика 3.2 Android Studio – главни прозор

Ознаке на слици 3.2 су:

1. Трака са алатима (*toolbar*) – омогућава бржи приступ одабраној групи радњи на траци менија.
2. Трака за навигацију (*navigation bar*) – помаже при кретању кроз пројекат и при отварању датотека. Пружа компактнији приказ структуре видљиве у *Project window*.
3. Прозор уређивача (*editor window*) – приказује садржај датотеке на којој програмер тренутно ради. То је место где се креира и мења програмски код.
4. Трака прозора алата (*tool window bar*) – налази се око спољашње стране главног прозора и садржи дугмад преко којих је могуће да се прошире или сакрију поједини прозори алата.
5. Прозори алата (*tool windows*) – дају приступ одређеним задацима као што су управљање пројектима, претрага, контрола, итд. Могуће их је проширити, или смањити.
6. Статусна трака (*status bar*) – приказује информативне поруке о пројекту. Прелазак курсора миша изнад ставки на статусној траци пружиће опис тог поља.

Корисник може да организујете главни прозор тако да добије више простора на екрану скривањем или померањем трака и прозора са алатима. Такође, могуће је да се коришћењем „пречица“ са тастатуре приступи већини *IDE* функција [11].

Реализована апликација у оквиру дипломског рада је написана у програмском језику *JAVA*, у радном окружењу *Android Studio*. *Android Studio* је развојно окружење (*IDE*) за развој мобилних апликација засновано на *IntelliJ* окружењу. Сваки пројекат садржи један или више модула са датотекама изворних кодова и датотекама ресурса. Постоје следећи типови модула: *Android app*, *Library* и *Google App Engine* модули. *Android Studio* приказује пројекат у окружењу као на слици 3.3 [12].



Слика 3.3 *Android View* окружење

Овај изглед је организован по модулима да би се обезбедио брз приступ главним изворним датотекама. Сваки модул апликације има следеће директоријуме [12]:

- **manifests** - садржи *AndroidManifest.xml* датотеку,
- **java** - садржи Java изворне кодове, укључујући *JUnit* тест код,
- **res** - садржи све ресурсе који нису кодови, као што су *XML layouts*, *UI strings* и *bitmap* слике.

3.2 Arduino Software (IDE)

Добра карактеристика свих *Arduino* плоча је да се оне могу програмирати помоћу *Arduino Software IDE*-а. *Arduino* има интегрисано развојно окружење и програм *IDE* (*Integrated Development Environment*) се покреће на рачунару и преко њега се управља самом плочом (слика 3.4). Одговарајућа верзија софтвера може се преузети са веб сајта [13]. Интегрисано развојно окружење садржи текст едитор за писање програмског кода, подручје за поруке, траку са алатима са тастерима за уобичајене функције и низ менија.



Слика 3.4 Веза *Arduino* плоче са рачунаром

Општи кораци за писање и учитавање програма на *Arduino UNO* плочу су следећи [14]:

- Повезати *Arduino UNO* плочу са USB прикључком на рачунару.
- Покренути *Arduino IDE* на рачунару.
- Кликнути на *Tools* → *Board* и изабрати тип плоче *Arduino/Gerduino Uno*.
- Кликнути на *Tools* → *Port* и изабрати серијски порт са којим је повезана *Arduino UNO* плоча.
- Написати и сачувати програм.
- кликнути на *Sketch* → *Verify/Compile* да би се извршило компајлирање програма. Проверити да ли има грешака приликом компајлирања.
- Кликнути на *Sketch* → *Upload* да би се послао извршни код у програмску меморију *Arduino UNO* плоче.

Програми написани помоћу Ардуино софтвера (*IDE*) називају се скице и имају екстензију *.ino*. Извршни програм је у бинарном машинском језику и претварање програмског језика у бинарни код врши компајлер.

Програмско окружење је једноставно и јасно, а сам *Arduino IDE* софтвер је прилагођен почетницима, али је и довољно флексибилан да га користе и искуснији програмери. *Arduino IDE* софтвер је креиран као *open - source* алат који може да се надограђује и проширује. *Arduino* плоче су објављене под лиценцом *Creative Commons* тако да искусни дизајнери могу да израде и побољшају сопствени модел *Arduino* модула, али и релативно неискусни корисници су у прилици да формирају различите верзије

модула како би боље разумели како све функционише за релативно мало уложених новчаних средстава.

Arduino је заједнички назив за фамилију микроконтролерских платформи које се користе у развоју апликација које на једноставан начин остварују везу између хардверских и софтверских елемената система. Хардвер се састоји од штампане плоче засноване на 8-битном или 32-битном *Atmel* микроконтролеру. Развој софтвера је омогућен коришћењем *Open source* интегрисаног развојног окружења. Веза са хардвером остварена је преко серијског *USB* интерфејса који се налази на самој плочи. Преко њега се програм, написан и компајлиран у развојном окружењу, пребацује у програмску *Flash* меморију микроконтролера [15].

Arduino плоча је настала у Италији 2005. године, а креирана је од стране студената. Своју популарност је стекла због своје једноставности. Само програмирање плоче не захтева додатни хардвер (програматор) као за остале микроконтролерске системе, него је довољан *USB* кабл који се може повезати са сваким рачунаром. *Arduino* се може програмирати из Windows-a, Mac-a, Linux-a, Android-a.

Arduino плоча су релативно јефтине у односу на друге микроконтролере. Представљају једноставну електронску платформу која омогућава прикљученим електронским компонентама да шаљу и примају податке. Постоје многе компоненте, укључујући моторе, потенциометре, сензоре и зујалице које се могу прикључити на *Arduino*. Поред едукације, главна намена *Arduina* је да олакша посао при пројектовању уређаја овог типа али и да омогући једноставну проверу усвојених решења, тј. да ли замисао функционише у пракси. Обично, када се докаже функционалност у пракси, *Arduino* суштински више није потребан и уместо њега на штампану плочу може да се постави микроконтролер који ће обављати улогу коју је претходно имао микроконтролер на прототипској платформи.

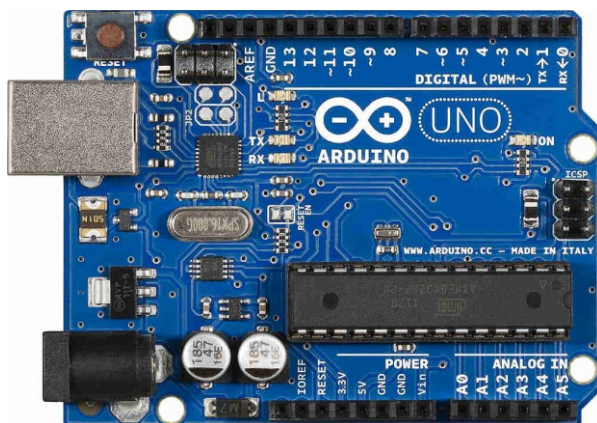
Верзија *Arduino Uno* се први пут појављује током јесени 2010. године када је представљена у оквиру сајма посвећеном љубитељима технике „уради сам“, који је организовао познати амерички часопис *Make*. Није тајна да добар део своје популарности *Arduino* платформа дугује управо том часопису. *Uno* значи један на италијанском језику и изабран је за обележавање издања *Arduino*. Данас је ова верзија плоче најчешће коришћен модел плоче у оквиру брэнда *Arduino*. Често се уз назив *Uno* модела може видети ознака R3 која представља трећу ревизију плоче.

3.3 *Arduino UNO R3* плоча

Arduino плоча је израђена од великог броја компонената, укључујући микроконтролер, дигиталне и аналогне пинове, пинове за напајање, отпорнике, диоду, кондензатор и LED.

Модел *Arduino UNO Rev3* садржи 8-битни ATmega328 микроконтролер. Микроконтролер садржи централну процесорску јединицу (*CPU - Central Processing Unit*) која обрађује и усмерава све команде. Основни изглед плоче приказан је на слици

3.5. На плочи се налазе све неопходне компоненте које омогућавају њен рад, као и повезивање са рачунаром и другим периферијским плочама. Она садржи 14 дигиталних улазно/излазних пинова и 6 аналогних излаза који су смештени на ободима плоче. Дигитални и аналогни пинови се користе за слање и пријем дигиталних и аналогних података. Пинови су обично груписани у логичке целине које се називају портови. Кварцни кристал (у металном кућишту) ради на брзини од 16 MHz, а на плочи је конектор за напајање, *ICSP (in-circuit serial programming)* заглавље, као и дугме за *reset*.



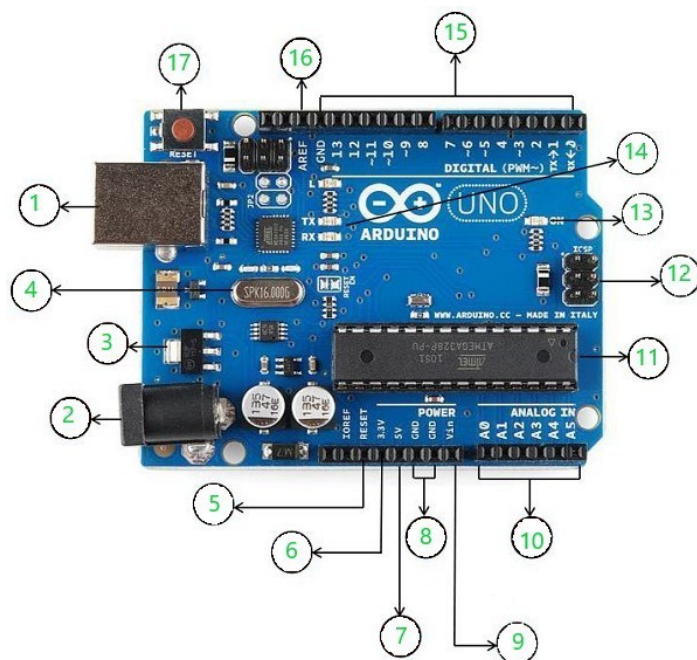
Слика 3.5 Arduino UNO Rev3 плоча

Повезивање са рачунаром се врши преко серијског *USB* интерфејса који има следећу улогу:

- Пријем новог програмског кода преко серијске везе и његово смештање у програмску меморију контролера.
- Током уобичајеног режима рада у којем контролер извршава програм који је већ смештен у *Flash* меморији, *USB* интерфејс се може користити за размену података између апликација које се извршавају на *Arduinu* и на рачунару.
- *Arduino* плоча обично прима напона напајања од 5 V са *USB* линије. Ако се од *Arduina* захтева да ради самостално, без повезивања са рачунаром (*Stand alone application*), напајање се може довести са посебног конектора.

Arduino је по својој функцији *U/I* плоча (*I/O board*), што значи да преко својих извода омогућава рад са улазним и излазним уређајима. За прикључивање се користе пластични конектори који се традиционално називају пиновима и налазе се са две бочне стране плочице. Ту су два пина за уземљење (*GND*), излазни пинови за 3,3 V и 5 V, пин за улазни напон (*VIN*), пин за довођење *RESET* сигнала. Верзија R3 плоче поседује и пин (*AREF - Analog REference*)), чија је функција да усклади напон додатног уређаја са напонем самог уређаја. Подразумевана вредност је 5 V и 3,3 V за уређаје који немају напајање од пет волти. Довођење већег напона на овај пин може да поквари уређај. Пинови названи A0-A5 имају намену да прихвате информације у аналогном облику. У примени је *I²C* магистрала као један од најједноставнијих протокола за серијски пренос података. Брзине преноса ове магистрале се крећу од 1 – 5 Mb/s.

Основне компоненте плоче *Arduino UNO Rev3* су детаљно приказане на слици 3.6, микроконтролер је приказан на слици 3.7 а кабл за везу на слици 3.8.



Слика 3.6 Основне компоненте плоче *Arduino UNO Rev3*



Слика 3.7 Микроконтролер *ATmega328P*



Слика 3.8 Кабл за везу са *USB* прикључком

- 1 USB конектор
- 2 Конектор за напајање
- 3 Регулатор напона: регулише и стабилизује улазни и излазни напон
- 4 Кристални осцилатор: бележи време и регулише фреквенцију процесора
- 5 *Reset* пин
- 6 3,3 V пин: користи се као 3,3 V излаз
- 7 5 V пин: користи се као 5 V излаз
- 8 GND пин: користи се за уземљење кола
- 9 Vin пин: користи се за напајање плоче
- 10 10. Аналогни пинови (A0-A5): користе се за читање аналогних сигнала на плочи
- 11 Микроконтролер (ATMega328): процесорска и логичка јединица плоче
- 12 ICSP пин: заглавље за програмирање
- 13 ЛЕД индикатор напајања: показује стање напајања плоче
- 14 RX и TX LED: пријем (RX) и пренос (TX) - лед лампице трепере приликом слања, или пријема, серијских података
- 15 Дигитални I/O пинови:
- 16 AREF пин: за постављање референтног напона (горње границе за аналогне пинове)
- 17 Дугме за ресетовање: може се користити за ресетовање плоче

Са горње стране плоче налазе се два конектора (8 и 10 пинова) који су намењени раду са дигиталним сигнаlima. Пинови са ознакама 0 – 13, по потреби могу да имају функцију како улазних, тако и излазних конектора. Поред пинова 3, 5, 6, 9, 10 и 11 налази се знак „~” који напомиње да се они могу користити као псеудоаналогни излазни портови. Пошто ATmega328 микроконтролер нема *DAC* (*Digital-to-Analog Converter*) логику, користи се техника *PWM* (*Pulse Width Modulation*) за генерисање аналогних сигнала путем ширинска модулације квадратног таласа.

Техничке карактеристике плоче наведене су у табели 3.1.

Табела 3.1 Техничке карактеристике *Arduino UNO*

<i>Arduino UNO Rev3</i>	
Микроконтролер	ATmega328P
Радни напон	5 V
Улазни напон (препоручен)	7-12 V
Улазни напон (горња граница)	6-20 V
Дигитални I/O пинови	14
Аналогни улазни пинови	6
Максимална струја на I/O пиновима	40 mA
Максимална струја на 3,3 V пину	50 mA
<i>Flash</i> меморија	32 KB
SRAM	2 KB
EEPROM	1 KB
Фреквенција	16 MHz
Дужина	68,6 mm
Ширина	53,4 mm
Маса	25 g

На први поглед 32 килобајта делује као мала количина меморије, међутим *AVR* (*Automatic Voltage Regulation*) архитектура нуди брзину извршавања од милион инструкција у секунди, што уз 16 мегахерца даје довољно процесорске снаге за обраду информација [16]. Најуочљивији елемент на плочи је сам микроконтролер ATmega328P (P је ознака за „*PicoPower*” технологију уштеде енергије). Од осталих уочљивијих елемената могуће је издвојити тастер за ресетовање уређаја, регулатор напона који се налази поред улаза за напајање и кристал од 16 MHz у препознатљивом металном кућишту. Ту су и четири минијатурна *LED* светла од којих два показују слање у пријем података преко серијског порта (RX и TX), једно приказује да је уређај под напоном, док је четврто физички повезано са пином 13 и служи као индикатор његове активности.

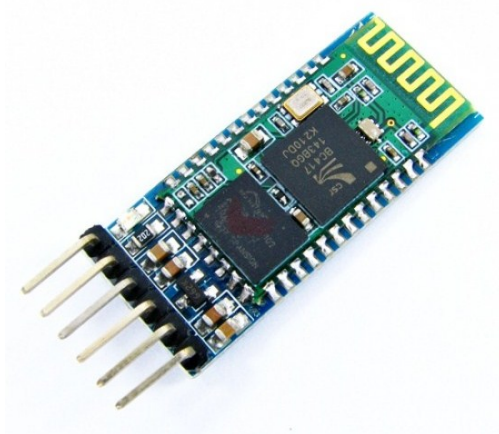
3.4 *Bluetooth* модул HC-05

Bluetooth технологија је начин бежичног преноса информација, осмишљен од стране компаније Ериксон (*Ericsson*) 1994. године. Упаривање уређаја је врло једноставно и уређаји који се повезују не морају бити физички видљиви један другом. Како би избегао међусобну интеракцију са другим уређајима који користе исте фреквенције, *Bluetooth* шаље врло слаб сигнал (око 1 mW). Ради поређења, сигнал јачих мобилних телефона је 3 W. То му ограничава домет на 10 m, који се може повећати и до 100 m.

Bluetooth технологија је прилично отпорна на широкопојасне сметње и омогућава више уређаја на истој локацији да комуницирају истовремено, а да се међусобно не ометају. Ова технологија се широко користи у телефонима, таблетима и лаптоповима.

Bluetooth модул HC-05 је дизајниран да оствари бежичну конекцију са контролером или рачунаром. Помоћу овог модула може се остварити комуникација између два микроконтролера као што је *Arduino*, или комуникација са било којим уређајем са *Bluetooth* функцијом, попут телефона или преносног рачунара. Модул је врло једноставан за коришћење и користан је за разна читавања где је потребна бежична комуникација. Изглед модула дат је на слици 3.9.

Постоје многе андроид апликације на основу којих корисник, применом овог бежичног модула може пренети податке са свог рачунара, или мобилног телефона, на микроконтролер, и обрнуто.



Слика 3.9 *Bluetooth* модул HC-05

Модул са ознаком HC-05 ради у опсегу од 2,4 GHz до 2,48 GHz и остварује размену података међу уређајима на раздаљини до 10 метара. Модул троши највише струје током процеса остваривања везе, до 40 милиампера, док је током рада потрошња знатно нижа и износи око 8 милиампера [17].

Неке од главних карактеристика HC-05 модула су:

- серијски *Bluetooth* модул за *Arduino* и остале микроконтролере,
- радни напон: 4 V до 6 V (обично 5 V),
- радна струја: 30 mA,

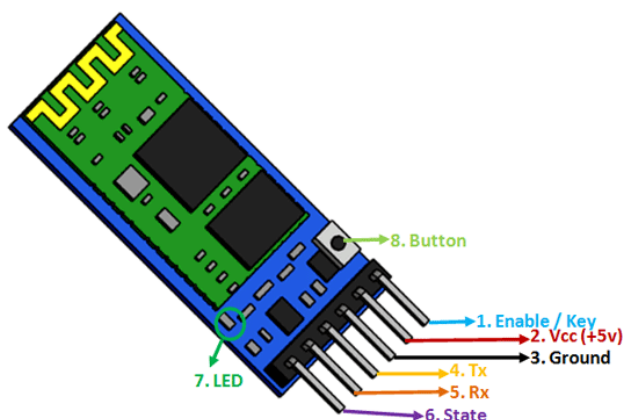
- распон: <10 m,
- IEEE 802.15.1 стандардни протокол,
- користи фреквенцијски распон FHSS (*Frequency-hopping spread spectrum*),
- може да ради у *Master*, *Slave*, или *Master/Slave* моду,
- лако повезивање са преносним или мобилним телефонима са Bluetooth-ом,
- подржане стандардне брзине преноса.

Техничке карактеристике *Bluetooth* модула HC-05 наведене су у табели 3.2.

Табела 3.2 Техничке карактеристике модула HC-05

<i>Bluetooth</i> модул HC-05	
Протокол	Bluetooth v2,0 + EDR
Радна фреквенција	2,4 GHz
Брзина	Асинхроно: до 2,1 Mbps / 160 kbps, Синхроно: 1Mbps / 1 Mbps
Осетљивост	≤ -84 dBm
Безбедност	Енкрипција и аутентификација
Модулација	GFSK (<i>Gaussian Frequency Shift Keying</i>)
Напајање	3,3 V - 5 V
Радна температура	-20 ~ +75°C
Димензије	27 mm x 14 mm x 2,5 mm

Ознаке пинова *Bluetooth* модула HC-05 приказане су на слици 3.10 [18].



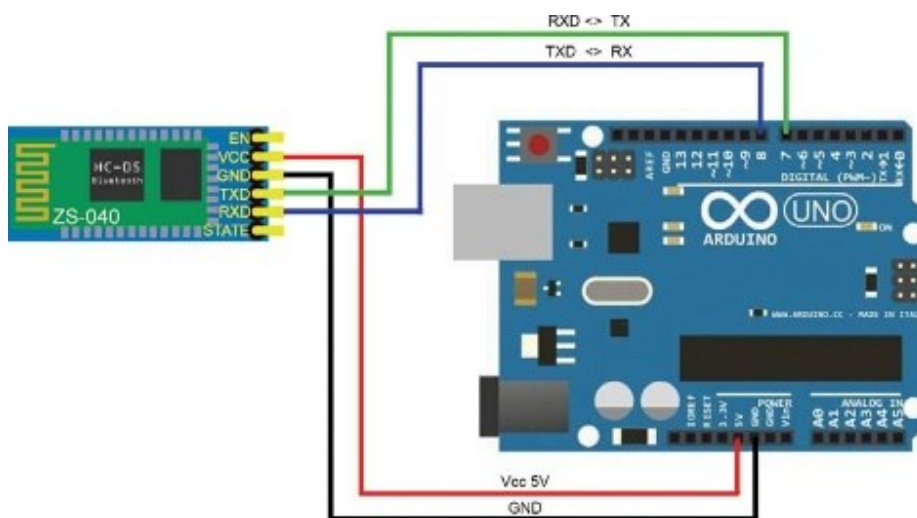
Слика 3.10 Пинови *Bluetooth* модула HC-05

Конфигурација пинова *Bluetooth* модула HC-05 наведене су у табели 3.3 [18].

Табела 3.3 Конфигурација пинова *Bluetooth* модула *HC-05*

Број пина	Име пина	Опис
1	Enable/key	За пребацивање између управљачког и рада са подацима
2	VCC	Напајање модула (5 V)
3	GND	Уземљење модула
4	TX	Пренос серијских података
5	RX	Пријем серијских података
6	State	Пин стања, повезан са LED-ом може се користити као повратна информација о исправном раду <i>Bluetooth</i> -а
7	LED	Означава статус модула: - трептање једном у две секунде – модул је у управљачком начину рада, - понављање трептања – чека на везу у моду за пренос података, - трептање два пута у једној секунди – успешно повезивање.
8	Button	За пребацивање између управљачког и рада са подацима

Bluetooth модул *HC-05* користи серијску (RX, TX) комуникацију са плочом на 3,3 V, па је у случају *Arduina* на 5 V неопходно користити разделник напона. RX (*receiver*) пин модула *HC-05* је повезан на дигитални пин 1 (TX) на *Arduino* микроконтролеру, док је TX (*transmitter*) на модулу *HC-05* повезан на пин 0 (RX) на *Arduino* микроконтролеру чиме је остварена серијска комуникација. За напајање се користи 5 V са *Arduino* микроконтролера. Начин везе је приказан на слици 3.11.



Слика 3.11 Начин везе *Bluetooth* модула *HC-05*

3.5 Piezzo buzzer

Пиезоелектрични звучник (познат као *Piezzo buzzer* или *Beep speaker* због свог начина рада) је звучник који користи пиезоелектрични ефекат за генерисање звука. Иницијално механичко кретање на пиезоелектричном материјалу се типично претвара у звук помоћу дијафрагми и резонатора. Звучници су релативно једноставне конструкције и често се користе за стварање звука у дигиталним кварцним сатовима и другим електронским уређајима. Углавном користе у апликацијама где су јачина звука и висока висина звука важнији од квалитета звука. Звукови који се обично користе да би се означило да је притиснуто дугме су клик, звоно или звучни сигнал.

На слици 3.12 је приказан *Piezzo buzzer MH-FMD* коришћен у овом раду. Овај модул зујалице је пасиван јер нема унутрашњу електронику за генерисање звука или тона. Спољна електроника, или уређај заснован на микроконтролеру, као што је Ардуино, је потребан да би модул произвео звук. Пошто је уређај пасиван, делује више као сићушни звучник, него као зујалица. Генерално, у примени је материјал који мења облик дејством електричне струје. У основи, извор звука је контакт пиезоелектричног диска и танке металне плоче (долази до савијања материјала напред-назад).



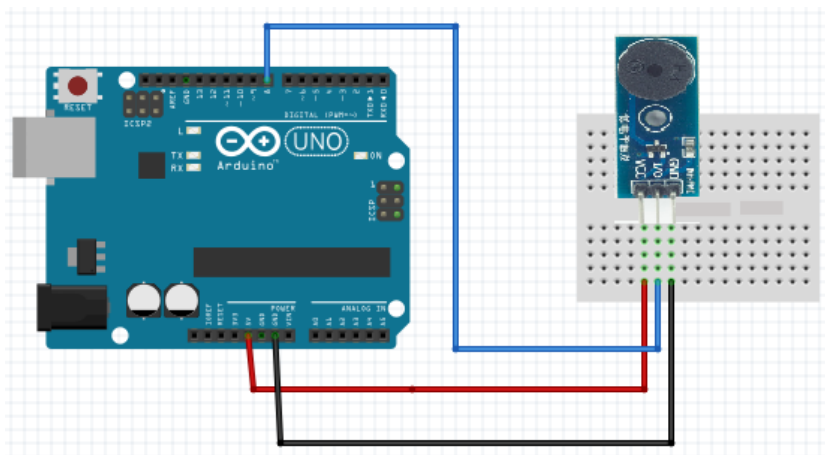
Слика 3.12 *Piezzo buzzer MH-FMD*

Модул садржи три пина за повезивање са Ардуино платформом:

- VCC – служи за напајање модула (5 V)
- GND – користи се за уземљење модула
- I/O – служи за управљање модулом

Зујалица се широко користи у рачунарима, штампачима, копирним уређајима, алармима, електронским играчкама, аутомобилској електронској опреми. Типична употреба ових уређаја (*buzzers* и *beepers*) код алармних уређаја укључује и потврду корисничког уноса попут клика мишем, или притиска тастера.

Начин везе зујалице и *Arduino* плоче приказан је на слици 3.13.



Слика 3.13 Начин везе Piezzo buzzer и Arduino плоче

3.6 Ултразвучни сензор растојања HC-SR04

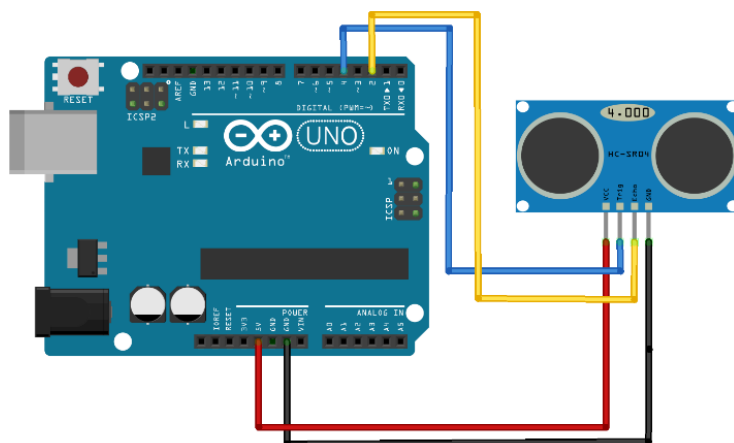
Као што им и само име говори, ултразвучни сензори растојања се користе за мерење растојања између сензора и објекта који се налази испред њега. Ови сензори нуде добру прецизност, једноставни су за употребу, ценовно доступни [19]. Једна од главних предности које имају ултразвучни сензори у односу на сличне модуле који користе ИС светлост јесте могућност прецизног мерења, без обзира на боју препреке, пошто тамни предмети упијају светлост и тиме компликују рад светлосних сензора.

Један од најчешће коришћених ултразвучних модула носи ознаку HC-SR04 и ради на фреквенцији од 40 мегахерца, док по спецификацији може детектовати предмете са прецизношћу од 3 mm на раздаљини од 2 cm до 4 m и са ширином мерења и до 30 степени. Сензор је компатибилан са *Arduino* платформом и изглед могула приказан је на слици 3.14.



Слика 3.14 Ултразвучни сензор растојања HC-SR04

Начин везе ултразвучног сензора растојања са *Arduino* плочом приказан је на слици 3.15 [20].



Слика 3.15 Начин везе Bluetooth модула HC-SR04

Модул се састоји од ултразвучног предајника, ултразвучног пријемника и контролне електронике. Један од цилиндара служи за генерисање звучног таласа, док је улога другог да детектује одбијени талас. У складу са тим, осим пинова за напајање, постоје и два додатна пина који служе за слање сигнала преко сензора (*Trigger*) и за прихватање рефлексије емитованог сигнала (*Echo*). Техничке карактеристике модула HC-SR04 наведене су у табели 3.4.

Табела 3.4 Техничке карактеристике модула HC-SR04 [7- Аутоматика]

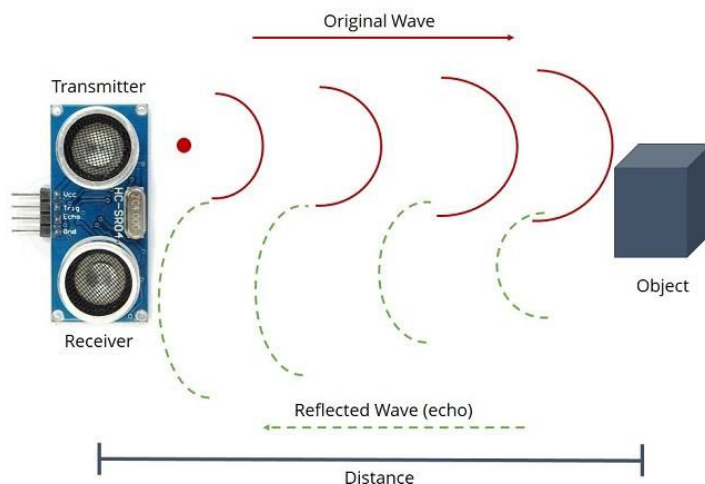
Ултразвучни сензор растојања HC-SR04	
Домет	2 – 500 cm
Прецизност	3 mm
Ефективни угао мерења	15°
Струја мировања	< 2 mA
Радна струја	15 mA
Напајање	5 V
Радна фреквенција	40°kHz
Димензије	45 mm x 20 mm x 15 mm

Конфигурација пинова модула HC-SR04 наведене су у табели 3.5 [20].

Табела 3.5 Конфигурација пинова модула HC-SR04

Број пина	Име пина	Опис
1	VCC	Напајање модула (5 V)
2	Trig	улазни пин (окидање/активирање мерења)
3	Echo	Излазни пин (повратни сигнал, дужина импулса пропорционална растојању)
4	GND	Уземљење модула

Сам концепт рада сензора растојања се састоји у томе да сензор емитује звучне импулсе високе фреквенције, који се у случају да се испред сензора налази препрека, одбијају од ње ка сензору. Ако су импулси детектовани након емитовања, може се претпоставити да се испред сензора налази препрека. Емитовани талас ће отићи до препреке и вратити се скоро истом брзином. Пошто је позната брзина кретања ваздуха (340 m/s) а у сензору се може измерити време које протекне да се талас, након емитовања, одбије од препреке и врати до сензора, могуће је утврдити дужину пута који је талас прешао, и самим тим и растојање препреке од сензора (слика 3.16).



Слика 3.16 Принцип рада сензора растојања HC-SR04

3.7 Сензор додира TTP223B

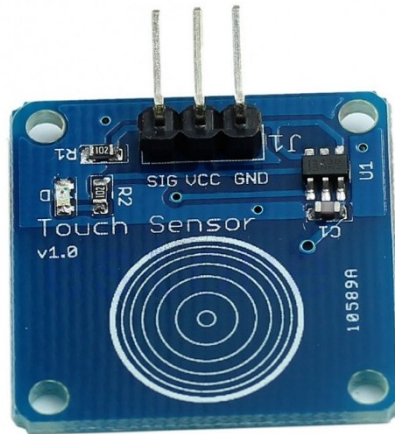
Сензор додира је електронски сензор који се користи за откривање и снимање физичког додира. То је мали, једноставни, јефтин сензор направљен да замени старе механичке прекидаче.

Сензор додира *TTP223B* је базиран на интегралном колу *TTP223* и у суштини, модул се понаша као тастер. Када дође до контакта, додира, или притиска на површини сензора за додир, он отвара електрични круг и омогућава струјама да пролазе кроз њега. Ако сензор не региструје додир, има стање логичке нуле, тј. *Output* је *Low*. Ако додир постоји, стање се мења на *High* и након престанка додира враћа се на *Low*. Сензори за додир имају разноврсну примену и користе се за управљање многим уређајима. (у роботици, аутомобилској индустрији, кућним апаратима, има их у кухињским славинама, лампама за светло, преносивим уређајима, у паметним телефонима, итд.) [21]. Модул је малих димензија, водоотпоран је и садржи три пина за повезивање:

- VCC – служи за напајање модула (5 V)
- GND – користи се за уземљење модула
- SIG – спаја се са улазним дигиталним пином *Arduina*

Ово је „тренутна“ врста сензора – чим се додирне укључује се, реагује и на крају се сам гаси (слика 3.17). С обзиром да сензор региструје додир и кроз танке материјале,

као што су папир, стакло, плексиглас или PVC фолија, згодан је да се постави или сакрије у зиду, радним површинама или неком другом месту. Садржи четири рупе на крајевима које служе за његову монтажу. Изглед сензора додира *TTP223B* дат је на слици 1.X. У случају да се више од 12 секунди не региструје додир, модул прелази у *low-power* режим у којем троши веома мало енергије.

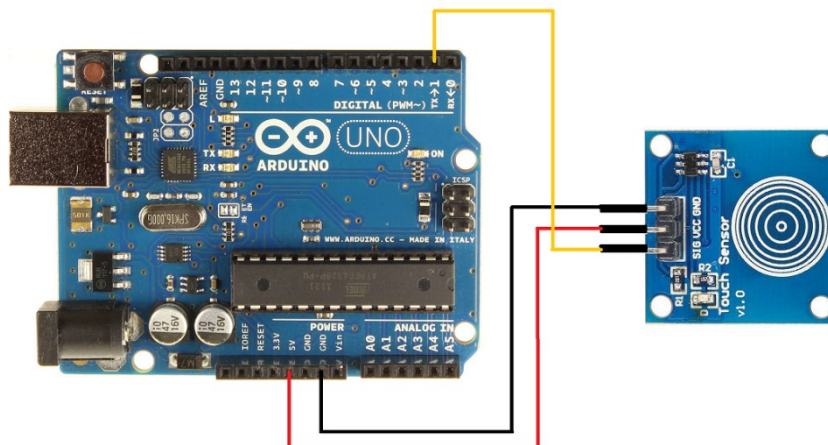


Слика 3.17 Сензор додира *TTP223B*

Главне карактеристике сензора су:

- ради на напонима од 2 V до 5 V,
- време одзива (режим мале снаге): 220 ms,
- време одзива (у режиму додира): 60 ms,
- димензије: 22 mm x 24 mm x 7,2 mm,
- маса: 2 g.,

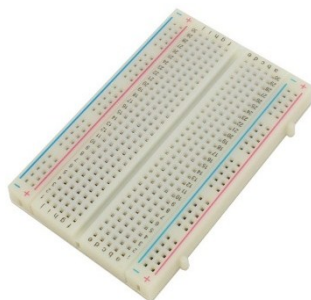
Начин везе сензора додира са *Arduino* плочом дат је на слици 3.17.



Слика 3.17 Начин везе сензора додира и *Arduino* плоче

3.8 Прототипска плоча

За израду одговарајућих прототипских решења у електроници најбоље је користити прототипску плочу. Помоћу ње могуће је прикључити компоненте на *Arduino* без лемљења. Направљена је од пластике и има низ рупица за пинове компонената и проводнике (слика 3.18). Обично постоје два низа рупица са обе стране, за напајање и уземљење. Унутар прототипске плоче се налазе металне траке које су проводне. Са овом металним тракама се повезују проводници (проводне жице) и пинови како би се формирало струјно коло. Прототипске плоче се израђују и продају у различитим величинама.



Слика 3.18 Прототипска плоча

3.9 Проводници за везу

Arduino комплет се испоручује са великим бројем проводника, који се током израде пројекта користе да би се формирало коло између *Arduina* и компонената уз коришћење прототипске плоче (слика 3.19). У примени су жице са одговарајућим конекторима. На свом крају оне имају одговарајући конектор који се користи за међусобно повезивање компонената плоче, интерно, или са другом опремом или компонентама, без лемљења. Појединачне жице се постављају уметањем њихових крајњих конектора у слотове или у део опреме за испитивање.

Постоје различите врсте жица за везу. Неке имају исти тип електричног конектора на оба краја, док други имају различите конекторе. Омогућавају једноставну везу елемената са плочом, правилан распоред компонената без страха од кратког споја. Израђене су од проводних материјала и разликују се по величини и боји да би се разликовали различити радни сигнали. Генерално, постоје три врсте жица (каблова): мушко-мушки, женско-мушки и мушко-женски.



Слика 3.19 Жице за везу

4. РЕАЛИЗАЦИЈА КОНТРОЛЕРА СИГУРНОСНОГ СИСТЕМА ЗА АРДУИНО ПЛАТФОРМУ

Поједини аутори су се бавили пројектима кућне безбедности на бази Ардуино платформе. Пројекат постављања магнетног сензора на кућна врата за Ардуино у оквиру сигурносног система, представљен је у [22]. У [23] је показано како се *Arduino UNO* може користити у развоју кућног сигурносног система мобилизацијом мреже сензора, који шаљу повратно упозорења на *Arduino UNO* када се активирају аларми.

Рад на *Arduino* платформи омогућава креирање различитих електронских компоненти. Обухвата читаву колекцију хардвера и софтвера отвореног кода која омогућава да се прикључе и контролишу друге компоненте у оквиру креираног струјног кола [24].

Реализација пројекта сигурносног система базираног на *Arduino* платформи обухватала је следеће активности:

- повезивање компонената са *Arduino* микроконтролером,
- писање програма за контролу компонената (*Arduino IDE*),
- провера да ли је програм правилно написан,
- преношење програма на *Arduino UNO* плочу.
- развој мобилне апликације за контролу рада сигурносног система (*Android Studio*).

Изглед коришћених модула повезаних на *Arduino UNO* плочу, ради реализације сигурносног система заснованог на Ардуино платформи дат је на слици 4.1.

Све компоненте су постављене на прото плоче и повезане су помоћу жица са *Arduino UNO* микроконтролером.

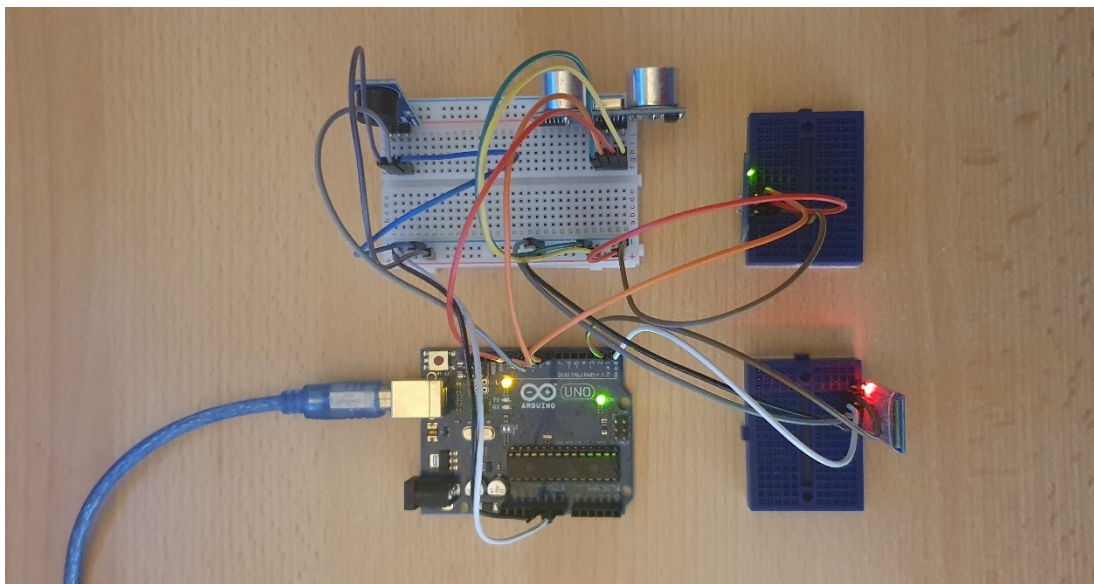
Зујалица *Piezzo buzzer MH-FMD* повезана је на следећи начин:

- GND пин је повезан са GND пином плоче
- VCC пин је повезан са напајањем од 5 V са плоче
- I/O – пин је повезан са дигиталним пином (10) као *output*.

Све компоненте су постављене на прото плоче и повезане су помоћу жица са *Arduino UNO* микроконтролером.

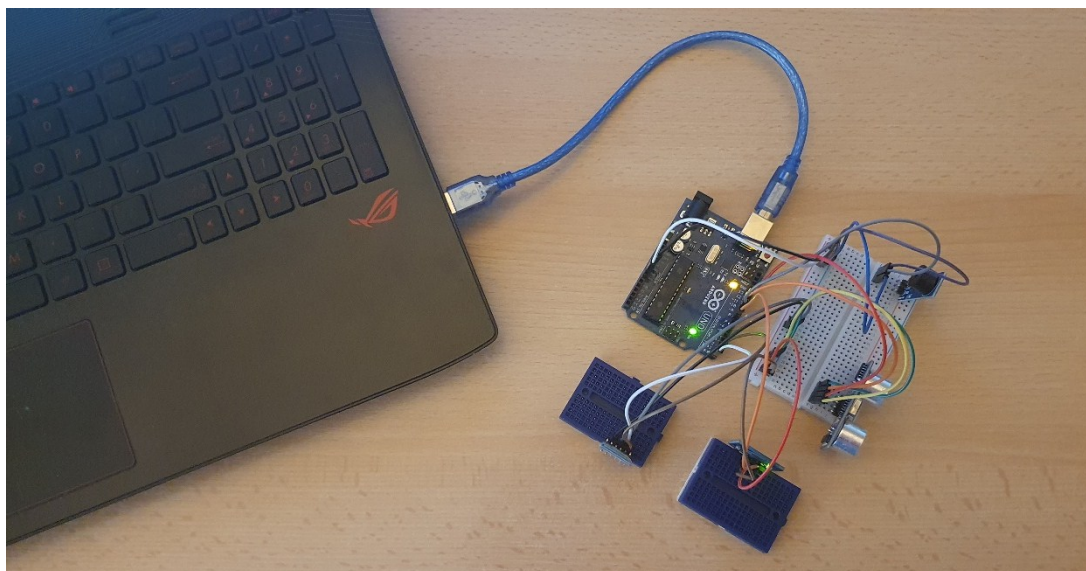
Зујалица *Piezzo buzzer MH-FMD* повезана је на следећи начин:

- GND пин је повезан са GND пином плоче
- VCC пин је повезан са напајањем од 5 V са плоче
- I/O – пин је повезан са дигиталним пином (10) као *output*.



Слика 4.1 Изглед Ардуино платформе

Ардуино плоча је повезана са рачунаром помоћу USB прикључка (слика 4.2).



Слика 4.2 Веза Ардуино плоче са рачунаром

Ултразвучни сензор растојања HC-SR04 повезан је на следећи начин:

- VCC пин је повезан са напајањем од 5 V са плоче
- GND пин је повезан са GND пином плоче
- Trig пин је повезан са дигиталним пином (12)
- Echo пин је повезан са дигиталним пином (11)

Сензор додира TTP223B повезан је на следећи начин:

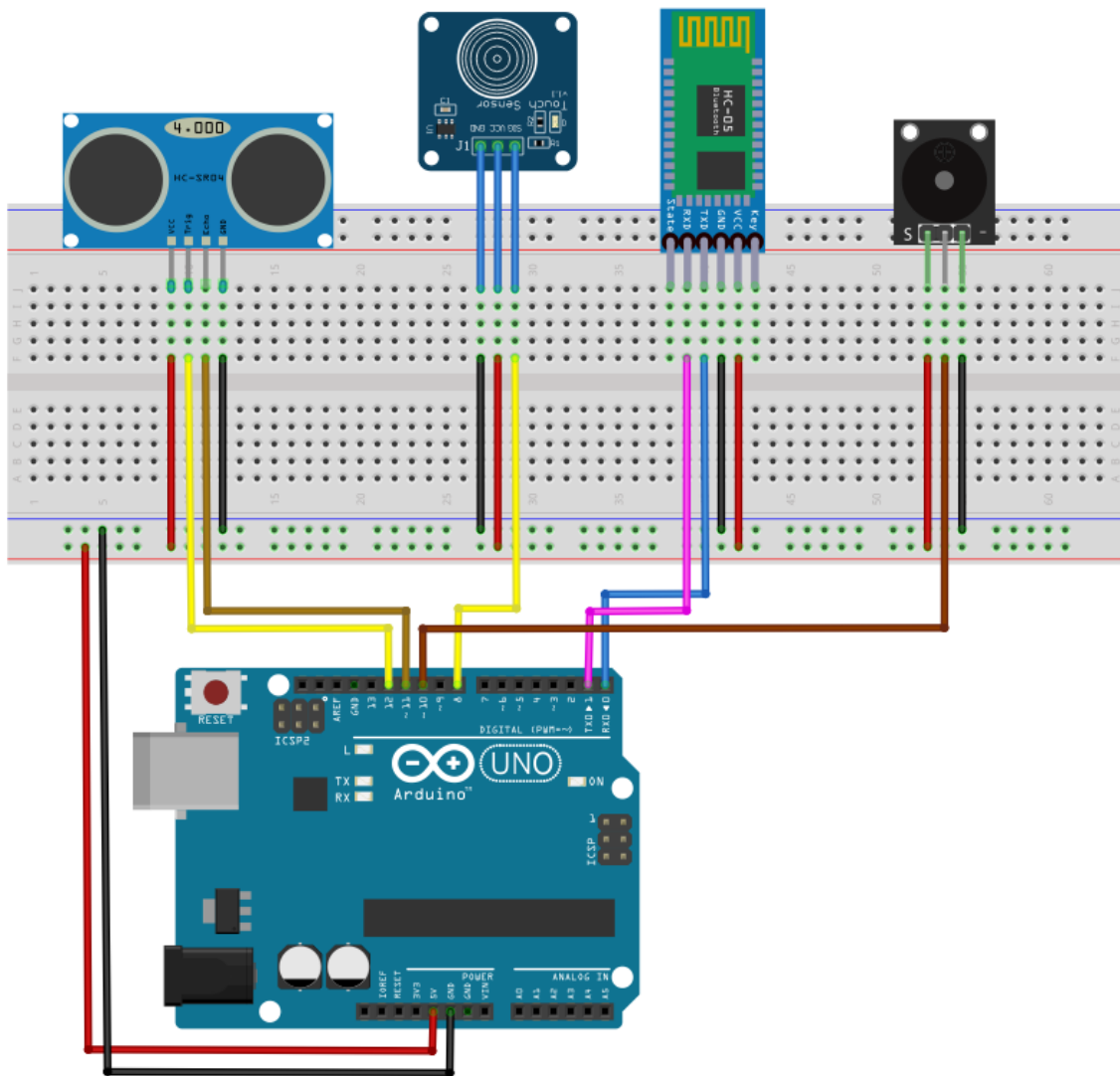
- VCC пин је повезан са напајањем од 5 V са плоче
- GND пин је повезан са GND пином плоче

- SIG пин повезан са дигиталним пином (8) као *input*.

Bluetooth модул HC-05 повезан је на следећи начин:

- VCC пин је повезан са напајањем од 5 V са плоче
- GND пин је повезан са GND пином плоче
- TX пин је повезан са дигиталним пином (0) тј. RX пином
- RX пин је повезан са дигиталним пином (1) тј. TX пином

Изглед шеме ожичења приказан је на слици 4.3.



Слика 4.3 Шема ожичења

Комплетан код написан у програмском окружењу *Arduino IDE* налази се на слици 4.4.



```

Diplomski_Marko_Miloradovic_575-2016 | Arduino 1.8.13
File Edit Sketch Tools Help

Diplomski_Marko_Miloradovic_575-2016 §

#include <NewPing.h>
#define TRIGGER_PIN 12
#define ECHO_PIN 11
#define MAX_DISTANCE 500

NewPing sonar(TRIGGER_PIN, ECHO_PIN, MAX_DISTANCE);

char incomingByte;

unsigned int pingSpeed = 50;
unsigned long pingTimer;
int flag = 0;

void setup() {
  Serial.begin(9600);
  pingTimer = millis();
  pinMode(10, OUTPUT);
  pinMode(8, INPUT);
}

void loop() {
  if(Serial.available() > 0 ){
    incomingByte = Serial.read();
  }
  if (millis() >= pingTimer) {
    pingTimer += pingSpeed;
    sonar.ping_timer(echoCheck);
    if(digitalRead(8)==HIGH){
      Serial.println("Sensor is touched");
      delay(500);
    }
  }
  if (flag == 1 && incomingByte=='1')
  {
    digitalWrite(10, HIGH);
    delay(100);
    digitalWrite(10, LOW);
    delay(100);
    digitalWrite(10, HIGH);
    delay(100);
    digitalWrite(10, LOW);
    delay(100);
  }
  else
  {
    digitalWrite(10, HIGH);
  }
}

void echoCheck() {
  if (sonar.check_timer()) {
    Serial.print("Ping: ");
    Serial.print(sonar.ping_result / US_ROUNDTRIP_CM);
    Serial.println("cm");
    if ((sonar.ping_result / US_ROUNDTRIP_CM) < 10 || digitalRead(8)==HIGH)
      flag = 1;
    else if ((sonar.ping_result / US_ROUNDTRIP_CM) > 10)
      flag = 0;
  }
}

```

Слика 4.4 Комплетан код Arduino IDE

Да би рад са ултразвучним сензором растојања био лакши прво је импортована библиотека *NewPing.h* која садржи корисне методе за рад са овим сензором. Затим су дигитални пинови 11 и 12 дефинисани као *ECHO_PIN* и *TRIGGER_PIN*, респективно. Такође је дефинисано максимално растојање до којег сензор ефективно ради (5 m) као *MAX_DISTANCE*. Затим се сензор подешава за рад помоћу претходно дефинисаних пина и максималног растојања. Следи дефинисање променљивих: *incomingByte (char)* у којој се чува податак послат помоћу *Bluetooth* серијске комуникације, *pinkSpeed (unsigned int)* која има вредност 50 и говори о томе колико често се шаље пинг (у ms), *pinkTimer (unsigned long)* и *flag (int)* чија је вредност нула.

У *setup* функцији дефинисан је дигитални пин 10 као излаз, дигитални пин 8 као улаз. Променљивој *pinkTimer* је додељена вредност функције *millis()* која враћа број милсекунди који је протекао од када је покренут тренутни програм на плочи. Затим се поставља и иницијализује серијска комуникација која је изражена кроз *baud rate* 9600.

У *loop* функцији прво се проверава да ли је примљен податак преко *bluetooth* комуникације и ако јесте чува се у променљивој *incomingByte*. Затим се проверава да ли је активиран сензор додира и да ли је ултразвучни сензор детектовао покрет у дефинисаној зони рада (*flag=1*). Ако јесте и ако је аларм активиран преко телефона уз помоћ мобилне апликације зујалица ће емитовати пар кратких звучних сигнала.

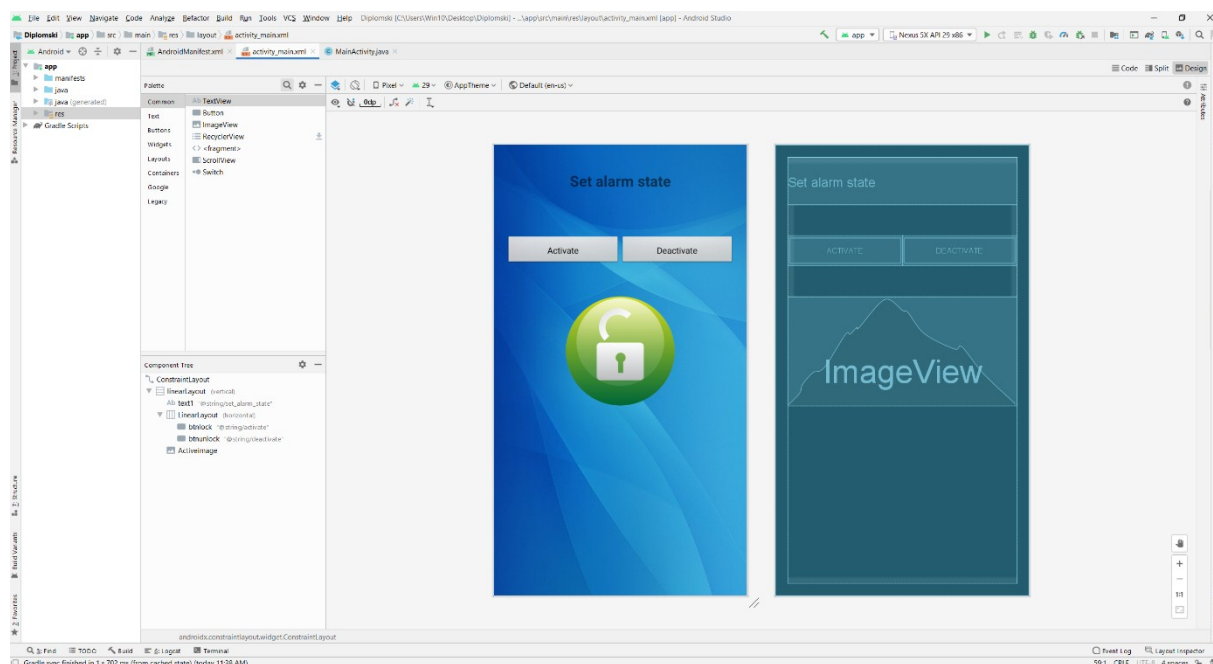
Помоћна функција *echoCheck* има улогу да провери да ли је дошло до додира са сензором додира, или је детектован покрет у дефинисаној зони ултразвучног сензора. Ако јесте, променљивој *flag* се додељује вредност 1.

Након што је програм написан, следи верификација и *upload* програма на микроконтролерску плочу.

Ради контроле рада сигурносног система развијена је андроид апликација применом Андроид студио програма у *Java* програмском језику. Апликација омогућава кориснику да активира или деактивира аларм при чему на свом мобилном телефону добија повратну информацију о тренутном стању система у виду поруке на екрану и слике. Изглед креиране апликације приказан је на слици 4.5.

Апликација садржи два дугмета:

- *Activate* – служи да се сигурносни систем постави у активно стање,
- *Deactivate* - служи да се сигурносни систем искључи.



Слика 4.5 Изглед апликације

Изглед слика које корисник добија у зависности од тога да ли је аларм активан или не, дат је на сликама 4.6 а) и 4.6 б).



а)



б)

Слика 4.6 Изглед дугмади: а) аларм активиран, б) аларм деактивиран

Поруке које корисник добија у зависности од тренутног стања система су:

- *Alarm activated!* – сигурносни систем је активиран,
- *Alarm already activated!* – сигурносни систем је већ раније активиран,
- *Alarm deactivated!* - сигурносни систем је искључен,
- *Alarm already deactivated!* - сигурносни систем је већ раније искључен.

Пре него што се почне са развијањем андроид апликације, потребно је да се у манифест фајлу апликације додају одређена одобрења самој апликацији да може да користи *Bluetooth*. (слика 4.7).

```
<uses-permission android:name="android.permission.BLUETOOTH" />
<uses-permission android:name="android.permission.BLUETOOTH_ADMIN" />
```

Слика 4.7 Одобрења у манифест фајлу апликације

Комплетан код развијене андроид апликације која служи за комуникацију са модулом наведен је на слици 4.8.

```
package com.example.diplomski;

import androidx.appcompat.app.AppCompatActivity;

import android.bluetooth.BluetoothAdapter;
import android.bluetooth.BluetoothDevice;
import android.bluetooth.BluetoothSocket;
import android.content.Intent;
import android.os.Build;
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.ImageView;
import android.widget.Toast;

import java.io.IOException;
import java.io.OutputStream;
import java.lang.reflect.Method;
import java.util.UUID;

public class MainActivity extends AppCompatActivity {
    private static final String TAG = "HC-05";
    private int alarm_state=0;
    Button btnLock,btnUnlock;
    ImageView iv1;

    private BluetoothAdapter btAdapter = null;
    private BluetoothSocket btSocket = null;
    private OutputStream outputStream = null;

    private static final UUID MY_UUID = UUID.fromString("00001101-0000-1000-8000-00805F9B34FB");
    private static String address = "00:18:E4:34:CB:51";

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        btnLock= (Button) findViewById(R.id.btnLock);
        btnUnlock= (Button) findViewById(R.id.btnunLock);
        iv1=(ImageView) findViewById(R.id.Activeimage);
        btAdapter = BluetoothAdapter.getDefaultAdapter();
        checkBTState();
    }
}
```

Слика 4.8 Комплетан код апликације

```

        btnLock.setOnClickListener((v) -> {
            if(alarm_state==0){
                sendData("1");
                Toast.makeText(getBaseContext(), text: "Alarm activated!", Toast.LENGTH_SHORT).show();
                iv1.setImageResource(R.drawable.Locked);
                alarm_state=1;
            }else{
                Toast.makeText(getBaseContext(), text: "Alarm already activated!", Toast.LENGTH_SHORT).show();
            }
        });

        btnUnlock.setOnClickListener((v) -> {
            if(alarm_state==1){
                sendData("2");
                Toast.makeText(getBaseContext(), text: "Alarm deactivated!", Toast.LENGTH_SHORT).show();
                iv1.setImageResource(R.drawable.unlocked);
                alarm_state=0;
            }else{
                Toast.makeText(getBaseContext(), text: "Alarm already deactivated!", Toast.LENGTH_SHORT).show();
            }
        });
    }

    private BluetoothSocket createBluetoothSocket(BluetoothDevice device) throws IOException {
        if (Build.VERSION.SDK_INT >= 10) {
            try {
                final Method m = device.getClass().getMethod( name: "createInsecureRfcommSocketToServiceRecord", new Class[]{UUID.class});
                return (BluetoothSocket) m.invoke(device, MY_UUID);
            } catch (Exception e) {
                Log.e(TAG, msg: "Could not create Insecure RFComm Connection", e);
            }
        }
        return device.createRfcommSocketToServiceRecord(MY_UUID);
    }

    @Override
    public void onResume() {
        super.onResume();
        Log.d(TAG, msg: "...onResume - trying to connect...");
        BluetoothDevice device = btAdapter.getRemoteDevice(address);

        try {
            btSocket = createBluetoothSocket(device);
        } catch (IOException e1) {
            errorExit( title: "Fatal Error", message: "In onResume() and socket create failed: " + e1.getMessage() + ".");
        }
        btAdapter.cancelDiscovery();
    }

```

Слика 4.8 Комплетан код апликације - наставак 1

```

Log.d(TAG, msg: "...Connecting...");
try {
    btSocket.connect();
    Log.d(TAG, msg: "...Connection ok...");
} catch (IOException e) {
    try {
        btSocket.close();
    } catch (IOException e2) {
        errorExit( title: "Fatal Error", message: "In onResume() and unable to close socket during connection failure" + e2.getMessage() + ".");
    }
}

Log.d(TAG, msg: "...Create Socket...");

try {
    outputStream = btSocket.getOutputStream();
} catch (IOException e) {
    errorExit( title: "Fatal Error", message: "In onResume() and output stream creation failed:" + e.getMessage() + ".");
}
}

@Override
public void onPause() {
    super.onPause();

    Log.d(TAG, msg: "...In onPause()...");

    if (outStream != null) {
        try {
            outStream.flush();
        } catch (IOException e) {
            errorExit( title: "Fatal Error", message: "In onPause() and failed to flush output stream: " + e.getMessage() + ".");
        }
    }
}
try {
    btSocket.close();
} catch (IOException e2) {
    errorExit( title: "Fatal Error", message: "In onPause() and failed to close socket." + e2.getMessage() + ".");
}
}

private void checkBTState() {
    if (btAdapter == null) {
        errorExit( title: "Fatal Error", message: "Bluetooth not supported");
    } else {
        if (btAdapter.isEnabled()) {
            Log.d(TAG, msg: "...Bluetooth ON...");
        } else {
            Intent enableBtIntent = new Intent(BluetoothAdapter.ACTION_REQUEST_ENABLE);
            startActivityForResult(enableBtIntent, requestCode: 1);
        }
    }
}

private void errorExit(String title, String message) {
    Toast.makeText(getBaseContext(), text: title + " - " + message, Toast.LENGTH_LONG).show();
    finish();
}

private void sendData(String message) {
    byte[] msgBuffer = message.getBytes();
    Log.d(TAG, msg: "...Send data: " + message + "...");

    try {
        outputStream.write(msgBuffer);
    } catch (IOException e) {
        String msg = "In onResume() and an exception occurred during write: " + e.getMessage();
        errorExit( title: "Fatal Error", msg);
    }
}

```

Слика 4.8 Комплетан код апликације - наставак 2

У оквиру андроид апликације развијене за овај пројекат коришћене су библиотеке приказане на слици 4.9.

```
import android.bluetooth.BluetoothAdapter;
import android.bluetooth.BluetoothDevice;
import android.bluetooth.BluetoothSocket;
import android.content.Intent;
import android.os.Build;
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.ImageView;
import android.widget.Toast;

import java.io.IOException;
import java.io.OutputStream;
import java.lang.reflect.Method;
import java.util.UUID;
```

Слика 4.9 Андроид библиотеке

Неке од најзначајнијих библиотека неопходних за рад са Ардуино платформом су:

- *android.bluetooth.BluetoothAdapter*,
- *android.bluetooth.BluetoothDevice*,
- *android.bluetooth.BluetoothSocket*,
- *java.util.UUID*.

Прве три библиотека служе да омогуће рад апликације са *bluetooth* модулом. *BluetoothAdapter* омогућава коришћење фундаменталних *bluetooth* операција – претрагу доступних *bluetooth* уређаја унутар опсега нашег модула као и креирање листе упарених уређаја. *BluetoothDevice* представља удаљени *bluetooth* уређај са којим се успоставља конекција. Унутар њега се смештају неке основне информације као што су име, адреса, класа и стање повезаности са удаљеним уређајем. *BluetoothSocket* представља почетак, или крај везе, у којој се размењују подаци са удаљеним *bluetooth* уређајем. *UUID* (*universally unique identifier*) се користи за постављање глобалног идентификатора који се не мења и чија је дужина 128 бита.

Потребне променљиве за рад апликације су:

- *alarm_state* - означава да ли је сигурносни систем активан, или не (1 – активан, 0 – неактиван),
- *btnLock*, *btnUnlock*, *iv1* – служе за дефинисање графичких компоненти (*Button*, *ImageView*).
- *btAdapter* - означава *BluetoothAdapter*,
- *btSocket* – означава *BluetoothSocket*,

- *outStream* – служи за слање података преко *bluetooth*-а,
- *MY_UUID* – јединствени идентификатор модула HC-05,
- *address* – MAC адреса *bluetooth* уређаја са којим се успоставља комуникација.

Наведене променљиве приказане су на слици 4.10.

```
private static final String TAG = "HC-05";
private int alarm_state=0;
Button btnLock,btnUnlock;
ImageView iv1;

private BluetoothAdapter btAdapter = null;
private BluetoothSocket btSocket = null;
private OutputStream outStream = null;

private static final UUID MY_UUID = UUID.fromString("00001101-0000-1000-8000-00805F9B34FB");
private static String address = "00:18:E4:34:CB:51";
```

Слика 4.10 Променљиве

У оквиру дела апликације који дефинише шта се дешава приликом покретања апликације (*onCreate*) успостављена је веза између дефинисаних променљивих *btnLock*, *btnUnlock*, *iv1* и графичких елемената који их представљају (слика 4.11). Затим се врши иницијализација *bluetooth* модула и проверава се да ли је тај модул доступан.

```
@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);

    btnLock= (Button) findViewById(R.id.btnlock);
    btnUnlock= (Button)findViewById(R.id.btnunlock);
    iv1=(ImageView)findViewById(R.id.Activeimage);
    btAdapter = BluetoothAdapter.getDefaultAdapter();
    checkBTState();
}
```

Слика 4.11 *onCreate* део апликације

Ако је сигурносни систем угашен а корисник притисне дугме *Activate*, апликација ће послати поруку сигурносном систему да се активира (слика 4.6 а), на екрану ће се приказати слика 4.6 б), уз одговарајућу поруку.

Ако је сигурносни систем укључен, а корисник притисне дугме *Deactivate*, апликација ће послати поруку сигурносном систему да се искључи (слика 4.6 б), на екрану ће се приказати слика 4.6 а), уз одговарајућу поруку.

Део кода који регулише понашање апликације након што корисник притисне дугме *Activate* или *Deactivate* наведен је на слици 4.12.

```

btnLock.setOnClickListener((v) -> {
    if(alarm_state==0){
        sendData("1");
        Toast.makeText(getBaseContext(), text: "Alarm activated!", Toast.LENGTH_SHORT).show();
        iv1.setImageResource(R.drawable.Locked);
        alarm_state=1;
    }else{
        Toast.makeText(getBaseContext(), text: "Alarm already activated!", Toast.LENGTH_SHORT).show();
    }
});

btnUnlock.setOnClickListener((v) -> {
    if(alarm_state==1){
        sendData("2");
        Toast.makeText(getBaseContext(), text: "Alarm deactivated!", Toast.LENGTH_SHORT).show();
        iv1.setImageResource(R.drawable.unlocked);
        alarm_state=0;
    }else{
        Toast.makeText(getBaseContext(), text: "Alarm already deactivated!", Toast.LENGTH_SHORT).show();
    }
});
}

```

Слика 4.12 Activate или Deactivate код

Метода *createBluetoothSocket* служи за креирање *BluetoothSocket-a*, (слика 4.13).

```

private BluetoothSocket createBluetoothSocket(BluetoothDevice device) throws IOException {
    if (Build.VERSION.SDK_INT >= 10) {
        try {
            final Method m = device.getClass().getMethod( name: "createInsecureRfcommSocketToServiceRecord", new Class[]{UUID.class});
            return (BluetoothSocket) m.invoke(device, MY_UUID);
        } catch (Exception e) {
            Log.e(TAG, msg: "Could not create Insecure RfComm Connection", e);
        }
    }
    return device.createRfcommSocketToServiceRecord(MY_UUID);
}

```

Слика 4.13 Креирање *BluetoothSocket-a*

Метода *onResume* дефинише *BluetoothDevice* на основу MAC адресе (*address*) и регулише шта се дешава приликом настављања комуникације у оквиру истог *BluetoothSocket-a* (слика 4.14).

```
@Override
public void onResume() {
    super.onResume();
    Log.d(TAG, msg: "...onResume - trying to connect...");
    BluetoothDevice device = btAdapter.getRemoteDevice(address);

    try {
        btSocket = createBluetoothSocket(device);
    } catch (IOException e1) {
        errorExit( title: "Fatal Error", message: "In onResume() and socket create failed: " + e1.getMessage() + ".");
    }
    btAdapter.cancelDiscovery();

    Log.d(TAG, msg: "...Connecting...");
    try {
        btSocket.connect();
        Log.d(TAG, msg: "...Connection ok...");
    } catch (IOException e) {
        try {
            btSocket.close();
        } catch (IOException e2) {
            errorExit( title: "Fatal Error", message: "In onResume() and unable to close socket during connection failure" + e2.getMessage() + ".");
        }
    }

    Log.d(TAG, msg: "...Create Socket...");

    try {
        outputStream = btSocket.getOutputStream();
    } catch (IOException e) {
        errorExit( title: "Fatal Error", message: "In onResume() and output stream creation failed:" + e.getMessage() + ".");
    }
}
```

Слика 4.14 Део изворног кода методе *onResume*

Метода *checkBTState* служи да провери тренутну доступност *bluetooth* модула на уређају и ако је доступан, тражи се од андроид система да се укључи (слика 4.15).

```
private void checkBTState() {
    if (btAdapter == null) {
        errorExit( title: "Fatal Error", message: "Bluetooth not supported");
    } else {
        if (btAdapter.isEnabled()) {
            Log.d(TAG, msg: "...Bluetooth ON...");
        } else {
            Intent enableBtIntent = new Intent(BluetoothAdapter.ACTION_REQUEST_ENABLE);
            startActivityForResult(enableBtIntent, requestCode: 1);
        }
    }
}
```

Слика 4.15 Део изворног кода методе *checkBTState*

Метода *errorExit* служи да се прикажу различита обавештења на корисничком екрану настала као последица грешака у раду апликације, након чега долази до гашења апликације (слика 4.16).

```
private void errorExit(String title, String message) {
    Toast.makeText(getBaseContext(), text: title + " - " + message, Toast.LENGTH_LONG).show();
    finish();
}
```

Слика 4.16 Део изворног кода методе *errorExit*

Метода *sendData* служи за слање информација података путем *bluetooth* серијске комуникације (слика 4.17). Као улазни параметар ова метода има променљиву *String*. Потом се иницијализује низ бајтова (*msgBuffer*) унутар којег се смештају бајтови горе наведеног *String* -а (превођење променљиве *String* у променљиву типа *byte* се извршава помоћу методе *getBytes*). Затим се покушава слање тог податка путем методе *outStream.write* која шаље низ података (бајтова).

```
private void sendData(String message) {
    byte[] msgBuffer = message.getBytes();
    Log.d(TAG, "msg: "...Send data: " + message + "...");

    try {
        outStream.write(msgBuffer);
    } catch (IOException e) {
        String msg = "In onResume() and an exception occurred during write: " + e.getMessage();
        errorExit( title: "Fatal Error", msg);
    }
}
```

Слика 4.17 Део изворног кода методе *sendData*

4.1 Критички осврт на предности и мане реализованог уређаја

Анализом реализованог уређаја уочене су следеће његове предности:

- једноставност система,
- лакоћа употребе,
- могућност лаке надоградње новим, снажнијим компонентама,
- релативно ниска цена компонената,
- могућност надоградње система да контролисање система не буде ограничено само на мобилни телефон, већ и на друге паметне уређаје (даљински управљач, паметни сат, итд.),
- флексибилност у додавању нових сензора и
- релативно једноставан и разумљив програмски код.

Неки од уочених недостатака су:

- мали домет *Bluetooth* уређаја,
- неопходан *smart phone* за контролу и управљање сигурносним системом,
- корисник не добија нотификацију у случају ако се активира сензор додира или ултразвучни сензор, већ је једина повратна информација звук са зујалице,
- реализовани уређај не поседује своју батерију и зависи од USB напајања.

5. ЗАКЉУЧАК

У раду је разматрана реализација сигурносног система на бази Ардуино платформе.

Сигурносни системи су системи који раде у реалном времену и припадају групи мерно-информационих система. Фокусирани су на заштиту од специфичног ризика, на основу чега се врши и њихова класификација. У складу са тим разликују се следећи сигурносни системи: кућни, комерцијални, рачунарски, за дојаву пожара и за личну заштиту. Глобална структура сигурносних система је дефинисана међународним ИЕС стандардом.

У сигурносним системима се користе бројне врсте сензора. Најчешће коришћени сензори су: сензори за прозоре и врата, сензори покрета, сензори гасова и други. Сигурносни системи садрже и сигурносне камере и уређаје за упозорење - сирене. Сензори и детектори у сигурносним системима за заштиту од провале су уређаји који откривају упад. Они откривају провалнике различитим методама, као што су: праћење отварања врата и прозора, праћење појаве покрета, звука, лома стакла, вибрације, или других поремећаја.

Реализована апликација у оквиру дипломског рада је написана у програмском језику *JAVA*, у радном окружењу *Android Studio*. *Android Studio* је развојно окружење (*IDE*) за развој мобилних апликација засновано на *IntelliJ* окружењу.

Arduino је заједнички назив за фамилију микроконтролерских платформи које се користе у развоју апликација које на једноставан начин остварују везу између хардверских и софтверских елемената система.

Пројекат сигурносног система базираног на *Arduino* платформи реализован је кроз повезивање компонената са *Arduino* микроконтролером, писање програма за контролу компонената (*Arduino IDE*), проверу програма, преношење програм на *Arduino UNO* плочу и развој мобилне апликације за контролу рада сигурносног система (*Android Studio*).

Arduino платформа је успешно употребљена за идејно решење рада сигурносног система применом одговарајућих сензора. Систем је флексибилан, може се лако надоградити, чиме се могу превазићи уочени потенцијални недостаци.

6. ЛИТЕРАТУРА

- [1] Smith, S. *The History of Security Systems*. Hoyles Electronic Developments Ltd. [Online] 2016. [Cited: 1st September, 2020] <http://www.hoyles.com/blog/history-security-systems/>
- [2] SafeWise Team. *Home Safety and Security Stats and Facts*. SafeWise. [Online] 2018. [Cited: 1st September, 2020] <https://www.safewise.com/resources/security-stats-facts/>
- [3] De Guzman, R. et al. *Remote Home Security System using Open-Source Electronic Platform*. International Journal of Computer Applications, Vol. 178, No. 22, pp. 5-8, 2019.
- [4] Благојевић, М. *Технички системи заштите I*. Факултет заштите на раду у Нишу, Ниш, 2012.
- [5] hrv.kagutech.com. *Sigurnosni sustav za privatne kuće: pregled najboljih proizvođača i recenzija*. [Online] 2020. [Cited: 1st September, 2020] <https://hrv.kagutech.com/4271337-security-system-for-private-homes-an-overview-of-the-best-manufacturers-and-reviews>
- [6] International electrotechnical commission (IEC). *IEC 62642-1:2010 Alarm systems - Intrusion and hold-up systems - Part 1: System requirements*. IEC, Geneva, 2010.
- [7] Благојевић, М. *Алармни системи*. Факултет заштите на раду у Нишу, 2015.
- [8] Future Fibre Technologies. *The boundaries of security - global trends in perimeter security*. Future Fibre Technologies, Mulgrave, 2009.
- [9] SecuritySEE.com - Магазин за безбедност. *Видео надзор - Ефикасан систем заштите Вашег дома и пословног простора*. [Online] 2018. [Приступљено: 01.09.2020.] <https://www.securitysee.com/2018/10/video-nadzor-efikasan-sistem-zastite-vaseg-doma-i-poslovnog-prostora/>
- [10] Procar security. *Видео надзор - Савремени системи за већу безбедност*. [Online] 2017. [Приступљено: 15.09.2020.] <https://www.procar.rs/blog/video-nadzor-savremeni-sistemi-za-ve-u-bezbednost.html>
- [11] Smyth N. *Android Studio 3.0 Development Essentials – Android 8 Edition*. Payload Media, Inc., 2017
- [12] Android developers. *Meet Android Studio*. [online] 2020. [Cited: 15.09.2020.]. <https://developer.android.com/studio/intro>
- [13] Arduino. *Arduino IDE Software*. [online] 2020. [Downloaded: 15.09.2020.] <https://www.arduino.cc/en/Main/Software>

- [14] Ibrahim, D. *Колекција пројеката са сензорима: 40+ пројеката за Arduino, Raspberry Pi и ESP32*. Агенција Ехо, Ниш, 2020.
- [15] Теодоровић, П. *Увод у дигиталну и микрорачунарску електронику - Материјал за аудиторне вежбе – Arduino упутство*. Факултет техничких наука, Нови Сад, [Приступљено: 05.09.2020.] <https://www.elektronika.ftn.uns.ac.rs/elektronika-e2/wp-content/uploads/sites/87/2018/03/Arduino-uputstvo.pdf>
- [16] Ружић, И. *Arduino UNO*, Свет компјутера. [online] 2016. [Приступљено: 05. 09. 2020.] <https://www.sk.rs/arhiva/clanak/13678/arduino-uno>
- [17] Ружић, И. *Arduino: бeжично везивање*. Свет компјутера. [online] 2017. [Приступљено: 15. 09. 2020.] <https://www.sk.rs/2017/02/sklp05.html>
- [18] Components101. *HC-05 - Bluetooth Module*. [online] 2017. [Приступљено: 01.09.2020] <https://components101.com/wireless/hc-05-bluetooth-module>
- [19] Automatika.rs. *Upotreba ultrazvučnog senzora daljine [ARDUINO]*. [online] 2020. [Приступљено: 15.09.2020] <https://www.automatika.rs/projekti/upotreba-ultrazvucnog-senzora-daljine-arduino.html>
- [20] Abdulkhaleq, N. I., Hasan, I. J., Jalil Salih N. A. *Investigating the resolution ability of the HC-SRO4 ultrasonic sensor*, IOP Conference Series: Materials Science and Engineering, 745, 2019
- [21] ArduinoGetStarted.com. *Arduino - Touch Sensor*. [online] 2020. [Приступљено: 15. 09. 2020.] <https://arduinogetstarted.com/tutorials/arduino-touch-sensor>
- [22] Rustige, T. *Home Security Projects for Arduino*, TR Computers Limited, 2015
- [23] Castro, J. R. *Building a Home Security System with Arduino*, Packt Publishing Ltd., Birmingham, 2015
- [24] Knight, I. *Connecting Arduino to the Web*, Apress, 2018